Sustav za otkrivanje zlonamjernih čvorova u bežičnim senzorskim mrežama temeljenim na IPv6 protokolu

Grgić, Krešimir

SVEUČILIŠTE JOSIPA JURJA STROSSMAYERA

U OSIJEKU

ELEKTROTEHNIČKI FAKULTET

Krešimir Grgić

Sustav za otkrivanje zlonamjernih čvorova u bežičnim senzorskim mrežama temeljenim na IPv6 protokolu

System for Malicious Node Detection in IPv6-based Wireless Sensor Networks

Doktorska disertacija

Osijek, 2011.

Ova doktorska disertacija nastala je na Elektrotehničkom fakultetu

Sveučilišta J. J. Strossmayera u Osijeku (Zavod za komunikacije).

Mentor: prof. dr. sc. Drago Žagar

Povjerenstvo za ocjenu doktorske disertacije:

1. Dr. sc. Snježana Rimac-Drlje, red. prof. Elektrotehničkog fakulteta Osijek
2. Dr. sc. Drago Žagar, red. prof. Elektrotehničkog fakulteta Osijek
3. Dr. sc. Ignac Lovrek, red. prof. Fakulteta elektrotehnike i računarstva Zagreb

Povjerenstvo za obranu doktorske disertacije:

1. Dr. sc. Snježana Rimac-Drlje, red. prof. Elektrotehničkog fakulteta Osijek
2. Dr. sc. Drago Žagar, red. prof. Elektrotehničkog fakulteta Osijek
3. Dr. sc. Ignac Lovrek, red. prof. Fakulteta elektrotehnike i računarstva Zagreb
4. Dr. sc. Goran Martinović, izv. prof. Elektrotehničkog fakulteta Osijek
5. Dr. sc. Slavko Rupčić, docent Elektrotehničkog fakulteta Osijek

Datum obrane disertacije: 20. prosinca 2011. godine

Sadržaj

Popis slika

Popis tablica

1. Uvod

Značajan tehnološki napredak ostvaren posljednjih godina u području elektronike, minijaturnih elektro-mehaničkih sustava (MEMS) i bežičnih komunikacija doveo je do razvoja bežičnih senzorskih mreža kao nove podskupine bežičnih ad hoc mreža sa nekim naglašenim specifičnostima koje ih u velikoj mjeri razlikuju od „klasičnih“ bežičnih mreža. Bežična senzorska mreža predstavlja mrežu koju čini veliki broj čvorova koje karakteriziraju male dimenzije, niska potrošnja, mogućnost bežične komunikacije i strogo ograničeni računalni resursi. Ovakve mreže pružaju široke mogućnosti primjene u mnogobrojnim područjima – u industrijskoj i kućnoj automatizaciji, medicini, zaštiti okoliša, poljoprivredi, u vojne svrhe i sl.

Iako bežične senzorske mreže imaju dosta sličnosti sa drugim vrstama mreža (prvenstveno sa bežičnim ad hoc mrežama) vrlo stroga ograničenja u resursima (prvenstveno u pogledu kapaciteta napajanja) čine ih vrlo specifičnim. Zbog toga svi od ranije poznati mrežni mehanizmi razvijeni za druge vrste mreža (npr. mehanizmi usmjeravanja, sigurnosni mehanizmi) nisu izravno primjenjivi u bežičnim senzorskim mrežama, nego je nužna njihova znatna modifikacija i prilagodba, kao i razvoj novih, specifičnih rješenja. Zbog toga je područje bežičnih senzorskih mreža trenutačno jedno od istraživački najaktivnijih područja koje se intenzivno razvija.

U isto vrijeme, globalna svjetska mreža (Internet) dosegla je enormnu veličinu, te i dalje nezaustavljivo raste. Protokolna arhitektura današnjeg Interneta uglavnom se temelji na IP protokolu. Posljednja revizija aktualne inačice IP protokola (IPv4) datira još iz davne 1981. godine, kada je bilo nemoguće predvidjeti intenzitet razvoja i širenja globalne mreže. IP protokol se pokazao kao vrlo kvalitetno i robusno rješenje, što mu je i omogućilo da opstane dugi niz godina. Međutim, u okruženju kakvo predstavlja današnji Internet, sve više se ispoljavaju neki njegovi nedostaci (npr. iskorištenje adresnog prostora, sigurnosni problemi, složena konfiguracija, povećanje usmjerivačkih tablica i sl.). Zbog toga se pristupilo razvoju nove verzije protokola, Internet protokola verzije 6 (IPv6), koji bi u budućnosti u potpunosti trebao zamijeniti IPv4 protokol. Prvi temelji IPv6 protokola udareni su 1995. godine, dok je trenutno u tijeku postupak tranzicije na novu verziju protokola. Radi se o iznimno složenom i dugotrajnom procesu kojeg nije moguće provesti „preko noći“, te je stoga u narednih nekoliko

godina izvjesna koegzistencija IPv4 i IPv6 protokola. IPv6 protokol u odnosu na IPv4 protokol donosi neka značajna poboljšanja, poput proširenja adresnog prostora (zamjena 32-bitnih adresa 128-bitnim), jednostavnijeg zaglavlja fiksne duljine, autokonfiguracijskih mehanizama, sigurnosnih poboljšanja i sl.

Vrlo brzo nakon razvoja bežičnih senzorskih mreža javlja se ideja o njihovom povezivanju sa IP mrežama, što se najčešće i ostvaruje putem bazne stanice i gateway-a. Kasnije, usporedno sa daljim razvojem bežičnih senzorskih mreža, javlja se ideja o implementaciji IP protokola u samu senzorsku mrežu. Pri tome se stavlja naglasak na IP verzije 6, kao verziju IP protokola koja istiskuje IPv4 i koja je zbog ogromnog adresnog prostora pogodna za implementaciju u mrežama sa izuzetno velikim brojem čvorova, kakva može biti bežična senzorska mreža.

Znatni istraživački napori su uloženi kako bi se sveprisutni IP protokol implementirao u okruženje bežičnih senzorskih mreža. Ovi napori nedavno su rezultirali pojavom 6LoWPAN standarda *(IPv6 over Low Power Personal Area Networks)*, koji omogućava čvoru bežične senzorske mreže komunikaciju putem IP protokola. Ovu mogućnost 6LoWPAN standard pruža dodavanjem adaptacijskog sloja iznad IEEE 802.15.4 *(ZigBee)* sloja (IEEE 802.15.4 predstavlja trenutno najrašireniji komunikacijski standard u bežičnim senzorskim mrežama).

Bežične senzorske mreže temeljene na IPv6 protokolu kao relativno novi koncept predstavljaju područje intenzivnog istraživanja sa nizom problema za koje se još uvijek traži adekvatno rješenje, a i neka postojeća rješenja zahtijevaju daljnji razvoj i poboljšanja. Problematika sigurnosti predstavlja jedan od najvažnijih aspekata u području bežičnih senzorskih mreža temeljenih na IPv6 protokolu koji još uvijek zahtijeva pronalaženje kvalitetnih odgovarajućih rješenja. Kvalitetno rješavanje problematike sigurnosti jedan je od glavnih preduvjeta za šire prihvaćanje i praktičnu uporabu ove vrste mreža.

Jedan od najvažnijih sigurnosnih mehanizama koji je potrebno implementirati jest sustav za otkrivanje neovlaštenih upada i zlonamjernog ponašanja pojedinih čvorova u bežičnoj senzorskoj mreži. Zadaća ovakvog sustava jest otkriti pokušaje napada izvana, ali i detektirati kompromitaciju čvorova odnosno pojavu zlonamjernog (malicioznog) ponašanja unutar mreže. Za sada ne postoji adekvatno rješenje ovog problema za senzorsku mrežu temeljenu na IPv6 protokolu, a njegovo rješavanje predstavlja važan korak u razvoju ove vrste mreža koji bi vodio ka njihovom širem prihvaćanju i uporabi. Postojeća rješenja za klasične žične i bežične ad hoc mreže ne mogu se izravno implementirati, no mogu poslužiti kao polazna

točka za intenzivnije istraživanje koje bi rezultiralo adekvatnim sigurnosnim rješenjem namijenjenom bežičnim IPv6 senzorskim mrežama. Implementaciju sustava za otkrivanje upada ne treba analizirati niti promatrati izolirano, već isključivo kao dio jedinstvenog sigurnosnog okvira koji prožima sve slojeve mrežnog modela (*cross-layer* pristup) i koji kao cjelina osigurava krajnjem korisniku temeljne premise sigurnosti – povjerljivost, integritet, autentičnost i dostupnost informacije.

Ova disertacija orijentirana je na sigurnosnu problematiku bežičnih senzorskih mreža temeljenih na IPv6 protokolu. Budući da su ideja i realizacija implementacije IPv6 protokola u bežičnu senzorsku mrežu relativno novi, sigurnosni aspekti ovakvih novonastalih rješenja još uvijek su nedovoljno istraženi, te postoji potreba za dodatnim radom i istraživanjem u ovom području. Zbog toga ova disertacija nastoji analizirati sigurnosne aspekte bežičnih senzorskih mreža temeljenih na IPv6 protokolu, jer takve analize za sada nema, a zasigurno će doprinijeti daljem istraživanju i razvoju sigurnosnih mehanizama namijenjenih ovakvim mrežama. Nadalje, postoji potreba za kreiranjem jedinstvenog sigurnosnog okvira koji bi se mogao primijeniti na IPv6-temeljene BSM, prožimajući sve slojeve mrežnog modela. U disertaciji se analiziraju postojeća sigurnosna rješenja iz klasičnih BSM i IPv6 mreža koja bi se uz odgovarajuće adaptacije mogla integrirati unutar sigurnosnog okvira namijenjenoj IPv6-temeljenim BSM.

Važan dio sigurnosnog okvira koji bi se mogao primijeniti na ovakve mreže predstavlja sustav koji bi detektirao zlonamjerno ponašanje čvorova i napade u senzorskoj mreži. Uočeno je trenutačno nepostojanje ovakvog sustava, te je jedan od doprinosa ove disertacije upravo razvoj novog distribuiranog adaptivnog sustava za otkrivanje zlonamjernog ponašanja senzorskih čvorova u BSM temeljenoj na IPv6 protokolu. Predloženo rješenje moguće je implementirati kao važan sastavni dio cjelovitog sigurnosnog okvira namijenjenog IPv6-temeljenim BSM. Implementacija ovakvog rješenja predstavlja važan korak ka podizanju razine sigurnosti ovakvih mreža, što u konačnici zasigurno rezultira njihovom sve masovnijom primjenom (budući da je za velik broj mogućih primjena iznimno važna razina sigurnosti – primjerice u medicinskim ili vojnim primjenama). Rješavanju navedenog problema pristupilo se imajući u vidu distribuiranu prirodu senzorskih mreža i stroga ograničenja koja u njima postoje u pogledu resursa, što je rezultiralo prijedlogom distribuiranog sustava koji u minimalnoj mjeri stvara dodatno opterećenje ograničenim resursima mreže.

Disertacija je organizirana u sedam poglavlja. Prvo poglavlje je uvodno poglavlje. U drugom poglavlju detaljnije je prikazan i objašnjen koncept bežičnih senzorskih mreža s osvrtom na njihovu klasifikaciju i mogućnosti primjene. Treće poglavlje analizira problematiku implementacije IPv6 protokola u okruženje bežične senzorske mreže. Pri tome su objašnjeni razlozi napuštanja IPv4 protokola i novosti koje donosi IPv6 protokol (uz analizu njegovih sigurnosnih aspekata). Kroz analizu pojedinih slojeva prikazana je struktura protokolnog stoga BSM temeljene na IPv6 protokolu, uključujući adaptacijski sloj i usmjerivački sloj koji su posebno prilagođeni IPv6 protokolu. U četvrtom poglavlju provedena je detaljna analiza sigurnosnih aspekata IPv6-temeljenih BSM, što uključuje pregled postojećih sigurnosnih prijetnji i napada, te analizu problematike njihovog otkrivanja, uz pregled nekih postojećih sigurnosnih rješenja namijenjenih „klasičnim“ BSM. U petom poglavlju iznesen je prijedlog novog cjelovitog sigurnosnog okvira namijenjenog za BSM temeljene na IPv6 protokolu. Predloženi sigurnosni okvir prožima sve slojeve slojevitog mrežnog modela, a po svojoj prirodi je modularan i prilagodljiv potrebama konkretne aplikacije (dan je detaljan opis svih modula iz sigurnosnog okvira i funkcija koje oni obavljaju). Šesto poglavlje daje rješenje novog distribuiranog adaptivnog sustava za otkrivanje zlonamjernih čvorova namijenjenog IPv6-temeljenim BSM. Ovaj sustav predstavlja integralni dio cjelovitog sigurnosnog okvira. Detaljno su opisani njegova struktura, način rada i implementacija, te su analizirani i objašnjeni dobiveni rezultati. U sedmom poglavlju nalaze se zaključna razmatranja, te u nastavku popis korištene literature.

2. Bežične senzorske mreže (BSM)

U proteklih nekoliko godina ostvaren je značajan napredak i razvoj u mnogobrojnim područjima tehnike i tehnologije, posebice u područjima mikro-elektro-mehaničkih sustava *(MEMS, Micro-Electro-Mechanical Systems)*, bežičnih komunikacija i digitalne elektronike. Napredak u spomenutim tehnološkim granama omogućio je pojavu i razvoj nove podvrste bežičnih mreža – bežičnih senzorskih mreža *(WSN, Wireless Sensor Network)*. Tehnološki je postalo moguće proizvesti multifunkcionalni bežični senzorski čvor niske potrošnje, niske cijene, minijaturnih dimenzija i sa podrškom za bežičnu komunikaciju na kraćim udaljenostima. Razvoj ovakvog senzorskog čvora potaknuo je ideju međusobnog povezivanja velikog broja ovakvih čvorova, što je dovelo do stvaranja koncepta bežične senzorske mreže (BSM) [5].

Bežična senzorska mreža predstavlja značajno poboljšanje u odnosu na uporabu tradicionalnih senzora. Tradicionalni senzori obično se postavljaju na dva različita načina. Prvi način podrazumijeva postavljanje senzora daleko od promatranog fenomena, pri čemu se moraju koristiti kompleksni i skupi senzori koji su u stanju dobro razlučiti ciljani fenomen od okolnih smetnji. Drugi pristup podrazumijeva postavljanje nekoliko senzora koji služe isključivo za prikupljanje informacija, dok se procesiranje i agregacija podataka obavljaju na udaljenoj lokaciji. Pri tome je nužno riješiti problem ispravnog pozicioniranja senzora i problem komunikacije između senzora i udaljenog centralnog čvora.

Bežična senzorska mreža sastoji se od velikog broja jeftinih senzorskih čvorova koje je moguće gusto rasporediti vrlo blizu promatranog fenomena (čak i unutar njega). Točnu poziciju svakog bežičnog senzorskog čvora nije potrebno unaprijed odrediti već ih je moguće i slučajno rasporediti (npr. u nepristupačnoj sredini), budući da BSM ima samoorganizirajuća svojstva. Budući da senzorski čvorovi imaju mogućnost obrade prikupljenih podataka, njihove agregacije i međusobne komunikacije, izostaje potreba za korištenjem kompleksnih udaljenih senzora ili za postavljanjem složene komunikacijske infrastrukture između senzora i centralnog mjesta obrade podataka [10].

2.1. Koncept bežičnih senzorskih mreža

Bežične senzorske mreže zapravo predstavljaju posebnu podskupinu bežičnih ad hoc mreža *(MANET, Mobile Ad Hoc Network)*, no zbog vrlo strogih ograničenja (prvenstveno u pogledu napajanja i računalnih resursa senzorskih čvorova) BSM mreže pokazuju značajne razlike u odnosu na „klasične“ MANET mreže. BSM se sastoji od velikog broja jeftinih senzorskih čvorova i sve njezine funkcije temeljene su na međusobnoj suradnji između čvorova i kolaborativnim algoritmima. Međutim, zbog spomenutih razlika i ograničenja u BSM nije moguće izravno primijeniti postojeća tehnička i algoritamska rješenja iz MANET mreže, nego je nužan razvoj i implementacija novih posebnih rješenja specijaliziranih za BSM. Prema tome, područje BSM još uvijek predstavlja područje intenzivnog istraživanja i razvoja [126].

Svi protokoli i algoritmi koji se koriste u senzorskim mrežama moraju imati svojstva samokonfigurabilnosti. Sve projektirane funkcije BSM obavlja kooperativnim sudjelovanjem svih njezinih čvorova. Svaki senzorski čvor u BSM opremljen je procesorskom jedinicom (CPU), određenom količinom memorije, napajanjem (najčešće zamjenjiva baterija), te komunikacijskim podsustavom (radio primopredajnik). Ovi resursi su u pravilu vrlo ograničeni, zbog potrebe za malim dimenzijama čvora, niskom potrošnjom energije i niskom cijenom čvora. Međutim, dovoljni su da bežični senzorski čvor umjesto slanja „sirovih“ prikupljenih podataka lokalno obavi parcijalnu obradu i agregaciju podataka, te prosljeđuje dalje samo one podatke koji su potrebni.

Budući da je u BSM velik broj senzorskih čvorova postavljen „gusto“ (na relativno malim međusobnim udaljenostima), komunikacija između udaljenih čvorova odvija se kroz više skokova *(multihop communication)*, budući da se na taj način obično troši manje energije nego kod izravne komunikacije *(single hop communication)* između senzorskog čvora i udaljenog krajnjeg odredišta (bazne stanice).

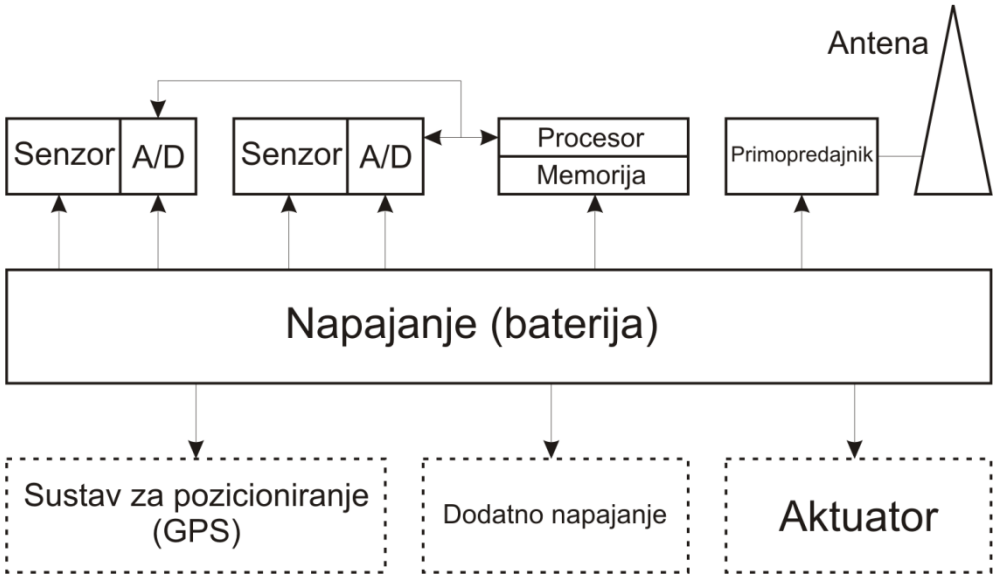
Jedan od najvećih ograničavajućih faktora u BSM je kapacitet napajanja. Senzorski čvorovi uglavnom su opremljeni ograničenim izvorima energije (baterijama) koji se vrlo često ne mogu zamijeniti. Zbog toga se svi protokoli i algoritmi koji se primjenjuju u BSM primarno fokusiraju na optimalizaciju potrošnje energije i maksimalnu moguću uštedu, kako bi se što je moguće više produljio životni vijek senzorskog čvora.

Razvoj različitih protokola i algoritama za primjenu u bežičnim senzorskim mrežama danas predstavlja jedno od područja najintenzivnijih istraživačkih aktivnosti. Poboljšanje postojećih te razvoj novih protokola za BSM zasigurno će doprinijeti njihovom još širem prihvaćanju te još više proširiti spektar njihove moguće praktične primjene [38].

Bežična senzorska mreža predstavlja složenu strukturu koju čini veliki broj međusobno povezanih senzorskih čvorova. Svaki čvor u BSM čine 4 osnovna dijela (slika 2.1):

- senzorski dio *(sensing unit)*
- računalni dio *(processing unit)*
- komunikacijski dio *(transceiver)*
- napajanje *(power unit)*

Dijelovi prikazani iscrtkanom linijom su opcionalni.



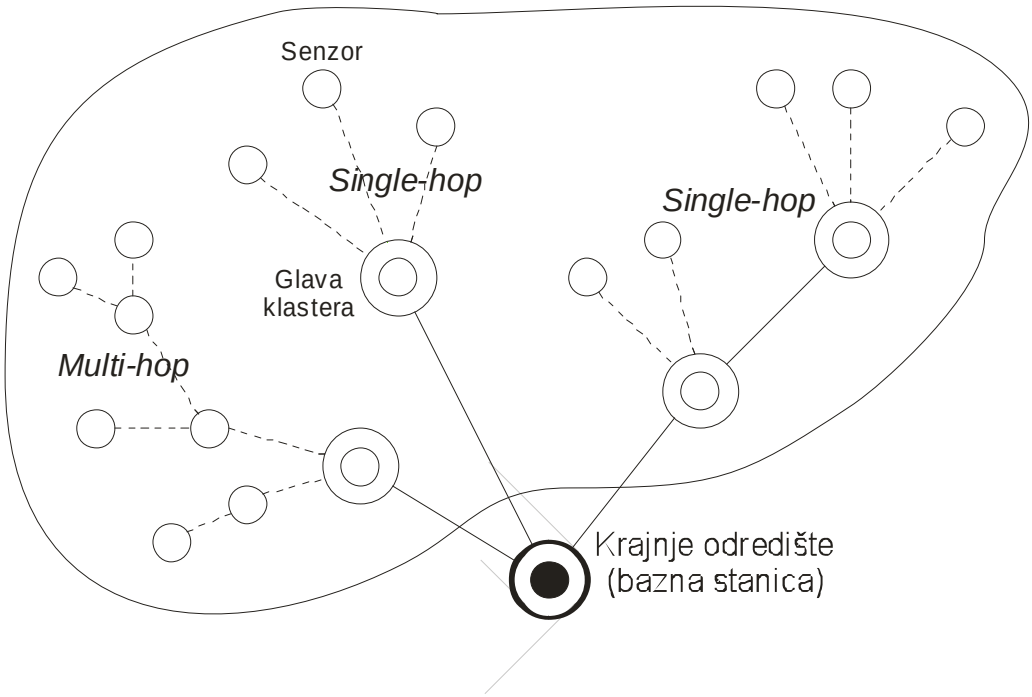
Slika 2.1 Struktura bežičnog senzorskog čvora

Senzorski dio čvora sastoji se od jednog ili više senzorskih elemenata koji mogu biti pasivni i aktivni. Primjeri pasivnih senzora su temperaturni, seizmički, akustički, optički senzori, senzori vlažnosti i slično. Karakterizira ih niska potrošnja energije. Aktivne senzore, za razliku od pasivnih, karakterizira visoka potrošnja energije (npr. radar ili sonar). Računalni dio senzorskog čvora čini mikroprocesorska jedinica (CPU) sa pripadajućom memorijom. Komunikacijski dio senzorskog čvora čini odgovarajući radio primopredajnik sa pripadajućom antenom. Napajanje senzorskog čvora u većini slučajeva je realizirano pomoću

baterije, no u nekim slučajevima mogu postojati i dodatni izvori energije (npr. solarne ćelije). Osim navedenih dijelova, senzorski čvor može sadržavati i još neke dodatne dijelove, ovisno o aplikaciji (npr. GPS modul za precizno pozicioniranje). Na slici 2.2 prikazan je primjer izvedbe jednog senzorskog čvora.

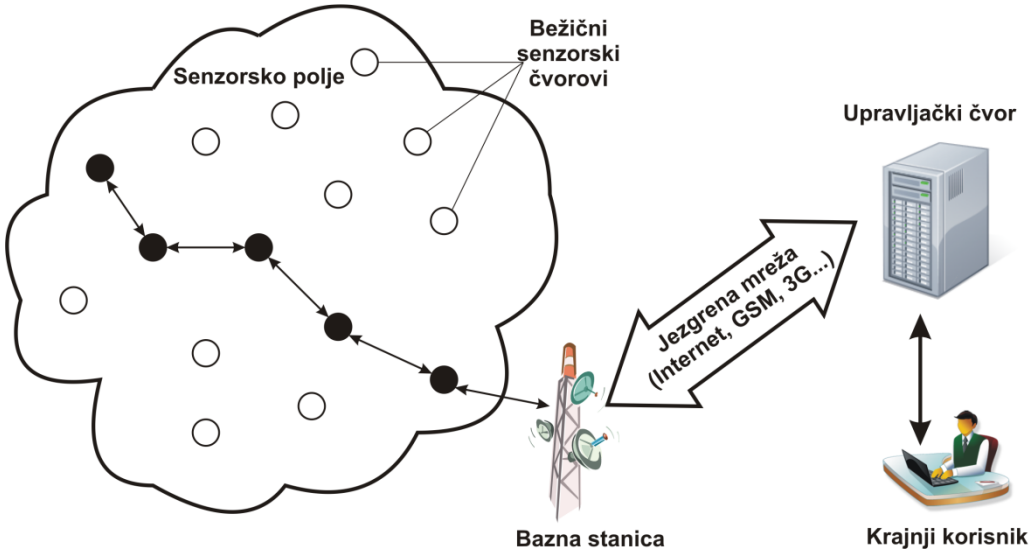
Slika 2.2 Primjer bežičnog senzorskog čvora (Crossbow MICAz 2.4 GHz)

Čvorovi bežične senzorske mreže mogu činiti jedinstveno polje ili biti podijeljeni u više zasebnih cjelina (klastera). Ukoliko je mreža podijeljena na klastere unutar svakog klastera izdvaja se pojedini čvor koji predstavlja glavu klastera. Glava klastera obično obavlja funkciju agregacije podataka sa područja klastera i prosljeđuje ih do sljedećeg čvora ili izravno do bazne stanice. Na slici 2.3 prikazana je tipična struktura bežične senzorske mreže.



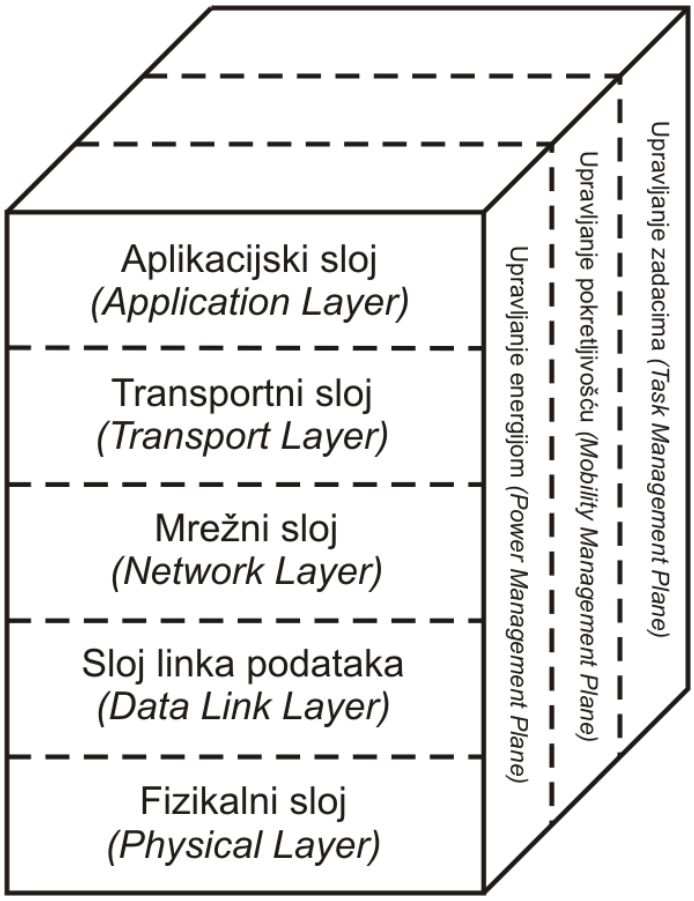
Slika 2.3 Tipična struktura bežične senzorske mreže

Senzorski čvorovi bežične senzorske mreže najčešće su raspršeni čineći tako senzorsko polje *(sensor field)*. Svaki od ovih čvorova u stanju je prikupljati podatke i slati ih prema krajnjem odredištu *(sink)*. Također, svaki čvor u mogućnosti je obavljati ulogu usmjerivača *(router*-a*)* i prosljeđivati prema odredištu podatkovne pakete koje je dobio od susjednog čvora (slika 2.4).



Slika 2.4 Tok podataka kroz bežičnu senzorsku mrežu

Kroz bežičnu senzorsku mrežu podaci se prema odredištu usmjeravaju i prenose bez pomoći središnje infrastrukture, već isključivo kooperativnim protokolima i algoritmima koje izvršavaju senzorski čvorovi. Protokolni stog *(protocol stack)* senzorske mreže prikazan je na slici 2.5.



Slika 2.5 Protokolni stog bežične senzorske mreže

Protokolni stog bežične senzorske mreže čini pet osnovnih slojeva:

- fizikalni sloj *(Physical Layer)*
- sloj linka podataka *(Data Link Layer)*
- mrežni sloj *(Network Layer)*
- transportni sloj *(Transport Layer)*
- aplikacijski sloj *(Application Layer)*

Na aplikacijskom sloju (najviši sloj) izvršavaju se korisničke aplikacije, kreirane ovisno o konkretnoj primjeni senzorske mreže. Transportni sloj pomaže prilikom uspostave i očuvanja podatkovnog toka, ukoliko to zahtijeva korisnička aplikacija. Na mrežnom sloju izvršavaju se

zadaće usmjeravanja podataka (podatkovnih paketa) koji pristižu sa transportnog sloja. Na sloju linka podataka izvršavaju se protokoli koji reguliraju pravo pristupa prijenosnom mediju *(MAC, Medium Access Control)*. Na fizikalnom sloju definirani su modulacijski postupci, te tehnike predaje i prijema radio signala.

Promatrano sa upravljačkog aspekta, moguće je izdvojiti tri upravljačke ravnine:

- upravljanje energijom *(Power Management Plane)*
- upravljanje pokretljivošću *(Mobility Management Plane)*
- upravljanje zadacima *(Task Management Plane)*

Putem upravljačke ravnine za upravljanje energijom regulira se način na koji senzorski čvor iskorištava energetske resurse koji mu stoje na raspolaganju. Primjerice, nakon prijema poruke od susjednog čvora senzorski čvor može isključiti svoj prijemnik na neko vrijeme, kako bi se izbjeglo primanje dupliciranih poruka. Također, ukoliko mu je baterija pri kraju senzorski čvor može obavijestiti svoje susjede da više nije u mogućnosti prosljeđivati podatkovne pakete i vršiti uslugu usmjeravanja. Putem upravljačke ravnine za upravljanje pokretljivošću prati se i nadzire kretanje senzorskih čvorova kako bi se u bilo kojem trenutku mogla uspostaviti odgovarajuća ruta od senzora do krajnjeg odredišta podataka. Putem upravljačke ravnine za upravljanje zadacima planiraju se i raspoređuju zadaci koje trebaju odraditi pojedinačni senzorski čvorovi, budući da ne moraju nužno na nekom području svi senzorski čvorovi biti istovremeno aktivni.

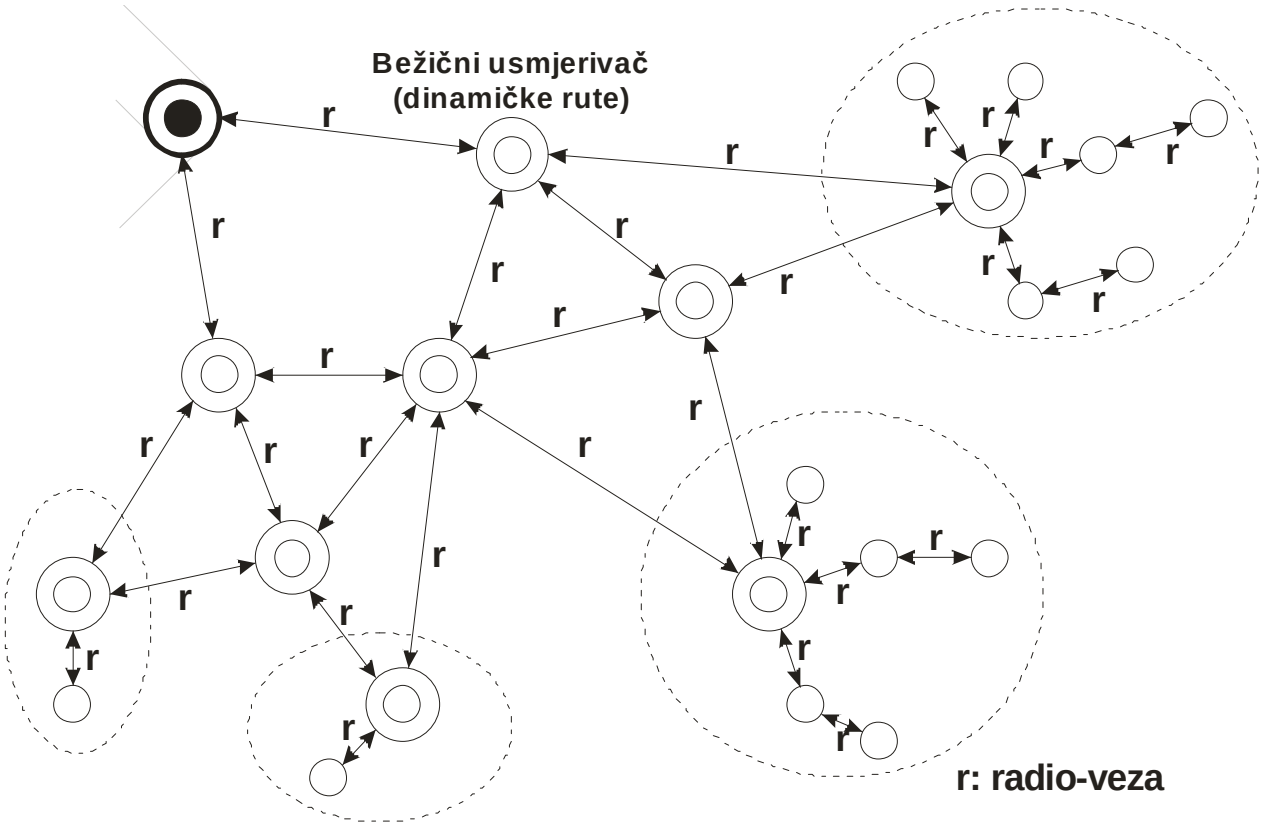
Ovakav složeni slojeviti model osigurava da senzorski čvorovi kooperativno izvršavaju svoje zadaće na energetski učinkovit način, te primjenom kolaborativnih algoritama prenose informacije do krajnjeg korisnika. Međusobnom suradnjom između senzorskih čvorova i primjenom kooperativnih algoritama povećava se učinkovitost, a s povećanjem učinkovitosti produljuje se i životni vijek bežične senzorske mreže.

2.2. Klasifikacija bežičnih senzorskih mreža

Bežične senzorske mreže moguće je klasificirati na temelju različitih kriterija (npr. veličina mreže, broj čvorova i sl.). Prilikom analize mogućih primjena bežičnih senzorskih mreža klasifikacija se najčešće vrši na osnovu broja skokova u komunikaciji između senzorskog čvora i središnjeg mjesta za prikupljanje i obradu podataka. Ovakva podjela se pokazala najprirodnijom budući da se i različite aplikacije senzorskih mreža mogu podijeliti na one kod kojih senzorski čvorovi izravno komuniciraju sa baznom stanicom *(point-to-point)* i one kod kojih se ova komunikacija odvija kroz više skokova *(multipoint-to-point)* [106].

Prema tome, bežične senzorske mreže moguće je klasificirati u dvije osnovne kategorije:

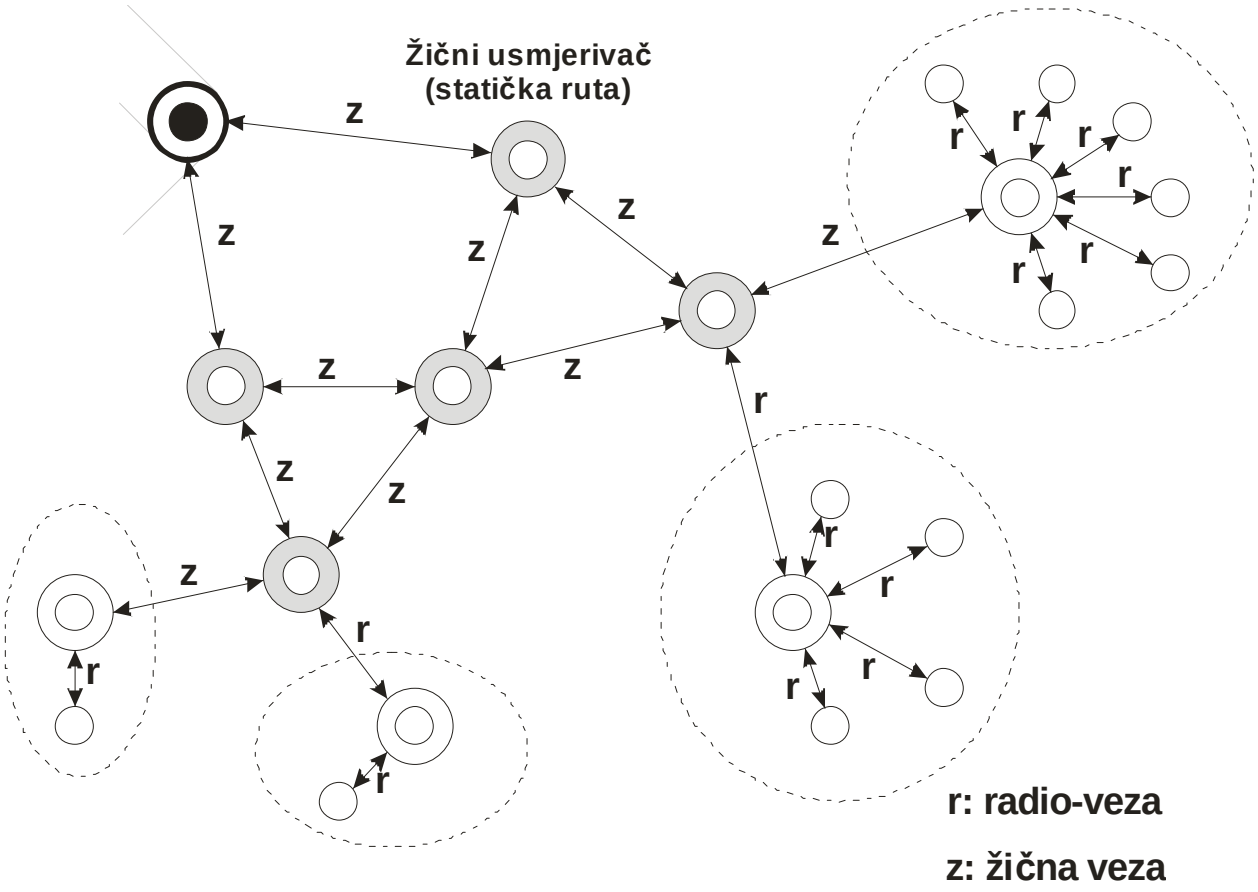
- **BSM kategorije 1** *(C1WSN, Category 1 WSN)*: BSM kod kojih se radio veza između senzorskih čvorova ostvaruje kroz više skokova *(multihop)*, pri čemu se koriste dinamički algoritmi usmjeravanja kako u bežičnom tako i u žičnom dijelu mreže
- **BSM kategorije 2** *(C2WSN, Category 2 WSN)*: BSM kod kojih se radio veza ostvaruje kroz samo jedan skok *(single-hop)*, pri čemu konekcija može biti od točke do točke *(point-to-point)* ili od više točaka prema jednoj točki *(multipoint-to-point)*, što zapravo predstavlja zvjezdastu topologiju; uglavnom koriste statičke algoritme usmjeravanja



Slika 2.6 BSM kategorije 1 (C1WSN)

Na slici 2.6 prikazana je BSM kategorije 1 (C1WSN). Kod ovakve mreže senzorski čvorovi mogu biti nekoliko skokova udaljeni od čvora za usmjeravanje i prosljeđivanje podataka baznoj stanici *(forwarding node)*. Ovaj čvor zapravo predstavlja bežični usmjerivač *(wireless router)* koji podržava dinamičko usmjeravanje i bežično je povezan sa preostalim usmjerivačima. Važne karakteristike BSM kategorije 1:

- senzorski čvorovi podržavaju komunikaciju kroz više skokova *(multihop)* i u slučaju potrebe ponašaju se kao usmjerivači, te prosljeđuju podatke na njihovoj putanji
- postoji više mogućih putanja koje povezuju različite dijelove mreže, pri čemu se pojedina putanja bira dinamičkim postupcima usmjeravanja
- domet radio veze između bežičnih usmjerivača je reda veličine nekoliko stotina metara do nekoliko kilometara
- usmjerivački čvorovi podržavaju procesiranje podataka

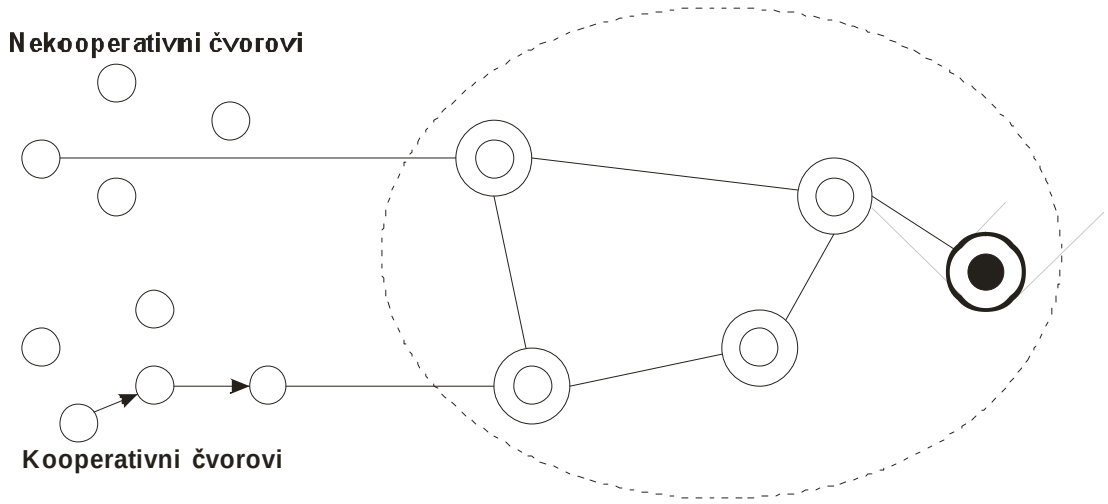


Slika 2.7 BSM kategorije 2 (C2WSN)

Na slici 2.7 prikazana je BSM kategorije 2 *(C2WSN)*. Kod ovakve mreže senzorski čvor je u mogućnosti uspostaviti izravnu radio vezu sa čvorom koji prosljeđuje podatke *(forwarding node)* i koji je povezan sa zemaljskom fiksnom mrežom. Važne karakteristike BSM kategorije 2:

- senzorski čvorovi ne podržavaju *multihop* komunikaciju, već isključivo izravnu komunikaciju sa usmjerivačkim čvorom
- usmjerivački čvor podržava isključivo statičko usmjeravanje prema fiksnoj zemaljskoj mreži prema kojoj posjeduje i fizički link
- domet radio veze seže do reda veličine nekoliko stotina metara
- usmjerivački čvorovi ne podržavaju procesiranje podataka

Ponašanje senzorskih čvorova u navedenim kategorijama senzorskih mreža može se okarakterizirati kao kooperativno *(cooperative)* i nekooperativno *(noncooperative)* (slika 2.8).



Slika 2.8 Kooperativni i nekooperativni čvorovi u BSM

U BSM kategorije 1 *(C1WSN)*, gdje senzorski čvorovi podržavaju *multihop* komunikaciju i ponašaju se kao usmjerivači, zastupljeno je kooperativno ponašanje čvorova, dok je u BSM kategorije 2 *(C2WSN)* zastupljeno nekooperativno ponašanje čvorova (budući da se čvorovi ne ponašaju kao usmjerivači i komuniciraju izravno sa *forwarding* čvorovima).

Distribuirani adaptivni sustav za otkrivanje zlonamjernog ponašanja senzorskih čvorova čije rješenje je predloženo u nastavku disertacije orijentiran je na BSM kategorije 1, koje su u potpunosti distribuirane i temeljene na kooperativnom ponašanju čvorova i njihovoj komunikaciji kroz više skokova *(multihop)*.

2.3. Mogućnosti primjene bežičnih senzorskih mreža

Činjenica da senzorski čvorovi mogu biti opremljeni različitim tipovima senzora otvara vrlo široke mogućnosti primjene bežičnih senzorskih mreža [57]. Temperaturni, infracrveni, seizmički, akustički, magnetski senzori samo su neki od mogućih primjera različitih senzora kakvi se mogu ugraditi u čvorove bežične senzorske mreže. Senzorski čvorovi opremljeni adekvatnim senzorima mogu se koristiti za kontinuirano praćenje promatranog fenomena i za detekciju različitih događaja. Osim detekcije, koriste se i za identifikaciju nastalog događaja i njegovo precizno lociranje. Također, senzorski čvor može lokalno biti povezan i sa različitim vrstama aktuatora [37].

Zbog velikog broja različitih mogućih primjena BSM teško je napraviti njihovu sustavnu klasifikaciju. Neka od mogućih područja primjene BSM su:

- **vojne primjene** *(military applications)*

  Bežične senzorske mreže mogu igrati vrlo važnu ulogu unutar vojnih sustava zapovijedanja, upravljanja i komunikacije. Svoju primjenu nalaze i na samom bojnom polju, za potrebe praćenja, prikupljanja informacija, navođenja i slično. Bežične senzorske mreže nalaze široku primjenu u velikom broju vojnih aplikacija zahvaljujući nekim svojim bitnim svojstvima, kao što su: brzo postavljanje, samoorganizacija i tolerancija na kvarove. Budući da se senzorska mreža sastoji od velikog broja jeftinih senzorskih čvorova, uništenje nekolicine čvorova ne predstavlja veliku štetu kakva bi nastala uništenjem tradicionalnih senzora. Neke od mogućih primjena bežičnih senzorskih mreža u vojne svrhe: praćenje i nadzor vlastitih vojnika, opreme i streljiva, nadgledanje bojnog polja, izviđanje neprijateljskih snaga i terena, precizno ciljanje i navođenje, procjena gubitaka i oštećenja, otkrivanje nuklearnog, biološkog ili kemijskog napada.

- **primjene u zaštiti okoliša** *(environmental applications)*

  Vrlo široke mogućnosti primjene bežične senzorske mreže nalaze u području praćenja i nadzora životnog okoliša i njegove zaštite. BSM je moguće koristiti za praćenje kretanja i životnih navika različitih vrsta životinja. Prednost ovakvog pristupa je u tome što nije nužna nazočnost čovjeka, čime bi se narušila prirodna ravnoteža i negativno utjecalo na uzorke ponašanja životinja. BSM se također koriste i za praćenje životinjskih staništa i uvjeta koji u njima vladaju. Postoji čitav niz uspješnih projekata diljem svijeta koji koriste bežične senzorske mreže za praćenje i proučavanje raznolikog životinjskog svijeta, od morskih sisavaca do različitih vrsta ptica. Bežične senzorske mreže svoju primjenu nalaze i u području poljoprivrede i proizvodnje zdrave hrane. BSM predstavljaju jednu od najvažnijih tehnologija koja omogućava koncept tzv. „precizne“ poljoprivrede *(precision agriculture)*. Primjenom bežičnih senzorskih mreža opremljenih senzorima za mjerenje vlažnosti i sastava tla moguće je postići optimalnu potrošnju vode za navodnjavanje, kao i optimalno doziranje umjetnog gnojiva. Time je moguće ostvariti značajne materijalne uštede, bez smanjenja prinosa i uz zadovoljavanje uvjeta ekološke proizvodnje. Osim u ratarstvu, bežične senzorske mreže primjenjuju se i u drugim granama poljoprivrede: voćarstvu i vinogradarstvu. U ovim granama se bežične senzorske mreže mogu koristiti za

otkrivanje bolesti i štetočina, ali i za optimalizaciju primjene zaštitnih agrotehničkih mjera. Bežične senzorske mreže moguće je koristiti i za vrlo rano otkrivanje šumskih požara, što omogućava njihovu brzu lokalizaciju i stavljanje pod nadzor i time sprečava nastanak velike materijalne štete, pa čak i ljudskih žrtava. Također, senzorski čvorovi mogu se koristiti i za detekciju poplave i potresa.

- **medicinske primjene** *(health applications)*

  Primjena bežičnih senzorskih mreža u medicini danas predstavlja jedno od najintenzivnijih područja istraživanja. Brojni su istraživački projekti diljem svijeta rezultirali različitim oblicima medicinskih senzorskih mreža uglavnom namijenjenih daljinskom praćenju pacijenata i njihovih vitalnih parametara. U posljednje vrijeme se čak izdvaja posebna podskupina bežičnih senzorskih mreža – BASN mreže *(Body Area Sensor Network)*, čiji čvorovi su namijenjeni postavljanju na ljudsko tijelo, pa čak i unutar njega (u obliku implantata). Senzorski čvorovi opremljeni adekvatnim senzorima u stanju su pratiti vitalne parametre pacijenta (npr. puls, krvni tlak, EKG i sl.), te ih prosljeđivati do središnje lokacije unutar odgovarajuće medicinske ustanove gdje su oni izravno dostupni liječniku. U slučaju značajnijih odstupanja vitalnih parametara od uobičajenih vrijednosti aktivira se alarm i moguće je promptno reagirati, čime se mogu spasiti mnogi ljudski životi. Senzorske mreže mogu se koristiti i za nadzor kroničnih bolesnika i starije populacije u okruženju njihovog vlastitog doma. Osim bolesnika, senzorske mreže mogu koristiti i zdravi ljudi, primjerice za praćenje i nadzor određenih parametara prilikom treninga i tjelovježbe, te pomoć u kreiranju individualiziranih programa tjelesne aktivnosti. Bežične senzorske mreže se u bolničkom okruženju osim za nadzor bolesnika mogu koristiti i za praćenje liječnika i drugog medicinskog osoblja, što omogućava pravodobnu reakciju u hitnim slučajevima. Također, senzorske mreže koriste se i za administraciju i upravljanje lijekovima unutar zdravstvene ustanove.

- **primjene u kućanstvu** *(home applications)*

  U posljednje vrijeme javlja se trend ugradnje inteligentnih bežičnih senzorskih čvorova u kućanske aparate različite namjene, što omogućava njihovu međusobnu interakciju, ali i omogućava korisniku upravljanje ovim uređajima sa jednog mjesta koje može biti i udaljeno (senzorska mreža je u tom slučaju povezana sa eksternom mrežom – Internetom). Primjenom tehnologije bežičnih senzorskih mreža u kućanstvu se kreira „inteligentno okruženje“ *(smart environment)*. Senzorski čvorovi ugrađeni u

namještaj i kućanske aparate mogu komunicirati međusobno i sa središnjim poslužiteljem. Poslužitelja može biti i više (npr. po jedan za svaku prostoriju), pri čemu su i oni međusobno umreženi. Na taj način kreira se složeni samo-organizirajući, samoregulirajući i adaptivni sustav koji u velikoj mjeri doprinosi kvaliteti čovjekovog življenja unutar „inteligentnog“ doma.

- **ostale komercijalne primjene**

  Osim do sada spomenutih postoji još čitav niz drugih mogućih primjena bežičnih senzorskih mreža. Senzorske mreže vrlo često se koriste u velikim poslovnim zgradama za regulaciju i nadzor sustava za grijanje/hlađenje i ventilaciju *(HVAC – Heating, Ventilating, Air Conditioning).* Primjenom bežične senzorske mreže moguće je precizno regulirati ambijentalne uvjete u svakoj prostoriji ponaosob. Također, unutar većih prostorija moguće je regulirati mikroklimatske uvjete u pojedinim dijelovima prostorije. Osim klimatskih uvjeta, bežične senzorske mreže koriste se i za regulaciju osvjetljenja unutar velikih zgrada. Ovakav precizan pristup regulaciji ambijentalnih uvjeta unutar velikih zgrada omogućava značajne uštede u potrošnji energije, koje višestruko nadmašuju inicijalne troškove ugradnje i održavanja ovakvih sustava. Senzorske mreže koriste se i kao važne komponente sigurnosnih sustava, gdje se koriste za detekciju uljeza ali i u protuprovalnim, vatrodojavnim i protupožarnim sustavima. Koriste se i u industriji – nadzor kvalitete, upravljanje i vođenje automatiziranih postrojenja, lokalna kontrola aktuatora, praćenje stanja inventara i skladišta i sl. U proteklih nekoliko godina intenzivno se razvijaju i šire i bežične mreže namijenjene različitim vrstama vozila, koje omogućavaju međusobnu komunikaciju ovako opremljenih vozila, ali i komunikaciju vozila sa „inteligentnom“ prometnom infrastrukturom.

3. IPv6 protokol i njegova implementacija u BSM

3.1. TCP/IP međumrežni rad

Osnovni problem u komunikacijskim mrežama jest omogućiti međusobno povezivanje mrežnih čvorova isključivo na temelju poznavanja njihovih jedinstvenih adresa (bez potrebe za poznavanjem bilo kojih drugih podataka). Da bi tako nešto bilo moguće, moraju se zadovoljiti sljedeći preduvjeti:

- Svaki mrežni uređaj (čvor) mora biti identificiran na jedinstven način
- Svaki čvor u mreži mora imati mogućnost slanja i prijema podataka u obliku razumljivom svim preostalim mrežnim čvorovima
- Mora biti omogućen pouzdan prijenos podataka od jednog do drugog mrežnog čvora (s poznatim mrežnim adresama)

Internet protokol *(Internet protocol, IP)*, kao skup pravila za usmjeravanje i razmjenu podataka između različitih mreža, rješava ovaj problem (pri čemu zadovoljava navedene preduvjete).

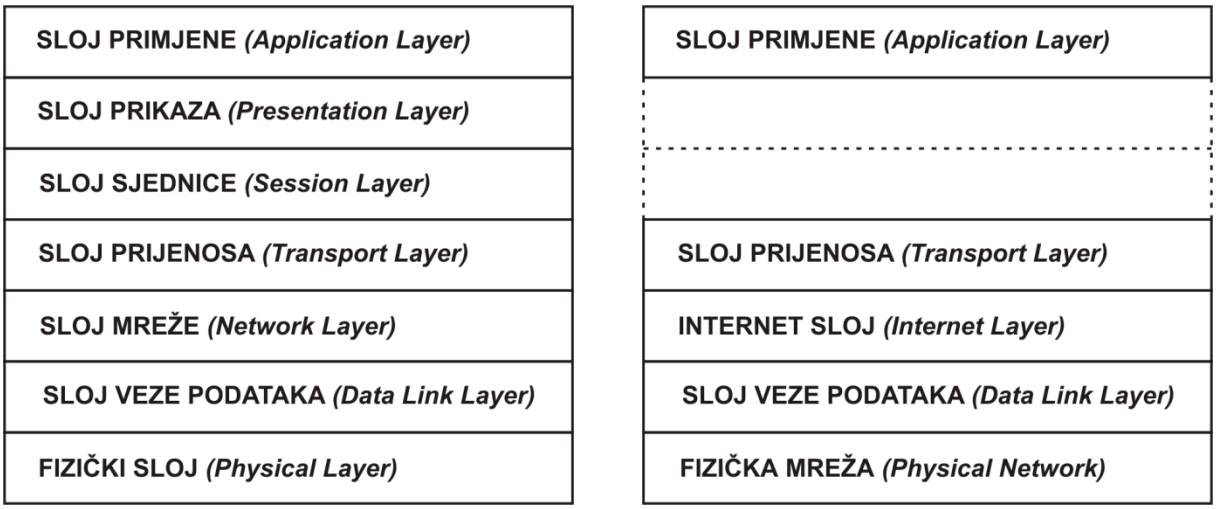
Jednostavnu mrežu čini više mrežnih čvorova međusobno povezanih preko jedinstvenog mrežnog medija (bakreni vodič, svjetlovod, radio-veza...). Svaki uređaj (čvor) u ovakvoj mreži jedinstveno je adresiran, što je i osnovni preduvjet za uspješnu mrežnu komunikaciju. Prema tome, i svaki podatak koji se prenosi preko mreže mora nositi jedinstvenu adresu izvora (kako bi izvorišni čvor mogao primiti odgovor ili eventualnu poruku o pogreški) i jedinstvenu adresu odredišta (odredišnog mrežnog čvora). U nekim izuzetnim slučajevima moguć je i višeodredišni prijenos podataka (višeodredišno slanje – *multicasting*, i razašiljanje podataka svim mrežnim čvorovima – *broadcasting*).

Veliki broj mreža koje je potrebno međusobno povezati različitog su tipa i međusobno se vrlo razlikuju (koriste međusobno različite formate za razmjenu podataka, kao i različite vrste prijenosnih medija). Kao rezultat rješavanja problema njihovog međusobnog povezivanja u jedinstvenu cjelinu nastao je slojeviti mrežni model *(Layered Internetworking Model)*. Slojeviti mrežni model predstavlja rješenje koje zadovoljava zahtjev da je za komunikaciju dovoljno poznavanje mrežne adrese odredišta. Kod slojevitog mrežnog modela djelovanje

mrežnog sustava razlaže se na nekoliko slojeva, gdje u svakom sloju postoji implementacija odgovarajućeg protokola. Implementacija ovih protokola često se prikazuje kao stog protokola *(protocol stack)*. Na svakom sloju ovakvog modela precizno je definiran način manipulacije podacima, kao i način razmjene podataka sa susjednim slojevima (svaki sloj u mogućnosti je izravno komunicirati sa svojim neposrednim susjedima, slojem iznad ili slojem ispod).

Kao standardni model mrežne arhitekture i komunikacijskih protokola prihvaćen je OSI slojeviti mrežni model *(Open Systems Interconnection)* kojeg je 1978. godine stvorila Međunarodna organizacija za standardizaciju *(ISO – International Organization for Standardization)*. Od tada ovaj model služi kao okvir pri utvrđivanju međunarodnih standarda za rad računalnih i komunikacijskih mreža raznorodnih arhitektura.

ISO-OSI model (slika 3.1) razlaže djelovanje mrežnog sustava na sedam odvojenih slojeva *(layer)*. Pri tome svaki od slojeva koristi resurse sloja koji je neposredno ispod, te daje usluge sloju neposredno iznad. Poruke koje slojevi mogu međusobno razmjenjivati u ovakvoj vertikalnoj hijerarhiji određene su odgovarajućim sučeljima i komunikacijskim protokolima. ISO-OSI model čine sljedeći slojevi (počevši od najnižeg): fizički sloj *(Physical Layer)*, sloj veze podataka *(Data Link Layer)*, sloj mreže *(Network Layer)*, sloj prijenosa *(Transport Layer)*, sloj sjednice *(Session Layer)*, sloj prikaza *(Presentation Layer)* i sloj primjene *(Application Layer)*.



Slika 3.1 Usporedni prikaz ISO-OSI modela i Internet modela

Prilikom izgradnje računalnih mreža u praksi se pokazalo da je moguće napraviti potpuno funkcionalnu višemrežnu arhitekturu korištenjem samo četiri sloja. Tako je nastao četveroslojni Internet model (danas najzastupljeniji slojeviti mrežni model) kao svojevrsno pojednostavljenje standardnog OSI modela (slika 3.1). Smanjenjem broja slojeva u mrežnom modelu postiže se jednostavnost, te veća brzina i učinkovitost (budući da se smanjenjem broja slojeva smanjuje i broj neophodnih interakcija među slojevima). Internet model čine sljedeći slojevi (počevši od najnižeg):

- **Sloj veze podataka** *(Data Link Layer)* – također poznat pod nazivom sloj mrežnog sučelja *(Network Interface Layer)* (na ovom sloju međusobno komuniciraju sustavi povezani u istu lokalnu mrežu – odbacuje se fizički sloj kao poseban sloj)
- **Internet sloj** *(Internet Layer)* – često se naziva i sloj mreže *(Network Layer)*, kao u OSI modelu (na ovom sloju sustavi komuniciraju, no nije moguće razlučiti međusobne interakcije pojedinačnih aplikacija)
- **Sloj prijenosa** *(Transport Layer)* – omogućava komunikaciju među procesima
- **Sloj primjene** *(Application Layer)* – sloj na kojem korisnik ostvaruje interakciju s mrežnom aplikacijom

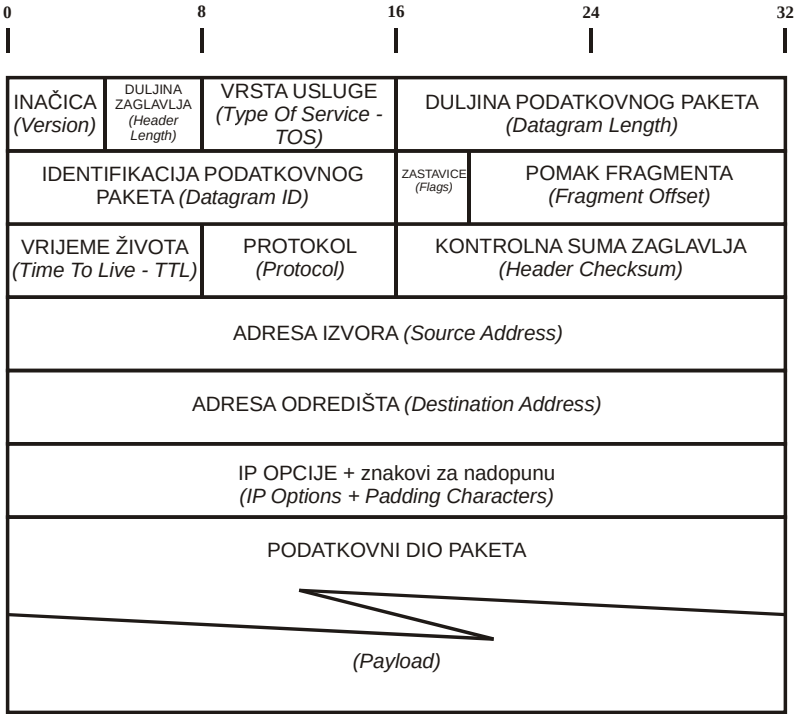
Internet slojeviti model često se naziva TCP/IP model. Ovaj naziv dobio je prema dva najznačajnija protokola koji se u njemu primjenjuju: IP protokol na Internet sloju *(Internet Protocol)* i TCP protokol na sloju prijenosa *(Transmission Control Protocol).* Trenutačno najraširenija verzija IP protokola jest verzija 4 (IPv4), koja je definirana u dokumentu RFC 791.

Interakcija između slojeva unutar slojevitog mrežnog modela uspješno se odvija zahvaljujući konceptu enkapsulacije (učahurivanja). To znači da se podaci „pakiraju“ u pakete, koji se općenito nazivaju protokolarnim jedinicama podataka *(Protocol Data Unit – PDU)*. Protokolarnoj jedinici podataka svaki sloj dodaje svoje zaglavlje u koje stavlja informacije koje su neophodne idućem sloju za pravilnu interpretaciju podataka koji se nalaze enkapsulirani unutar protokolarne jedinice podataka. Prilikom prijema podataka svaki sloj sa primljenog paketa podataka uklanja i procesira odgovarajuće („svoje“) zaglavlje, te podatke prosljeđuje sloju iznad sebe.

3.2. Problemi s IPv4 protokolom – razlozi prelaska na IPv6

Adresna arhitektura Internet protokola utemeljena je na posebno strukturiranim adresama. Svaka IPv4 adresa sastoji se od 32 bita (4 okteta), što teoretski daje brojku od 2^{32} mogućih adresa. 32-bitne IPv4 adrese obično se prikazuju kao 4 dekadska broja (u rasponu 0 – 255), međusobno razdvojena točkom. Svaku adresu čine dva dijela – prvi dio je tzv. mrežna adresa *(Network Address)*, a drugi dio je lokalna adresa *(Local Address)*. Izvan lokalne mreže važan je jedino mrežni dio adrese, dok je unutar lokalne mreže bitna jedino lokalna adresa (mrežni dio je irelevantan). Mrežne adrese dodjeljuju se pojedinim organizacijama, a potom te organizacije samostalno dodjeljuju lokalne adrese svojim računalima (i ostalim mrežnim uređajima). Mrežni administrator može adresni prostor koji mu je na raspolaganju organizirati hijerarhijski (što se obično u praksi i radi), te mrežu podijeliti na više podmreža *(subnet)*. Pri tome se jedan dio lokalne adrese maskira, te se taj dio koristi za adresiranje podmreže.

Svaki IPv4 podatkovni paket *(datagram)* sastoji se od zaglavlja *(header)* i podataka („teret“, *payload)*. Podaci su u IPv4 podatkovnom paketu organizirani u 32-bitne riječi. Struktura zaglavlja IPv4 podatkovnog paketa prikazana je na slici 3.2.



Slika 3.2 Struktura IPv4 zaglavlja

IPv4 protokol od svog nastanka (1981. godine) pa sve do danas nije doživio bitnije promjene. Pokazao se vrlo robusnim, jednostavnim za implementaciju i interoperabilnim, što mu je i omogućilo da ostane u uporabi dugi niz godina. Međutim, u vrijeme njegovog nastanka nije bilo moguće predvidjeti nezaustavljivi eksponencijalni rast Interneta, koji sa sobom donosi nove zahtjeve koje IPv4 protokol više ne može ispuniti na zadovoljavajući način, pa do izražaja počinju dolaziti njegovi nedostaci.

Neki karakteristični problemi koji se nisu mogi predvidjeti prilikom inicijalnog dizajna IP protokola su:

- **Iskorištenje adresnog prostora (nedostatak adresa) uslijed eksponencijalnog rasta Interneta**

  Zbog naglog porasta broja uređaja povezanih u globalnu mrežu 32-bitni adresni prostor pokazuje se kao nedovoljno velik. Upravo je iskorištenje adresnog prostora jedan od najvećih problema IPv4 protokola koji zahtijeva što brže rješavanje, posebno imajući u vidu porast broja različitih uređaja (osim osobnih računala) koji dobivaju mogućnost povezivanja na Internet (mobilni telefoni, različiti kućanski aparati, uređaji ugrađeni u razna prometala, bežični senzorski čvorovi i sl.). Danas se u praksi često koristi translator mrežnih adresa *(Network Address Translator – NAT)* kao rješenje koje omogućava racionalnije iskorištavanje adresnog prostora i koje donekle produljuje životni vijek IPv4 protokola. Ideja NAT sustava jest mapiranje više privatnih IP adresa na jednu javnu IP adresu, te se NAT zapravo ponaša kao sučelje između privatne i javne mreže.
- **Naglo povećanje usmjerivačkih tablica**

  Povećanjem broja mreža unutar globalne mreže (Interneta) naglo se povećava broj ruta koje usmjerivači moraju imati pohranjene u svojim tablicama. Problem je posebno izražen kod usmjerivača koji se nalaze na okosnicama Interneta (jezgreni dio mreže, *backbone)* i čije tablice danas sadržavaju na desetke tisuća ruta. Povećanje usmjerivačkih tablica (porast broja ruta) postavlja sve veće hardverske zahtjeve na usmjerivače te uzrokuje smanjenje brzine obrade podataka.
- **Potreba za jednostavnijom konfiguracijom**

  Većina današnjih IPv4 implementacija mora biti konfigurirana ručno ili koristi neki konfiguracijski protokol, poput DHCP-a *(Dynamic Host Configuration Protocol)*. Ručna konfiguracija podrazumijeva poznavanje i ručno podešavanje prilično kompliciranog skupa parametara (naziv računala – *host name*, IP adresa, maska

podmreže – *subnet mask*, podrazumijevani usmjerivač – *default router*, i nekih drugih, ovisno o implementaciji). Prilikom konfiguracije putem DHCP-a klijentsko računalo spaja se na DHCP server koji mu prosljeđuje IP adresu i ostale konfiguracijske parametre. Međutim, porast broja mrežnih čvorova zahtijeva još jednostavniji konfiguracijski postupak koji bi bio još više automatiziran i ne bi zahtijevao dodatnu infrastrukturu i njezinu administraciju (kao što je slučaj kod DHCP-a).

- **Sigurnosni zahtjevi na razini Internet protokola**

  Privatna komunikacija putem javnog medija (poput Interneta) zahtijeva zaštitu podataka od neovlaštenog pristupa ili čak njihove modifikacije prilikom prijenosa. To implicira nužnost enkripcije podatkovnog dijela unutar IP paketa. Do sada se implementacija sigurnosnih rješenja uglavnom provodila na nekom od viših slojeva unutar slojevitog mrežnog modela (obično unutar aplikacijskog sloja – npr. SHTTP, *Secure HyperText Transmission Protocol* ili, rjeđe, unutar prijenosnog sloja – npr. SSL, *Secure Socket Layer* protokol). Tendencija je u budućnosti implementirati sigurnosne mehanizme već na razini Internet protokola, dakle unutar mrežnog (Internet) sloja.

- **Nužnost bolje podrške za isporuku podataka u stvarnom vremenu**

  Bolja podrška isporuci paketa podataka u stvarnom vremenu od iznimne je važnosti kod audio-video prijenosa. Unutar IPv4 zaglavlja postoji polje TOS *(Type of Service)* pomoću kojeg se usmjerivaču određuje na koji način je potrebno procesirati paket. No, ova ideja nije osobito zaživjela u praksi. Jedan od glavnih razloga jest činjenica da se implementacijom ovog pristupa drastično usporava i otežava usmjeravanje paketa, budući da bi svaki usmjerivač morao pratiti znatno više informacija o svakoj ruti (latencija, propusnost, pouzdanost, dostupnost rute) i uzeti ih u obzir prilikom procesiranja paketa. Prema tome, nameće se nužnost iznalaženja boljeg i kvalitetnijeg rješenja za podršku protoka podataka u stvarnom vremenu.

3.3. Novosti i promjene koje donosi IPv6 protokol

Kako bi se otklonili uočeni nedostaci IPv4 protokola i uvela dodatna poboljšanja, međunarodna organizacija IETF *(Internet Engineering Task Force)* započela je sa razvojem novog skupa protokola koji bi zamijenio postojeći IPv4. Ovi napori rezultirali su novom

verzijom IP protokola (Internet protokol verzija 6, IPv6), čija je specifikacija po prvi puta u cjelovitoj formi objavljena 1995. godine (RFC 1883). Iste godine pojavili su se još neki dokumenti koji se pobliže bave drugim područjima vezanim uz IPv6 (npr. arhitektura adresiranja, protokol kontrolnih poruka i sl.). Ovi dokumenti su kasnije zamijenjeni novijim, proširenim i dopunjenim verzijama.

Internet protokol verzija 6 otklanja nedostatke uočene kod stare verzije protokola, te donosi niz novih poboljšanja [13]. Najvažnije novosti i promjene koje donosi IPv6 protokol su sljedeće:

- **Prošireno adresiranje**

  IPv6 protokol umjesto 32-bitnog adresiranja uvodi 128-bitno adresiranje, što daje enormnu brojku od 2^{128} mogućih adresa. IPv6 donosi i neke promjene u pogledu tipova adresa. Ukidaju se *broadcast* adrese, no uvodi se koncept *anycast* adresa. *Unicast* i *multicast* tipovi adresa ostaju gotovo nepromijenjeni u odnosu na IPv4.
- **Pojednostavljen format zaglavlja**

  Zaglavlje kod IPv6 protokola fiksne je duljine od 40 okteta i sastoji se od 8 polja, nasuprot zaglavlju kod IPv4 protokola koje se sastoji od najmanje 12 polja i čija duljina varira od 20 do 60 okteta (ovisno o tome koriste li se opcijska polja). Fiksna duljina i smanjen broj polja kod IPv6 zaglavlja u velikoj mjeri doprinose povećanju brzine i učinkovitosti kod usmjeravanja, budući da je takva zaglavlja moguće brže procesirati. Budući da je zaglavlje sada fiksne duljine iz njega je izbačeno polje „duljina zaglavlja“ *(Header Length)* kao nepotrebno. Kod IPv6 protokola fragmentacija paketa dozvoljena je samo na izvoru (nije moguća fragmentacija paketa na čvorovima preko kojih paket putuje od izvora do odredišta), pa su iz zaglavlja izbačena i polja koja se odnose na fragmentaciju. Izbačena je i kontrolna suma zaglavlja *(checksum)* pošto se ona ionako provodi na protokolima višeg sloja (TCP ili UDP).
- **Poboljšana podrška za proširenja i opcije**

  Za razliku od IPv4 protokola (kod kojeg se opcije dodaju na kraj postojećeg zaglavlja) kod IPv6 protokola opcije se dodaju unutar odvojenih proširenih zaglavlja. Prema tome, dodatno zaglavlje s opcijama bit će procesirano samo ukoliko je to potrebno, pa se na taj način ubrzava procesiranje IPv6 paketa prilikom usmjeravanja.

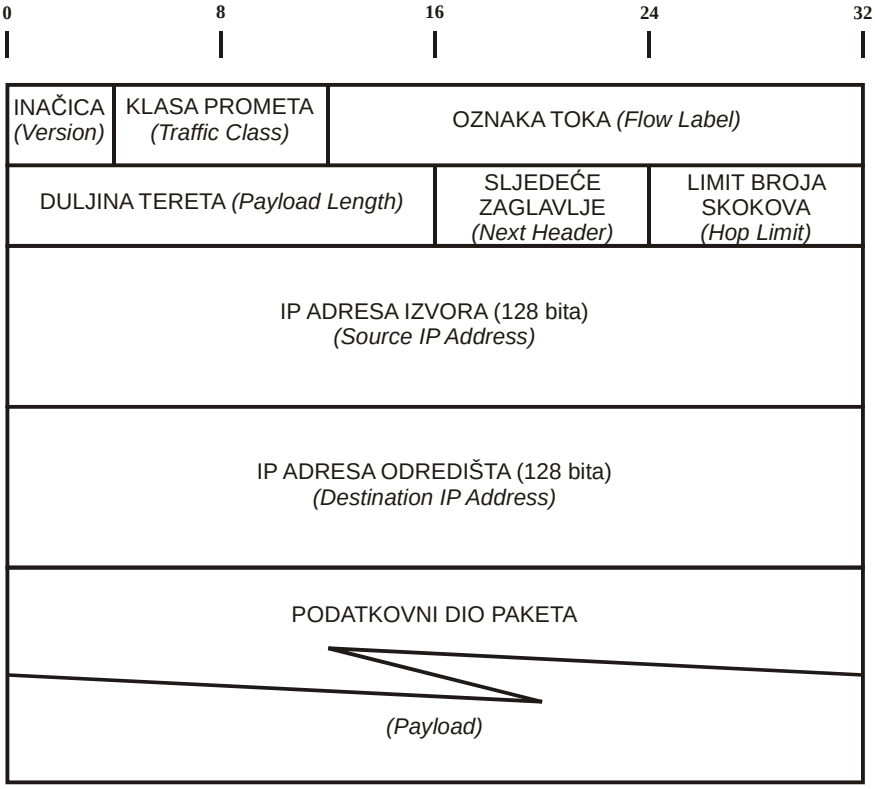
- **Označavanje toka paketa**

  Kod IPv4 protokola svi paketi se tretiraju pojedinačno, neovisno jedan o drugom – usmjerivač ne prati pojedine nizove paketa koji putuju između dva određena čvora. IPv6 protokol implementira koncept toka *(flow)* kojeg usmjerivači mogu pratiti. Na taj način usmjerivač je u stanju zapamtiti dio informacije koji ostaje nepromijenjen kod svakog paketa u nizu, pa je moguća njihova brža i učinkovitija obrada (budući da nije potrebno procesirati kompletno zaglavlje svakog paketa).

- **Utvrđivanje autentičnosti i privatnost**

  IPv6 protokol implementira sigurnosna proširenja u vidu dodatnih sigurnosnih zaglavlja – AH *(Authentication Header)* i ESP *(Encapsulating Security Payload)*. Pošiljatelj na temelju podataka koji se šalju odgovarajućim postupkom izračunava vrijednost koju upisuje u zaglavlje AH. Primatelj potom izračunava istu vrijednost i uspoređuje dobiveni rezultat sa vrijednošću upisanom u AH. Ukoliko se te dvije vrijednosti razlikuju za pretpostaviti je da je prilikom prijenosa došlo do oštećenja paketa ili do njegove namjerne neovlaštene modifikacije. ESP zaglavlje osigurava mehanizam enkripcije čitavog IP paketa ili samo njegovog podatkovnog dijela *(payload)*. Ukoliko se enkriptira samo podatkovni dio (dok zaglavlje ostaje nekriptirano) neovlaštena osoba može doći do podataka o izvoru i odredištu paketa (kao i ostalih informacija o paketu koje se mogu iščitati iz zaglavlja). Pomoću ESP-a moguće je enkriptirati i cijeli IP paket, pri čemu se on enkapsulira u novi IP paket – koncept na kojem se temelje virtualne privatne mreže *(Virtual Private Network – VPN)*.

Zaglavlje IPv6 paketa ima fiksnu duljinu od 40 okteta. Struktura IPv6 zaglavlja prikazana je na slici 3.3.



Slika 3.3 Struktura IPv6 zaglavlja

Kod IPv4 protokola dodatne opcije unutar zaglavlja podatkovnog paketa mogle su se dodavati unutar polja „IP opcije“ *(IP Options)*. Međutim, time se mijenjao oblik IPv4 zaglavlja te bi na taj način izmijenjena zaglavlja zahtijevala poseban tretman prilikom usmjeravanja. Budući da su usmjerivači optimizirani za tipičan i najčešći oblik paketa (bez dodatnih opcija) dodavanje polja opcija unutar IPv4 zaglavlja drastično je narušavalo performanse pri usmjeravanju paketa. To i jest jedan od glavnih razloga zašto se ovo polje vrlo rijetko koristi.

Implementacija proširenja zaglavlja kod IPv6 protokola napravljena je tako da se problem pada performansi prilikom usmjeravanja u potpunosti eliminira. Kod IPv6 protokola opcije se iz zaglavlja „premještaju“ u podatkovni dio paketa *(payload)*. Prema tome, glavno zaglavlje ostaje uvijek fiksne duljine, dok opcijska zaglavlja slijede iza njega. Pri tome vrijednost polja „sljedeće zaglavlje“ *(Next Header)* unutar glavnog zaglavlja ukazuje na tip proširenog zaglavlja koje slijedi (ukoliko nema proširenog zaglavlja vrijednost ovog polja ukazuje na zaglavlje nekog protokola više razine). Ovakvim pristupom ne smanjuje se brzina usmjeravanja paketa, budući da usmjerivači na jednak način procesiraju i pakete koji sadrže i

one koji ne sadrže opcijska dodatna (proširena) zaglavlja. Za sve usmjerivače osim krajnjih čvorova opcijska polja IPv6 paketa ostaju skrivena (izuzetak je opcijsko polje „korak po korak“, *hop-by-hop*, koje se procesira na svakom usmjerivaču). Način dodavanja proširenja (proširenih zaglavlja) iza glavnog zaglavlja otvara mogućnost jednostavnog specificiranja i dodavanja nekih novih opcija u budućnosti. Jedinstvene oznake proširenih zaglavlja (upisuju se u polje *Next Header* u glavnom zaglavlju), kao i redoslijed proširenih zaglavlja (ukoliko ih ima više) jednoznačno su određeni unutar IPv6 standarda.

128-bitne IPv6 adrese najčešće se prikazuju pomoću 8 četvoroznamenkastih heksadekadskih brojeva razdvojenih dvotočkom (gdje svaka znamenka zamjenjuje 4 bita). Primjer ispravne IPv6 adrese: ABCD:9BFF:3333:1256:A77C:87F1:450A:1111. Često se u IPv6 adresi pojavljuje dugački niz nula (npr. 2005:0:0:0:0:0:0:1), pa je moguć i skraćeni zapis, gdje se niz nula zamjenjuje s dvije dvotočke (npr. 2005::1).

Postoji tri osnovna tipa IPv6 adresa. To su *unicast*, *multicast* i *anycast* adrese. *Unicast* i *multicast* tipovi adresa nisu bitnije promijenjeni u odnosu na IPv4. *Broadcast* tip adresa (koji je postojao kod IPv4) je ukinut, budući da je često znao stvarati probleme. Ideja je bila da se na *broadcast* adrese šalju podaci koji su namijenjeni nekolicini čvorova. Međutim, više *broadcast* prijenosa unutar jedne mreže znalo je narušavati njezine performanse, budući da je svaki čvor morao procesirati sve *broadcast* pakete, iako je većina od njih za njega bila irelevantna. Zbog toga *broadcast* ne nalazi mjesto u novom standardu. Ipak, ukoliko se ponekad ukaže potreba, isti učinak kakav je postizao *broadcast* u IPv4 mreži moguće je u IPv6 mreži postići uporabom *multicast* adresa usmjerenih na sve čvorove u mreži [80, 81].

Unicast adresa identificira jedno IPv6 mrežno sučelje *(interface).* Ukoliko neki mrežni čvor ima više od jednog mrežnog sučelja mora imati i više adresa (svakom mrežnom sučelju mora biti pridružena po jedna *unicast* adresa). *Multicast* adresa identificira skup mrežnih sučelja (koja obično pripadaju različitim mrežnim čvorovima). Paket poslan na *multicast* adresu biva dostavljen na sva mrežna sučelja koja identificira ta adresa (pri čemu se čvorovi u mreži „pretplaćuju“ na određene *multicast* adrese). *Multicast* adrese mogu se koristiti samo kao odredišne adrese – ne smije se dogoditi da se generira podatkovni paket čija bi adresa izvora bila neka *multicast* adresa. IPv6 *multicast* adresu jedinstveno identificira njezin prvi oktet koji sadrži sve jedinice (tj. svaka *multicast* adresa započinje heksadekadskim nizom „FF“). *Anycast* adresa (jednako kao i *multicast* adresa) identificira skup mrežnih sučelja koja pripadaju različitim mrežnim čvorovima. Međutim, paket poslan na *anycast* adresu isporučuje

se samo jednom od sučelja (čvorova) koje ona identificira. Paket se isporučuje „najbližem“ čvoru, prema mjerama udaljenosti protokola za usmjeravanje. Razlika u odnosu na *multicast* je u tome što se paket uvijek šalje samo „najbližem“ čvoru (dok se paketi adresirani na *multicast* adresu šalju svim pretplaćenim čvorovima). *Anycast* adrese dijele adresni prostor s *unicast* adresama (tj. po svojem obliku ne razlikuju se od *unicast* adresa). Zbog toga čvorovi kojima je pridružena *anycast* adresa moraju biti eksplicitno konfigurirani na način da tu određenu adresu prepoznaju kao *anycast* adresu.

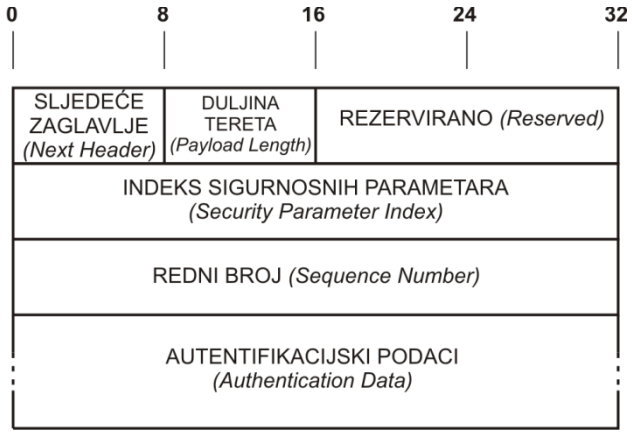
3.4. Sigurnosni aspekti IPv6 protokola

Kvalitetno rješavanje problematike sigurnosti u komunikacijskim mrežama predstavlja jedan od najvažnijih preduvjeta za njihovu široku uporabu. Kada je riječ o sigurnosti, obično se definiraju određeni ciljevi koji moraju biti zadovoljeni kako bi se moglo smatrati da su sigurnosni mehanizmi uspostavljeni na zadovoljavajući način [131, 132]. Neki od glavnih ciljeva koji se nastoje postići implementacijom sigurnosnih mehanizama su:

- **Autentifikacija** *(Authentication)* – utvrđivanje autentičnosti, što podrazumijeva mogućnost da se pouzdano utvrdi da je poslani podatak uistinu i primljen, te da je pošiljatelj podataka uistinu onaj koji se predstavlja primatelju
- **Integritet** *(Integrity)* – podrazumijeva mogućnost pouzdanog utvrđivanja je li podatak bio modificiran na svom putu od izvora do odredišta
- **Povjerljivost** *(Confidentiality)* – podrazumijeva prijenos podataka koje će moći pročitati samo ovlašteni primatelj, i nitko drugi osim njega

Sigurnosni mehanizmi i mehanizmi utvrđivanja autentičnosti (autentifikacijski mehanizmi) do sada su uglavnom bili implementirani u mrežnim protokolima viših slojeva. Zbog sve većih problema sa sigurnošću komunikacije (stalni porast broja napada i neovlaštenih upada) u posljednje vrijeme javlja se tendencija spuštanja sigurnosnih i autentifikacijskih mehanizama već na razinu Internet protokola. IPv6 protokol upravo omogućava implementaciju ovih mehanizama na razini samog Internet protokola pravilnom implementacijom i uporabom sigurnosnih zaglavlja (AH i ESP zaglavlja). AH zaglavlje omogućava izvorišnom čvoru digitalno potpisivanje paketa, dok ESP zaglavlje omogućava enkripciju sadržaja IPv6 paketa.

AH zaglavlje *(Authentication Header)* koristi se za utvrđivanje autentičnosti i integriteta IP podatkovnih paketa, kao i za zaštitu od napada ponavljanjem slanja paketa (slika 3.4). Ukoliko se koriste i neka druga proširena zaglavlja, AH zaglavlje uvijek mora biti postavljeno iza svih zaglavlja koja se procesiraju na svakom čvoru (usmjerivaču) preko kojih paket prolazi, a ispred svih zaglavlja koja se procesiraju samo na odredišnom čvoru.



Slika 3.4 AH zaglavlje (Authentication Header)

AH zaglavlje sadrži sljedeća polja:

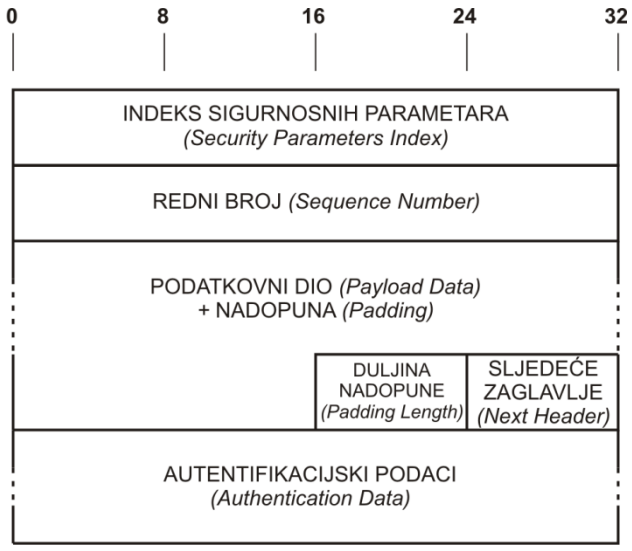
- **Sljedeće zaglavlje** *(Next Header)* – 8-bitno polje koje naznačava protokol zaglavlja koje slijedi
- **Duljina tereta** *(Payload Length)* – 8-bitno polje koje pokazuje ukupnu duljinu AH zaglavlja u jedinicama od po 32 bita, minus dva (ta vrijednost predstavlja ukupnu duljinu autentifikacijskih podataka zajedno sa poljem *Sequence Number*, redni broj)
- **Rezervirano** *(Reserved)* – 16-bitno polje rezervirano za buduću uporabu (za sada se ne koristi i svi njegovi bitovi postavljaju se u nulu)
- **Indeks sigurnosnih parametara** *(SPI, Security Parameter Index)* – 32-bitno polje čija je vrijednost proizvoljna (vrijednost 0 je samo za lokalnu uporabu, a vrijednosti od 1 do 255 rezervirane su za buduću uporabu od strane organizacije IANA)
- **Redni broj** *(Sequence Number)* – 32-bitna vrijednost koja predstavlja brojač (vrijednost mu kreće od nule, inkrementira se sa svakim poslanim paketom i služi za sprečavanje napada ponovljenim slanjem paketa)
- **Autentifikacijski podaci** *(Authentication Data)* – polje duljine *n* 32-bitnih jedinica, predstavlja najvažniji dio AH zaglavlja; ovo polje sadrži ICV vrijednost *(Integrity Check Value)* – vrijednost za provjeru integriteta (njegova vrijednost izračunava se

prema određenom algoritmu, na osnovu podatkovnog dijela IPv6 datagrama i nepromjenjivih dijelova zaglavlja)

Svrha ESP zaglavlja *(Encapsulating Security Payload)* jest omogućiti mrežnim čvorovima slanje i prijem datagrama čiji je podatkovni dio enkriptiran (slika 3.5). Preciznije, ESP zaglavlje omogućava nekoliko različitih usluga (od kojih se neke i preklapaju s uslugama AH zaglavlja):

- Povjerljivost podatkovnog paketa (postignuta zahvaljujući enkripciji)
- Utvrđivanje autentičnosti porijekla podataka (zahvaljujući enkripciji pomoću javnog ključa)
- Zaštita od napada ponavljajućim paketima (zahvaljujući mehanizmu brojača, kao kod AH zaglavlja)
- Ograničena povjerljivost podatkovnog toka (uporabom sigurnosnih *gateway*-a)

Iako se može koristiti i samostalno, preporučuje se uporaba ESP zaglavlja zajedno s AH zaglavljem. ESP zaglavlje dolazi iza svih zaglavlja koja se moraju procesirati na čvorovima između izvora i odredišta (budući da je sav sadržaj iza ESP zaglavlja enkriptiran).



Slika 3.5 ESP zaglavlje (Encapsulating Security Payload)

ESP zaglavlje sadrži sljedeća polja:

- **Indeks sigurnosnih parametara** *(Security Parameters Index)* – 32-bitno polje, identično istom polju kod AH zaglavlja

- **Redni broj** *(Sequence Number)* – 32-bitni brojač, identičan brojaču unutar AH zaglavlja
- **Podatkovni dio, „teret“** *(Payload Data)* – polje varijabilne duljine koje sadrži enkriptirani dio podatkovnog paketa (zajedno sa eventualnim dodatnim podacima nužnim za rad enkripcijskog algoritma – npr. inicijalizacijskim podacima)
- **Nadopuna** *(Padding)* – dodatni niz bitova koji se dodaje podatkovnom dijelu kako bi se njegova duljina proširila do zadanih granica (na cijeli broj 32-bitnih blokova)
- **Duljina nadopune** *(Padding Length)* – ukazuje na veličinu dodane nadopune
- **Sljedeće zaglavlje** *(Next Header)* – ukazuje na sljedeće zaglavlje (netipično je što se kod ESP zaglavlja ovo polje nalazi pri kraju zaglavlja, dok se kod drugih tipova IPv6 zaglavlja obično nalazi na početku zaglavlja)
- **Autentifikacijski podaci** *(Authentication Data)* – ovo polje sadrži ICV vrijednost *(Integrity Check Value)* izračunatu na temelju cjelokupnog ESP zaglavlja (opcionalno)

3.4.1. Sigurnosne prijetnje i sigurnosna arhitektura u IPv6 mrežama

U mrežama otvorenog tipa, kakav je i Internet, vrlo teško je uspostaviti potrebnu razinu sigurnosti. U ovakvoj okolini čak i uz uporabu enkripcije i digitalnih potpisa postoje značajne sigurnosne prijetnje. Postoji više različitih vrsta i metoda napada i sigurnosnih prijetnji. Neke od poznatijih su:

- **Presretanje prometa** *(Interception)*

  Pod presretanjem prometa podrazumijeva se situacija kada neovlašteni napadač C prati (prisluškuje) promet (komunikaciju) koja se odvija između čvorova A i B, a da čvorovi A i B toga nisu svjesni
- **Napadi uskraćivanjem usluge** *(Denial of Service, DoS)*

  Napadi uskraćivanjem usluge nastaju kada neovlašteni entitet koristi mrežni prijenos kako bi na određeni način autoriziranom korisniku uskratio pristup mrežnim resursima.

- **Napadi lažnim predstavljanjem** *(Spoofing)*

  Primjer ove vrste napada jest slučaj kada neovlašteni zlonamjerni entitet šalje mrežni promet (pakete) čiji izvor je lažno predstavljen (npr. slanje IPv6 paketa s falsificiranom adresom izvora).

U IPv6 mrežama obvezna je implementacija sigurnosne arhitekture Internet protokola *(IPsec)*, koja omogućava uporabu sigurnosnih mehanizama na IP razini. *IPsec* pruža skup alata neophodnih za razmjenu informacija između dva sustava („pregovaranje“) prilikom uspostave sigurne (zaštićene) veze sa sigurnosnim mehanizmima na razini prihvatljivoj za oba sustava. Svaki sustav mora omogućavati komunikaciju primjenom nekoliko prihvatljivih enkripcijskih algoritama, što mu onda otvara mogućnost „pregovaranja“ s drugim sustavom o tome koji će se od tih algoritama koristiti (pri čemu drugi sustav mora podržavati barem jedan enkripcijski algoritam koji podržava prvi sustav). Sigurnosne usluge koje se smatraju dijelom sigurnosne arhitekture Internet protokola uključuju sljedeće:

- **Kontrola pristupa** *(Access Control)*

  Pod kontrolom pristupa podrazumijeva se omogućavanje pristupa pojedinim uslugama ili sustavima isključivo uz posjedovanje valjane zaporke.
- **Beskonekcijski integritet** *(Connectionless Integrity)*

  Pod ovim pojmom podrazumijeva se mogućnost korištenja *IPsec* arhitekture za provjeru integriteta bilo kojeg pojedinačnog IP paketa, neovisno o ostalim paketima.
- **Provjera autentičnosti porijekla podataka** *(Data Origin Authentication)*

  Pod ovim pojmom podrazumijeva se mogućnost identificiranja izvora podatka koji se prenosi unutar IP paketa.
- **Zaštita od napada ponovljenim slanjem paketa** *(Defense Against Packet Replay Attacks)*

  Budući da je Internet protokol beskonekcijski protokol, moguć je scenarij napada kod kojeg napadač neprekidno ponavlja slanje paketa kojeg je odredišni čvor već primio, pri čemu dolazi do preopterećenja resursa napadnutog čvora i on postaje nedostupan. *IPsec* pruža mehanizam zaštite od ovakvog napada koji se temelji na implementaciji brojača paketa.
- **Enkripcija** *(Encryption)*

  Korištenjem enkripcije podataka nastoji se osigurati povjerljivost podataka te spriječiti neovlaštene osobe da pristupe podacima.

Sve navedene funkcije moguće je ostvariti pravilnom uporabom AH *(Authentication Header)* i ESP *(Encapsulating Security Payload)* zaglavlja. Postoji nekoliko mogućih načina implementacije sigurnosne arhitekture Internet protokola *(IPsec)*:

- **Implementacija IPsec-a kao dijela IPv6 stoga**
  Ovakav pristup podrazumijeva punu podršku za sigurnosna zaglavlja Internet protokola unutar mrežnog stoga *(stack)* Internet protokola, čime sigurnosna arhitektura postaje integralnim dijelom implementacije protokola. Pri ovakvoj implementaciji potrebna je softverska i/ili hardverska nadogradnja stoga Internet protokola.
- **BITS implementacija IPsec-a *(„Bump In The Stack“)***
  Ovaj pristup podrazumijeva umetanje softverskog koda koji funkcionira između Internet sloja i sloja veze podataka. Ovaj softver presreće podatkovne pakete koji putuju sa stoga Internet protokola na sučelje sloja veze podataka i prije nego što ih proslijedi najprije obavlja procesiranje paketa vezano uz implementaciju sigurnosnih mehanizama. Prednost ovakve implementacije je u tome što ju je moguće provesti bez potrebe za reprogramiranjem softvera stoga Internet protokola.
- **BITW implementacija IPsec-a *(„Bump In The Wire“)***
  BITW pristup podrazumijeva uporabu vanjskog hardvera za sigurnosno procesiranje. Taj vanjski IP uređaj obično funkcionira kao neka vrsta sigurnosnih vrata *(Security Gateway)* za sve podatkovne pakete koji putuju do sustava na kojeg je povezan. Jedan BITW uređaj može istovremeno implementirati zaštitne mehanizme za nekoliko sustava.

Jedno od najvažnijih poboljšanja koje sa sobom donosi nova inačica Internet protokola jest i poboljšanje postojećih i uvođenje novih autokonfiguracijskih mehanizama. Osnovna ideja je omogućiti tzv. *plug-and-play* način rada, što znači da bi se mrežni uređaj mogao koristiti odmah po priključenju na IPv6 mrežu, bez potrebe za ikakvim „ručnim“ podešavanjem ili bilo kojom drugom intervencijom od strane korisnika ili mrežnog administratora. Ovakvim postupkom nastoji se maksimalno pojednostaviti uporaba mrežnih tehnologija, te ih se nastoji na taj način učiniti dostupnijim što širem krugu korisnika.

IPv6 protokol poznaje dvije glavne vrste autokonfiguracijskih postupaka. To su *stateful* i *stateless* autokonfiguracija. *Stateful* autokonfiguracija podrazumijeva postojanje poslužitelja (servera) na kojem su pohranjene statusne informacije svih čvorova u mreži i koji obavlja administraciju nad tim informacijama. Kod *stateless* autokonfiguracije ne postoji poslužitelj

koji bi administrirao informacije o svim čvorovima i kojem bi čvorovi u mreži morali eksplicitno postavljati upit o konfiguracijskim parametrima. *Stateless* autokonfiguracija podrazumijeva mehanizam koji bi pojedinim čvorovima omogućio konfiguraciju potrebnih parametara za povezivanje u mrežu bez prethodnog povezivanja na ovakav središnji server. Nedostatak *stateful* autokonfiguracije jest upravo nužnost postojanja posebnog autokonfiguracijskog servera, budući da on zahtijeva održavanje i administriranje. Glavni nedostatak *stateless* autokonfiguracijskog postupka jest nemogućnost potpunog nadzora nad čvorovima koji pristupaju mreži (što često može predstavljati problem, pogotovo u korporativnom okruženju).

Stateful autokonfiguracija temelji se na tzv. DHCP protokolu *(Dynamic Host Configuration Protocol)* koji je dobio i svoju DHCPv6 inačicu. Kako bi se koristio ovaj mehanizam autokonfiguracije u mreži mora biti instaliran i administriran DHCP poslužitelj. DHCP poslužitelj posjeduje listu čvorova kojima smije dodjeljivati konfiguracijske parametre. Također, DHCP poslužitelj prati koje su IP adrese trenutačno u uporabi, a koje su slobodne i dostupne za ponovnu dodjelu nekom čvoru koji zatraži pristup mreži. Prilikom svakog spajanja na mrežu mrežni uređaji se najprije povezuju na DHCP poslužitelj koji im prosljeđuje potrebne konfiguracijske parametre.

Stateless autokonfiguracijski postupak ne zahtijeva povezivanje na središnji poslužitelj. Kod ovog postupka čvor najprije mora odrediti svoju lokalnu adresu (to može biti adresa koja se posebnim postupkom i prema određenom standardu izvodi iz 48-bitne MAC adrese, koja je jedinstvena za svako mrežno sučelje). Jedan od standarda koji se koristi pri izvođenju lokalne adrese jest standard IEEE EUI-64. Potom je nužno verificirati jedinstvenost formirane adrese. Konačno, čvor mora odrediti koji konfiguracijski parametri su mu potrebni i na koji način može do njih doći. Jedna mogućnost jest da se konfiguracija dalje nastavlja *stateful* postupkom, te da čvor dobije konfiguracijske parametre od poslužitelja. Druga mogućnost jest da čvor „osluškuje“ poruke koje usmjerivači periodički šalju svim čvorovima u mreži (na *multicast* adrese) i unutar kojih se nalaze potrebni konfiguracijski parametri (poput mrežne adrese). Zbog toga je nužno da čvorovi koji se konfiguriraju *stateless* postupkom podržavaju *multicast*. Umjesto da čeka periodičku poruku usmjerivača, čvor može poslati i izravan zahtjev usmjerivaču (upućen na *multicast* adresu namijenjenu svim usmjerivačima) za slanjem odgovarajuće poruke s konfiguracijskim parametrima.

Stateless i *stateful* autokonfiguracijski postupak ne isključuju jedan drugog, nego, naprotiv, često koegzistiraju i funkcioniraju zajedno (npr. situacija kada čvor koji se spaja na mrežu koristi *stateless* postupak kako bi došao do IP adrese, te se potom s tom adresom spaja na DHCP server od kojeg prima i ostale konfiguracijske parametre).

3.5. IPv6 protokol u bežičnim senzorskim mrežama

Implementacija sveprisutnog i općeprihvaćenog IP protokola u bežične senzorske mreže i ostale mreže kratkog dometa i ograničenih resursa (npr. PAN mreže, *Personal Area Network)* u početku njihovog razvoja smatrala se nepraktičnom i neadekvatnom (prvenstveno zbog strogo ograničenih resursa). Smatralo se da je IP protokol prezahtjevan, te da ne može na zadovoljavajući način funkcionirati na slabim mikrokontrolerima i niskoenergetskim niskopropusnim bežičnim linkovima. Zbog toga se IP uglavnom zaobilazio i pronalazila su se alternativna rješenja u vidu protokola specijaliziranih za senzorske mreže. Međutim, raznolikost protokola i nepostojanje jedinstvenog standarda dodatni je faktor koji ograničava povezivost i interoperabilnost senzorskih mreža sa drugim tipovima mreža. Zbog toga se u posljednje vrijeme (posljednjih nekoliko godina) počinju ulagati značajniji napori da se IP protokol uz odgovarajuće prilagodbe implementira u BSM [30, 33, 44, 47, 115] . Budući da je i u klasičnim mrežama prisutan aktivan prelazak na IP verzije 6 (IPv6) i u senzorskim mrežama je stavljen naglasak na implementaciju upravo ove verzije IP protokola [1]. IPv6 protokol donosi i iznimno velik adresni prostor, što čak omogućava i jedinstveno globalno identificiranje čvorova senzorske mreže (kojih može biti izuzetno velik broj). Težnja za implementacijom IPv6 u BSM rezultirala je i formiranjem određenih radnih skupina unutar IETF *(Internet Engineering Task Force),* kao što su radna skupina 6LoWPAN *(IPv6 over Low power Wireless Personal Area Network),* ili radna skupina ROLL *(Routing Over Low power and Lossy networks).* Dosadašnji rad ovih skupina rezultirao je nekolicinom RFC dokumenata i određenim brojem dokumenata koji su još u statusu nacrta *(draft).*

IPv6 protokol nije moguće izravno implementirati unutar protokolnog stoga karakterističnog za BSM bez odgovarajuće prilagodbe. Prilagodbu je nužno napraviti kako bi se IPv6 paketi mogli prenijeti unutar okvira koji se koriste na fizikalnom sloju BSM, a koji su u većini slučajeva puno manji. Ovaj problem rješava se umetanjem odgovarajućeg

adaptacijskog sloja unutar protokolnog stoga. Također, i protokol usmjeravanja koji se primjenjuje u mreži treba uključivati podršku za IPv6.

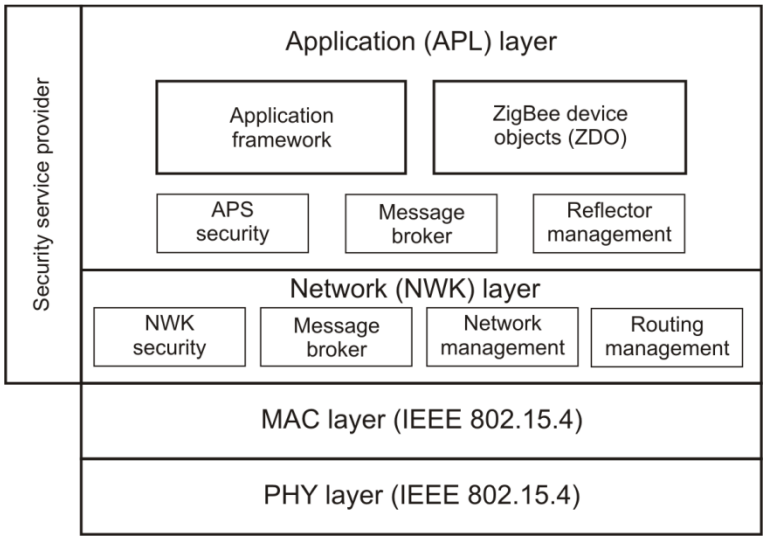
Na fizikalnom sloju velike većine današnjih BSM primjenjuje se standard IEEE 802.15.4 koji definira fizikalni sloj i sloj pristupa mediju. Zbog toga se prilikom implementacije IPv6 protokola u BSM on najprije nastojao implementirati u mreže temeljene upravo na IEEE 802.15.4 standardu. Kao rezultat ovih nastojanja nastao je 6LoWPAN adaptacijski sloj, koji omogućava prilagodbu IPv6 paketa za prijenos pomoću IEEE 802.15.4 okvira. Prvi (za sada i jedini) usmjerivački protokol namijenjen senzorskim mrežama sa podrškom za IPv6 (kojeg je moguće implementirati unutar protokolnog stoga IPv6-temeljene BSM iznad adaptacijskog sloja) jest RPL protokol. Kroz nekoliko sljedećih potpoglavlja analiziraju se IEEE 802.15.4 sloj, 6LoWPAN adaptacijski sloj i RPL usmjerivački protokol, budući da su to sastavni dijelovi protokolnog stoga bežične senzorske mreže temeljene na IPv6 protokolu i njihova pravilna implementacija nužan je preduvjet za realizaciju IPv6-temeljene BSM.

3.5.1. IEEE 802.15.4 (ZigBee) sloj

Senzorski čvorovi unutar bežične senzorske mreže međusobno i sa baznom stanicom komuniciraju bežičnim putem. Za realizaciju bežične komunikacije moguće je primijeniti više različitih trenutno postojećih standarda, a neprestano se radi i na razvoju novih rješenja. Budući da radio primopredajnik unutar senzorskog čvora predstavlja njegovu energetski najzahtjevniju komponentu, u praksi se nastoji primjenjivati komunikacijska rješenja koja su energetski najučinkovitija. Pri tome je potrebno pronaći kompromis između energetskih zahtjeva i potrebnih performansi u pogledu potrebnog dometa i brzine komunikacije.

Kao komunikacijski standard u BSM se danas najčešće primjenjuje IEEE 802.15.4 (ZigBee) koji se pojavio 2004. godine. Standardom su definirani fizikalni sloj (PHY) i sloj pristupa mediju (MAC, *Media Access Control*). Standard IEEE 802.15.4 definira DSSS *(Direct Sequence Spread Spectrum)* radio komunikaciju u nelicenciranom području od 2.4 GHz i brzine do 250 kbit/s. Postoje i alternative u pojasevima od 868 MHz i 900 MHz, uz nešto manju brzinu (20 kbit/s i 40 kbit/s). Definiranje IEEE 802.15.4 standarda stvorilo je standardiziranu osnovu u vidu fizikalnog i MAC sloja koja omogućava daljnju nadogradnju kroz mrežni i aplikacijski sloj [20, 124].

ZigBee standard izgrađen je „iznad“ 802.15.4 fizikalnog i MAC sloja i uključuje kompletan mrežni stog za bežičnu senzorsku mrežu. Protokolni stog ZigBee standarda prikazuje slika 3.6.



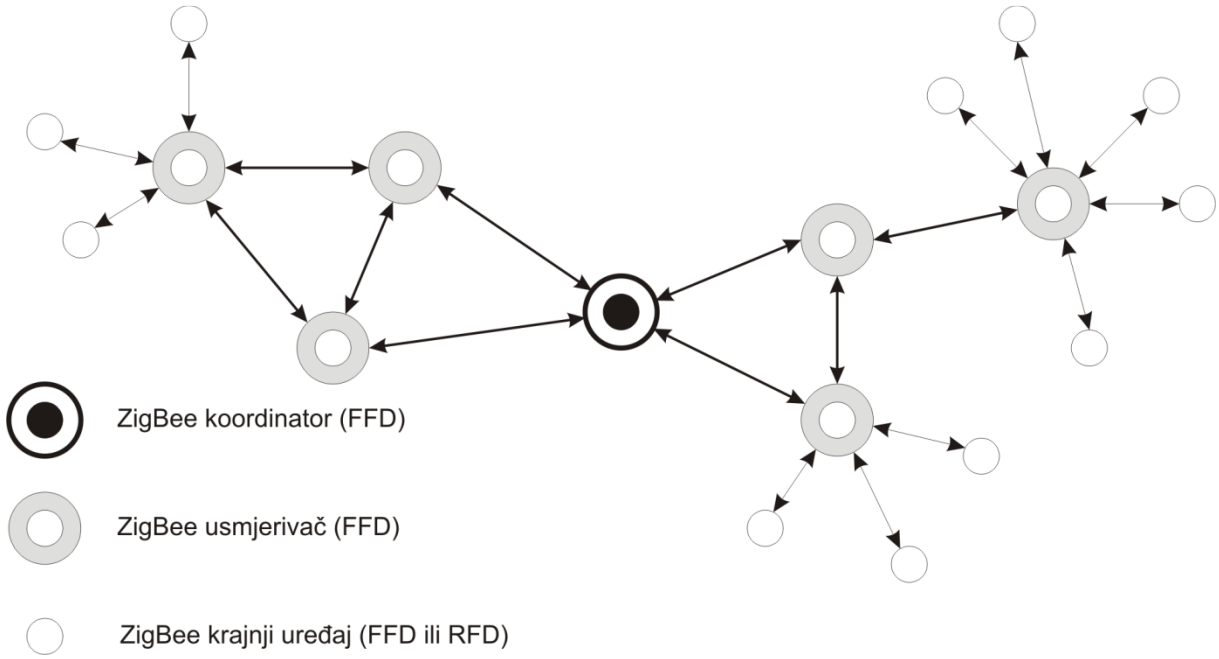
Slika 3.6 ZigBee protokolni stog

Osnovne funkcionalnosti koje rješava ZigBee standard su adresiranje, mrežno usmjeravanje, sigurnost i upravljanje uređajima. ZigBee standard podržale su mnoge tvrtke, tako da danas na tržištu postoji čitav niz SoC *(system-on-chip)* i SiP *(system-in-package)* uređaja raznih proizvođača kompatibilnih sa ZigBee standardom. 2007. godine standard je nadograđen, proširen i poboljšan (ZigBee Pro).

Za adresiranje ZigBee standard koristi stablastu strukturu. Čvor koordinator adresira čvorove duž stabla i uspostavlja rute. Kod ovakvog pristupa postoje ograničenja u pogledu „dubine“ stabla i broja mogućih grana, što se pokazuje problematičnim u mrežama sa velikim brojem čvorova (može doći do nedostatka adresa). Zbog toga ZigBee Pro uvodi puno skalabilniju shemu adresiranja temeljenu na „slučajnom“ *(random)* dodjeljivanju adresa. Za adresiranje se koristi 16-bitni adresni prostor, a čvor koji se priključuje mreži bira adresu putem slučajnog izbora iz dostupnog adresnog prostora. Budući da i najveće mreže rijetko prelaze brojku od nekoliko tisuća čvorova do adresnog konflikta dolazi vrlo rijetko. Međutim, u mrežni stog ipak je implementiran i mehanizam za razrješavanje adresnog konflikta *(address conflict resolution mechanism)*. ZigBee Pro također omogućava uporabu dva usmjerivačka protokola u istoj mreži, kako bi se postupak usmjeravanja mogao što bolje

optimizirati i time smanjiti zahtjeve za memorijom čvorova i propusnošću linkova (smanjenjem količine kontrolnog prometa).

Kako bi se maksimalno smanjili troškovi proizvodnje i implementacije ZigBee tehnologije postoje dva tipa ZigBee uređaja: potpuno funkcionalni uređaji *(FFD, Full Function Device)* i uređaji sa smanjenom funkcionalnosti *(RFD, Reduced Function Device)*. FFD ZigBee uređaj može funkcionirati u bilo kojoj topologiji, može obavljati funkciju mrežnog koordinatora i usmjerivača i u stanju je komunicirati s bilo kojim drugim ZigBee uređajem. RFD ZigBee uređaj je vrlo jednostavne implementacije, ograničen je na topologiju zvijezde, ne može obavljati funkciju mrežnog koordinatora i može komunicirati isključivo sa mrežnim koordinatorom. Slika 3.7 prikazuje tipičnu arhitekturu mreže temeljene na ZigBee (IEEE 802.15.4) standardu.



Slika 3.7 Tipična arhitektura IEEE 802.15.4 mreže

Značajna prednost ZigBee tehnologije u odnosu na konkurentne jest značajno manja potrošnja, što otvara široku mogućnost njezine primjene u bežičnim senzorskim mrežama. Smanjena potrošnja omogućava veću autonomiju senzorskih čvorova i produžava životni vijek senzorske mreže. Životni vijek senzorskog čvora jako ovisi o konkretnoj primjeni, no u nekim BSM temeljenim na ZigBee tehnologiji čvor napajan standardnom AAA baterijom može funkcionirati čak i dulje od dvije godine.

Kako se ZigBee standard širi i postaje opće prihvaćen, tako se na tržištu pojavljuje sve više alata i komponenata koji su potrebni za dizajn, razvoj, proizvodnju i implementaciju bežičnih senzorskih mreža koje kao komunikacijski standard koriste ZigBee. Sada su na tržištu dostupna potpuno integrirana *system-on-chip* rješenja koja uključuju 802.15.4 RF sučelje, mikroprocesor, *flash* memoriju, RAM te ulazno/izlaznu jedinicu. Pojava ovakvih rješenja na tržištu omogućava projektiranje i implementaciju jeftinijih BSM, što značajno doprinosi njihovom daljnjem širenju. Zahvaljujući tome BSM se sve više sele iz područja istraživanja u područje komercijalnih aplikacija.

3.5.2. 6LoWPAN adaptacijski sloj

6LoWPAN standard *(IPv6 over Low power Wireless Personal Area Network)* uvodi odgovarajući adaptacijski sloj koji omogućava učinkovitu IPv6 komunikaciju preko IEEE 802.15.4 bežičnih linkova kakvi se koriste u bežičnim senzorskim mrežama. Ovaj adaptacijski sloj implementira kompresiju IPv6 zaglavlja i na taj način znatno smanjuje količinu kontrolnog prometa koji putuje mrežom *(overhead)* [16, 45, 101].

Radna skupina 6LoWPAN *(IPv6 over Low power Wireless Personal Area Network)* unutar IETF-a ulaže značajne istraživačke napore u smjeru adekvatnog rješavanja problema prijenosa IPv6 prometa putem IEEE 802.15.4 bežičnih linkova, kakvi su najzastupljeniji u bežičnim senzorskim mrežama. Kao rezultat rada ove skupine do sada su nastala dva RFC dokumenta (dok je još nekolicina u statusu aktivnog nacrta):

- RFC 4919 [85]: *„IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs): Overview, Assumptions, Problem Statement, and Goals“*
- RFC 4944 [86]: *„Transmission of IPv6 Packets over IEEE 802.15.4 Networks“*

Pod LoWPAN mrežama *(Low-power Wireless Personal Area Networks)* obično se podrazumijevaju mreže koje se sastoje od uređaja koji podržavaju IEEE 802.15.4 standard (najčešće se radi o bežičnim senzorskim čvorovima). Karakterizira ih komunikacija kratkog dometa, mala propusnost i stroga ograničenost uređaja u pogledu računalnih resursa i napajanja. Neke glavne karakteristike IEEE 802.15.4 kompatibilnih LoWPAN mreža (koje imaju izravan utjecaj na problematiku implementacije IP protokola u takve mreže) jesu:

- **Mali podatkovni paketi:** maksimalna veličina paketa na fizikalnom sloju iznosi 127 okteta, što rezultira maksimalnom veličinom okvira na MAC sloju od samo 102 okteta. Ukoliko se na sloju podatkovnog linka primjenjuje neka od metoda enkripcije, to dodatno može smanjiti maksimalan broj okteta za prijenos podataka na samo 81 oktet.
- **Podrška za kratke 16-bitne i proširene IEEE 64-bitne MAC adrese**
- **Mala širina pojasa:** moguće su brzine prijenosa od 250 kb/s, 40 kb/s, 20 kb/s za svaki od trenutno definiranih fizikalnih slojeva na 2.4 GHz, 915 MHz i 868 MHz
- **Zvjezdasta *(star)* i potpuno isprepletena *(mesh)* topologija**
- **Mali kapacitet napajanja:** uglavnom svi uređaji rade na baterije ograničenog kapaciteta
- **Niska cijena**
- **Velik broj uređaja**
- **Neodređene lokacije uređaja:** u većini slučajeva uređaji se postavljaju na ad hoc način, tako da njihova točna pozicija nije unaprijed određena
- **Nepouzdanost uređaja:** uređaji su nepouzdani iz čitavog niza razloga: nepouzdana radio veza, pražnjenje baterije, fizičko uništenje ili otuđenje uređaja...
- **Mod „spavanja“ *(sleep mode)*:** radi uštede energije uređaji se većinu vremena nalaze u neaktivnom modu, kada nisu u mogućnosti komunicirati s drugim uređajima

Međutim, unatoč brojnim problemima koje je potrebno riješiti prilikom implementacije IP (IPv6) protokola u LoWPAN mreže, njegova implementacija zasigurno donosi brojne dobitke, između ostalog sljedeće:

- Mogućnost uporabe vrlo raširene i sveprisutne postojeće IP infrastrukture
- Mogućnost uporabe postojećih, dobro poznatih i provjerenih tehnologija temeljenih na IP protokolu (čija specifikacija je u potpunosti otvorena i slobodno dostupna)
- Mogućnost uporabe postojećih alata za dijagnostiku i upravljanje IP mrežama
- Mogućnost izravnog povezivanja sa ostalim mrežama temeljenim na IP protokolu, bez potrebe za *gateway*-ima i *proxy*-jima

Kada je riječ o implementaciji IP protokola u LoWPAN mreže, kao vrlo pogodnom pokazuje se upravo njegova verzija 6 (IPv6) koja bi i u klasičnim IP mrežama u dogledno vrijeme trebala zamijeniti verziju 4 (IPv4). Budući da u LoWPAN mrežama može biti jako veliki broj uređaja nužna je implementacija samostalnih autokonfiguracijskih mehanizama, a

upravo takvi mehanizmi dolaze sa IPv6 protokolom. Također, veliki broj uređaja zahtijeva velik adresni prostor, što je također karakteristika IPv6 protokola. Implementacijom IPv6 protokola LoWPAN mreža postaje izravno poveziva sa ostalim IP mrežama i Internetom.

Budući da LoWPAN mreže zbog svoje raznolikosti moraju podržavati različite topologije, uključujući zvjezdastu *(star)* i potpuno isprepletenu *(mesh)*, nužno je implementirati i odgovarajući usmjerivački protokol, koji će podržavati IPv6 protokol i usmjeravanje kroz više skokova *(multi-hop)*. Pri tome je nužno voditi računa da implementirani usmjerivački protokol unosi što manje kontrolnog prometa (tj. da ima što manji *overhead*) i da bude energetski učinkovit. Potrebno je voditi računa i o veličini IEEE 802.15.4 okvira, te nastojati kad god je to moguće „uklopiti“ podatkovni paket unutar granica okvira kako bi se izbjegla potreba za fragmentacijom. Također, nužno je obratiti pozornost i na sigurnosne aspekte ovakvih mreža. Iako IEEE 802.15.4 standard omogućava uporabu enkripcije na sloju podatkovne veze (AES, *Advanced Encryption Standard*), potrebno je implementirati odgovarajuće sigurnosne mehanizme i na višim slojevima. Prema tome, adaptacijski sloj između IEEE 802.15.4 i IPv6 sloja mora učinkovito riješiti sljedeće probleme:

- **Fragmentacija i ponovno sastavljanje paketa:** zbog premalog IEEE 802.15.4 okvira neophodno je implementirati mehanizam fragmentacije i ponovnog slaganja paketa
- **Kompresija zaglavlja:** budući da je IPv6 zaglavlje veliko 40 okteta (bez opcijskih zaglavlja), kada bi se implementiralo u izvornom obliku za protokole viših slojeva preostao bi svega 41 oktet. Zbog toga je potrebno implementirati tehnike za kompresiju zaglavlja, kako bi se uštedjelo na prostoru i time smanjile potrebe za fragmentacijom paketa.
- **Autokonfiguracija adresa:** adaptacijski sloj treba implementirati mehanizam generiranja jedinstvenih identifikatora sučelja na temelju EUI-64 adrese dodijeljene IEEE 802.15.4 uređajima. Samostalni autokonfiguracijski mehanizam smanjuje potrebu za komunikacijom u mreži, te time značajno smanjuje količinu kontrolnog prometa i ostvaruje uštedu resursa (prije svega energetskih).
- **Usmjeravanje:** nužno je implementirati usmjerivački protokol s podrškom za IPv6 i *multi-hop* komunikaciju
- **Upravljanje mrežom:** potrebno je prilagoditi postojeće upravljačke i kontrolne protokole (npr. SNMP, *Simple Network Management Protocol*) kako bili primjenjivi u LoWPAN mrežama, ili definirati novi protokol posebno dizajniran za takve mreže

- **Sigurnost:** potrebno je pozorno analizirati sigurnosne prijetnje i propuste koji postoje na različitim slojevima, te implementirati odgovarajuće sigurnosne mehanizme (koji se također moraju prilagoditi specifičnostima LoWPAN mreža)

Napori da se udovolji nekim od navedenih zahtjeva koje treba ispuniti prilikom implementacije IPv6 protokola u LoWPAN mreže rezultirali su definicijom tzv. 6LoWPAN *(IPv6 over Low power Wireless Personal Area Network)* adaptacijskog sloja koji omogućava učinkovitu IPv6 komunikaciju preko IEEE 802.15.4 bežičnih linkova.

6LoWPAN adaptacijski sloj definiran je u dokumentu RFC 4944 *(Transmission of IPv6 Packets over IEEE 802.15.4 Networks)*, a u tijeku je postupak standardizacije i vrlo je izgledno da će (uz eventualne manje modifikacije) biti prihvaćen kao IEEE standard. Dokument definira format okvira za prijenos IPv6 paketa u IEEE 802.15.4 mrežama, metode formiranja adresa lokalnih veza *(link-local addresses)* i metode samostalnog podešavanja adresa u IEEE 802.15.4 mrežama. Dodatne specifikacije uključuju metode kompresije zaglavlja IPv6 protokola radi lakšeg prijenosa putem IEEE 802.15.4 linkova i uštede u resursima.

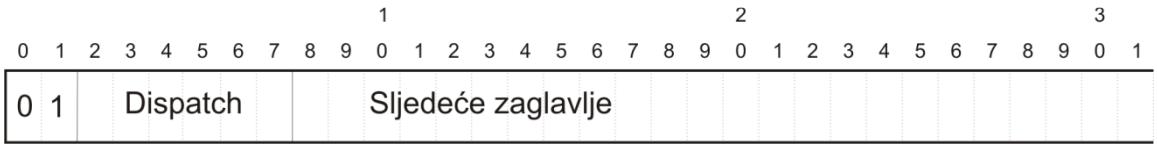
IEEE 802.15.4 standard definira 4 vrste okvira: *beacon* okviri *(beacon frames)*, MAC komandni okviri *(MAC command frames)*, okviri za potvrdu *(acknowledgement frames)* i podatkovni okviri *(data frames)*. IPv6 paketi mogu se prenositi isključivo unutar podatkovnih okvira. Opcionalno, podatkovni paketi mogu zahtijevati potvrdu prijema (što je preporučljivo radi lakšeg oporavka nakon eventualnog gubitka paketa). IEEE 802.15.4 definira nekoliko modova adresiranja: omogućava uporabu proširenih IEEE 64-bitnih adresa ili skraćenih 16-bitnih adresa jedinstvenih unutar PAN-a.

IPv6 protokol povećava adresni prostor na 128 bita te povećava minimalnu MTU vrijednost *(Maximum Transmission Unit)* sa 576 (kod IPv4) na 1280 okteta. Fragmentacija paketa moguća je samo na izvorišnom čvoru, dok više nije dozvoljena na čvorovima između izvora i odredišta. Jasno je da je puni IPv6 paket prevelik za IEEE 802.15.4 okvir (koji je na fizikalnom sloju veličine 127 okteta). Uz maksimalni kontrolni promet *(overhead)* od 25 okteta dobije se maksimalna veličina okvira (na MAC sloju) od 102 okteta, što se još dodatno smanjuje ukoliko se primjenjuje enkripcija (AES) na sloju podatkovnog linka. AES-CCM-128 enkripcija donosi *overhead* od 21 okteta, što višim slojevima na raspolaganju ostavlja samo 81 oktet (enkripcija AES-CCM-64 ima *overhead* 13 okteta, a AES-CCM-32 9 okteta). Standardno IPv6 zaglavlje duljine je 40 okteta, što bi u najgorem slučaju protokolima gornjih

slojeva (poput npr. UDP protokola) ostavilo samo 41 oktet. UDP protokol uzima dodatnih 8 okteta za svoje zaglavlje, što aplikacijskom sloju ostavlja samo 33 okteta raspoloživa za prijenos podataka. Iz navedenog je jasno da mora biti razrađen postupak fragmentacije. Međutim, budući da sam postupak fragmentacije dodatno troši ionako vrlo ograničene resurse, nastoji ga se kad god je to moguće izbjeći. Budući da se u IEEE 802.15.4 mrežama u velikoj većini slučajeva prenosi relativno mala količina podataka, 6LoWPAN adaptacijski sloj veliku pozornost posvećuje mogućnostima kompresije zaglavlja, kako bi se u konačnici dobili paketi koji se mogu uklopiti unutar IEEE 802.15.4 okvira, i time u većini slučajeva izbjegla potreba za fragmentacijom.

3.5.2.1. Format LoWPAN okvira

Prilikom formiranja LoWPAN okvira i enkapsulacije pojedinih zaglavlja nužno je voditi računa o njihovom redoslijedu. Ukoliko u jednom paketu postoji više LoWPAN zaglavlja, ona se moraju pojaviti sljedećim redoslijedom: *mesh* adresno zaglavlje *(Mesh Addressing Header)*, *broadcast* zaglavlje *(Broadcast Header)*, fragmentacijsko zaglavlje *(Fragmentation Header)*. Na početku se nalazi *dispatch* vrijednost, koja je zapravo 6-bitni selektor koji identificira vrstu zaglavlja koje neposredno slijedi (slika 3.8).



Slika 3.8 Formiranje LoWPAN okvira

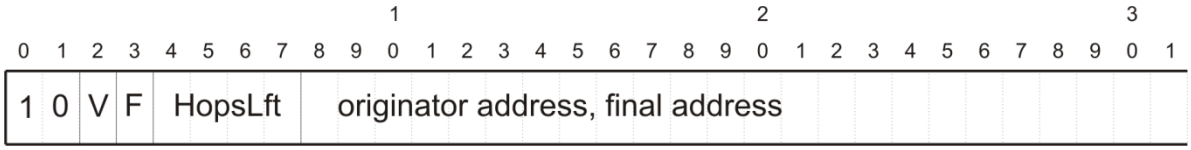
Sve moguće *dispatch* vrijednosti prikazane su na slici 3.9.

Uzorak	Vrsta zaglavlja	Značenje
00 xxxxxx	NALP	Bitovi koji slijede nisu dio LoWPAN enkapsulacije, što znači da svaki LoWPAN čvor koji naiđe na ovu vrijednost odbacuje paket (omogućava koegzistenciju drugih protokola sa LoWPAN čvorovima)
01 000001	IPv6	Slijedi nekomprimirano IPv6 zaglavlje
01 000010	LOWPAN_HC1	Slijedi komprimirano IPv6 zaglavlje
01 010000	LOWPAN_BC0	Slijedi zaglavlje za broadcast/multicast podršku
01 111111	ESC	Slijedi dodatno 8-bitno polje za *dispatch* vrijednost (omogućava da bude veća od 127)
10 xxxxxx	MESH	Slijedi *mesh* zaglavlje
11 000xxx	FRAG1	Slijedi prvo fragmentacijsko zaglavlje
11 100xxx	FRAGN	Slijedi fragmentacijsko zaglavlje (n-to)

Slika 3.9 Sve moguće "dispatch" vrijednosti

Svi preostali mogući uzorci (koji nisu prikazani na prethodnoj slici) rezervirani su za buduću uporabu.

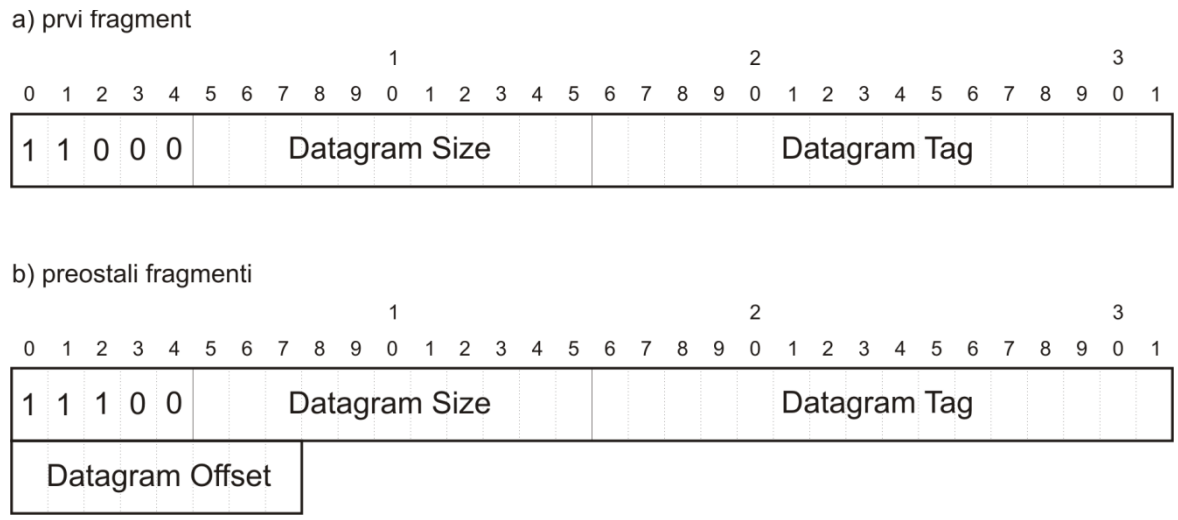
Slika 3.10 prikazuje strukturu *mesh* adresnog zaglavlja.



Slika 3.10 Struktura mesh adresnog zaglavlja

Bitovi V i F omogućavaju kombinaciju 16-bitnog i 64-bitnog (EUI-64) adresiranja. Pri tome bit V odgovara adresi izvora, a bit F odgovara adresi krajnjeg odredišta, pri čemu u oba slučaja vrijednost 0 označava uporabu EUI-64 adrese, a vrijednost 1 indicira da se radi o skraćenom 16-bitnom adresiranju. 4-bitno polje *„Hops Left“* dekrementira se prilikom svakog prosljeđivanja paketa (kada mu je vrijednost nula paket se dalje ne prosljeđuje). Ukoliko se postavi vrijednost 0xF slijedi ga 8-bitno polje *„Deep Hops Left“* koje omogućava izvorišnom čvoru specifikaciju mogućeg broja skokova većeg od 14. Polje *„Originator Address“* sadrži adresu izvorišnog čvora, dok polje *„Final Destination Address“* sadrži adresu krajnjeg odredišta (radi se o adresama na sloju podatkovnog linka).

U slučaju da se IPv6 paket ne može uklopiti unutar jednog IEEE 802.15.4 okvira dolazi do fragmentacije, te u slijedu enkapsuliranih zaglavlja mora postojati i fragmentacijsko zaglavlje. Na slici 3.11 je prikazano zaglavlje prvog fragmenta i zaglavlje sljedećih fragmenata, koje se od prvog razlikuje po tome što uključuje dodatno polje *„Datagram Offset“* (pomak datagrama).

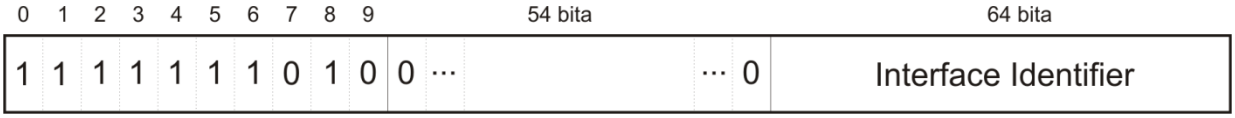


Slika 3.11 Fragmentacija prilikom formiranja LoWPAN okvira

11-bitno polje *„Datagram Size“* (veličina datagrama) definira veličinu cjelokupnog IP paketa (prije fragmentacije na sloju podatkovnog linka, ali nakon fragmentacije na IP sloju). Ovo polje ne mora nužno biti u svakom paketu, nužno je da postoji unutar prvog fragmenta (iako njegovo postojanje u svakom fragmentu olakšava ponovno sastavljanje paketa. Polje *„Datagram Tag“* (oznaka datagrama – 16 bita) predstavlja jedinstvenu oznaku datagrama i mora biti jednako kod svih fragmenata istog paketa. 8-bitno polje *„Datagram Offset“* definira pomak fragmenta (u koracima od po 8 okteta) u odnosu na prvi oktet datagrama. Ove informacije iz fragmentnih zaglavlja omogućavaju odredišnom čvoru da alocira memorijski prostor odgovarajuće veličine u koji će smještati odgovarajuće pristigle fragmente prilikom postupka njihovog slaganja. Pri tome je potrebno definirati vremenski interval unutar kojeg svi fragmenti moraju pristići (maksimalno 60 sekundi). Ukoliko unutar tog intervala ne pristignu svi fragmenti i paket se ne uspije sastaviti bivaju odbačeni i oni fragmenti koji su pristigli na odredište.

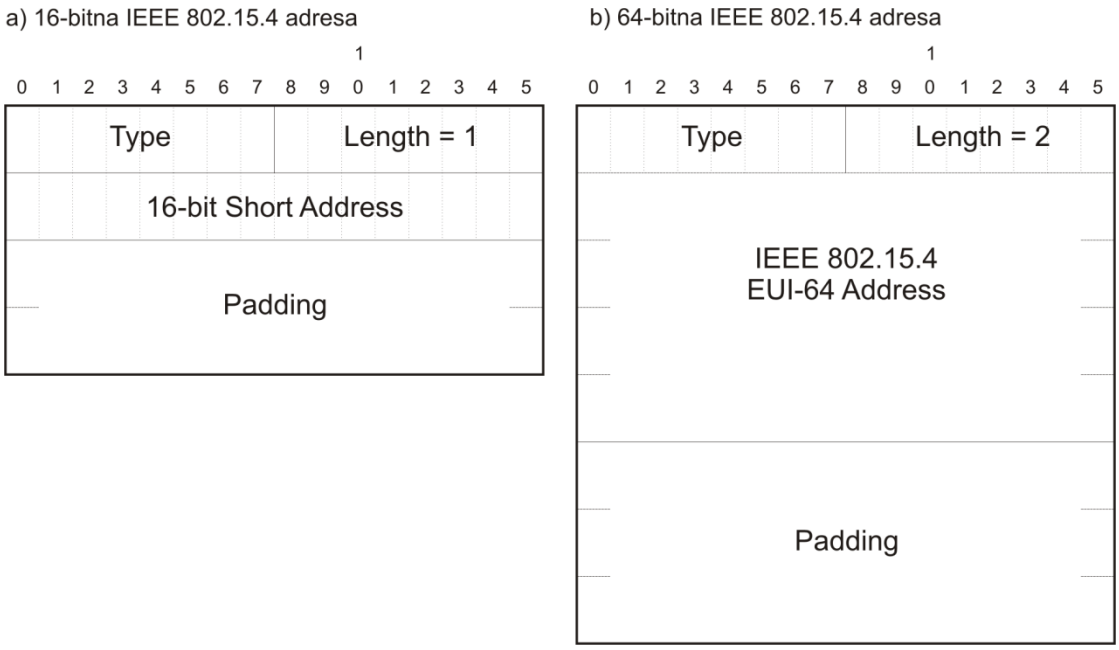
3.5.2.2. Samostalna autokonfiguracija adrese

Identifikator sučelja *(Interface Identifier)* za IEEE 802.15.4 sučelje može se temeljiti na EUI-64 identifikatoru koji je dodijeljen IEEE 802.15.4 uređaju [125]. U tom se slučaju identifikator sučelja formira iz EUI-64 adrese sukladno specifikaciji RFC 2464 *(„Transmission of IPv6 Packets over Ethernet Networks“)* [77]. Osim IEEE EUI-64 adrese IEEE 802.15.4 uređaj može imati i kratku 16-bitnu adresu. U tom slučaju se najprije formira „pseudo-adresa“ od 48 bita, tako što se najprije na 16-bitnu oznaku PAN-a (PAN ID) dodaje još 16 bitova postavljenih u nulu. Na tako dobivena 32 bita dodaje se 16-bitna kratka adresa, što daje 48-bitnu pseudo-adresu, od koje se formira identifikator sučelja sukladno specifikaciji RFC 2464. IPv6 adresni prefiks koji se koristi u postupku samostalne autokonfiguracije adrese *(stateless address autoconfiguration)* mora biti duljine 64 bita (sukladno sa RFC 4862 [84]) *(„IPv6 Stateless Address Autoconfiguration“)*. Adresa lokalne veze *(Link-local Address)* (RFC 4291) [82] formira se tako što se ispred ovako dobivenog identifikatora sučelja postavi prefiks FE80::/64 (slika 3.12).



Slika 3.12 Formiranje adrese lokalne veze

Postupak razlučivanja adrese *(address resolution)* i mapiranja jednoznačnih (jednoodredišnih) IPv6 adresa *(unicast address)* odvija se sukladno proceduri definiranoj u RFC 4861 [83]. Prema tome, adrese na sloju linka podataka imaju oblik prikazan na slici 3.13 (ovisno o tome koriste li se 64-bitne ili 16-bitne IEEE 802.15.4 adrese).



Slika 3.13 Adrese na sloju linka podataka

Pri tome polje *„Type“* ima vrijednost 1 za adresu izvora, a 2 za adresu odredišta, dok polje *„Length“* ima vrijednost 1 za kratke 16-bitne adrese, a vrijednost 2 za EUI-64 adrese.

3.5.2.3. Kompresija zaglavlja

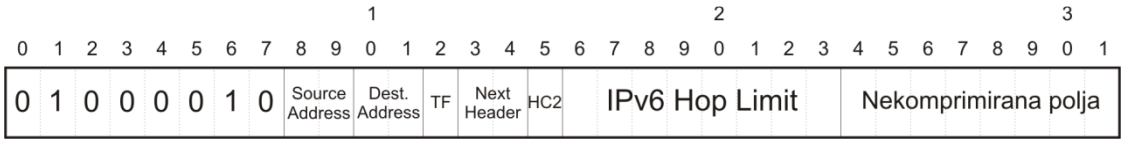
RFC 4944 *(„Transmission of IPv6 Packets over IEEE 802.15.4 Networks“)* definira HC1 (za IPv6 zaglavlje) i HC2 (za UDP zaglavlje) formate kompresije zaglavlja, no otvorena je mogućnost definiranja i novih formata kompresije. Pri tome je bitno da svaki novi format kompresije mora zadovoljavati ranije prikazani osnovni format paketa (i koristiti različite *dispatch* vrijednosti).

Različite metode kompresije zaglavlja poznate su i primjenjivane i u klasičnim mrežama, gdje su one uglavnom usmjerene na podatkovne tokove iz kojih uklanjaju redundantne informacije (npr. nije potrebno u svakom paketu prenositi neke dijelove zaglavlja ako se radi o kontinuiranom toku paketa između istog izvora i odredišta). U slučaju 6LoWPAN mreža metode kompresije zaglavlja orijentirane su na načelu da se iz zaglavlja mogu ukloniti one informacije koje su zajedničke cijeloj mreži. Također, podrazumijeva se pristup kroz više slojeva, pa se tako iz zaglavlja jednog sloja mogu ukloniti informacije koje je moguće iščitati

iz zaglavlja nekog drugog sloja. Takvim pristupom je zapravo moguće polja zaglavlja iz adaptacijskog, mrežnog i transportnog sloja sažeti i kombinirati u svega nekoliko okteta.

Unutar 128-bitne IPv6 adrese prva 64 bita definiraju mrežni prefiks, dok naredna 64 bita identificiraju mrežno sučelje *(IID, Interface Identifier)*. 6LoWPAN standard mrežni prefiks zamjenjuje jednim bitom (podrazumijeva se zajednički mrežni prefiks za cijelu 6LoWPAN mrežu), a IID se može izostaviti ukoliko se adresa odredišta može izvesti iz odgovarajuće adrese iz IEEE 802.15.4 zaglavlja sa sloja linka podataka. Polje *„Next Header“* komprimira se na dva bita, budući da postoje samo tri mogućnosti – UDP, TCP ili ICMPv6. Nadalje, polja *„Traffic Class“* i *„FlowLabel“* zamjenjuju se sa po jednim bitom (koji se postavlja u nulu). Polje *„Payload Length“* se u potpunosti izostavlja, budući da se odgovarajući podatak može izvući iz IEEE 802.15.4 zaglavlja (polje *„Frame Length“* unutar IEEE 802.15.4 PPDU) ili iz fragmentacijskog zaglavlja (polje *„Datagram Size“*). Polje *„Version“* se također izostavlja. Jedino polje u IPv6 zaglavlju koje se uvijek prenosi u cijelosti je 8-bitno polje *„Hop Limit“*. Ovisno o trenutnom kontekstu okruženja, neka polja iz IPv6 zaglavlja se mogu komprimirati, dok se neka moraju prenijeti nekomprimirana *(„in-line“)*. U najboljem slučaju cijelo IPv6 zaglavlje moguće je sažeti na dva okteta (što uz dodatni oktet sa odgovarajućom *dispatch* vrijednosti raste na svega 3 okteta).

U slučaju da se na IPv6 paket može primijeniti HC1 kompresija zaglavlja, najprije je potrebno postaviti odgovarajuću *dispatch* vrijednost „LOWPAN_HC1“ (8 bita, 01000010), iza koje slijedi 8-bitno polje *„HC1 encoding“*, pa potom nekomprimirana polja (slika 3.14).



Slika 3.14 HC1 kompresija zaglavlja

Adresni bitovi unutar *„HC1 encoding“* okteta označavaju jesu li mrežni prefiks i identifikator sučelja komprimirani ili nisu. Skraćeno:

PN – prefiks nekomprimiran (prenosi se u cijelosti)

PK – prefiks komprimiran (podrazumijeva se link-lokalni prefiks)

IN – identifikator sučelja nekomprimiran (prenosi se u cijelosti)

IK – identifikator sučelja komprimiran (izostavljen – moguće ga je izvesti iz adrese sloja podatkovnog linka)

Četiri moguće kombinacije od po dva bita *„Source Address“* (prvi i drugi bit) i *„Destination Address“* (treći i četvrti bit) označavaju sljedeće:

00 – PN, IN

01 – PN, IK

10 – PK, IN

11 – PK, IK

Bit TF (5. bit) ukazuje na kompresiju polja *„Traffic Class“* (8 bita) i *„Flow Label“* (20 bita). Ukoliko je postavljen u nulu ova polja se šalju nekomprimirana, a ukoliko je 1 ova polja se sažimaju na jedan bit (postavljen na 0). Bitovi *„Next Header“* (6. i 7. bit) ukazuju na sljedeće zaglavlje, pri čemu kombinacija 00 označava da nema kompresije i da slijedi svih 8 bita, kombinacija 01 ukazuje na UDP zaglavlje, 10 na ICMP zaglavlje a 11 na TCP zaglavlje. Bit HC2 (8. bit) ukoliko je postavljen u 1 ukazuje na to da slijedi HC2 kompresijsko zaglavlje (ukoliko je u nuli slijede nekomprimirana zaglavlja).

HC2 kompresija zaglavlja odnosi se na kompresiju UDP, TCP i ICMP zaglavlja (na što ukazuju *„Next Header“* bitovi u HC1 zaglavlju, pri čemu i bit HC2 mora biti postavljen u 1). RFC 4944 za sada definira samo kompresiju UDP zaglavlja. U tom slučaju iza zaglavlja HC1 neposredno slijedi zaglavlje HC2 (slika 3.15).

Slika 3.15 HC2 kompresija zaglavlja

Primjenom HC2 kompresije unutar UDP zaglavlja moguće je komprimirati sljedeća polja: izvorišni port *(source port)*, odredišni port *(destination port)* i duljina *(length)*, dok se kontrolna suma *(checksum)* prenosi u cijelosti. Ovakav pristup omogućava da se UDP zaglavlje sa početnih 8 sažme na samo 4 okteta. Jedino polje unutar UDP zaglavlja čija se

vrijednost može izvesti iz informacija koje su dostupne na drugom mjestu (u drugim zaglavljima) jest polje *„Length“*. Ostala polja se moraju prenositi, bilo u izvornom ili komprimiranom obliku.

6LoWPAN standard uvodi podrazumijevani raspon UDP portova, od 61616 (0xF0B0) do 61631 (0xF0BF), pa se gornjih 12 bitova iz broja porta mogu izostaviti. Ukoliko su i izvorišni i odredišni port iz ovog raspona, zajedno se mogu komprimirati na jedan oktet. Prema tome, u najboljem slučaju (kada se koristi lokalna *unicast* komunikacija) primjenom HC1 i HC2 kompresije UDP i IPv6 zaglavlje se zajedno daju komprimirati na veličinu od 7 okteta.

Bit *„UDP Source Port“* iz HC2 zaglavlja indicira prenosi li se izvorišni port u cijelosti (16 bita) ili se komprimira. Ukoliko je ovaj bit u nuli UDP port se prenosi bez kompresije, a ukoliko je u jedinici iza HC2 zaglavlja slijedi skraćena vrijednost porta (4 bita). Stvarni 16-bitni port dobije se zbrajanjem ove skraćene vrijednosti sa 61616 (0xF0B0).

Bit *„UDP Destination Port“* iz HC2 zaglavlja ukazuje prenosi li se odredišni port u cijelosti (vrijednost 0) ili se prenosi skraćena 4-bitna vrijednost porta (vrijednost 1). Slično izvorišnom portu, prava vrijednost porta (16-bitna) dobije se zbrajanjem ove skraćene vrijednosti sa 61616 (0xF0B0).

Bit *„Length“* označava prenosi li se odgovarajuće polje *„Length“* iz UDP zaglavlja u cijelosti (vrijednost 0) ili se komprimira (vrijednost 1). Ukoliko se ovo polje ne prenosi, njegova vrijednost može se dobiti tako da se od vrijednosti polja *„Payload Length“* iz IPv6 zaglavlja oduzmu duljine svih ekstenzijskih zaglavlja koja se nalaze između IPv6 zaglavlja i UDP zaglavlja.

Prethodno analizirani LOWPAN_HC1 i LOWPAN_HC2 načini kompresije zaglavlja najučinkovitiji su za *unicast* komunikaciju na lokalnom linku *(link-local)*, gdje IPv6 adresa sadrži prefiks lokalnog linka i identifikator sučelja *(IID, Interface Identifier)* izravno izveden iz IEEE 802.15.4 adrese. Međutim, iako se adrese lokalne veze *(link-local addresses)* najčešće koriste za lokalnu interakciju među protokolima poput IPv6 ND, DHCPv6 ili usmjerivačkim protokolima, one se obično ne koriste za podatkovni prijenos na aplikacijskom sloju. Ova činjenica zapravo ograničava primjenjivost ovih mehanizama kompresije.

Ukoliko uređaji unutar 6LoWPAN mreže moraju izravno komunicirati sa uređajima izvan mreže moraju se koristiti rutabilne IPv6 adrese. Rutabilne adrese moraju se koristiti i u konfiguracijama 6LoWPAN mreža u kojima se javlja IP usmjeravanje (*route-over*

konfiguracija). U slučaju rutabilne adrese, HC1 model zahtijeva prijenos mrežnog prefiksa (64 bita) u cijelosti (bez kompresije), kako za izvorišnu tako i za odredišnu adresu. U slučaju da se ne koriste *mesh* adresna zaglavlja mora se u cijelosti prenositi i IID rutabilnih adresa (64 bita), i nije ga moguće skratiti čak i ako je izveden iz kratkih 16-bitnih IEEE 802.15.4 adresa. Također, ukoliko je odredište grupna IPv6 adresa *(multicast),* HC1 model zahtijeva prijenos 128-bitne adrese u cijelosti.

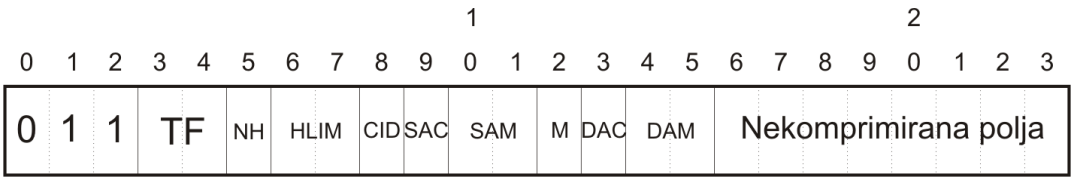
Kako bi se ostvarila bolja kompresija zaglavlja (u većini realnih scenarija) predložen je poboljšani format kompresije zaglavlja, tzv. LOWPAN_IPHC kompresija (ovaj format još nije standardiziran, a specifikacija mu je u statusu nacrta – *draft*) [23]. Uvodi se pojam konteksta *(context)* kao dijeljenog (zajedničkog) stanja za sve čvorove unutar mreže, pri čemu svaki kontekst ima svoj odgovarajući prefiks. Kontekst se označava sa 4 bita, što znači da može postojati do 16 različitih konteksta.

Primjena IPHC kompresije zaglavlja podrazumijeva da sljedeći parametri vrijede za 6LoWPAN komunikaciju u cijeloj mreži:

- Verzija protokola (polje *„Version“*) je 6
- Polja *„Traffic Class“* i *„Flow Label“* su postavljena na nulu
- *„Payload Length“* izvodi se iz zaglavlja nižih slojeva (6LoWPAN fragmentacijsko zaglavlje ili IEEE 802.15.4 zaglavlje)
- Polje *„Hop Limit“* postavlja se na vrijednost poznatu izvorištu
- Adrese dodijeljene IPv6 sučeljima formiraju se pomoću link-lokalnih prefiksa ili malog skupa rutabilnih prefiksa dodijeljenih cjelokupnoj 6LoWPAN mreži
- IID dio unutar adrese formira se izvođenjem iz 16-bitnog ili 64-bitnog oblika IEEE 802.15.4 adrese

IPHC zaglavlje koristi 13 bitova, od kojih je 5 iz *„dispatch type“* zaglavlja, a može se proširiti i na dodatni oktet radi podrške za dodatne kontekste. IPHC zaglavlje slijede nekomprimirana polja iz IPv6 zaglavlja. U najboljem slučaju IPv6 zaglavlje može se svesti na 2 okteta (slučaj lokalne komunikacije na linku): *dispatch* zaglavlje i IPHC zaglavlje. U slučaju IP usmjeravanja i komunikacije kroz više skokova, IPHC može komprimirati IPv6 zaglavlje na 7 okteta: 1 oktet *dispatch* vrijednost, 1 oktet IPHC zaglavlje, 1 oktet polje *„Hop Limit“*, 2 okteta adresa izvora i 2 okteta adresa odredišta.

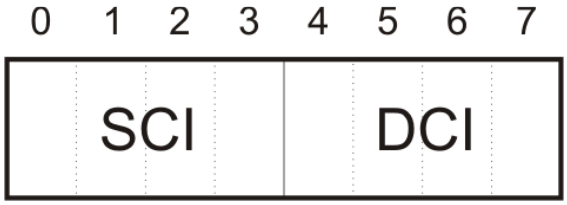
IPHC zaglavlje, koje zapravo definira na koji način je komprimirano IPv6 zaglavlje, može zauzimati 2 okteta (osnovno enkodiranje) ili 3 okteta (prošireno enkodiranje, u slučaju potrebe za enkodiranjem dodatnog konteksta). Slika 3.16 prikazuje osnovni format IPHC zaglavlja.



Slika 3.16 Osnovni format IPHC zaglavlja

Detaljno objašnjenje značenja i dozvoljenih vrijednosti za pojedina polja iz IPHC zaglavlja dani su u dokumentu RFC 4944. Postavljanjem odgovarajućih vrijednosti za ova polja moguće je definirati načine kompresije polja *„Traffic Class“* i *„Flow Label“* (polje TF u IPHC zaglavlju), kompresiju polja *„Next Header“* (polje NH), kompresiju polja *„Hop Limit“* (polje HLIM). Način kompresije adresa definira se pomoću polja SAC *(Source Address Compression)*, SAM *(Source Address Mode)*, M *(Multicast Compression)*, DAC *(Destination Address Compression)* i DAM *(Destination Address Mode).*

Informacije o odgovarajućem kontekstu dijele se između mrežnog čvora koji vrši kompresiju zaglavlja i mrežnih čvorova koji zaglavlje trebaju rekonstruirati. Specifikacija dozvoljava uporabu do 16 različitih konteksta. Ukoliko je u IPHC zaglavlju bit CID postavljen u jedinicu *(Context Identifier Extension)* slijedi dodatni oktet koji identificira kontekste za kompresiju izvorišne i odredišne adrese (ne moraju nužno biti isti) (slika 3.17).



Slika 3.17 Identifikatori konteksta za kompresiju adrese

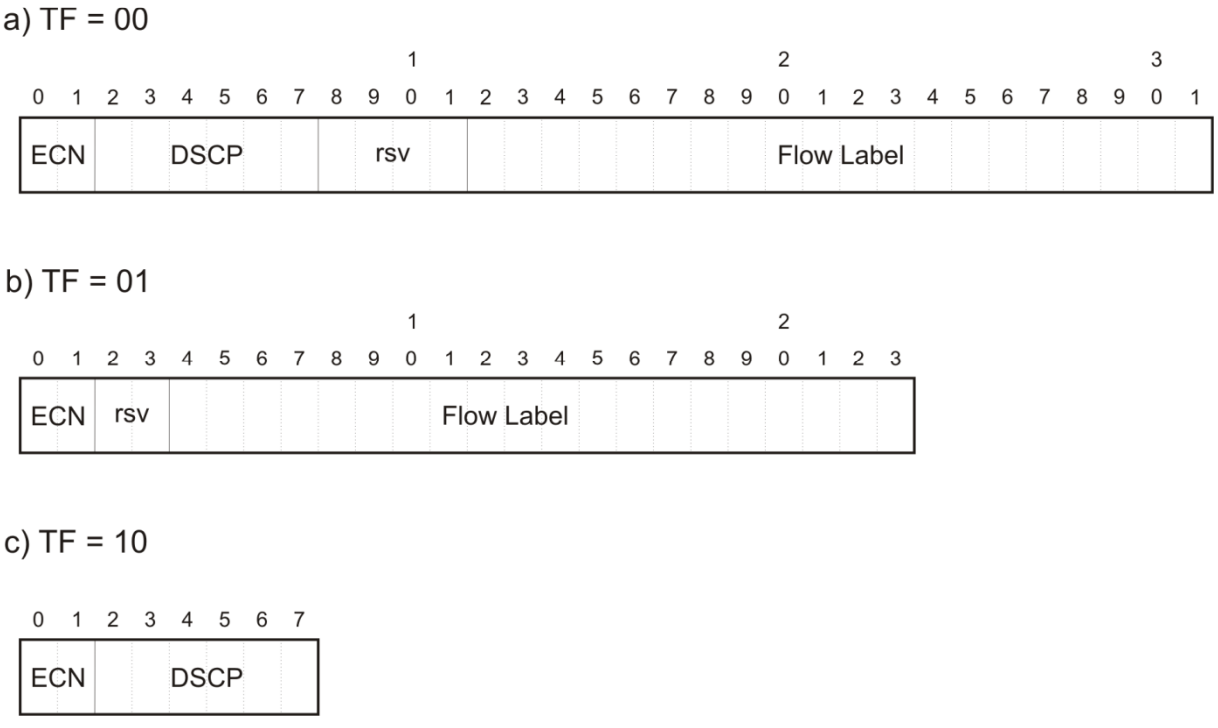
SCI: *Source Context Identifier* – identificira prefiks koji se koristi kada se adresa izvora komprimira ovisno o kontekstu (4 bita)

DCI: *Destination Context Identifier* – identificira prefiks koji se koristi kada se adresa odredišta komprimira ovisno o kontekstu (4 bita)

3.5.2.4. Kompresija polja iz IPv6 zaglavlja

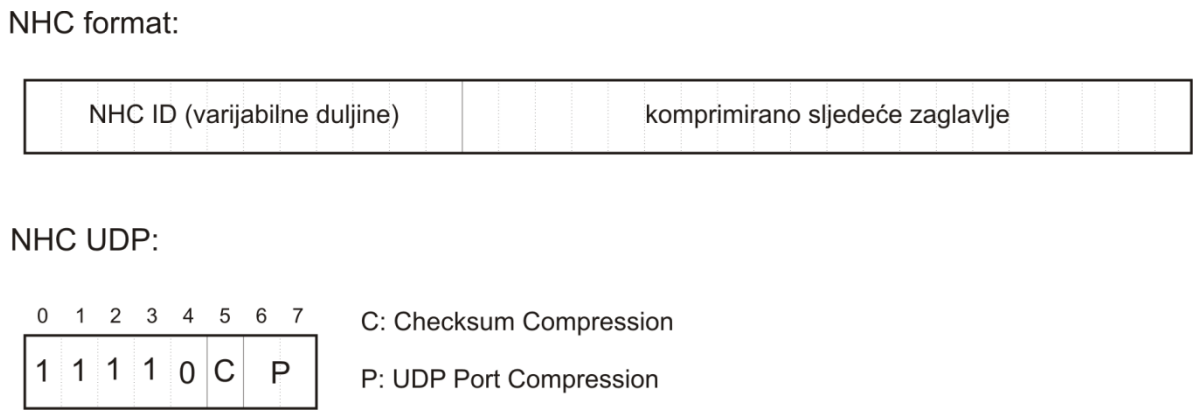
Polja iz IPv6 zaglavlja uvijek se pojavljuju jednakim redoslijedom, sukladno specifikaciji IPv6 protokola (RFC 2460) [76], bez obzira jesu li komprimirana ili se prenose u cijelosti. Polje *„Version“* uvijek se izostavlja, *unicast* adresa komprimira se na 64 ili 16 bita (ili u potpunosti izostavlja), dok se *multicast* adresa komprimira na 8, 32 ili 48 bita. Polje *„Payload Length“* uvijek se izostavlja, dok je za polja *„Traffic Class“* i *„Flow Label“* definiran način kompresije.

Polje TF iz IPHC zaglavlja definira način na koji se komprimiraju ova dva polja. Polje *„Traffic Class“* sastoji se od 6 bita koji predstavljaju *diffserv* ekstenziju (RFC 2474) [78] i 2 bita koja predstavljaju ECN *(Explicit Congestion Notification)* (RFC 3168) [79]. Slika 3.18 prikazuje različite varijante kompresije ovih polja.



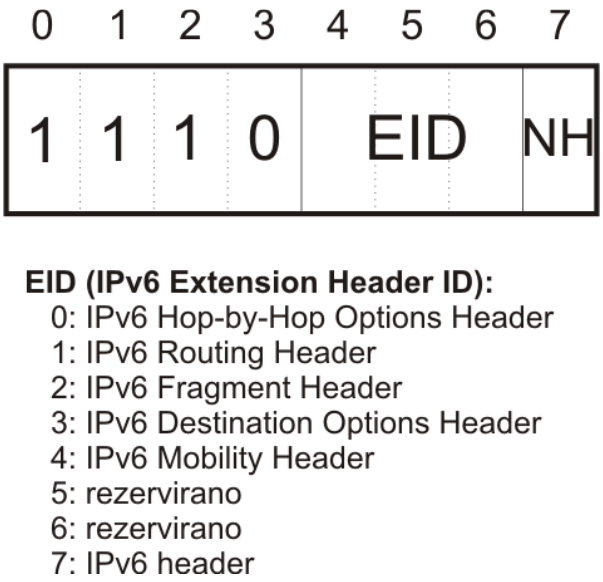
Slika 3.18 Kompresija polja Traffic Class i Flow Label

Format HC također definira i novi okvir za kompresiju proizvoljnih sljedećih zaglavlja – NHC *(Next-header Compression).* Za razliku od HC2 formata (RFC 4944) koji omogućava kompresiju tri tipa sljedećih zaglavlja (TCP, UDP i ICMPv6) (te za sada definira kompresiju UDP zaglavlja), NHC definira novi identifikator *„Next Header“* varijabilne duljine, što omogućava buduću definiciju proizvoljnih načina kodiranja kompresije sljedećih zaglavlja (slika 3.19).



Slika 3.19 Kompresija sljedećih zaglavlja

NHC kodiranje za IPv6 proširena zaglavlja *(IPv6 Extension Headers)* sastoji se od jednog okteta, iza kojeg slijedi IPv6 prošireno zaglavlje (slika 3.20).



Slika 3.20 Kodiranje proširenih zaglavlja

Posljednji bit (NH) postavljen u nulu označava da slijedi nekomprimirano zaglavlje, dok jedinica označava da slijedi zaglavlje komprimirano u formatu LOWPAN_NHC.

Za kompresiju UDP portova koristi se isti raspon podrazumijevanih portova (61616-61631), no u potpunosti se izbacuje *„Payload Length“* polje (budući da se uvijek može izvesti iz IPv6 zaglavlja). Također, NHC omogućava izostavljanje polja *„UDP Checksum“* ukoliko se provjera integriteta poruke radi na nekom od viših slojeva, što je tipičan slučaj kada se koristi neki od sigurnosnih mehanizama transportnog ili aplikacijskog sloja. Ukoliko je bit C (slika 3.19) postavljen u nulu 16-bitna kontrolna suma se prenosi u cijelosti, dok se u slučaju jedinice izostavlja. Dva bita označena sa P ukazuju na način kompresije izvorišnog i odredišnog UDP porta, pri čemu postoje 4 mogućnosti:

00: izvorišni i odredišni port prenose se u cijelosti (16 bita)

01: prenosi se svih 16 bita izvorišnog porta, dok se kod odredišnog porta prvih 8 bita izostavlja (podrazumijeva se vrijednost 0xF0), a narednih 8 prenosi

10: prvih 8 bita izvorišnog porta se izostavljaju (podrazumijeva se vrijednost 0xF0), a narednih 8 se prenose, dok se odredišni port prenosi u cijelosti (16 bita)

11: prvih 12 bita izvorišnog i odredišnog porta se izostavlja (podrazumijeva se vrijednost 0xF0B), dok se preostala 4 bita prenose. Redoslijed polja iz UDP zaglavlja koja se prenose u cijelosti ili komprimirana sukladan je specifikaciji RFC 768 [91].

Prema tome, UDP zaglavlje se u najboljem slučaju može komprimirati na svega dva okteta. Kao i kod RFC 4944, uporabom IPHC i NHC formata za kompresiju zaglavlja najbolja učinkovitost kompresije postiže se u slučaju lokalne *unicast* komunikacije. U najboljem slučaju UDP i IPv6 zaglavlje moguće je komprimirati na ukupno 6 okteta. Prednosti IPHC formata kompresije u odnosu na HC1 dolaze do izražaja u slučajevima *multicast* i globalne komunikacije, kada omogućava znatno bolju kompresiju od HC1 formata.

3.5.3. RPL usmjerivački protokol

Problem usmjeravanja paketa kroz mrežu predstavlja jedan od temeljnih problema koji zahtijeva adekvatno i učinkovito rješenje u svim paketski orijentiranim mrežama, pa tako i u svim mrežama temeljenim na IP protokolu. U proteklih nekoliko desetljeća uporabe klasičnih žičnih mreža temeljenih na IP protokolu (IPv4) razvio se čitav niz usmjerivačkih protokola koji se danas intenzivno koriste. Neki od njih su, primjerice, OSPF *(Open Shortest Path First)* i IS-IS *(Intermediate System To Intermediate System)* (oba spadaju u skupinu IGP protokola, *Interior Gateway Protocols*, koji služe za usmjeravanje unutar autonomnih sustava) ili BGP protokol *(Border Gateway Protocol)*, koji služi za usmjeravanje prometa između autonomnih sustava *(AS, Autonomous System)*.

Svojstva klasičnih žičnih mreža, za koje su ovi protokoli projektirani i razvijani, u velikoj mjeri razlikuju se od svojstava bežičnih senzorskih mreža temeljenih na IP protokolu. Senzorske mreže karakterizira višestruko veći broj čvorova, čvorovi senzorske mreže strogo su ograničeni u pogledu resursa, znatno su nestabilniji (podložni kvarovima i nestanku napajanja), a i linkovi u senzorskim mrežama su također znatno nestabilniji, podložni pogreškama u prijenosu i znatno manje propusnosti. Osim bežičnih senzorskih mreža, ovi protokoli usmjeravanja nisu zadovoljavajući niti za neke druge tipove mreža male snage sa gubicima *(LLN, Low-power Lossy Networks)*. Primjerice, osim bežičnih senzorskih mreža veliku podskupinu LLN mreža čine PLC mreže *(Power Line Communication)*. Zbog toga je unutar IETF *(Internet Engineering Task Force)* formirana radna skupina ROLL *(Routing Over Low power and Lossy networks)*. Inicijalna zadaća ROLL radne skupine bila je detaljno specificirati zahtjeve za protokole usmjeravanja u LLN mrežama te u tom kontekstu evaluirati postojeće usmjerivačke protokole i definirati skup zahtjeva koje mora zadovoljiti protokol usmjeravanja u LLN mreži. Napori ROLL radne skupine rezultirali su nastankom RPL usmjerivačkog protokola [26]. RPL protokol predstavlja prvi usmjerivački protokol sa podrškom za IPv6 namijenjen LLN mrežama, u koje spadaju i IPv6-temeljene bežične senzorske mreže. Pri tome je RPL protokol u najvećoj mjeri uspio udovoljiti početno definiranim zahtjevima koje bi usmjerivački protokol namijenjen ovakvim mrežama trebao ispunjavati. U potpoglavljima koja slijede dana je specifikacija RPL protokola i prikazan način njegove implementacije i funkcioniranja unutar protokolnog stoga IPv6-temeljene BSM [116].

3.5.3.1. Specifikacija RPL protokola

Mogući spektar aplikacija LLN mreža vrlo je širok (kućna automatizacija, automatizacija zgrada, industrijska automatizacija, vojne primjene, primjene u zaštiti okoliša, medicini, prometu, poljoprivredi, i mnogim drugim djelatnostima). Zbog iznimno širokog područja primjene vrlo je teško pronaći jedinstveno rješenje za usmjeravanje prometa koje bi jednako kvalitetno zadovoljilo sve moguće aplikacije. Zato je unutar ROLL skupine odlučeno da se opseg zahtjeva za protokole usmjeravanja segmentira na četiri glavna područja primjene: industrijska automatizacija, urbane mreže, kućna automatizacija i automatizacija zgrada. Kao rezultat analize ove problematike radna skupina ROLL kreirala je četiri dokumenta sa specifikacijama zahtjeva za ova četiri područja primjene:

- *Urban WSNs Routing Requirements in Low-Power and Lossy Networks [87]*
- *Industrial Routing Requirements in Low-Power and Lossy Networks [88]*
- *Home Automation Routing Requirements in Low-Power and Lossy Networks [89]*
- *Building Automation Routing Requirements in Low-Power and Lossy Networks [90]*

Sukladno definiranim specifikacijama ROLL skupina provela je detaljnu analizu postojećih usmjerivačkih protokola koji se najčešće primjenjuju u žičnim i bežičnim ad hoc mrežama: RIP *(Routing Information Protocol)*, OSPF *(Open Shortest Path First)*, IS-IS *(Intermediate System to Intermediate System)*, OLSR *(Optimized Link State Routing)*, TBRPF *(Topology Dissemination Based on Reverse Path Forwarding)*, AODV *(Ad-hoc On Demand Vector Routing)*, DSR *(Dynamic Source Routing)* i DYMO *(Dynamic Mobile On-Demand Routing)*. Glavni kriteriji za evaluaciju navedenih protokola bili su:

- Skalabilnost protokola s obzirom na broj linkova i čvorova u mreži
- Reakcija na promjenu stanja linka (reakcija bi trebala biti lokalna, bez pokretanja globalne rekonfiguracije)
- Količina dodatnog kontrolnog (usmjerivačkog) prometa
- „Cijena“ („težina“) linka – mora se uzeti u razmatranje prilikom izračunavanja rute

Na temelju detaljne analize sukladno navedenim kriterijima ROLL radna skupina usuglasila se da niti jedan postojeći usmjerivački protokol ne udovoljava specifikacijama prethodno definiranim u navedenim dokumentima. Zbog toga se grupa orijentirala ka

specificiranju novog usmjerivačkog protokola koji će udovoljiti svim zadanim zahtjevima, što je tijekom 2010. godine rezultiralo specifikacijom novog usmjerivačkog protokola namijenjenog LLN *(Low-power and Lossy Networks)* mrežama – nastao je RPL protokol *(Routing Protocol for Low-power and Lossy Networks)*.

Unutar ROLL radne skupine za mreže male snage s nestabilnim linkovima koristi se termin LLN *(Low-power and Lossy Network)*, dok se unutar radne skupine 6LoWPAN koristi termin LoWPAN *(Low power Wireless Personal Area Network)*. Ova dva termina su u određenoj mjeri ekvivalentna, budući da se odnose na mreže koje se sastoje od čvorova ograničenih u pogledu računalnih i energetskih resursa koji su međusobno povezani putem nestabilnih linkova. Međutim, termin LLN nešto je općenitiji od termina LoWPAN, budući da je termin LoWPAN ograničen na mreže koje koriste IEEE 802.15.4 linkove, dok pojam LLN osim LoWPAN (i 6LoWPAN) mreža obuhvaća i druge mreže koje koriste nestabilne linkove male snage (primjerice PLC mreže, *Power Line Communication*).

Usmjerivački protokol RPL *(Routing Protocol for Low-power and Lossy Networks)* namijenjen je mrežama temeljenim na IP (IPv6) protokolu u kojima su čvorovi međusobno povezani nestabilnim linkovima (tj. linkovima koji imaju puno veći BER, *Bit Error Rate*, od, primjerice, optičkih ili Ethernet linkova, kao i puno veću vjerojatnost kolizije i gubitka paketa). Dizajniran je tako da udovoljava svim zahtjevima koje je ROLL radna skupina specificirala u dokumentima koji su prethodili specifikaciji samog protokola.

Osnovni zahtjevi koje bi, sukladno specifikacijama, usmjerivački protokol trebao zadovoljiti:

- **Podrška za *unicast, anycast* i *multicast* promet**
- **Adaptivno usmjeravanje *(adaptive routing)*:** podrazumijeva da protokol podržava dinamičko i automatsko preračunavanje ruta ukoliko se promijene uvjeti u mreži (npr. zbog pokretljivosti čvorova ili zbog kvara linka). Također, podrazumijeva da protokol podržava primjenu različitih metrika za izračunavanje ruta (npr. minimalna latencija, maksimalna propusnost i sl.).
- **Ograničeno usmjeravanje *(constraint-based routing)*:** podrazumijeva da protokol prilikom definiranja rute uzima u obzir različite karakteristike i ograničenja čvorova (npr. CPU, memorija, baterija), kao i atribute linkova (npr. latencija).
- **Karakteristike prometa *(traffic characteristics)*:** podrazumijeva podršku za različite tipove prometa: MP2P *(multipoint-to-point*, najčešće od senzorskih čvorova ka baznoj stanici), P2MP *(point-to-multipoint*, najčešće od bazne stanice ka senzorskim

čvorovima) i P2P *(point-to-point*, između bilo koja dva čvora iz mreže), kao i za održavanje višestrukih (paralelnih) ruta

- **Skalabilnost *(scalability)*:** podrazumijeva podršku za mreže sa jako velikim brojem čvorova (čak do reda veličine 10^4).
- **Konfiguracija i upravljanje *(configuration and management)*:** podrazumijeva da je protokol u stanju provesti postupak autokonfiguracije (bez potrebe za intervencijom korisnika), kao i naknadne rekonfiguracije u slučaju nastanka određenih promjena u mreži
- **Atributi čvorova *(node attribute)*:** budući da u LLN mrežama čvorovi radi uštede energije često prelaze u modove rada sa smanjenom potrošnjom *(idle, sleep)* protokol mora prepoznati odgovarajuće modove rada čvorova kako bi mogao detektirati je li čvor u datom trenutku u mogućnosti proslijediti podatkovni paket
- **Performanse:** podrazumijeva da protokol mora udovoljiti odgovarajuće zahtjeve u pogledu performansi. Ovi zahtjevi variraju ovisno o veličini i namjeni mreže, no obično se zahtijeva da protokol nakon promjene u mreži konvergira u rasponu od nekoliko sekundi do nekoliko minuta
- **Sigurnost:** potrebe za odgovarajućim mjerama sigurnosti također ovise o konkretnoj namjeni same mreže, budući da u nekim aplikacijama zadovoljavajuća čak i minimalna razina sigurnosti, dok u nekim aplikacijama sigurnost predstavlja apsolutni imperativ

Kreirati jedinstveni usmjerivački protokol koji bi istovremeno udovoljio svim ovim zahtjevima predstavlja izuzetno tešku, praktički nemoguću zadaću. Ograničeni resursi senzorskih mreža zahtijevaju jednostavan protokol, a objedinjavanje svih ovih zahtjeva svakako bi rezultiralo iznimno kompleksnim protokolom. Jasno je da konkretna aplikacija diktira uvjete koje protokol mora zadovoljiti, a koji se od slučaja do slučaja mogu značajno razlikovati (npr. senzorska mreža za kućnu automatizaciju ima potpuno različite zahtjeve od senzorske mreže za nadzor bojnog polja). Iz navedenih razloga rješenje koje bi zadovoljilo sve ove zahtjeve mora biti u potpunosti modularno. Zbog toga je RPL protokol dizajniran kao modularni usmjerivački protokol. To znači da specifikacija RPL protokola definira njegov jezgreni dio i opcionalna svojstva koja se mogu aktivirati kada i gdje je to potrebno.

Kao osnovna logička topologija usmjeravanja kod RPL protokola definiran je destinacijski orijentirani usmjereni aciklički graf *(DODAG, Destination Oriented Directed*

Acyclic Graph). Specifikacija RPL protokola definira način na koji se kreira (izgrađuje) DODAG, no karakteristike samog DODAG-a specificirane su unutar objektivne funkcije *(OF, Objective Function)*.

3.5.3.2. Metrike usmjeravanja i izbor rute

Usmjerivačke metrike predstavljaju jednu od najvažnijih komponenata strategije usmjeravanja. Većina današnjih IP usmjerivačkih protokola koriste statičke metrike linkova. Za konfiguriranje metrika linkova obično je odgovoran mrežni administrator. Metrike linkova najčešće reflektiraju propusnost linka, kašnjenje na linku, ili se izvode kombiniranjem nekoliko različitih metrika, pri čemu svaka komponenta ima odgovarajući težinski faktor (npr. metrika linka može se izvesti uzimanjem u obzir njegove propusnosti, kašnjenja i cijene). Usmjerivački protokol izračunava najkraću rutu temeljem poznatih statičkih metrika linkova. Bilo je određenih pokušaja uvođenja dinamičkih metrika linkova, što podrazumijeva da se metrika dinamički izračunava na temelju odgovarajućeg stanja u mreži (npr. prosječna duljina redova čekanja). Ovakve strategije uglavnom su se napuštale zbog velikih poteškoća u pogledu stabilnosti sustava (često dolazi do nestabilnosti u sustavu, što rezultira povećanim oscilacijama prometa i većim varijacijama kašnjenja). Također, karakteristično je za postojeće usmjerivačke protokole da su metrike orijentirane na linkove, budući da u postojećim mrežama većina usmjerivača ne predstavlja „usko grlo“ prilikom usmjeravanja prometa.

Ovakav pristup nije posve prikladan za bežične senzorske mreže, budući da resursima ograničeni i kvarovima podložni senzorski čvorovi ujedno obnašaju i ulogu usmjerivača. Zbog toga RPL protokol predviđa uporabu usmjerivačkih metrika *(routing metrics)* i usmjerivačkih ograničenja *(routing constraints)*. Pri tome se pod metrikom podrazumijeva odgovarajuća skalarna vrijednost koja se koristi prilikom određivanja najbolje rute sukladno odgovarajućoj objektivnoj funkciji. Metrika može reflektirati različite parametre linkova, poput propusnosti, kašnjenja ili kvalitete usluge [25]. Usmjerivačka ograničenja koriste se kako bi se na temelju specificiranih kriterija određeni linkovi uključili ili eliminirali iz putanje. Primjerice, objektivna funkcija može definirati da se iz mogućih putanja izbacuju one koje prolaze preko čvorova čiji je kapacitet baterije pao ispod 10%. Objektivna funkcija može kombinirati metrike i ograničenja vezana uz čvorove ili linkove u mreži [24]. Za RPL protokol postoji specifikacija koja definira metrike i ograničenja linkova i čvorova u mreži.

Jedna od u praksi najčešće korištenih metrika koja je prikladna i za BSM temeljene na IPv6 protokolu jest ETX metrika *(Expected Transmission Count)*. U osnovi, ETX metrika temelji se na prosječnom broju transmisija paketa koje su potrebne da bi se paket uspješno prenio. Prema tome, ETX metrika usko je povezana sa propusnošću duž putanje paketa. ETX metrika pronalazi putanju na kojoj će očekivano biti potreban najmanji broj transmisija (uključujući i retransmisije) za prijenos paketa do njegovog odredišta. Broj potrebnih retransmisija predviđa se na temelju mjerenja omjera izgubljenih paketa na svakom pojedinom bežičnom linku (u oba smjera). ETX metrika omogućava pronalaženje putanje sa najvećom propusnošću, unatoč gubicima. ETX vrijednost izračunava se kao: ETX = 1 / (Df * Dr), gdje je Df vjerojatnost da je poslani paket uspješno primljen na susjednom čvoru *(forward delivery ratio)*, a Dr vjerojatnost da je uspješno primljena potvrda (ACK paket) za poslani paket *(reverse delivery ratio)*. Neke prednosti primjene ETX metrike u BSM su njezina izravna povezanost sa propusnošću linkova, favorizacija ruta sa manjim brojem skokova i prepoznavanje asimetrije linkova (budući da se uzima u obzir vjerojatnost isporuke paketa u oba smjera). RPL protokol za pojedinu putanju prikazuje kumulativnu ETX vrijednost, koja predstavlja sumu ETX vrijednosti svih pojedinačnih linkova duž putanje.

Za izračunavanje optimalne putanje nije dovoljno samo definirati metrike i ograničenja. Potrebno je izabrati i odgovarajuću objektivnu funkciju koja će na temelju ulaznih parametara (metrike i ograničenja linkova i čvorova) odrediti optimalnu putanju u datom trenutku. Bežične senzorske mreže po svojoj strukturi mogu biti vrlo raznolike u pogledu kvalitete i propusnosti linkova, kapaciteta napajanja, kašnjenja i sl. Također, prisutni su i različiti tipovi prometa (npr. alarm, telemetrijski podaci i sl.). Zbog toga RPL protokol omogućava uporabu više objektivnih funkcija unutar jedne mreže. To se kod RPL protokola postiže na način da se kreira više DODAG-a, svaki sa svojom objektivnom funkcijom. Tako se, primjerice, unutar iste mreže može implementirati jedna objektivna funkcija koja favorizira propusnost linkova, i druga objektivna funkcija koja favorizira latenciju linkova. U tom slučaju se prema potrebi (odnosno prema vrsti prometa) primjenjuje jedna ili druga objektivna funkcija, i sukladno tome izabire optimalna putanja za prijenos podatkovnih paketa.

RPL usmjerivački protokol predstavlja protokol temeljen na vektorima udaljenosti *(distance vector protocol)*. On trenutno predstavlja jedini usmjerivački protokol koji podržava IPv6 protokol u bežičnim senzorskim mrežama. Kao osnova logičke topologije koristi se destinacijski orijentirani usmjereni aciklički graf *(DODAG, Destination Oriented Directed Acyclic Graph)*. Unutar DODAG-a konstruiraju se putanje od svih čvorova mreže prema

korijenu DODAG-a *(DODAG root)*. Korijen DODAG-a najčešće je bazna stanica ili rubni usmjerivač, LBR *(lossy network border router)*. Postoji više razloga zbog kojih je RPL protokol utemeljen upravo na vektorima udaljenosti, nasuprot mogućnosti da se temelji na stanjima linkova (kao kod *link state* protokola). Primarni razlog je stroga ograničenost resursa senzorskih čvorova. Protokol temeljen na stanjima linkova zahtijevao bi značajno veće resurse, prvenstveno memorijske. Prednost protokola temeljenog na stanjima linkova jest činjenica da svaki mrežni čvor detaljno poznaje cjelokupnu topologiju mreže, no potrebni su dodatni memorijski resursi za pohranu baze podataka o stanjima linkova *(LSDB, Link State Database)*. Također, ovakav protokol bi dodatno iscrpljivao resurse potrebom za povećanom količinom kontrolnog prometa potrebnog za održavanje i sinkronizaciju LSDB baza podataka.

RPL protokol predviđa da se unutar bežične senzorske mreže jedan ili više čvorova konfiguriraju kao korijeni DODAG-a (najčešće od strane administratora). Ukoliko u mreži postoji samo jedan korijen DODAG-a najčešće se radi o baznoj stanici ili rubnom usmjerivaču. Za izgradnju DODAG-a koristi se mehanizam otkrivanja čvorova temeljen na ICMPv6 porukama. RPL protokol definira dvije nove ICMPv6 poruke: DIO poruka *(DIO, DODAG Information Object)* i DAO poruka *(Destination Advertisement Object)*. DIO poruke senzorski čvorovi razašilju kako bi ostalim čvorovima oglasili informacije o DODAG-u. Ove informacije uključuju identifikacijsku oznaku DODAG-a (DODAGID), objektivnu funkciju (OF), rang DODAG-a *(DODAG rank)*, redni broj DODAG-a *(DODAGSequenceNumber)*, zajedno sa usmjerivačkim parametrima (metrikama i ograničenjima). Kada čvor zahvaljujući ovim porukama otkrije informacije o susjedima na temelju različitih definiranih pravila odlučuje hoće li se i na kojoj poziciji priključiti DODAG-u. Na taj način je omogućeno formiranje i proširivanje DODAG-a dodavanjem novih čvorova u mrežu.

Kada se senzorski čvor priključi DODAG-u poznate su mu informacije o ruti ka korijenu DODAG-a *(DODAG root)* i podržava MP2P promet od perifernih čvorova ka korijenu (smjer prema „gore“). U pogledu smjera prometa RPL specifikacija definira smjer prema „gore“ i smjer prema „dolje“. Pri tome se pod smjerom prema gore podrazumijeva smjer od perifernih čvorova ka korijenskom čvoru, dok smjer prema dolje podrazumijeva smjer od korijena prema perifernim čvorovima. Također, koristi se terminologija „roditelj“/“dijete“ („roditeljski čvor“, *parent node*, i „čvor dijete“, *child node*). Roditeljski čvor je onaj čvor koji je neposredno „iznad“ čvora djeteta, tj. nalazi se na ruti prema korijenskom čvoru „iznad“ čvora „djeteta“ (bliže je korijenskom čvoru). RPL specifikacija definira i pojam „bratskih“ čvorova *(sibling nodes)* – dva čvora su „bratska“ ukoliko su istog ranga (mogu, a ne moraju imati

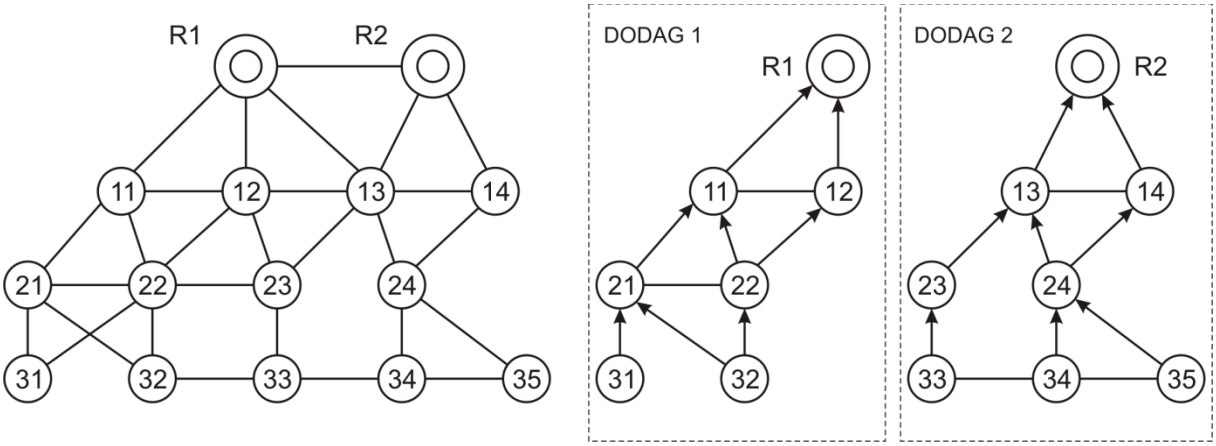
zajedničkog roditelja). DODAG može biti „utemeljen“ *(grounded DODAG)* ili „plutajući“ *(floating DODAG)*. DODAG je „utemeljen“ ukoliko je povezan sa „ciljem“ *(goal)*. Pod „ciljem“ se u RPL terminologiji podrazumijeva čvor koji je povezan sa eksternom mrežom (privatnom IP mrežom ili Internetom). „Plutajući“ DODAG je DODAG koji nije povezan sa „ciljem“. Za održavanje DODAG-a RPL protokol koristi iteracije koje kontrolira korijenski čvor (u svakoj iteraciji inkrementira se redni broj DODAG-a, *DODAG SequenceNumber*, koji zapravo predstavlja brojač iteracija).

DAO poruke koriste se za slanje usmjerivačkih informacija u smjeru prema dolje, od korijena ka perifernim čvorovima. DAO poruka nosi informacije o mrežnom prefiksu, vremenu života i duljini (težinskom faktoru) rute, kako bi krajnji čvor mogao odrediti svoju udaljenost od odredišta, kao i starost informacije o ruti do odredišta. RPL protokol također podržava i P2P *(peer-to-peer)* promet. Ukoliko dva čvora koji pokušavaju ostvariti P2P komunikaciju nisu u izravnom dosegu, čvor će proslijediti paket svojem „roditelju“ (roditeljskom čvoru). Paket putuje prema „gore“ sve dok ne dosegne čvor koji je zajednički nadređeni čvor *(ancestor node)* i izvorišnom i odredišnom čvoru. Nakon toga usmjerava se i prosljeđuje prema „dolje“, sve do odredišnog čvora. Ukoliko su dva čvora u izravnom dosegu radio veze moguće je ostvariti izravnu komunikaciju, bez posredstva DODAG-a.

Postupak usmjeravanja paketa unutar mreže u potpunosti je funkcionalan tek nakon što se uspostavi DODAG i kreiraju tablice usmjeravanja. Ukoliko dođe do kvarova čvorova ili prekida linkova putanje se rekonstruiraju primjenom lokalnih i globalnih mehanizama. Lokalni mehanizmi podrazumijevaju brzo pronalaženje pričuvne putanje bez pokušaja za kompletnom rekonstrukcijom i optimizacijom cijelog DODAG-a. Globalni mehanizmi podrazumijevaju pokretanje postupka reoptimizacije cjelokupnog DODAG-a, pri čemu postupak inicira i njime upravlja korijenski čvor.

Specifikacija RPL protokola podržava postojanje više instanci DODAG-a, pri čemu se svakoj dodjeljuje jedinstveni identifikator *(RPLInstanceID)*. Ovaj koncept omogućava formiranje različitih topologija na temelju različitih skupova usmjerivačkih ograničenja i objektivnih funkcija. U tom slučaju mrežni čvor se može uključiti u nekoliko instanci DODAG-a (npr. jedan DODAG koji je optimiziran u pogledu pouzdanosti linkova, i drugi koji je optimiziran s obzirom na kašnjenje na pojedinim linkovima). U tom slučaju se paketi prosljeđuju kroz DODAG koji odgovara zahtjevima konkretne aplikacije.

DODAG zapravo predstavlja skup čvorova koji su povezani usmjerenim linkovima bez petlji. RPL protokol kreira DODAG formiranjem skupa putanja od svakog rubnog čvora ka korijenskom čvoru. Nasuprot topologiji stabla *(tree)* DODAG sadrži redundantne putanje, što je u senzorskim mrežama neophodno. To znači da, ukoliko to topologija mreže omogućava, uvijek postoji više od jedne rute između perifernih čvorova i korijena DODAG-a.



Slika 3.21 DODAG i njegove instance

Na slici 3.21 prikazan je primjer višestrukih instanci DODAG-a unutar jedne fizičke topologije.

3.5.3.3. Formati ICMPv6 poruka kod RPL protokola

Unutar specifikacije RPL protokola definirane su tri vrste ICMPv6 poruka: DIO *(DODAG Information Object)*, DAO *(DODAG Destination Advertisement)*, DIS *(DODAG Information Solicitation)*.

Senzorski čvorovi šalju DIO poruke kako bi oglasili informacije o DODAG-u i njegovim karakteristikama. Prema tome, DIO poruke koriste se u postupku otkrivanja, formiranja i održavanja DODAG-a. Unutar DIO poruke postoje obvezne informacije i dodatne opcije. Unutar DIO poruke sadržane su sljedeće zastavice i polja:

- G *(grounded)*: označava da li je DODAG „utemeljen“, odnosno je li korijenski čvor DODAG-a ujedno i cilj objektivne funkcije

- T *(Destination Advertisement Trigger)*: koristi se za pokretanje postupka osvježavanja ruta u smjeru prema dolje (silazne rute)
- S *(Destination Advertisement Stored)*: označava da je čvor određene informacije iz DAO poruke pohranio u tablicu usmjeravanja
- A *(Destination Advertisement Supported)*: zastavica koja se postavlja kada korijenski čvor podržava i omogućava oglašavanje mrežnih prefiksa unutar DODAG-a
- Prf *(DODAGPreference)*: polje od 3 bita koje omogućava korijenskom čvoru da definira preferenciju DODAG-a, i time određeni DODAG mrežnim čvorovima učini „atraktivnijim“ za pridruživanje
- *DODAGSequenceNumber*: redni broj DODAG-a koji karakterizira iteraciju DODAG-a i kojeg kontrolira korijenski čvor
- *RPLInstanceID*: koristi se za identifikaciju instance DODAG-a i definira ga korijenski čvor
- DTSN *(Destination Advertisement Trigger Sequence Number)*: 8-bitni cijeli broj kojeg postavlja čvor koji šalje DIO poruku, a koristi se u postupku održavanja silaznih ruta
- DODAGID: cjelobrojna vrijednost koja jedinstveno identificira DODAG (postavlja je korijenski čvor)
- *DODAG Rank*: rang senzorskog čvora koji šalje DIO poruku (rang čvora određuje njegovu relativnu poziciju unutar DODAG-a, izračunava se na temelju objektivne funkcije i koristi se za izbjegavanje pojave petlji prilikom usmjeravanja)

DAO poruke koriste se za razmjenu informacija o odredištu kroz DODAG u smjeru prema gore, kako bi čvorovi mogli ažurirati svoje tablice usmjeravanja. DAO poruke uključuju sljedeće informacije:

- *DAO Sequence*: brojač kojeg inkrementira čvor koji posjeduje oglašeni mrežni prefiks svaki puta kada se pošalje nova DAO poruka
- *RPLInstanceID*: identifikacijska oznaka RPL instance
- *DAO Rank*: odgovara rangu čvora koji posjeduje odgovarajući mrežni prefiks
- *DAO Lifetime*: odgovara vremenu života mrežnog prefiksa (izražava se u sekundama)
- *Route tag*: cjelobrojna vrijednost koja se koristi za označavanje „kritičnih“ ruta
- *Destination Prefix*: definira broj bitova u mrežnom prefiksu
- *Reverse Route Stack*: sadrži broj IPv6 adresa koje se koriste u mreži sa čvorovima koji ne mogu pohraniti tablice usmjeravanja

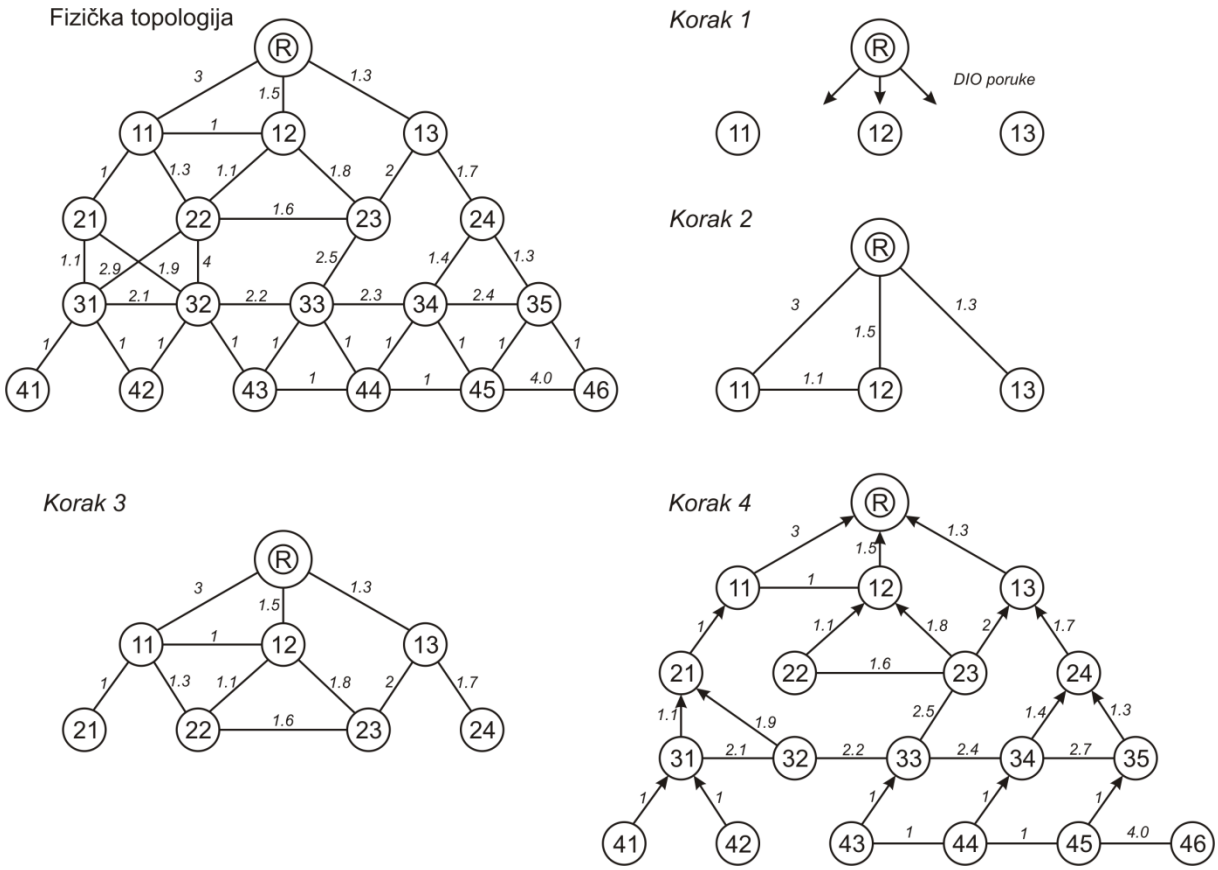
DIS poruke koriste se za otkrivanje DODAG-a u susjedstvu i traženje DIO poruka od susjednih RPL čvorova.

3.5.3.4. Postupak kreiranja DODAG-a

Prilikom kreiranja DODAG-a korijenski čvor šalje DIO poruke sukladno brojilu vremena (tajmeru). Osnovna ideja prilikom uvođenja brojila vremena bila je omogućiti češće slanje DIO poruka u slučaju da nastupi nekakav poremećaj unutar DODAG-a (npr. detektira se nekonzistentnost ili postojanje petlje ili se mreži priključi novi čvor). Nakon što se situacija stabilizira DIO poruke se šalju rjeđe, kako bi se smanjila količina kontrolnog prometa i time uštedjeli resursi.

Prilikom pristupanja mreži čvor se može ponašati na više načina. Prvi način podrazumijeva da čvor čeka dok ne primi DIO poruku koja oglašava postojeći DODAG. Drugi način podrazumijeva da čvor koji želi pristupiti mreži šalje DIS poruku, te vrlo brzo dobije DIO poruku od susjednih čvorova. Treća mogućnost je da novi čvor formira novi plutajući *(floating)* DODAG i započne sa slanjem DIO poruka na više adresa *(multicasting)*.

Nakon prijema DIO poruke čvor utvrđuje njezinu ispravnost. Ukoliko je poruka neispravna odbacuje se. Ukoliko je poruka ispravna, čvor analizira je li ju poslao čvor koji bi mu mogao biti susjedni (tj. čvor mora utvrditi može li mu čvor koji šalje DIO poruku postati nadređeni čvor, „roditelj“). Primjerice, moguća je i konfiguracija u kojoj čvor ne reagira na prvu primljenu DIO poruku, nego čeka određeno vremensko razdoblje kako bi se uvjerio da je link sa susjednim čvorom dovoljno pouzdan. Potom čvor analizira je li DIO poruka povezana sa DODAG-om kojem i sam pripada. Ukoliko je rang čvora koji šalje DIO poruku manji od ranga novog čvora (uvećanog za dodatnu konfigurabilnu vrijednost *DAGMaxRankIncrease*) DIO poruka će biti procesirana. DIO poruka se također procesira ako je šalje čvor nižeg ranga, ali iz drugog DODAG-a, koji eventualno omogućava bolju rutu sukladno objektivnoj funkciji. DIO poruka mora biti procesirana i u slučaju da je šalje čvor „roditelj“ *(parent)* za drugi DODAG, budući da postoji mogućnost da je roditeljski čvor prešao u drugi DODAG. Ukoliko dva čvora istovremeno pokušavaju poslati DIO poruku može doći do kolizije, što će se u sljedećem pokušaju izbjeći zahvaljujući primjeni tajmera sa slučajnim intervalom čekanja. Postupak kreiranja DODAG-a ilustriran je na slici 3.22.



Slika 3.22 Postupak kreiranja DODAG-a

Slika 3.22 prikazuje fizičku topologiju, zajedno sa ETX metrikama pojedinih linkova, te kroz 4 koraka ilustrira postupak kreiranja DODAG-a. Zadaća objektivne funkcije jest pronalazak putanje koja ima minimalnu ETX vrijednost, pri čemu se ETX vrijednost za cijelu putanju izračunava kao suma ETX vrijednosti za pojedine linkove od kojih se putanja sastoji.

U prvom koraku korijen DODAG-a (rubni usmjerivač) razašilje DIO poruke. Moguće je i da neki od čvorova pošalje DIS poruku, na koju korijenski čvor DODAG-a odmah odgovara s DIO porukom. Čvorovi 11, 12 i 13 primaju i procesiraju primljenu DIO poruku (korak 2). Budući da je poruka pristigla od čvora koji ima niži rang od njih (korijenski čvor), oni ga postavljaju za svoj „roditeljski“ čvor. Potom čvorovi 11, 12 i 13 izračunavaju svoj novi rang (na temelju broja skokova do korijenskog čvora), te se izračunavaju ETX vrijednosti za putanje. Korak 3 na slici 3.22 ilustrira DODAG nakon sljedeće iteracije. Korak 4 na slici 3.22 prikazuje konačni DODAG.

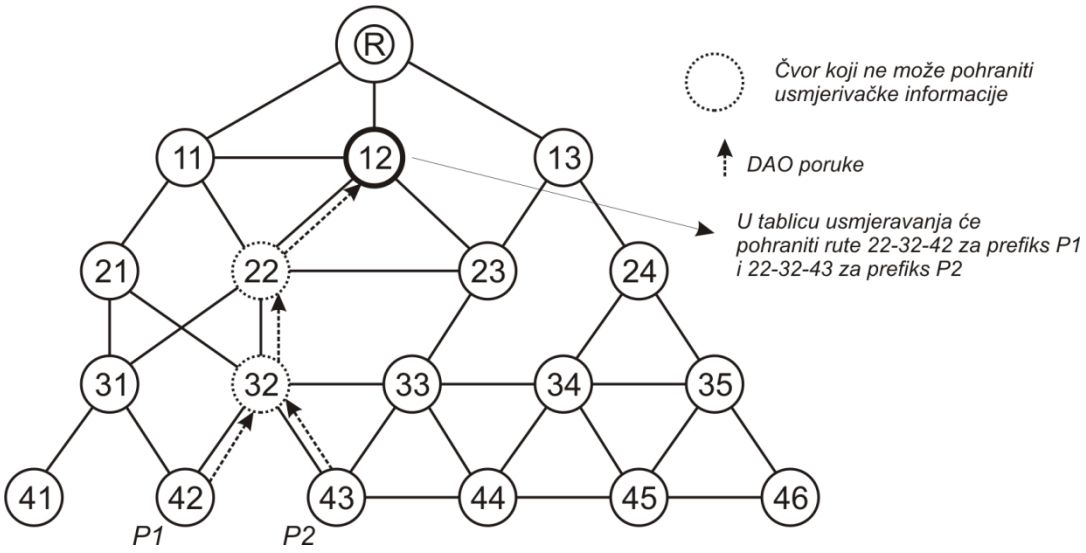
Ukoliko se unutar mreže formira više DODAG-a, čvorovi mogu prelaziti između njih. To znači da senzorski čvor u nekom trenutku za roditeljski čvor može izabrati čvor koji se nalazi

u drugom DODAG-u. Preporučljivo je da čvor može prelaziti u drugi DODAG tek nakon što proslijedi sve pakete (kada mu se red čekanja u potpunosti isprazni). Prilikom prelaska čvor treba zapamtiti identifikator RPL instance *(RPLInstanceID)*, identifikator DODAG-a *(DODAGID)*, redni broj DODAG-a *(DODAGSequenceNumber)* i svoj rang unutar DODAG-a. Čvor se može kretati i unutar DODAG-a, pri čemu može izabrati novi roditeljski čvor nižeg ili višeg ranga nego što je rang njegovih trenutnih roditeljskih čvorova. Ukoliko se čvor unutar DODAG-a pomiče u smjeru prema gore rang se smanjuje, dok se prilikom pomaka u smjeru prema dolje rang povećava.

Moguća je i situacija da čvor primi DIO poruku koja specificira objektivnu funkciju koja mu je nepoznata (ne podržava je). U tom slučaju čvor se neće priključiti DODAG-u ili će se priključiti kao periferni čvor, što znači da neće biti u mogućnosti obavljati ulogu usmjerivača. Takav čvor će moći primati i procesirati DIO poruke i slati DAO poruke, no neće moći slati DIO poruke i ponašati se kao RPL usmjerivač.

Nakon što se formira DODAG, sljedeći korak u konfiguracijskom postupku jest kreiranje tablica usmjeravanja na čvorovima iz DODAG-a. Potrebne informacije kroz DODAG se propagiraju pomoću DAO poruka. Redni broj koji se prenosi unutar DAO poruke omogućava detekciju zastarjelih ili dupliciranih poruka. DAO poruka sadrži i rang čvora koji posjeduje oglašeni mrežni prefiks, što može pomoći pri odluci o izboru optimalne rute čvoru koji je primio više DAO poruka sa istim mrežnim prefiksom destinacije.

U nekim mrežama je moguća pojava da određeni čvorovi nemaju dovoljno memorijskih resursa za pohranu informacija o silaznim rutama. Budući da nisu u mogućnosti pohraniti usmjerivačke informacije takvi čvorovi ne mogu usmjeravati P2MP ili P2P promet ka perifernim čvorovima. Unutar RPL specifikacije definirane su odgovarajuće ekstenzije kako bi se i ovakvi čvorovi mogli uklopiti u mrežu.



Slika 3.23 Primjena stoga reverzne rute u DAO poruci

U primjeru prikazanom na slici 3.23 čvorovi 22 i 32 ne mogu pohranjivati usmjerivačke informacije. P1 i P2 su IPv6 prefiksi koji odgovaraju čvorovima 42 i 43, i putem DAO poruke oglašeni su čvoru 32. Nakon primitka DAO poruke čvor 32 dodaje IPv6 prefiks čvora 42 unutar stoga reverzne rute *(reverse route stack)* primljene DAO poruke. Po primitku DAO poruke od čvora 32 čvor 22 (koji također ne može pohraniti usmjerivačke informacije) obavlja sličnu operaciju i dodaje IPv6 adresu čvora 32. Konačno, kada DAO poruka stigne do čvora koji može pohraniti informacije (čvor 12) ovaj čvor će detektirati da je poruka prošla kroz područje sa čvorovima bez mogućnosti pohrane informacija. Tada će čvor 12 napraviti ekstrakciju skupa potrebnih skokova pridruženih odgovarajućem prefiksu, te ih lokalno pohraniti u svoju tablicu usmjeravanja. Nakon toga će, zahvaljujući pohranjenim informacijama, paket usmjeren u područje mreže sa prefiksom P1 čvor 12 ispravno proslijediti čvoru 42.

Ukoliko čvor izgubi povezivost s podređenim čvorom (za kojega ima pridruženi prefiks) on uklanja odgovarajući unos iz tablice usmjeravanja i svojim roditeljskim čvorovima oglašava gubitak rute slanjem *no-DAO* poruke (DAO poruka u kojoj je vrijeme života odgovarajućeg prefiksa postavljeno na nulu).

Pojava zatvorenih petlji prilikom usmjeravanja krajnje je nepoželjna, te je jedna od najvažnijih zadaća usmjerivačkih protokola izbjeći nastanak usmjerivačkih petlji (kao i detektirati njihov nastanak ukoliko do njega ipak dođe).

U brzim mrežama sa velikom količinom prometa vrijeme života paketa *(TTL, Time To Live)* dekrementira se pri svakom skoku, tako da i u slučaju pojave petlje paket biva brzo uništen. Pojava kratkotrajnih privremenih petlji moguća je čak i kod usmjerivačkih protokola temeljenih na stanju linka (poput OSPF-a) zbog privremenih izostanaka sinkronizacije LSDB baze *(Link State Database)* među čvorovima. Međutim, kod brzih mreža čak i pojava kratkotrajnih petlji može dovesti do zagušenja linka i odbacivanja paketa.

U bežičnim senzorskim mrežama situacija je nešto drugačija, budući da su količina mrežnog prometa i brzina prijenosa općenito vrlo mali. Zbog toga će eventualni nastanak usmjerivačkih petlji imati ograničen utjecaj na mrežu. U senzorskim mrežama također je nužno izbjeći nastanak petlji kad god je to moguće, detektirati ih ukoliko ipak nastanu, no iznimna brzina reakcije nije od presudne važnosti.

Implementacija mehanizma koji bi jamčio da ne mogu nastati privremene petlje bila bi izuzetno kompleksna i neadekvatna za nestabilno i resursima ograničeno okruženje bežične senzorske mreže. Zbog toga RPL protokol ne jamči nemogućnost nastanka privremenih petlji, nego implementira odgovarajući mehanizam za njihovu detekciju.

4. Sigurnost u bežičnim senzorskim mrežama

Jedan od ključnih problema koji su znatno izraženiji u bežičnim mrežama u odnosu na klasične žične mreže jest problem sigurnosti. Zbog otvorene prirode komunikacijskog medija sve vrste bežičnih mreža znatno je teže osigurati od različitih mogućnosti napada i neovlaštene zlouporabe nego žične mreže. Prema tome, sigurnosni problemi u bežičnim ad hoc mrežama *(MANET, Mobile Ad Hoc Network)* višestruko su veći i izazovniji nego u žičnim mrežama (kakav je, primjerice, jezgreni dio Interneta). Iako bežične senzorske mreže zapravo predstavljaju posebnu podskupinu MANET mreža, zbog njihovih vrlo strogih ograničenja u resursima implementacija sigurnosnih mehanizama i uspostavljanje odgovarajuće razine sigurnosti predstavljaju još veći izazov i problem nego što je to u MANET mrežama [118, 128].

Bežične mreže sa sobom donose čitav niz prednosti u odnosu na žične mreže. Prije svega donijele su iznimnu fleksibilnost, kako iz perspektive korisnika, tako i iz perspektive mrežnih operatera. Implementacija bežičnih mrežnih rješenja omogućava sveprisutnu pokrivenost i dostupnost, kako lokalno tako i na širem području, uz vrlo niske troškove implementacije i održavanja (budući da postavljanje i održavanje fiksne infrastrukture u pravilu iziskuje znatno veća materijalna sredstva). Također, u nekim područjima čak je i nemoguće postaviti fiksnu infrastrukturu (npr. zbog konfiguracije terena ili administrativnih zabrana). U tom slučaju bežične mreže predstavljaju vrlo elegantno i ekonomično rješenje. Također, vrlo važno svojstvo bežičnih mreža jest podrška pokretljivosti korisnika, pogotovo u vrijeme kada je sve veći broj pristupnih uređaja vrlo malih dimenzija i korisnik ih može neprestano nositi sa sobom (npr. laka prijenosna računala, ručna računala, napredniji mobilni telefoni i sl.).

Budući da se i u većini bežičnih mreža primjenjuje TCP/IP protokolni stog, gotovo sve postojeće sigurnosne prijetnje poznate u žičnim mrežama prisutne su i u bežičnim mrežama. Nadalje, u bežičnim mrežama dodatno se javlja još i čitav niz drugih prijetnji (koje ne postoje u žičnim mrežama), a prouzrokovane su specifičnostima bežičnog okruženja (nepouzdanost i otvorenost bežičnog medija, ograničena propusnost, ograničen kapacitet napajanja i sl.) [110].

Iako su po nekim svojim karakteristikama bežične senzorske mreže vrlo slične tradicionalnim bežičnim MANET mrežama postoje i neke značajne razlike koje u velikoj mjeri utječu na problematiku sigurnosti u BSM [60]. Iako već postoji čitav niz sigurnosnih protokola i algoritama razvijenih za tradicionalne MANET mreže, zbog ovih razlika oni nisu

izravno primjenjivi u BSM. Neke od značajnijih razlika između BSM i MANET mreža, a koje bitno utiču na projektiranje i implementaciju sigurnosnih rješenja, jesu:

- Broj senzorskih čvorova u BSM može biti i za nekoliko redova veličine veći od broja čvorova u MANET mreži
- Senzorski čvorovi u BSM su obično „gušće“ raspoređeni (na manjim međusobnim udaljenostima) nego čvorovi u MANET mreži
- Senzorski čvorovi skloniji su kvarovima (zbog ambijentalnih utjecaja i ograničenog napajanja)
- Topologija senzorske mreže se znatno češće mijenja (zbog kvarova ili pokretljivosti čvorova)
- Senzorski čvorovi znatno su ograničeniji od tipičnih čvorova u MANET mreži u pogledu napajanja i računalnih resursa (količina memorije i brzina procesora)
- U BSM se komunikacija uglavnom temelji na načelu razašiljanja *(broadcast)*, dok su MANET mreže uglavnom temeljene na komunikaciji od točke do točke *(point-to-point)*
- Senzorski čvorovi u BSM vrlo često nemaju jedinstvenu globalnu identifikacijsku oznaku *(global ID)*.

Navedene razlike značajno utječu na implementaciju sigurnosnih mehanizama u BSM. Tako su, primjerice, BSM znatno ranjivije na napade uskraćivanjem resursa *(denial-of-service)* uslijed bežične radio-komunikacije i znatno ograničenih energetskih resursa. Naprednije tehnike protiv elektroničkog ometanja nije moguće implementirati zbog njihove kompleksnosti i energetskih zahtjeva. Također, poznate kriptografske metode temeljene na javnom ključu su praktički neprimjenjive u BSM zbog svoje prevelike zahtjevnosti za računalnim resursima. Nadalje, primjena kriptografskih metoda u BSM za sobom povlači nužnost implementacije kvalitetnih mehanizama za upravljanje i distribuciju kriptografskih ključeva, kao i mehanizama za njihov opoziv u slučaju kompromitacije. Razvoj i implementacija sigurnih protokola usmjeravanja u BSM također predstavlja veliki izazov i problem. Zbog energetskih ograničenja poželjno je implementirati mehanizme za agregaciju podataka, za što je također nužno osigurati mehanizam koji će osigurati integritet i povjerljivost informacije. Budući da je zbog svojih karakteristika BSM vrlo ranjiva struktura u kojoj lako može doći do kompromitacije određenog broja čvorova, potrebno je implementirati odgovarajući sigurnosni mehanizam koji omogućava otkrivanje

kompromitiranih čvorova i njihovo isključivanje iz mreže, pri čemu ostatak mreže nastavlja sa normalnim radom [102, 108].

Kvalitetan sigurnosni okvir koji bi se mogao implementirati u BSM mora prožimati sve slojeve u protokolnom stogu kako bi omogućio visoku razinu sigurnosti i zaštite. Protokolni stog koji se najčešće susreće u BSM uključuje sljedeće slojeve:

- **Fizikalni sloj** *(Physical layer)*: odgovoran za izbor frekvencije, generiranje frekvencije nosioca, generiranje signala, modulaciju i eventualnu enkripciju podataka
- **Sloj podatkovnog linka** *(Data link layer)*: odgovoran za multipleksiranje podatkovnih tokova, detekciju podatkovnih okvira, pristup mediju i kontrolu pogrešaka, kao i osiguranje pouzdane konekcije (od točke do točke, *point-to-point*, kao i od jedne prema više točaka, *point-to-multipoint*)
- **Mrežni sloj** *(Network layer)*: odgovoran za adresiranje i prosljeđivanje paketa
- **Transportni sloj** *(Transport layer)*: specificira način pouzdanog prijenosa paketa
- **Aplikacijski sloj** *(Application layer)*: specificira način na koji senzorski čvor zahtijeva ili pruža odgovarajuću informaciju, kao i interakciju sa krajnjim korisnikom

Na implementaciju odgovarajućih sigurnosnih rješenja na pojedinim slojevima najviše utječu stroga ograničenja BSM u pogledu energije, računalnih resursa (procesor i memorija) i dometa primopredajnika. Glavni potrošači energije unutar senzorskog čvora su mjerni pretvornik senzora, mikroprocesor i radio primopredajnik. Komunikacija u BSM je znatno energetski zahtjevnija od procesiranja, pa je primjerice energija potrebna za procesiranje jednog bita za oko 800-1000 puta manja od energije potrebne za njegov prijenos radio vezom [113]. Računalni dio senzorskog čvora znatno je slabiji od tipičnog čvora iz MANET mreže, prvenstveno zbog manje potrošnje energije i minijaturizacije samog uređaja. U pravilu je i primopredajnik u BSM slabijeg dometa nego u MANET mrežama, budući da se i na taj način ostvaruje ušteda u potrošnji energije.

Navedena ograničenja i specifičnosti potrebno je uzeti u obzir prilikom razvoja sigurnosnih mehanizama namijenjenih BSM. Implementacijom različitih sigurnosnih mehanizama nastoji se udovoljiti sljedećim zahtjevima:

- **Dostupnost** *(Availability)*: osigurava da su željene informacije i mrežne usluge dostupne legalnom korisniku, čak i u slučaju pojave napada uskraćivanjem resursa *(denial-of-service)*

- **Autorizacija** *(Authorization)*: osigurava da su isključivo autorizirani senzorski čvorovi uključeni u proces prikupljanja i razmjene informacija putem mreže
- **Autentifikacija** *(Authentication)*: osigurava autentičnost komunikacije između čvorova u mreži (sprečava mogućnost da se maliciozni čvor predstavlja kao legalni čvor)
- **Povjerljivost** *(Confidentiality)*: osigurava da pojedina poruka može biti pročitana isključivo od strane legalnog primatelja
- **Integritet** *(Integrity)*: osigurava da poruka nije modificirana na svom putu kroz više skokova između izvorišnog i odredišnog čvora
- **Neopovrgavanje** *(Nonrepudiation)*: osigurava da čvor ne može opovrgnuti slanje poruke koju je ranije poslao
- **„Svježina“** *(Freshness)*: podrazumijeva da su podaci „svježi“ i osigurava da napadač ne može ponavljati slanje starih podataka u mrežu

4.1. Sigurnosne prijetnje i napadi u BSM

Fizičko osiguravanje svakog senzorskog čvora u BSM iziskivalo bi značajne troškove, što bi svakako bilo i u suprotnosti sa konceptom senzorske mreže kao mreže jeftinih umreženih senzorskih čvorova. Zbog toga se senzorske mreže u velikoj većini slučajeva ne smatraju otpornim na fizičke napade, odnosno napadač često može fizički pristupiti senzorskom čvoru. Prilikom razmatranja problematike sigurnosti u BSM uglavnom se polazi od pretpostavke da se bazna stanica može smatrati sigurnom i povjerljivom, a da su senzorski čvorovi podložni kompromitaciji. Međutim, ovakav pristup nije u potpunosti ispravan, pogotovo u senzorskim mrežama koje se temelje na IP protokolu i izravno su povezane sa drugim mrežama, pa i Internetom. Senzorsku mrežu je iznimno teško zaštititi od fizičkog napada, budući da napadač u slučaju fizičkog pristupa čvoru može doći do informacija koje su na njemu pohranjene (uključujući i ključeve, ukoliko se koriste neke od kriptografskih metoda). Sigurnosni mehanizmi za BSM, koji predstavljaju aktivno područje intenzivnog istraživanja i razvoja, uglavnom podrazumijevaju različite metode za prevenciju i zaštitu od različitih tipova napada koji ne podrazumijevaju izravan fizički kontakt između napadača i senzorskih čvorova [51, 54].

Napade na BSM moguće je klasificirati prema više različitih kriterija. Ovisno o kriteriju klasifikacije, razlikuju se sljedeće kategorije napada:

- **Vanjski i unutrašnji napadi** *(outsider and insider attacks)*: vanjski napadi su inicirani od strane čvorova koji ne pripadaju napadnutoj BSM, dok unutrašnji napadi nastaju kada se legitimni čvor iz mreže počne ponašati zlonamjerno (maliciozno)
- **Pasivni i aktivni napadi** *(passive and active attacks)*: pasivni napadi podrazumijevaju prisluškivanje radio komunikacije i praćenje paketa koji putuju mrežom, dok aktivni napadi podrazumijevaju određene modifikacije podatkovnih tokova u mreži ili kreiranje novih podatkovnih tokova od strane napadača
- ***Mote-class* i *laptop-class* napadi:** kod *mote-class* napada se podrazumijeva da napadač koristi jedan ili više čvorova sličnih mogućnosti kao što su čvorovi u napadnutoj BSM, dok *laptop-class* napad podrazumijeva da napadač koristi znatno snažniji uređaj (sa većim dometom primopredajnika, većim kapacitetom napajanja i većom procesorskom snagom – npr. prijenosno računalo).

Napade u senzorskoj mreži moguće je klasificirati i na temelju toga koji sigurnosni zahtjev narušavaju:

- **Napadi na tajnost i autentičnost:** moguće ih je prevenirati uporabom kriptografskih metoda
- **Napadi na dostupnost mreže *(denial-of-service, DoS)*:** mogu biti usmjereni na bilo koji mrežni sloj
- **Napadi na integritet usluge:** cilj napadača obično je ubacivanje lažnih podataka i vrijednosti u mrežu, moguća prevencija je implementacija sustava za otkrivanje i neutralizaciju malicioznih čvorova

Zbog velikog broja različitih mogućnosti napada i njihovih brojnih varijacija vrlo je teško napraviti sustavni prikaz svih mogućih sigurnosnih prijetnji i napada koji postoje u senzorskim mrežama. Jedan od mogućih pristupa jest analiza sigurnosnih prijetnji po slojevima mrežnog modela [97].

4.1.1. Sigurnosne prijetnje na fizikalnom sloju

Fizikalni sloj mrežnog modela u bežičnim senzorskim mrežama odgovoran je za izbor frekvencije, generiranje frekvencije nosioca, detekciju signala, modulacijske postupke i enkripciju podataka. Kao i u svim bežičnim RF mrežama, tako i u BSM postoji mogućnost elektroničkog ometanja *(jamming)*. Također, senzorski čvorovi često mogu biti raspoređeni u neprijateljskom okruženju i biti izloženi fizičkom pristupu od strane zlonamjernog napadača.

4.1.1.1. Elektroničko ometanje (jamming)

Pod elektroničkim ometanjem *(jamming)* podrazumijeva se napad kod kojeg napadač pomoću svojeg predajnika namjerno izaziva interferenciju na radijskim frekvencijama koje se koriste u BSM. Predajnik kojim napadač ometa mrežu često može emitirati višestruko većom snagom od predajnika koji se nalaze na senzorskim čvorovima. Tako napadač najčešće sa jednim predajnikom može onemogućiti komunikaciju u čitavoj senzorskoj mreži. Ukoliko koristi predajnik manje snage napadač će onemogućiti komunikaciju u dijelu mreže, no već i to može biti dovoljno da onemogući normalan rad mreže. Nadalje, postoji i mogućnost „pokrivanja“ cijele mreže pomoću nekoliko raspoređenih predajnika za ometanje [40].

Mogući učinkoviti način obrane od ovakve vrste napada jest primjena FHSS metode komunikacije *(Frequency-Hopping Spread Spectrum)*. FHSS predstavlja metodu emitiranja signala koja podrazumijeva brzo prebacivanje frekvencije nosioca između različitih vrijednosti (kanala) prema pseudoslučajnoj tajnoj sekvenci koja je poznata predajniku i prijemniku. Budući da ta sekvenca napadaču nije poznata, on ne zna na kojoj frekvenciji se u datom trenutku odvija komunikacija u mreži, pa je ne može ni ciljano ometati. U tom slučaju bi napadač eventualno mogao ometati široki spektar frekvencija, budući da je broj kanala koji se mogu koristiti za komunikaciju unutar BSM ograničen. Međutim, ovakve napredne metode povećavaju kompleksnost senzorskih čvorova, te povećavaju njihovu cijenu i potrošnju energije. Zbog toga se u većini senzorskih mreža komunikacija ograničava na jedan kanal, pa su kao takve vrlo osjetljive na napad elektroničkim ometanjem.

4.1.1.2. Neovlašteni fizički pristup (tampering)

U velikom broju slučajeva čvorovi senzorske mreže nemaju posebnu fizičku zaštitu, pa su kao takvi izloženi mogućnosti fizičkog pristupa neovlaštene osobe. U slučaju fizičkog pristupa senzorskom čvoru napadač je u mogućnosti doći do osjetljivih i povjerljivih informacija, poput kriptografskih ključeva ili drugih podataka koji su na njemu pohranjeni. Osim pristupa povjerljivim informacijama, napadač je u tom slučaju u mogućnosti izmijeniti neke podatke ili programski kod, te na taj način u potpunosti kontrolirati kompromitirani čvor i iskoristiti ga za dalje maliciozne aktivnosti. Od ovakvog napada senzorske čvorove je vrlo teško učinkovito zaštititi, budući da svaka fizička zaštita senzorskog čvora drastično povećava troškove implementacije BSM. Budući da je senzorske čvorove gotovo nemoguće fizički zaštititi, svi sigurnosni mehanizmi koji se implementiraju u BSM moraju predvidjeti mogućnost kompromitacije određenog broja čvorova, te čak i u tom slučaju omogućiti daljnji rad mreže isključivanjem takvih čvorova.

4.1.2. Sigurnosne prijetnje na sloju podatkovnog linka

Sloj podatkovnog linka u mrežnoj arhitekturi BSM odgovoran je za multipleksiranje podatkovnih tokova, detekciju okvira, pristup mediju i kontrolu pogrešaka. Zadaća ovog sloja je omogućiti pouzdanu konekciju od točke do točke *(point-to-point)* i od točke ka više točaka *(point-to-multipoint)* unutar bežične senzorske mreže. Mogući napadi na sloju podatkovnog linka uključuju namjerno izazivanje kolizije paketa i namjerno iscrpljivanje resursa.

4.1.2.1. Kolizija (collision)

U slučaju da dva ili više čvorova istovremeno pokušavaju sa emitiranjem na istoj frekvenciji doći će do kolizije paketa. U slučaju pojave kolizije dolazi do pogrešaka u prijenosu paketa (paket na odredište dolazi „oštećen“) ili do potpunog gubitka paketa. Napadač može namjerno izazivati koliziju, te na taj način prouzročiti zastoj u radu mreže.

Vrlo čest je slučaj da napadač namjerno izaziva koliziju u trenutku slanja kontrolnih poruka koje potvrđuju ispravan prijem poruke (ACK), pa ove poruke bivaju izgubljene (izvorišni čvor ne dobiva potvrdu o primitku poruke od strane odredišta). Moguća obrana od namjerno izazvanih kolizija jest implementacija i uporaba kodova za ispravljanje pogrešaka *(error-correcting codes)*. Primjena ovakvih zaštitnih kodova učinkovita je u slučaju rjeđe pojave kolizije paketa, što je u svim mrežama neizbježno, a prouzročeno je utjecajem okoliša i samog sklopovlja (radi se o probabilističkim pogreškama čija je učestalost pojave poznata). Međutim, ako se radi o sustavnom i namjernom izazivanju kolizije od strane napadača niti ovakva metoda ne pokazuje preveliku učinkovitost. Pojavu namjernog izazivanja kolizije u mreži od strane napadača moguće je detektirati, no iznimno je teško obraniti se od ove vrste napada.

4.1.2.2. Iscrpljivanje resursa (resource exhaustion)

Ponavljanje namjerno izazvanih kolizija može prouzročiti iscrpljivanje resursa bežičnih senzorskih čvorova (prije svega, gubitak napajanja uslijed pražnjenja baterije). Ukoliko nastane kolizija senzorski čvor će kontinuirano pokušavati sa retransmisijom paketa, što će vrlo brzo isprazniti njegovu bateriju. Zbog toga je poželjna implementacija mehanizma koji bi bio u stanju detektirati ovakvu situaciju (niz bezuspješnih pokušaja retransmisije) i zaustaviti daljnje uzaludne pokušaje slanja paketa [122, 123]. Moguće rješenje jest primjena ograničenja na učestalost pristupa mediju (na MAC sloju), tako da se niz uzastopnih zahtjeva za pristupom mediju može ignorirati, te na taj način onemogućiti niz uzastopnih slanja paketa i spriječiti pražnjenje baterije senzorskog čvora. Druga mogućnost zaštite jest primjena vremenskog multipleksiranja *(time-division multiplexing)*, pri čemu se svakom senzorskom čvoru pridjeljuje odgovarajući vremenski slot unutar kojeg može prenositi podatke. Ovakav pristup eliminira potrebu arbitriranja za svaki pojedini okvir, ali i dalje ostavlja mogućnost pojave kolizije paketa [75].

4.1.2.3. Unfairness („nepoštenje“)

Umjesto potpunog sprečavanja pristupa mreži, napadač ga može u određenoj mjeri otežati. To obično postiže na način da periodički primjenjuje određene tehnike napada na slojeve iznad sloja podatkovnog linka, čime postiže da određeni čvorovi ne mogu zadovoljiti vremenski okvir unutar kojeg trebaju obaviti transmisiju (što je određeno stvarnovremenskim MAC protokolom koji se primjenjuje u mreži). Učinak ovakve vrste napada može se smanjiti korištenjem manjih okvira, budući da se tako smanjuje vremenski interval unutar kojeg napadač može zauzeti komunikacijski kanal. Nedostatak ovakvog pristupa jest mala učinkovitost komunikacije – relativno velika količina kontrolnog prometa u odnosu na korisnu informaciju.

4.1.3. Sigurnosne prijetnje na mrežnom sloju

Mrežni i usmjerivački sloj u bežičnim senzorskim mrežama po svojoj koncepciji sličan je mrežnom sloju u klasičnim mrežama, no postoje određeni principi koji u BSM moraju biti zadovoljeni, koji u velikoj mjeri određuju dizajn mrežnih mehanizama koji funkcioniraju na mrežnom sloju (prije svega mehanizam usmjeravanja). Zasigurno najvažniji princip koji mora biti zadovoljen jest mala potrošnja energije i energetska učinkovitost. Nadalje, većina senzorskih mreža je podatkovno orijentirana (naglasak je na podatku, a ne na svakom pojedinom čvoru), te je i adresiranje najčešće temeljeno na atributima (rijetko se javlja potreba za adresiranjem svakog pojedinačnog čvora). U idealnom slučaju, čvorovi su svjesni i svoje točne lokacije u prostoru. Budući da na mrežnom sloju funkcioniraju složeni mrežni mehanizmi od čijeg normalnog funkcioniranja u velikoj mjeri ovisi ispravan rad cijele mreže (npr. usmjerivački mehanizmi), na ovom sloju događa se i najviše do sada poznatih napada u BSM.

4.1.3.1. Lažne, izmijenjene ili ponovljene usmjerivačke informacije (spoofed, altered, or replayed routing information)

Većina izravnih napada na usmjerivačke mehanizme orijentirana je na usmjerivačke informacije koje se razmjenjuju između čvorova. Pri tome napadač može lažirati *(spoof)*, ili izmijeniti ove podatke, kao i ponavljati slanje ranije poslanih informacija, a s ciljem narušavanja normalnog toka mrežnog prometa. Na taj način napadač namjerno može kreirati usmjerivačke petlje, privući ili odbijati mrežni promet, produljiti ili skratiti postojeće izvorne rute, generirati lažne poruke o pogreški, povećati latenciju prilikom prijenosa, particionirati mrežu na segmente i sl. Kao protumjera protiv lažiranja i izmjene usmjerivačkih informacija može poslužiti dodavanje autentifikacijskog koda na kraj svake poruke *(MAC, message authentication code)*. Provjerom autentifikacijskog koda primatelj poruke može utvrditi i provjeriti je li poruka lažirana ili modificirana. Mehanizmi za zaštitu od ponavljanja starih poruka uglavnom podrazumijevaju implementaciju određenih brojača ili vremenskih oznaka *(timestamps)* pojedinih poruka.

4.1.3.2. Selektivno prosljeđivanje (selective forwarding)

Mreže u kojima se komunikacija odvija kroz više skokova *(multihop)*, a gdje pripadaju i BSM, obično se temelje na pretpostavci da će svi čvorovi koji sudjeluju u komunikaciji vjerno prosljeđivati primljene poruke ka njihovom odredištu. Ova pretpostavka se često zlorabi od strane napadača, pri čemu se najčešće radi o selektivnom prosljeđivanju paketa. U slučaju selektivnog prosljeđivanja zlonamjerni čvor može namjerno odbiti prosljeđivanje određenih poruka ka njihovom odredištu, i jednostavno ih odbaciti te na taj način onemogućiti njihovu dalju propagaciju. Najjednostavniji oblik ovakvog napada jest situacija kada maliciozni čvor odbija proslijediti bilo koji paket – ponaša se, figurativno, kao „crna rupa“ *(black hole attack)*. Međutim, ovu varijantu napada najlakše je i otkriti. Zadaća otkrivanja senzorskih čvorova koji se ponašaju poput „crne rupe“ leži na njihovim susjedima, koji su pomoću odgovarajućeg sigurnosnog mehanizma (ukoliko je implementiran u mrežu) u mogućnosti detektirati ovu vrstu malicioznog ponašanja. U slučaju otkrivanja ovakvog zlonamjernog čvora potrebno je provesti rekonfiguraciju ruta u mreži, tako da se ovi čvorovi iz njih izostave.

Puno sofisticiraniji oblik napada je situacija u kojoj zlonamjerni čvor selektivno prosljeđuje pakete. U tom slučaju napadač izabire nekolicinu čvorova čije poruke želi ukloniti ili modificirati, dok promet sa preostalih čvorova prosljeđuje na uobičajen način. Na taj način će zlonamjerno ponašanje biti puno teže otkriveno, jer će susjedni čvorovi puno teže „posumnjati“ na zlonamjerni čvor, budući da se dio prometa regularno odvija.

Najčešći tip napada selektivnim prosljeđivanjem poruka jest situacija u kojoj se zlonamjerni čvor nalazi izravno na putanji (ruti) kojom promet putuje od izvora ka odredištu. Međutim, moguća je i varijanta u kojoj se maliciozni čvor ne nalazi izravno na putanji, nego je u susjedstvu (u dometu radio veze) nekog od čvorova sa rute. U tom slučaju maliciozni čvor može „prisluškivati“ podatkovni tok koji prenose susjedni čvorovi i pri tome emulirati selektivno prosljeđivanje na način da svojim emitiranjem namjerno izaziva koliziju sa onim paketima za koje želi da budu odbačeni. Srećom, ovakav oblik napada je znatno kompliciranije izvesti, pogotovo u slučajevima ako svaki par čvorova komunicira na promjenjivim frekvencijama *(frequency hopping)*, pa se i rjeđe susreće u praksi. Jedna od mogućnosti obrane od ove vrste napada jest uporaba višestrukih ruta i prosljeđivanje prometa različitim rutama od izvorišnog do odredišnog čvora.

4.1.3.3. Sinkhole („ponor“)

Kod *sinkhole* („ponor“) napada osnovni cilj napadača jest privući gotovo sav promet iz određenog dijela mreže prema malicioznom čvoru, koji se figurativno nalazi u središtu „ponora“. Napadač to najčešće postiže na način da falsificira usmjerivačke informacije [56, 68]. Primjerice, napadač može oglasiti postojanje kvalitetne rute ka baznoj stanici (lažiranjem usmjerivačkih informacija). Na taj način napadač će privući sve susjedne čvorove da pakete namijenjene baznoj stanici proslijede upravo njemu. Uspješno izveden *sinkhole* napad omogućava jednostavno provođenje napada selektivnim prosljeđivanjem *(selective forwarding)*, budući da nakon uspješnog *sinkhole* napada sav promet iz određenog područja mreže prolazi preko malicioznog čvora. Na *sinkhole* napad u dobroj mjeri su otporni geografski usmjerivački protokoli. Radi se o protokolima koji se prilikom postupka usmjeravanja oslanjaju na podatke o točnoj geografskoj lokaciji pojedinih čvorova, dok se većina ostalih temelji na razmjeni (razašiljanju) usmjerivačkih informacija između čvorova.

4.1.3.4. Sybil napad

Sybil predstavlja napad kod kojega se napadač predstavlja mreži sa nekoliko različitih identiteta, tj. ostali čvorovi iz mreže napadača ne vide kao jednog, već kao nekoliko legitimnih čvorova. Pri tome se napadač može lažno predstavljati kao neki već postojeći mrežni čvor (preuzima njegov identitet) ili se predstaviti kao nekolicina novih legitimnih čvorova. *Sybil* napad prvi put je uočen i opisan u kontekstu *peer-to-peer* mreža, da bi se pojavom BSM zaključilo da on predstavlja opasnost i u takvom okruženju [67, 107].

Postoji nekoliko različitih varijanti *Sybil* napada. Jedan način provođenja ovog napada jest izravna komunikacija malicioznih čvorova sa legitimnim čvorovima. Druga mogućnost je da maliciozni čvorovi lažno oglašavaju dostupnost rute ka *Sybil* čvorovima (čvorovi koji zapravo ne postoje već predstavljaju lažne identitete napadača, dok ih legitimni čvorovi „vide“ kao normalne mrežne čvorove), pa im legitimni čvorovi prosljeđuju promet namijenjen *Sybil* čvorovima. Nadalje, *Sybil* napadi razlikuju se prema načinu preuzimanja identiteta. Prva mogućnost jest da napadač kreira nove lažne identitete, do tada nepostojeće u mreži. Druga mogućnost jest da napadač preuzme („ukrade“) identitet nekima od legitimnih čvorova. U BSM je često iz sigurnosnih razloga onemogućeno dodavanje novih čvorova, pa time i uvođenje novih identiteta u mrežu. Da bi proveo *Sybil* napad u takvoj situaciji napadač mora preuzeti identitete postojećih legitimnih čvorova, pri čemu legitimni čvorovi čiji su identiteti ukradeni bivaju privremeno onesposobljeni ili uništeni.

Problem preuzimanja identiteta postojećih čvorova od strane *Sybil* napadača vrlo je sličan problemu replikacije identiteta *(identity replication),* pri čemu se isti identitet koristi više puta i na različitim lokacijama unutar mreže. Napad replikacijom identiteta ipak se ne svrstava među *Sybil* napade, budući da kod ovakvog napada jedan uređaj (maliciozni čvor) ima jedan replicirani identitet (a ne kao kod *Sybil* napada, gdje jedan uređaj preuzima više identiteta).

Nadalje, podvrste *Sybil* napada moguće je razlikovati i na temelju kriterija simultanosti. Kod simultanog *Sybil* napada napadač pokušava istovremeno sudjelovati u mreži sa svim svojim lažnim identitetima. Budući da se napadačev hardver u jednom trenutku može ponašati samo kao jedan čvor, on mora ciklički mijenjati sve svoje lažne identitete, kako bi se iz perspektive legitimnih čvorova činilo da su svi ovi identiteti istovremeno prisutni u mreži.

Ovo je u većini slučajeva moguće, budući da napadač uglavnom raspolaže hardverom koji to može izvesti (npr. prijenosno računalo) dovoljno brzo kako bi bilo neprimjetno legalnim mrežnim čvorovima, koji raspolažu bitno manjim hardverskim resursima. Za razliku od ovakvog pristupa, moguć je i pristup kod kojeg napadač posjeduje veliki broj različitih identiteta tijekom određenog vremenskog intervala, ali ih ne koristi sve istovremeno (simultano). U tom slučaju se iz perspektive legalnih čvorova čini da neki čvorovi napuštaju mrežu, dok na njihova mjesta dolaze novi. Također je mogući scenarij u kojem napadač koristi nekoliko fizičkih uređaja (sa više različitih identiteta).

Različiti mrežni mehanizmi mogu biti osjetljivi na *Sybil* napad. Najizloženiji su mu mehanizmi za distribuiranu pohranu podataka i usmjerivački mehanizmi. U mreži može postojati mehanizam za distribuiranu pohranu podataka, pri čemu se redundancija postiže tako što se isti podatak pohranjuje na različitim lokacijama u mreži. Ukoliko napadač pomoću *Sybil* napada preuzme identitete svih ovih lokacija podatak se prividno nalazi distribuiran na nekoliko čvorova, dok se u stvarnosti nalazi pohranjen samo na jednom mjestu, na čvoru napadača (sličan problem kao u *peer-to-peer* mrežama). Na *Sybil* napade osjetljivi su i mehanizmi usmjeravanja. Posebno su osjetljivi mehanizmi koji omogućavaju višestazno *(multipath)* ili disperzno usmjeravanje. Pri tome je moguć scenarij kod kojeg nekoliko različitih putanja zapravo prolaze preko istog malicioznog čvora koji se predstavlja višestrukim identitetima. Čak su i geografski mehanizmi usmjeravanja (koji se oslanjaju na točne pozicije čvorova) osjetljivi na ovu vrstu napada, budući da se maliciozni čvor može prividno pojaviti sa bilo kojim koordinatama.

Radi uštede u resursima (prvenstveno energetskim) u senzorskim mrežama se do krajnjeg odredišta ne šalju podaci sa svih senzorskih čvorova, nego se vrši njihova agregacija unutar mreže. *Sybil* napad može ozbiljno ugroziti i postupak agregacije ubacujući lažne informacije među stvarne podatke. Naime, ukoliko napadač raspolaže samo sa jednim ili sa nekoliko malicioznih čvorova davanjem netočnih podataka neće moći u velikoj mjeri negativno utjecati na rezultat agregacije, budući da će većina ulaznih informacija biti korektne (sa legitimnih mrežnih čvorova). Međutim, ukoliko napadač primijeni *Sybil* napad on preuzima višestruki identitet (predstavlja se kao više čvorova na određenom području), te na taj način u velikoj mjeri može utjecati na rezultat agregacije namjernim davanjem krivih podataka.

Također, velik dio mrežnih mehanizama u BSM oslanja se na distribuirane algoritme, što podrazumijeva i distribuirano odlučivanje koje se u većini situacija odvija na temelju

„glasovanja“ svih čvorova *(voting)*. Zahvaljujući činjenici da posjeduje višestruke identitete napadač značajno može utjecati na rezultat glasovanja i time izravno utjecati na odlučivanje. Na ovaj način napadač može utjecati i na rad mehanizama za detekciju zlonamjernih čvorova (kod kojih se također odluke u većini slučajeva donose „glasovanjem“). Štoviše, napadač može legitimni čvor namjerno proglasiti zlonamjernim i zbog višestrukih identiteta „glasovanjem“ odlučiti da se legitimni čvor isključi iz mreže.

Mjere zaštite od *Sybil* napada moraju uključivati mogućnost provjere (validacije) identiteta čvorova. Zadaća ove provjere je utvrditi valjanost i jedinstvenost identiteta unutar mreže. Pri tome su moguće dvije vrste validacije: izravna i neizravna validacija. Izravna validacija podrazumijeva da senzorski čvor izravno provjerava identitet čvora s kojim stupa u komunikaciju. Neizravna validacija podrazumijeva da prethodno provjereni čvorovi obavljaju provjeru ostalih čvorova (rjeđe se susreće u praksi zbog distribuirane prirode mreže). Većina tehnika za prevenciju *Sybil* napada podrazumijeva metodu izravne validacije.

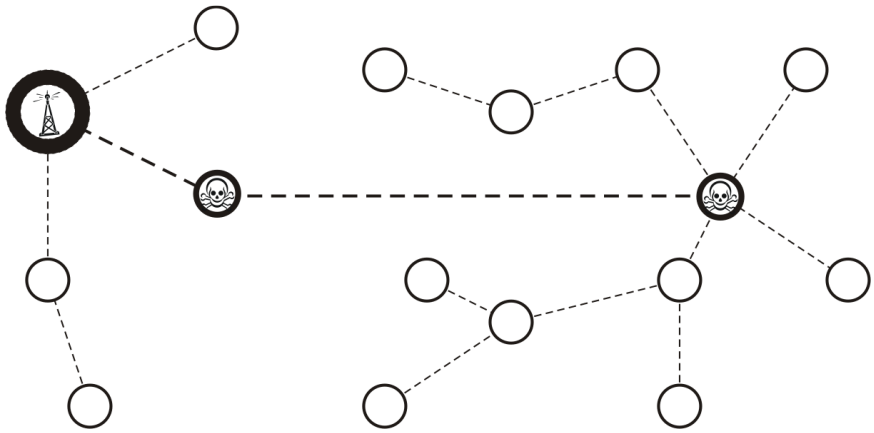
Jedna od učinkovitijih metoda otkrivanja *Sybil* napada jest testiranje radijskih resursa *(Radio Resource Testing)*. Ova metoda temelji se na pretpostavci da svaki senzorski čvor ima samo po jedan radio primopredajnik. Također, pretpostavka je da on ne može simultano obavljati slanje ili prijem podataka na više kanala. Ukoliko čvor želi provjeriti posjeduje li netko od njegovih susjeda lažni identitet (tj. je li neki od susjeda *Sybil* čvor) on svakom od svojih susjeda dodjeljuje različiti kanal za komunikaciju. Potom metodom slučajnog izbora „sluša“ neki od ovih kanala. Ukoliko je čvor kojemu je pridijeljen taj kanal legitiman on će primiti poruku. Drugi pristup zaštiti od *Sybil* napada podrazumijeva primjenu kriptografskih metoda, što za sobom povlači izbor odgovarajuće tehnike za predistribuciju kriptografskih ključeva. Jedan od najčešćih pristupa je predistribucija određenog broja ključeva slučajnim izborom, tako da susjedni čvorovi među ključevima koji su im dodijeljeni mogu pronaći jedan zajednički ključ (ili ga određenim metodama izračunati).

4.1.3.5. Wormhole napad („crvotočina“)

Kod *wormhole* napada napadač kreira brzi link male latencije od jednog do drugog dijela mreže („crvotočina“). Zahvaljujući ovom linku napadač je u mogućnosti tunelirati poruke primljene u jednom dijelu mreže i ponoviti ih u drugom udaljenom dijelu mreže. Pri tome je

karakteristično da link koji povezuje udaljene dijelove mreže ima manju latenciju nego regularni linkovi u mreži. Najjednostavniji oblik ovog napada podrazumijeva maliciozni čvor postavljen između dva legitimna čvora, pri čemu maliciozni čvor vrši prosljeđivanje poruka između dva legitimna čvora. Nešto složenija i puno češća varijanta *wormhole* napada je scenarij u kojem napadač raspolaže sa dva uređaja (najčešće se radi o prijenosnim računalima). Ovi uređaji međusobno su povezani brzim linkom niske latencije, na kanalu koji nije dostupan legitimnim čvorovima, tako da legitimni mrežni čvorovi nisu niti svjesni postojanja ovog linka (on je dostupan isključivo napadaču).

Napadač postavljanjem malicioznog čvora blizu bazne stanice i kreiranjem „crvotočine“ *(wormhole)* koja ga povezuje sa udaljenim dijelom mreže u potpunosti može poremetiti mehanizam usmjeravanja u mreži. Zahvaljujući tunelu („crvotočini“) napadač može „uvjeriti“ čvorove koji se nalaze u udaljenom dijelu mreže (više skokova udaljeni od bazne stanice) da se nalaze samo jedan ili dva skoka (kroz tunel) od bazne stanice. Na taj način se u udaljenom dijelu mreže kreira „ponor“ *(sinkhole)* sa malicioznim čvorom u središtu, prema kojem se usmjerava promet sa velikog broja legitimnih čvorova. „Ponor“ se kreira zbog činjenice da maliciozni čvor na udaljenom kraju tunela na umjetan način (zahvaljujući tunelu) pruža kvalitetnu rutu ka baznoj stanici (mali broj skokova i niska latencija), puno kvalitetniju od alternativnih legitimnih ruta. Kada je krajnja točka tunela relativno udaljena od bazne stanice gotovo sav mrežni promet iz udaljenog dijela mreže bit će usmjeren ka njoj (slika 4.1).



Slika 4.1 Wormhole napad

Kreiranjem „crvotočine“ napadač može izravno utjecati na „uvjete utrkivanja“ koji postoje kod nekih mehanizama usmjeravanja *(routing race conditions)*. Naime, kod nekih mehanizama usmjeravanja čvor poduzima određene akcije inicirane prvom instancom poruke

koju dobije od svojih susjeda (kasnije primljene instance iste poruke se ignoriraju). Budući da raspolaže brzim linkom napadač odgovarajuću poruku (koja sadrži usmjerivačke informacije) može isporučiti brže nego što bi ona stigla legalnim putem (preko više skokova). Na taj način napadač može posredno utjecati na topologiju mreže, čak i u slučaju da se u mreži koriste mehanizmi za enkripciju i provjeru autentičnosti. Naime, zahvaljujući „crvotočini“ napadač će jednostavno „uvjeriti“ dva udaljena čvora da su susjedi, te usmjeravati pakete između njih. *Wormhole* napadi se najčešće događaju u kombinaciji sa drugim vrstama napada, poput selektivnog prosljeđivanja *(selective forwarding)*, prisluškivanja *(eavesdropping)* ili *Sybil* napada, što dodatno i znatno otežava njihovo otkrivanje.

Jedan od mogućih pristupa za otkrivanje i obranu od *wormhole* napada opisan u [43] primjenjiv je i u bežičnim senzorskim mrežama. Ovaj pristup uvodi pojam „paketne trake“ *(packet leash)*. „Paketna traka“ zapravo predstavlja dodatnu informaciju koja se dodaje paketu kako bi se ograničila maksimalna dozvoljena udaljenost na koju se paket prenosi. Postoje „vremenske trake“ *(temporal leashes)* i „geografske trake“ *(geographical leashes)*. Geografske trake osiguravaju da se primatelj paketa nalazi unutar određene maksimalne geografske udaljenosti od pošiljatelja. Vremenske trake osiguravaju da paket ima definirano maksimalno „vrijeme života“, čime se također (posredno) ograničava udaljenost na koju ga se može prenijeti. Primjena vremenske ili geografske trake omogućava primatelju da utvrdi je li paket putovao dalje nego što je dopušteno ograničenjem unutar trake.

Za konstrukciju geografske trake čvorovi moraju poznavati svoju točnu geografsku lokaciju i moraju imati međusobno strogo sinkronizirane satove. Prilikom slanja paketa pošiljatelj dodaje informaciju o svojoj točnoj poziciji kao i o točnom vremenu slanja. Prilikom prijema primatelj ove informacije uspoređuje s podacima o vlastitoj poziciji i vremenu prijema paketa. Ukoliko je poznato maksimalno odstupanje između satova predajnika i prijemnika, kao i gornja granica brzine prijenosa, moguće je odrediti gornju granicu udaljenosti između predajnika i prijemnika.

$$d_{sr} \leq \|p_s - p_r\| + 2v(t_r - t_s + \Delta) + \delta$$

gdje je:

d_{sr} – udaljenost između predajnika i prijemnika

p_s – lokacija predajnika

p_r – lokacija prijemnika

v – maksimalna brzina bilo kojeg čvora

t_r – vrijeme prijema paketa (lokalno na prijemniku)

t_s – vrijeme slanja paketa (iz vremenske značke paketa)

Δ - maksimalno odstupanje satova na čvorovima

δ - maksimalna pogreška u podacima o lokaciji

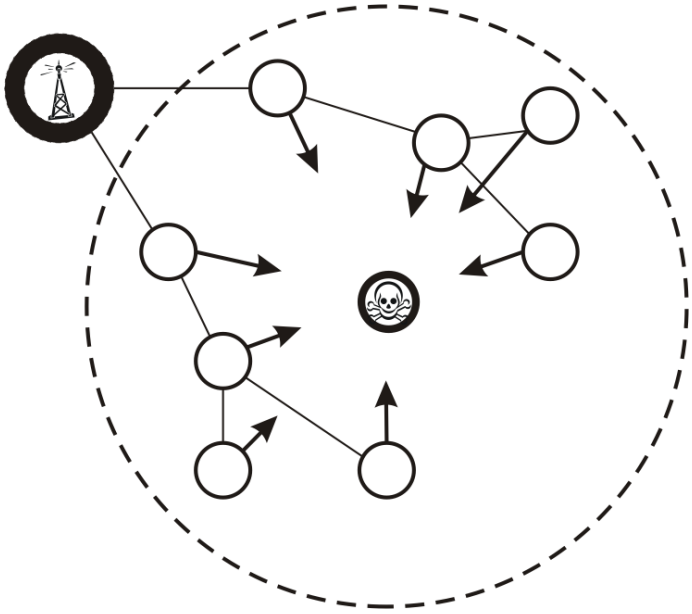
U određenim situacijama čak i limitiranje udaljenosti između izvorišnog i odredišnog čvora može biti nedovoljno za sprečavanje *wormhole* napada. Primjerice, u slučaju da određena fizička prepreka onemogućava regularnu komunikaciju između dva čvora (koji bi inače bili u međusobnom dometu) moguće je uspostavljanje „crvotočine“ između ova dva čvora koja se ne može otkriti na temelju njihove fizičke udaljenosti.

Za konstrukciju vremenske trake *(temporal leash)* satovi na svim čvorovima moraju biti strogo sinkronizirani, uz maksimalno odstupanje Δ, čiji iznos mora biti poznat svim čvorovima. Za praktičnu učinkovitost ove metode iznos Δ bi trebao biti najviše reda veličine nekoliko mikrosekundi, što je poprilično teško postići u uvjetima kakvi postoje u većini bežičnih senzorskih mreža, a dodatni problem je činjenica da je i sam signal vremenske sinkronizacije podložan napadu i zlonamjernoj modifikaciji. Jedna mogućnost je da pošiljatelj u vremensku traku upisuje točno vrijeme slanja paketa, koje primatelj uspoređuje s vremenom prijema. Druga mogućnost je da pošiljatelj u vremensku traku upisuje vrijeme do kojeg paket mora stići na odredište *(expiration time)*.

4.1.3.6. Napadi poplavljivanjem HELLO paketima (HELLO flood attacks)

Većina usmjerivačkih protokola u bežičnim senzorskim mrežama podrazumijeva da senzorski čvorovi svoje susjedne čvorove o svojem statusu izvještavaju razašiljanjem *(broadcast)* pozdravnih (HELLO) poruka. Senzorski čvor koji primi HELLO poruku zaključuje da se nalazi u dometu radijske veze s pošiljateljem, odnosno zaključuje da su susjedi. Međutim, ovaj mehanizam se lako može zlorabiti. Primjerice, napadač sa prijenosnim računalom može razašiljati informacije većom predajnom snagom nego što je to u mogućnosti legitimni čvor. Na taj način napadač može pokriti cijelu ili veći dio mreže i lažno uvjeriti legitimne čvorove da je njihov susjed. Napadač pri tome može oglašavati da je povezan vrlo kvalitetnom rutom sa baznom stanicom, te na taj način navesti legitimne mrežne čvorove da

ga uvrste kao sljedeći korak (skok) na svoju rutu ka baznoj stanici [41]. Međutim, budući da je u stvarnosti maliciozni čvor izvan radijskog dometa senzorskih čvorova u mreži nastaje konfuzija budući da senzorski čvorovi uzaludno nastoje poslati pakete. Ova vrsta napada ima izravan utjecaj na sve mrežne protokole koji se temelje na lokaliziranoj razmjeni informacija između susjednih čvorova radi održavanja mrežne topologije ili kontrole toka podataka. Za provođenje *Hello Flood* napada napadač ne mora čak niti kreirati legitimni promet (nove HELLO poruke). Dovoljno je da ponovno razašilje HELLO poruke koje je primio, samo sa većom predajnom snagom kako bi pokrio cijelu mrežu (slika 4.2).



Slika 4.2 Poplavljivanje HELLO porukama

Budući da napadi poplavljivanjem predstavljaju prilično velik problem u senzorskim mrežama, postoji više prijedloga za odgovarajuće protumjere protiv ove vrste napada. Najjednostavnija metoda obrane od *Hello Flood* napada jest provjera dvosmjernosti (bidirekcionalnosti) pojedinih linkova, prije no što se poduzme bilo kakva akcija na temelju primljene HELLO poruke. Međutim, ovakva metoda je manje učinkovita ukoliko napadač raspolaže osjetljivijim radio-prijemnikom i snažnijim radio-predajnikom, budući da bi u tom slučaju linkovi između napadača i legitimnih čvorova bili dvosmjerni i *Hello Flood* napad lokalno ne bi mogao biti otkriven. Moguće rješenje problema je pristup u kojem čvor najprije mora utvrditi autentičnost svojih susjeda (autentificirati ih), što za sobom povlači nužnost implementacije odgovarajućeg protokola za provjeru autentičnosti [104].

Za prevenciju napada poplavljivanjem primjenjuju se i kriptografske metode. Primjena kriptografskih metoda podrazumijeva da senzorski čvorovi posjeduju odgovarajuće tajne ključeve (budući da se u pravilu radi o metodama simetrične kriptografije).

4.1.3.7. Lažiranje potvrde (acknowledgement spoofing)

Usmjerivački algoritmi koji se primjenjuju u bežičnim senzorskim mrežama često koriste mehanizam potvrde (npr. potvrda o uspješnom prijemu paketa). Ovaj mehanizam se također može lako zlorabiti od strane zlonamjernog napadača. Napadač može osluškivati promet koji se šalje njegovim susjedima. Potom napadač lažira informacije u potvrdnom paketu, odnosno šalje lažnu potvrdu o prijemu paketa. Na taj način, primjerice, napadač može prividno „oživjeti“ nekog od čvorova koji zapravo više nisu aktivni (npr. prestali su s radom zbog gubitka napajanja).

4.1.4. Sigurnosne prijetnje na transportnom sloju

Transportni sloj u slojevitom mrežnom modelu primijenjenom na bežične senzorske mreže odgovoran je za upravljanje konekcijama „s kraja na kraj“ *(end-to-end)*. Neki od napada na sigurnost bežične senzorske mreže usmjereni su upravo na ovaj sloj.

4.1.4.1. Poplavljivanje (flooding)

U bilo kojoj situaciji u kojoj komunikacijski protokol mora održavati stanje konekcije moguće je primijeniti metodu iscrpljivanja resursa poplavljivanjem. Primjerice, napadač može slati opetovane zahtjeve za konekcijom sve dok se resursi koje je potrebno alocirati za svaku konekciju u potpunosti ne iscrpe ili dosegnu gornju granicu uporabe. U tom slučaju daljnji legitimni zahtjevi za konekcijom bit će ignorirani zbog nedostatka resursa. Jedan od mogućih pristupa za sprečavanje poplavljivanja jest postavljanje „zagonetke“ *(puzzle)* klijentu koji pokušava ostvariti konekciju. Ovaj pristup zasniva se na ideji da klijent neće uzaludno trošiti

resurse na rješavanje „zagonetke“ (pogotovo ako se radi o strogo ograničenim resursima senzorskog čvora) ukoliko doista ne želi ostvariti konekciju. Budući da niti napadač nema na raspolaganju beskonačno velike resurse on neće biti u mogućnosti dovoljno brzo slati zahtjeve za konekcijom (budući da mora prije svakog pokušaja konekcije riješiti „zagonetku“) da bi na taj način onemogućio pristup serverskom čvoru. Međutim, ovakav pristup zaštiti od poplavljivanja nije pretjerano učinkovit u situacijama kada napadač raspolaže višestruko većim resursima od regularnih mrežnih čvorova (primjerice, prijenosno računalo u odnosu na bežični senzorski čvor). Nadalje, rješavanje „zagonetke“ unosi i potrebu za dodatnim procesiranjem, što troši resurse i legitimnim čvorovima. Međutim, u većini slučajeva je i ovo prihvatljivije od prekomjerne komunikacije, budući da radio primopredajnik troši i do 1000 puta više energije od mikroprocesora.

4.1.4.2. Desinkronizacija (desynchronization)

Pod desinkronizacijom se obično podrazumijeva ometanje ili potpuni prekid postojeće konekcije. Napadač primjerice može opetovano slati lažne poruke klijentu pomoću kojih zahtijeva retransmisiju izgubljenih okvira. Na taj način napadač bitno degradira komunikaciju (a može je čak i prekinuti) tako što prisiljava čvorove na oporavak od pogrešaka koje zapravo nisu niti postojale. Moguće rješenje ovog problema podrazumijeva implementaciju autentifikacijskih mehanizama koji omogućavaju autentifikaciju svakog pojedinačnog paketa, te na taj način onemogućavaju napadaču slanje lažnih poruka klijentu.

4.1.5. Sigurnosne prijetnje na aplikacijskom sloju

Određeni broj sigurnosnih prijetnji koje postoje u bežičnim senzorskim mrežama usmjeren je izravno na aplikacijski sloj slojevitog mrežnog modela.

4.1.5.1. Napad „obasipanjem“ (overwhelm attack)

Pod napadom „obasipanjem“ *(overwhelm attack)* podrazumijeva se pokušaj napadača da prekomjerno stimulira senzore na čvorovima u BSM. Na taj način napadač izaziva slanje velike količine informacija putem bežične senzorske mreže prema baznoj stanici, što u većoj mjeri iscrpljuje mrežne resurse (propusnost mreže, kapacitet napajanja). Ovakve napade vrlo je teško izbjeći, no moguće je poduzeti odgovarajuće mjere kako bi se njihov negativni učinak smanjio. Potrebno je što preciznije podesiti senzore, kako bi reagirali isključivo na specifični fenomen, a ne bi ga stimulirali drugi slični fenomeni (npr. senzor koji treba detektirati kretanje vozila ne bi se smio aktivirati kretanjem pješaka). Nadalje, poželjno je ograničiti učestalost slanja podataka sa senzora ka baznoj stanici. Također, primjena učinkovitih algoritama za agregaciju podataka u senzorskoj mreži također umanjuje negativne učinke *overwhelm* napada.

4.1.5.2. Napad reprogramiranjem (reprogram attack)

U većini bežičnih senzorskih mreža postoji mogućnost udaljenog reprogramiranja senzorskih čvorova putem mreže (bez potrebe za neposrednim fizičkim pristupom čvoru koji se reprogramira). Iako ovakvi mehanizmi pružaju veliki komfor prilikom upravljanja senzorskom mrežom (pogotovo mrežom sa većim brojem čvorova raspoređenim na velikom prostoru) oni mogu predstavljati velik sigurnosni problem ukoliko nisu adekvatno zaštićeni. Ukoliko napadač dobije pristup ovom mehanizmu u mogućnosti je reprogramirati čvorove prema vlastitom nahođenju i na taj način ovladati cjelokupnom mrežom ili njezinim većim dijelom. Zbog toga je iznimno preporučljivo iz sigurnosnih razloga onemogućiti udaljeno programiranje čvorova u mrežama u kojima ono uistinu nije krajnje neophodno.

4.1.6. Usporedni prikaz napada u BSM

U tablici 4.1 dan je sažeti prikaz karakterističnih napada i mogućih protumjera koje je moguće poduzeti radi njihove prevencije ili ublažavanja njihovih posljedica.

TABLICA 4.1 Usporedni prikaz napada u BSM

Sloj	Napad	Moguće protumjere
Fizikalni sloj *(Physical layer)*	Elektroničko ometanje *(jamming)*	FHSS *(Frequency-Hopping Spread Spectrum)*
	Neovlašteni fizički pristup *(tampering)*	Fizička zaštita senzorskih čvorova
Sloj podatkovnog linka *(Data link layer)*	Kolizija *(collision)*	Uporaba kodova za ispravljanje pogrešaka *(error correcting codes)*
	Iscrpljivanje resursa *(resource exhaustion)*	Ograničenje učestalosti pristupa mediju (na MAC sloju) i primjena vremenskog multipleksiranja
	„Nepoštenje“ *(unfairness)*	Uporaba manjih podatkovnih okvira
Mrežni sloj *(Network layer)*	Napadi na usmjerivačke informacije	Dodavanje autentifikacijskog koda na kraj svake poruke *(MAC, Message Authentication Code)*; Implementacija brojača ili vremenskih oznaka pojedinih poruka
	Selektivno prosljeđivanje *(selective forwarding)*	Uporaba višestrukih ruta i prosljeđivanje prometa različitim rutama
	„Sinkhole“ napad („ponor“)	Primjena „geografskih“ usmjerivačkih protokola
	„Sybil“ napad	Mehanizam za provjeru identiteta čvorova (izravnu ili neizravnu); Testiranje radijskih resursa *(Radio Resource Testing)*; Primjena kriptografskih metoda
	„Wormhole“ napad („crvotočina“)	Paketne trake *(packet leashes)*: vremenske *(temporal)* i geografske *(geographical)* – za ograničenje udaljenosti na koju se paket prenosi
	Poplavljivanje HELLO porukama *(HELLO flooding)*	Provjera dvosmjernosti pojedinih linkova uz autentifikaciju susjednih čvorova; primjena kriptografskih metoda
	Lažiranje potvrde *(acknowledgement spoofing)*	Mehanizmi za autentifikaciju
Transportni sloj *(Transport layer)*	Poplavljivanje *(flooding)*	Postavljanje „zagonetke“ *(puzzle)* klijentu koji pokušava ostvariti konekciju
	Desinkronizacija *(desynchronization)*	Mehanizmi za autentifikaciju svakog pojedinačnog paketa
Aplikacijski sloj *(Application layer)*	Napad „obasipanjem“ *(overwhelm attack)*	Precizno ugađanje senzora (kako bi reagirao isključivo na specifični fenomen); Ograničavanje učestalosti slanja podataka ka baznoj stanici; Primjena učinkovitih algoritama za agregaciju podataka
	Napad reprogramiranjem *(reprogram attack)*	Onemogućavanje udaljenog programiranja senzorskih čvorova

4.2. Otkrivanje upada u bežičnim senzorskim mrežama

4.2.1. Sustavi za otkrivanje upada – vrste i način rada

Štete prouzrokovane neovlaštenim upadima u računalne sustave i zlonamjernim ponašanjem mrežnih čvorova mogu biti ogromne i sa nesagledivim posljedicama. Zbog toga su znatni istraživački napori uloženi u razvoj i implementaciju sustava za otkrivanje neovlaštenih upada *(IDS, Intrusion Detection System)*, koji danas predstavljaju jedan od najvažnijih sigurnosnih mehanizama koji se primjenjuju za zaštitu računalnih i telekomunikacijskih mreža. Intenzivno istraživanje u području IDS sustava započelo je još prije tridesetak godina, u vrijeme apsolutne dominacije žičnih mreža. Iako IDS sustavi namijenjeni žičnim mrežama i dalje napreduju, danas ih se zasigurno može smatrati razvijenom i zrelom tehnologijom [9, 65, 95].

Pojava i naglo širenje bežičnih mreža svih mogućih vrsta (od osobnih, preko lokalnih pa sve do regionalnih) postavlja nove izazove u razvoju IDS sustava za bežične mreže. Nadalje, bežično mrežno okruženje po pitanju sigurnosti puno je zahtjevnije od žičnih mreža jer je bežična mreža zbog otvorene prirode medija znatno izloženija različitim sigurnosnim prijetnjama. Širenje bežičnih mreža u središte pozornosti postavilo je razvoj sustava za otkrivanje neovlaštenih upada u bežičnim ad hoc mrežama *(MANET, Mobile Ad Hoc Network)* [52, 64]. Pojavom bežičnih senzorskih mreža *(WSN, Wireless Sensor Network)* kao specijalne podvrste bežičnih ad hoc mreža javlja se potreba za razvojem odgovarajućih IDS sustava i za BSM. Iako BSM imaju određene sličnosti sa MANET mrežama, one se od njih u velikoj mjeri i razlikuju, prvenstveno u pogledu dostupnih resursa (energetskih i računalnih). Zbog ovih razlika postojeća rješenja za otkrivanje upada u MANET mrežama ne mogu se izravno primijeniti u senzorskim mrežama, nego je nužno pristupiti razvoju IDS sustava specijaliziranih za bežične senzorske mreže. Razvoj IDS sustava prilagođenih bežičnim senzorskim mrežama danas predstavlja područje vrlo intenzivnog istraživanja [55, 58, 120, 127].

Sustavi za otkrivanje neovlaštenih upada (IDS sustavi) zapravo predstavljaju softverske ili hardverske sustave koji automatiziraju postupak nadzora nad događanjima u računalnom sustavu ili mreži, analizirajući ih u potrazi za naznakama sigurnosnih problema. Pod pojmom „neovlaštenog upada“ podrazumijevaju se svi pokušaji koji imaju za cilj kompromitaciju

povjerljivosti, integriteta ili dostupnosti mrežnog uređaja ili cjelokupne mreže, kao i svi pokušaji zaobilaska sigurnosnih mehanizama. Neovlašteni upad može izvršiti napadač izvan sustava ili autorizirani korisnik sustava koji pokušava ostvariti dodatne privilegije (ovlasti) ili zlorabiti postojeće.

Danas postoji više različitih tipova IDS sustava, no funkcioniranje svakog od njih se generički može razložiti na tri komponente:

- **Prikupljanje informacija**
  IDS sustavi koriste različite izvore informacija o događajima u sustavu kako bi mogli odrediti je li došlo do neovlaštenog upada. Ovi izvori informacija mogu biti na različitim razinama sustava (npr. na razini mreže, na razini pojedinačnih čvorova u mreži, ili čak na razini pojedinačne aplikacije koja se izvršava na nekom čvoru u mreži).
- **Analiza informacija**
  Prikupljene informacije analitički dio IDS sustava organizira i obrađuje, te na temelju dobivenih rezultata utvrđuje je li došlo do neovlaštenog upada. Dva najčešća pristupa pri analizi informacija su detekcija zlouporabe *(misuse detection)* i detekcija anomalija *(anomaly detection)*.
- **Reakcija (odgovor)**
  Funkcionalna komponenta IDS sustava zadužena za reakciju u slučaju otkrivanja neovlaštenog upada obuhvaća skup akcija i mjera koje sustav poduzima u slučaju da se upad događa ili se već dogodio. Ove mjere se obično dijele na aktivne (koje podrazumijevaju neki oblik automatske intervencije) i pasivne (koje podrazumijevaju obavještavanje ovlaštene osobe, od koje se potom očekuje poduzimanje daljnje akcije).

Klasifikaciju IDS sustava moguće je napraviti na temelju više različitih kriterija. Na osnovu upravljačke (kontrolne) strategije IDS sustave je moguće podijeliti na centralizirane, djelomično distribuirane i potpuno distribuirane. Kod centraliziranih sustava upravljanje funkcijama nadzora, detekcije i izvještavanja obavlja se sa jedne središnje lokacije. Kod djelomično distribuiranog IDS sustava funkcijama nadzora i detekcije upravlja se sa lokalnih upravljačkih čvorova koji su hijerarhijski povezani sa jednom ili više središnjih lokacija. Kod potpuno distribuiranog IDS sustava sve odluke vezane za nadzor, detekciju i reakcije na napade donose se na samom mjestu analize, na lokalnim čvorovima [105].

Na osnovu vremena koje protekne između bilježenja različitih događaja i njihove analize razlikuju se intervalni i stvarno-vremenski IDS sustavi. Kod intervalnih IDS sustava *(Interval-Based IDS* ili *Batch Mode IDS)* tok informacija od točke nadzora do mjesta njihove analize nije kontinuiran. Informacije se prikupljaju i pohranjuju, pa u određenim vremenskim intervalima šalju na analizu. Kod stvarno-vremenskih IDS sustava *(Real-Time IDS* ili *Continuous IDS)* postoji kontinuirani tok informacija (u realnom vremenu) od mjesta prikupljanja do mjesta analize. Ovakvi IDS sustavi su u stanju u stvarnom vremenu i poduzeti potrebnu reakciju na detektirani napad.

Najčešći kriterij klasifikacije IDS sustava jest izvor informacija (područje iz kojeg sustav prikuplja informacije). Prema ovom kriteriju IDS sustave je moguće podijeliti na mrežno-orijentirane *(Network-Based IDS, NIDS)*, računalno-orijentirane *(Host-Based IDS, HIDS)* i aplikacijski orijentirane IDS sustave *(Application-Based IDS, AIDS)*, koji zapravo predstavljaju podvrstu računalno-orijentiranih IDS sustava.

Mrežno-orijentirani IDS sustav (NIDS) prati promet na mrežnom segmentu ili na preklopniku *(switch)*, te na taj način može štititi više mrežnih čvorova istovremeno. NIDS sustav se može sastojati i od više modula postavljenih na različite pozicije unutar mreže. Glavne prednosti NIDS sustava su mogućnost zaštite više mrežnih čvorova (čak se i relativno velika mreža može nadzirati i štititi sa samo nekoliko dobro postavljenih NIDS sustava), vrlo mali utjecaj na postojeću mrežu (obično se radi o pasivnim modulima koji „osluškuju“ mrežni promet bez ikakvih utjecaja i smetnji za normalan rad mreže) i mogućnost postizanja visoke razine zaštite od napada uz vrlo dobru prikrivenost (teško su vidljivi napadaču). Nedostatak NIDS sustava dolazi do izražaja u velikim mrežama i mrežama sa velikom količinom prometa, kada sustav može imati poteškoća prilikom procesiranja svih paketa, te se može dogoditi da sustav ne detektira pokušaje napada koji se dogode u trenucima velikog opterećenja mreže (problem se donekle može riješiti implementacijom potpunih hardverskih rješenja NIDS sustava, čime se postižu veća brzina i učinkovitost analize paketa). Dodatni problem predstavlja podjela mreže na više malih segmenata (pomoću preklopnika) čime se umanjuje glavna prednost NIDS sustava – mogućnost zaštite velikog broja čvorova odjednom. Problem NIDS sustavu može stvarati i enkripcija podataka (problem je sve više izražen s porastom uporabe virtualnih privatnih mreža, VPN).

Računalno-orijentirani IDS sustav (HIDS) prikuplja i analizira podatke i mrežni promet sa pojedinačnih računala (mrežnih čvorova), uglavnom prikupljajući podatke iz sistemskih

zapisa. Njihova prednost je mogućnost detekcije nekih pokušaja napada koji su „nevidljivi“ NIDS sustavu, kao i mogućnost rada u okruženju u kojem se koristi enkripcija (budući da dolazni promet mogu analizirati nakon dekriptiranja, a odlazni promet prije enkripcije). Također, na HIDS sustave ne utječe podjela mreže na manje segmente. Glavni nedostaci HIDS sustava su: povećani rizik da napadač prilikom napada onesposobi i sam HIDS sustav (budući da se izvori informacija i dio sustava zadužen za njihovu analizu nalaze na istom čvoru), otežana detekcija malicioznih aktivnosti usmjerenih na cjelokupnu mrežu (npr. pokušaj skeniranja mreže), mogućnost onesposobljavanja HIDS sustava pomoću *Denial of Service* napada, moguć pad performansi mreže (budući da dio resursa mrežnog čvora troši HIDS sustav).

Aplikacijski-orijentirani IDS sustavi (podvrsta HIDS sustava) usmjereni su na praćenje događaja povezanih sa pojedinačnom aplikacijom. Glavna prednost im je mogućnost nadzora interakcije između korisnika i aplikacije (što omogućava praćenje neautoriziranih aktivnosti pojedinih korisnika), kao i mogućnost rada u okruženju u kojem se koristi enkripcija. Nedostatak ovakvog sustava proizlazi iz činjenice da nadzire događaje na apstraktnoj korisničkoj razini, pa često nije u stanju detektirati određene vrste malicioznog softvera.

Kod IDS sustava postoje dva osnovna pristupa analizi događaja s ciljem otkrivanja napada – detekcija zlouporabe *(misuse detection)* i detekcija anomalija *(anomaly detection)*. Detekcija zlouporabe primjenjuje se u većini postojećih sustava, dok je tehnika detekcije anomalija još uvijek predmet intenzivnog istraživanja, pa se stoga rjeđe susreće implementirana u sustav. Kod detekcije zlouporabe analizira se aktivnost sustava u potrazi za događajima (ili nizovima događaja) koji odgovaraju predefiniranom uzorku („potpisu“) koji opisuje poznati napad. Ovakvi sustavi su brzi i učinkoviti, stvaraju vrlo mali broj lažnih uzbuna, no mogu otkriti samo poznate napade (tj. napade čiji „potpis“ imaju pohranjen u svojoj bazi). Sustavi zasnovani na tehnici detekcije anomalija identificiraju abnormalna i neobična ponašanja (anomalije) na računalu ili mreži. Tijekom određenog vremena normalnog rada sustav prati ponašanje korisnika, računala ili mreže, te na temelju prikupljenih rezultata formira se profil koji reprezentira normalno stanje sustava. Napadi se otkrivaju na temelju prepoznavanja odstupanja ponašanja sustava od ovoga profila. Ovakvi sustavi proizvode nešto veći broj lažnih alarma, no u mogućnosti su prepoznati i neke nove varijante napada. Neke od mjera i tehnika koje se mogu koristiti prilikom detekcije anomalija su:

- **Detekcija praga *(threshold detection)***

  Ovaj pristup temelji se na brojanju događaja koji na određeni način karakteriziraju ponašanje korisnika ili sustava (npr. broj datoteka kojima se pristupa tijekom određenog vremenskog intervala, broj neuspješnih pokušaja prijavljivanja u sustav, broj odbačenih mrežnih paketa, zauzeće procesora od strane nekog procesa i sl.), pri čemu se za svaki promatrani atribut postavljaju granice unutar kojih se vrijednost smatra normalnom (dozvoljenom). Ove granice mogu biti fiksne, a mogu se i heuristički mijenjati.
- **Statistička mjerenja *(statistical measures)***

  Statistička mjerenja mogu biti parametarska (kod kojih se pretpostavlja da razdioba vrijednosti promatranih atributa odgovara zadanom modelu) i neparametarska (kod kojih se razdioba vrijednosti atributa „uči“ na temelju prošlih vrijednosti promatranih tijekom određenog razdoblja).
- **Mjerenja temeljena na pravilima *(rule-based measures)***

  Ova mjerenja slična su neparametarskim statističkim mjerenjima po tome što se šabloni prihvatljive uporabe definiraju na temelju podataka dobivenih promatranjem tijekom određenog vremena, no razlikuju se po tome što su ovi šabloni specificirani kao pravila, a ne kao numeričke vrijednosti.
- **Ostali tipovi mjerenja** (uključuju neuronske mreže, genetičke algoritme i modele imunih sustava)

Detekcija praga i statistička mjerenja koriste se u komercijalnim IDS sustavima, dok je primjena ostalih spomenutih metoda uglavnom u eksperimentalnoj fazi. Sa pojavom IPv6 protokola postojao je problem podrške IDS sustava za novi protokol. U posljednje vrijeme sve više IDS sustava (kako komercijalnih, tako i nekomercijalnih) implementira punu podršku za IPv6 protokol.

4.2.2. Mogućnosti implementacije IDS sustava u BSM

Razvoj IDS sustava za bežične senzorske mreže susreće niz novih, dodatnih izazova koji nisu bili prisutni u infrastrukturnim IEEE 802.11 bežičnim mrežama ili MANET mrežama. Iako dostignuća i rezultati istraživanja do kojih se došlo u MANET mrežama mogu poslužiti

kao polazna točka u istraživanju IDS sustava za BSM, zbog specifične prirode bežičnih senzorskih mreža nije moguća primjena postojećih rješenja iz MANET mreža [62, 74, 112].

U klasičnim žičnim mrežama da bi pokrenuo napad i kompromitirao mrežnu sigurnost napadač je morao ostvariti fizički pristup mediju. U tipičnim infrastrukturnim bežičnim mrežama komunikacija između pristupne točke i klijenata je bežična, i napadaču je dovoljno da se nalazi bilo gdje u dometu radio primopredajnika da bi mogao pratiti mrežni promet, što predstavlja dodatni sigurnosni izazov mrežnom administratoru. Prilikom napada na žične mreže napadač obično ima za cilj kompromitirati mrežu, ostvariti neautorizirani pristup informacijama ili zlorabiti mrežne resurse za pokretanje drugog, opsežnijeg napada. Osim navedenih motiva, čest motiv napada na bežične mreže jest „krađa usluge“, najčešće u vidu povezivosti sa Internetom. Najčešći ciljevi i motivi napada na bežične senzorske mreže su remećenje ili potpuni prekid rada mreže, davanje lažnih informacija aplikaciji koja pomoću senzorske mreže prikuplja određene podatke ili neovlašteni pristup podacima pohranjenim u mreži (najčešće koncentriranim na baznoj stanici). Čest cilj napada upravo je bazna stanica (budući da sadrži podatke sa gotovo svih senzora), no na sreću ona je uglavnom i tehnološki naprednija od preostalih senzorskih čvorova, što joj omogućava implementaciju odgovarajućih naprednijih i zahtjevnijih zaštitnih mehanizama.

Implementacija IDS sustava u bežičnu senzorsku mrežu predstavlja vrlo velik izazov s obzirom na ograničene resurse, kao i brojne druge faktore koji izravno utiču na izbor odgovarajuće tehnike za otkrivanje upada koja će se primijeniti u BSM [7, 8, 18, 39, 94]. Neki od značajnijih faktora koji utječu na metode pristupa problemu otkrivanja upada u BSM su:

- **Mrežna topologija**

  Fizičko pozicioniranje senzorskih čvorova mora osigurati minimalnu razinu povezivosti i u većini slučajeva dovoljnu redundanciju. Iako BSM karakterizira mogućnost samostalnog organiziranja, ono se uglavnom odnosi na samostalno otkrivanje ruta ka baznoj stanici, a ne i na fizičko pozicioniranje čvorova. Čvorove unutar mreže fizički najčešće raspoređuje administrator, koji na taj način ima izravan utjecaj na topologiju mreže. U senzorskim mrežama najčešće se susreće potpuno isprepletena mrežna topologija *(mesh)*, budući da je najotpornija na kvarove i kompromitaciju čvorova. Kod stablaste *(tree)* topologije postoji opasnost od prekida veze s pojedinim dijelovima mreže uslijed kvara ili kompromitacije nekih čvorova.

Osim bazne stanice, napadima su najčešće izloženi čvorovi bliži baznoj stanici, budući da se na njima nalazi veća količina informacija nego na perifernim čvorovima.

- **Pokretljivost čvorova (pokretljivi ili stacionarni čvorovi)**

  Bežični senzorski čvorovi i bazna stanica u senzorskoj mreži mogu biti pokretljivi (mobilni) ili fiksni (stacionarni), a može postojati i kombinacija pokretljivih i fiksnih čvorova u mreži.

- **Otvorenost mreže (otvorena ili zatvorena senzorska mreža)**

  Otvorena senzorska mreža dozvoljava priključivanje novih čvorova u mrežu na ad hoc načelu, dok zatvorena mreža sprečava naknadno samostalno priključivanje čvorova. Zatvorena mreža omogućava više administrativne kontrole nad pojedinačnim čvorovima. Unutar zatvorene mreže moguća je primjena odgovarajućih specifičnih rješenja, dok otvorena mreža mora implementirati otvorene standarde i protokole radi interoperabilnosti sa novim čvorovima.

- **Mogućnost fizičkog pristupa**

  Za napad na senzorsku mrežu koji podrazumijeva praćenje komunikacije između čvorova napadaču je dovoljno da se približi senzorskoj mreži unutar dometa radio veze. Međutim, ukoliko napadač ostvaruje i neposredan fizički pristup mreži, on je u mogućnosti postavljati svoje uređaje (senzore), modificirati postojeće i pristupiti svim podacima na postojećim senzorskim čvorovima.

- **Područje primjene**

  Na problematiku otkrivanja upada u BSM bitno utječe i konkretna primjena mreže. Ukoliko je poznata primjena mreže poznate su i očekivane vrijednosti pojedinih parametara koji se prate putem senzora. Tako se, primjerice, analizom podataka na aplikacijskoj razini mogu otkriti eventualne nekonzistentnosti između rezultata mjerenja parametara promatranog fizikalnog fenomena. Međutim, često je vrlo teško razlučiti radi li se o zlonamjernom čvoru ili je u pitanju kvar legitimnog senzorskog čvora.

- **Vremenska kritičnost**

  Na implementaciju IDS sustava u BSM bitno utiče i vremenska kritičnost aplikacije. Ukoliko je aplikacija vremenski kritična podrazumijeva se prikupljanje i obrada podataka u stvarnom vremenu *(real-time)*. U tom slučaju i sustav za otkrivanje upada i eventualne protumjere također moraju biti stvarnovremenski.

- **Rizičnost okoline**

  Ovisno o konkretnoj primjeni, senzorski čvorovi često znaju biti raspoređeni u rizičnoj i opasnoj okolini *(hazardous environment)*. U tom slučaju izloženi su prisluškivanju prometa i napadima uskraćivanjem usluge, dok su manje izloženi fizičkom pristupu od strane napadača. Ukoliko okolina mreže nije opasna *(non-hazardous)* postoji i opasnost da napadač ostvari izravni fizički pristup senzorskim čvorovima.

- **Algoritmi usmjeravanja**

  Svi protokoli za senzorske mreže, uključujući i usmjerivačke protokole, razvijaju se tako da budu što jednostavniji i energetski što učinkovitiji. S druge strane, oni moraju biti dovoljno sofisticirani da zadovolje pretpostavke o samokonfigurabilnosti, skalabilnosti i interoperabilnosti u senzorskoj mreži. Implementacija sustava za otkrivanje upada usko je povezana sa algoritmima i protokolima usmjeravanja koji se primjenjuju u mreži, a koji najčešće bivaju žrtvom napada i zlouporabe.

- **Kriptografske metode**

  Primjena određenih kriptografskih metoda senzorskoj mreži omogućava implementaciju metoda za kontrolu pristupa, provjeru integriteta poruke i osiguranje autentičnosti. Metode asimetrične kriptografije (kriptografije javnog ključa), koje su vrlo raširene u klasičnim mrežama, u senzorskim mrežama ne nalaze svoju primjenu zbog prevelike zahtjevnosti za računalnim i energetskim resursima. U senzorskim mrežama primjenjuju se neke simetrične kriptografske tehnike (kriptografija tajnog ključa), koje su nešto manje zahtjevne, međutim i one značajno troše resurse i unose velik dodatni promet u mrežu, što predstavlja velik problem. IDS sustav koji se implementira u BSM u kojoj se primjenjuju određene kriptografske metode mora biti posebno prilagođen takvom okruženju.

- **Povezanost sa drugim mrežama**

  Budući da BSM najčešće služe za prikupljanje velike količine relevantnih podataka one su vrlo često povezane s drugim mrežama (žičnim ili bežičnim), kako bi ti podaci postali globalno dostupni. Povezanost s drugim mrežama (u konačnici najčešće s Internetom) otvara dodatne sigurnosne probleme, pa je u tom slučaju senzorsku mrežu potrebno osigurati i od napada sa Interneta. Mjere zaštite podrazumijevaju implementaciju odgovarajućih sigurnosnih mehanizama na *gateway*-u koji povezuje BSM sa ostatkom mreže.

U klasičnim žičnim mrežama postoje točke u kojima se u stvarnom vremenu može pratiti i nadzirati mrežni promet (preklopnici, usmjerivači, *gateway*-i). Za razliku od njih, u MANET i senzorskim mrežama, koje se ne oslanjaju na fiksnu infrastrukturu, ovakvih točaka nema. Također, dodatno ograničenje predstavlja činjenica da čvorovi mogu pratiti samo komunikaciju unutar dometa svog primopredajnika. Također, u bežičnim mrežama je puno teže razlučiti malicioznu aktivnost od tipičnih problema koji se u takvim mrežama javljaju (gubitak paketa, kolizija, kvarovi čvorova i sl.). Zbog svih ovih specifičnosti IDS sustav razvijen za bežičnu senzorsku mrežu morao bi zadovoljavati sljedeće:

- IDS sustav za bežičnu senzorsku mrežu trebao bi se temeljiti na distribuiranoj arhitekturi (kako za prikupljanje informacija, tako i za donošenje odluke), vodeći pri tome računa o minimalizaciji potrošnje resursa.
- Sustav mora u maksimalnoj mjeri štedjeti energiju. Budući da u senzorskoj mreži apsolutno najveći udio u potrošnji energije ima komunikacija, IDS sustav treba projektirati tako da se komunikacija neophodna za funkcioniranje sustava svede na najmanju moguću mjeru.
- Potrebno je pronaći kompromis između učinkovitosti IDS sustava i veličine područja unutar kojeg se podatkovni paketi prikupljaju i analiziraju.
- Zbog nedostatka centralizirane infrastrukture (osim bazne stanice) nužno je implementirati lokalno prikupljanje i analizu podataka.
- Zbog velike sigurnosne ranjivosti bežičnih senzorskih čvorova niti jedan čvor se ne smije smatrati apsolutno sigurnim i povjerljivim.
- Kompromitacija određenog senzorskog čvora ne smije negativno utjecati na normalno funkcioniranje preostalih čvorova.
- Poželjno je da IDS sustav funkcionira u stvarnom vremenu kako bi se minimalizirao negativni utjecaj napada u vremenski kritičnim aplikacijama.

4.2.3. Arhitekture IDS sustava u bežičnim senzorskim mrežama

Arhitektura bežične senzorske mreže specificira način na koji su senzorski čvorovi unutar mreže grupirani, kao i na koji način se senzorske informacije usmjeravaju kroz mrežu. U načelu, postoje dva osnovna tipa arhitekture senzorskih mreža: ravna *(flat)* arhitektura i

hijerarhijska *(hierarchical)* arhitektura. Kod ravne arhitekture svi senzorski čvorovi su međusobno ravnopravni i imaju podjednake resurse, a informacija se usmjerava od čvora do čvora (svaki čvor funkcionira i kao usmjerivač). Kod hijerarhijske arhitekture čvorovi su grupirani u skupine (klastere). Obično po jedan čvor iz svakog klastera predstavlja „glavu klastera“ *(„cluster head“)* i odgovoran je za funkcije usmjeravanja. U senzorskoj mreži sa hijerarhijskom arhitekturom čest je slučaj da čvorovi nisu međusobno jednaki, nego da glava klastera raspolaže nešto većim resursima. U slučaju da su svi čvorovi unutar klastera jednaki obično se po određenom algoritmu oni smjenjuju u ulozi glave klastera kako bi se postigla ravnomjerna potrošnja njihovih resursa [98].

Prilikom implementacije IDS sustava u senzorsku mrežu kao značajan problem javlja se pravilno pozicioniranje IDS modula unutar senzorske mreže za postizanje što bolje učinkovitosti u postupku otkrivanja upada. Postoji više različitih strategija pozicioniranja IDS modula, na čiji izbor u velikoj mjeri utječe i arhitektura same mreže. Neke od značajnijih strategija su:

- **Slobodni nadzor *(promiscuous monitoring)***
  Slobodni nadzor predstavlja jednostavnu strategiju koja podrazumijeva postavljanje IDS modula na svaki senzorski čvor, pri čemu svaki čvor „osluškuje“ promet koji je u dometu njegovog primopredajnika. Na taj način se lako može detektirati svaki maliciozni paket. Međutim, ovakav pristup, unatoč vrlo dobroj mogućnosti detekcije, dovodi do veće potrošnje energije.
- **Čvor nadzire isključivo pakete koji prolaze preko njega**
  Ovaj pristup također podrazumijeva postavljanje IDS modula na svaki senzorski čvor, no senzorski čvor analizira samo one pakete koji prolaze preko njega, što znači da se paket analizira na svakom čvoru na svojoj putanji od izvora do odredišta.
- **IDS modul na baznoj stanici**
  Ovaj pristup podrazumijeva postavljanje IDS modula na baznu stanicu, koji analizira cjelokupan promet iz senzorske mreže koji se na baznoj stanici prikuplja. Prednost ovakvog pristupa je u tome što ne ovisi o topologiji mreže niti o tehnici usmjeravanja koja se u mreži koristi. Također, ne dolazi do višestruke analize jednog te istog paketa. Međutim, ovaj pristup može dovesti do preopterećenja bazne stanice, a postoji realna opasnost da napadač kompromitira i samu baznu stanicu (često je se ne može smatrati apsolutno sigurnom).

- **IDS moduli na svim susjedima bazne stanice**

  Moguće je postaviti IDS module na sve čvorove koji su neposredni susjedi baznoj stanici. Na taj način smanjuje se procesno opterećenje bazne stanice. Međutim, nedostatak ovakvog pristupa je nemogućnost obrane od napada poplavljivanjem *(flooding)* budući da se paketi analiziraju tek na korak do odredišta.

- **IDS moduli na „glavama“ klastera**

  Ukoliko je senzorska mreža hijerarhijski strukturirana (podijeljena na klastere) moguće je IDS module postaviti na „glave“ klastera. Ovaj pristup podrazumijeva da svi čvorovi unutar klastera svoj podatkovni promet prosljeđuju glavi klastera, koja je zadužena za njegovo dalje prosljeđivanje ka baznoj stanici. Na taj način IDS modul postavljen na glavu klastera može analizirati kompletan promet iz klastera. Time se postiže da se svaki paket analizira samo po jednom, što doprinosi učinkovitosti sustava i uštedi u resursima. Međutim, ovakav pristup povećava količinu kontrolnog prometa u mreži *(overhead)*, budući da čvorovi ne biraju najkraću putanju, nego prosljeđuju sav promet preko glave klastera, koja ga dalje prosljeđuje ka baznoj stanici.

Izabrati odgovarajuću strategiju pozicioniranja IDS modula unutar bežične senzorske mreže nije nimalo jednostavan problem. Na pozicioniranje IDS modula unutar BSM utječu mnogobrojni faktori, poput arhitekture i veličine same mreže (broja čvorova), njezine topologije, vrste i količine prometa koji se mrežom prenosi, raspoloživih resursa, kao i očekivane razine sigurnosti (koja u najvećoj mjeri ovisi o namjeni senzorske mreže). Svaka od spomenutih strategija ima svoje prednosti i nedostatke, a zbog velike raznolikosti senzorskih mreža nije moguće izabrati jedno rješenje koje bi bilo primjenjivo u svim situacijama. Zbog toga je za svaku konkretnu BSM potrebno provesti odgovarajuću analizu, te odrediti optimalan broj i raspored IDS modula kako bi se očekivana razina sigurnosti dosegla uz što manju potrošnju resursa i što manji utjecaj na normalan rad mreže.

4.2.4. Pregled postojećih prijedloga IDS sustava za BSM

Istraživanja usmjerena ka implementaciji IDS sustava u bežičnu senzorsku mrežu proizvela su nekolicinu prijedloga IDS sustava namijenjenih za BSM. Ovi prijedlozi

međusobno su vrlo raznoliki, i teško ih je sustavno kategorizirati. Međutim, ipak je moguće napraviti relativno grubu podjelu na nekoliko kategorija [66]:

- IDS sustavi koji se oslanjaju na protokole usmjeravanja
- IDS sustavi temeljeni na praćenju ponašanja susjednih čvorova
- IDS sustavi temeljeni na inovativnim tehnikama detekcije
- IDS sustavi orijentirani na specifične vrste napada

Određeni broj IDS sustava predloženih za senzorske mreže izravno se oslanja na usmjerivačke protokole. Članak [21] predlaže shemu otkrivanja upada koja koristi podjelu mreže na klastere i prati uzorke usmjerivačkog prometa, te detektira svako odstupanje od uzoraka „normalnog“ prometa. Sustav je temeljen na detekciji anomalija, što znači da je u stanju detektirati i neke nove napade, nepoznate od ranije. Pristup podrazumijeva distribuirane IDS module, postavljene na svaki čvor u mreži. Moduli analiziraju informacije iz usmjerivačkih tablica svakog čvora, tako da nije potrebna komunikacija između modula, što u značajnoj mjeri štedi energetske resurse. Međutim, ogroman nedostatak ovog rješenja je njegova uska povezanost sa AODV *(Ad hoc On-demand Distance Vector)* usmjerivačkim protokolom. Naime, ovaj usmjerivački protokol često se koristi u MANET mrežama, no nije pogodan za bežične senzorske mreže i u njima ga se susreće vrlo rijetko.

Slično prethodnom rješenju, članak [12] predlaže metode otkrivanja upada koje prilikom prosesa otkrivanja upada koriste dostupne sistemske informacije, poput usmjerivačkih tablica, popisa susjednih čvorova, rasporeda aktivnog i neaktivnog stanja čvorova, te pokušavaju otkriti maliciozno ponašanje na više slojeva mrežnog modela. Nedostatak ovog rješenja je uska povezanost sa DSDV *(Destination-Sequenced Distance Vector routing)* i DSR *(Dynamic Source Routing)* usmjerivačkim protokolima, koji su česti u MANET mrežama, no iznimno rijetki u BSM.

Većina predloženih rješenja za otkrivanje upada u BSM temelji se na načelu praćenja ponašanja susjednih čvorova koji se nalaze unutar dometa primopredajnika. Po svojoj osnovnoj ideji i koncepciji ovakva rješenja slična su rješenjima koja nalaze primjenu u MANET mrežama.

IDS modul postavljen na senzorskom čvoru prati ponašanje susjednog čvora i pokušava ustanoviti prosljeđuje li on podatkovne pakete nakon prijema dalje ka odredištu. Ukoliko IDS modul primijeti da susjedni čvor ne prosljeđuje paket, namjerno unosi kašnjenje ili modificira

paket on to bilježi kao indikaciju mogućeg zlonamjernog ponašanja. Zbog toga svaki čvor tokom određenog vremenskog intervala bilježi anomalije u ponašanju svojih susjeda. Ukoliko se ove anomalije detektiraju češće nego što je to u normalnim uvjetima uobičajeno aktivira se alarm i za čvor se sumnja da je kompromitiran (zlonamjeran). Rješenje koje predlažu autori članka [19] prati pojavu tri različita događaja: modifikacija poruke, gubitak poruke i koliziju poruke. Ukoliko učestalost pojave nekog od ovih događaja odstupa od uobičajene, ponašanje se karakterizira kao maliciozno (zlonamjerno). Rješenje slično ovome predlaže članak [70], gdje se kao parametri analiziraju brzina pristizanja paketa *(packet arrival rate)* i srednja primljena razina snage *(received power level)* za svakog susjeda. Za analizu se koristi konačan broj posljednjih paketa, što je određeno veličinom međuspremnika. Kod oba ova rješenja IDS moduli međusobno ne surađuju, pa značajnu ulogu u pogledu učinkovitosti otkrivanja upada igra veličina međuspremnika.

Autori u članku [42] predlažu distribuirani sustav za nadzor bežične senzorske mreže koji prati aktivnost senzorskih čvorova. Sustav za nadzor je pasivan i također se temelji na načelu praćenja susjednih čvorova. U senzorskoj mreži izloženoj negativnim utjecajima okoliša kvarovi pojedinih senzorskih čvorova predstavljaju relativno čestu pojavu. Vrlo često je normalne kvarove teško razlikovati od zlonamjernog ponašanja. Zbog toga kod ovog rješenja svaki senzorski čvor svojim susjedima periodički šalje poruku dajući im na znanje da je aktivan. Svaki čvor prati aktivnost svojih susjeda, i ukoliko unutar određenog (prethodno definiranog) vremenskog intervala ne dobije ovu poruku zaključuje da je susjedni čvor neaktivan („mrtav“). Ova shema predviđa postojanje kontrolnog centra. Kontrolni centar (obično smješten na baznoj stanici) ne vrši analizu (analiza i odlučivanje provodi se lokalno), već samo prikuplja izvještaje od distribuiranih čvorova. Komunikacija između kontrolnih centara i perifernih čvorova reducirana je uvođenjem procedure slanja upita i potvrde upita pojedinim čvorovima. Ovakva shema podrazumijeva da se svakom čvoru može pristupiti iz kontrolnog centra.

Autori u [111] predlažu sustav za otkrivanje upada i reakciju u senzorskim mrežama temeljen na autentifikacijskim mehanizmima. Kao mjera prevencije upada koristi se mehanizam za autentifikaciju kontrolnih poruka koje se razmjenjuju među senzorskim čvorovima. Ovaj pristup podrazumijeva podjelu senzorske mreže na klastere. Glava klastera nadzire ostale čvorove unutar klastera. Na taj način se ostvaruje određena ušteda energije u odnosu na pristup kod kojeg svi čvorovi nadziru svoje susjede. Nakon detekcije malicioznog čvora slanjem alarma članovima klastera glava klastera će isključiti maliciozni čvor iz mreže.

Periodički, u ciklusima, provodi se i nadzor glave klastera od strane ostalih mrežnih čvorova. Nakon što se prime višestruki alarmi o malicioznom ponašanju glave klastera (prag tolerancije je unaprijed predodređen) glava klastera se isključuje iz mreže. Nedostatak predloženog mehanizma je u tome što ne omogućava naknadno dodavanje novih čvorova u mrežu, niti podržava pokretljivost čvorova (podrazumijeva da su čvorovi fiksni).

Autori članka [46] predlažu distribuirani sustav za otkrivanje upada u bežičnim senzorskim mrežama temeljen na unaprijed određenim specifikacijama za provođenje postupka detekcije. Ovaj sustav podrazumijeva postojanje IDS modula (agenta) na svakom senzorskom čvoru. Ovi agenti provode postupke nadzora mreže, donošenja odluke i odgovarajuće reakcije. Prilikom nadzora mreže svaki čvor prati svoje neposredne susjede i prikuplja određene podatke (broj odbačenih paketa, učestalost odbacivanja paketa i sl.). Nakon što određeni čvor za svojeg susjeda pretpostavi da je maliciozan on svoje zaključke razmjenjuje s ostalim čvorovima, pri čemu se provodi postupak kolektivnog odlučivanja (princip većinskog odlučivanja). Nakon što se napad detektira aktivira se lokalni modul za reakciju. Pri tome reakcija na napad može biti izravna i neizravna. Izravna reakcija podrazumijeva isključivanje sumnjivog čvora iz svih ruta (putanja) usmjeravanja, te pokretanje postupka revokacije i rekonfiguracije kriptografskih ključeva za ostatak susjedstva (ukoliko se u mreži koriste kriptografske metode). Neizravna reakcija podrazumijeva alarmiranje bazne stanice o sumnjivom ponašanju malicioznog čvora. Ovakav pristup pokazuje vrlo dobru detekciju, no zbog potrebe za međusobnom komunikacijom između IDS agenata u procesu kolektivnog odlučivanja nije osobito energetski učinkovit.

Određeni broj predloženih rješenja za otkrivanje upada u BSM temelji se na nekim inovativnim metodama i tehnikama koje ranije nisu nalazile primjenu u ove svrhe. Neki od primjera su model teorije igara i skriveni Markovljev model.

Članci [2, 3] predlažu primjenu modela teorije igara *(Game Theory Model)* u postupku otkrivanja upada u bežičnim senzorskim mrežama, pri čemu se primarno orijentiraju na otkrivanje napada uskraćivanjem usluge *(Denial of Service)*. Pristup prevenciji DoS napada uključuje teoriju igara na način da se predlaže protokol temeljen na teoriji igara koji će biti u stanju prepoznati kooperativnost čvorova. Protokol je u stanju detektirati čvorove koji su spremni proslijediti pakete, no iz određenih razloga nisu to u mogućnosti učiniti (najčešće ih napadač u tome sprečava) od onih čvorova koji se ponašaju nekooperativno. Modul za otkrivanje upada nalazi se na baznoj stanici (centralizirana arhitektura) i nadzire međusobnu

suradnju čvorova u senzorskom polju. Podaci o njihovoj međusobnoj kooperativnosti bilježe se tijekom određenog vremenskog intervala, te se na temelju prikupljenih podataka formira reputacija svakog čvora u senzorskoj mreži (formira je IDS modul na baznoj stanici). Pri tome predloženi protokol favorizira međusobnu suradnju čvorova, dok se nekooperativno ponašanje kažnjava (ukoliko se čvor nekooperativno ponaša smanjuje se njegova reputacija). Reputacija svakog pojedinog čvora koristi se kao metrika kojom se mjeri razina njegove povjerljivosti (pouzdanosti) i koristi ju se za statističko predviđanje budućeg ponašanja senzorskog čvora. Zahvaljujući podacima (pohranjenima na baznoj stanici) o ponašanju svakog čvora kroz određeno vrijeme moguće je kreirati putanje usmjeravanja preko čvorova sa boljom reputacijom (tj. izbjegavati čvorove niske reputacije prilikom usmjeravanja prometa). Na taj način se kroz određeno vrijeme maliciozni čvorovi izoliraju iz mreže. Nedostatak ovog pristupa je smanjena uspješnost detekcije u slučaju pojave većeg broja malicioznih čvorova.

Autori u radu [22] predlažu tehniku otkrivanja upada temeljenu na analizi fluktuacija u očitanjima senzora postavljenih na senzorskim čvorovima. U predloženom modelu na prikupljene informacije primjenjuje se skriveni Markovljev model *(HMM, Hidden Markov Model)*. HMM model predstavlja zapravo statistički Markovljev model kod kojeg se pretpostavlja da modelirani sustav predstavlja Markovljev proces sa skrivenim stanjima (stanjima koja nisu izravno vidljiva, ali je vidljiv njihov izlaz). Primjenom ovog modela omogućava se senzorskoj mreži prilagođavanje njezinom prirodnom okruženju, pri čemu se omogućava detekcija neuobičajenih aktivnosti unutar mreže. Ovakav sustav teško je „prevariti“ budući da su informacije koje se koriste prilikom otkrivanja upada jedinstvene za svaku pojedinu mrežu jer su vezane za njezinu lokaciju i prirodno okruženje u kojem se ona nalazi.

Velik broj predloženih rješenja za otkrivanje upada u bežičnim senzorskim mrežama orijentiraju se isključivo na pojedinačne specifične tipove napada, pri čemu zanemaruju ostale sigurnosne prijetnje i mogućnosti napada. Zbog toga se, unatoč njihovoj korisnosti, ovakva rješenja ne mogu smatrati potpunim i cjelovitim sustavima za otkrivanje neovlaštenih upada, budući da su orijentirana samo na pojedinačne tipove napada.

Autori u članku [69] orijentiraju se na problematiku otkrivanja *Sinkhole* napada i predlažu rješenje temeljeno na algoritmu s dva osnovna koraka. Prvi korak podrazumijeva kreiranje liste sumnjivih čvorova na temelju provjere konzistentnosti podataka. U drugoj fazi

analizira se tok podataka kroz mrežu koristeći pri tome resurse bazne stanice. Algoritam koristi činjenicu da je većina prometa u senzorskoj mreži usmjerena od više senzorskih čvorova ka jednoj baznoj stanici, pa se primarno oslanja na resurse bazne stanice (za koju se pretpostavlja da raspolaže značajno većim resursima nego senzorski čvor). Uzima se u obzir i mogućnost da više zlonamjernih čvorova kooperativno nastoje prikriti identitet pravog napadača, pri čemu se pravi napadač nastoji identificirati primjenom većinskog glasovanja.

Rješenje predloženo u članku [121] orijentira se na zaštitu od napada uskraćivanjem resursa *(Denial of Service)* provedenog namjernim unošenjem elektromagnetskih smetnji *(jamming)* i onemogućavanjem normalne komunikacije među senzorskim čvorovima. Sustav pokušava otkriti i označiti područja u kojima postoji smetnja, kako bi se ta područja mogla zaobići, te tako uspostaviti normalna komunikacija. Moduli za otkrivanje smetnji i mapiranje ometanog područja izvršavaju se na svakom senzorskom čvoru. U slučaju da otkriju moguće ometanje čvorovi o tome obavještavaju svoje susjede, te se područje zahvaćeno smetnjom mapira kako bi se negativni utjecaj smetnje umanjio, a komunikacija uspostavila zaobilaznim putem. Naravno, ovakav sustav učinkovit je samo u slučajevima kada je smetnja prostorno ograničena i zahvaća samo određene dijelove unutar mreže, a ne i mrežu u cijelosti.

U tablici 4.2 nalazi se pregledni prikaz osnovnih karakteristika spomenutih prijedloga IDS sustava namijenjenih bežičnim senzorskim mrežama.

TABLICA 4.2 Osnovne karakteristike postojećih IDS sustava

IDS	Arhitektura	Tehnika otkrivanja upada	Prednosti	Nedostaci
IDS sustavi koji se oslanjaju na protokole usmjeravanja				
[21]	Podjela mreže na klastere, IDS modul na svakom senzorskom čvoru	Detekcija anomalija u uzorcima usmjerivačkog prometa	Energetski učinkovit (nema komunikacije između IDS modula)	Uska povezanost sa AODV usmjerivačkim protokolom
[12]	Distribuirana	Detekcija anomalija u sistemskim zapisima	Analiza kroz više slojeva *(cross-layer* pristup)	Uska povezanost s DSDV i DSR usmjerivačkim protokolima
IDS sustavi temeljeni na praćenju susjednih čvorova				
[19]	Distribuirana, bez komunikacije među modulima	Praćenje modifikacije, gubitaka i kolizije poruka	Energetski učinkovit	Bitan utjecaj veličine međuspremnika na uspješnost detekcije
[70]	Distribuirana, bez komunikacije među modulima	Analiza brzine pristizanja paketa i srednje primljene razine snage	Energetski učinkovit	Bitan utjecaj veličine međuspremnika na uspješnost detekcije
[42]	Distribuirana, uz postojanje kontrolnog centra za prikupljanje izvještaja	Analiza periodičkih poruka koje se šalju susjednim čvorovima	Moguće udaljeno pristupanje svakom senzorskom čvoru iz kontrolnog centra	Veća potrošnja energije zbog slanja periodičkih poruka; teško razlikuje uobičajene kvarove od zlonamjernog ponašanja
[111]	Podjela mreže na klastere, glava klastera nadzire ostale čvorove unutar klastera	Autentifikacija kontrolnih poruka	Energetski učinkovitiji od rješenja u kojima svi čvorovi nadziru svoje susjede	Ne omogućava naknadno dodavanje novih čvorova; ne podržava pokretljivost čvorova
[46]	Distribuirana, IDS agent na svakom senzorskom čvoru	Detekcija temeljena na unaprijed određenim specifikacijama uz postupak kolektivnog odlučivanja	Vrlo visoka uspješnost detekcije	Veći energetski zahtjevi zbog potrebe za međusobnom komunikacijom agenata
IDS sustavi temeljeni na inovativnim tehnikama detekcije				
[2, 3]	Centralizirana, modul za otkrivanje upada postavljen na baznu stanicu	Primjena modela teorije igara za analizu kooperativnosti čvorova	Model favorizira kooperativno ponašanje čvorova, dok se nekooperativnost „kažnjava“	Smanjena mogućnost detekcije u slučaju većeg broja zlonamjernih čvorova
[22]	Distribuirana	Detekcija temeljena na analizi fluktuacija u očitanjima senzora uz primjenu skrivenog Markovljevog modela	Model se prilagođava prirodnom okruženju senzorske mreže	Vezanost za lokaciju senzorske mreže
IDS sustavi orijentirani na specifične vrste napada				
[69]	Centralizirana, primarno oslanjanje na resurse bazne stanice	Provjera konzistentnosti podataka temeljem analize podatkovnih tokova	Visoka uspješnost detekcije	Sustav orijentiran na *Sinkhole* napad
[121]	Distribuirana, modul za otkrivanje smetnji na svakom senzorskom čvoru	Detekcija elektromagnetskih smetnji	Mapira područje zahvaćeno smetnjom i uspostavlja komunikaciju zaobilaznim putem	Orijentiran na napad uskraćivanjem resursa proveden namjernim unošenjem EM smetnji

Svi spomenuti IDS sustavi namijenjeni su „klasičnim“ bežičnim senzorskim mrežama, te kao takvi nisu izravno primjenjivi u senzorskoj mreži temeljenoj na IPv6 protokolu. Da bi se neki od ovih sustava primijenio u IPv6-temeljenoj BSM nužno bi bilo napraviti odgovarajuće

modifikacije i prilagodbe. Za sada još ne postoji IDS sustav koji je izvorno namijenjen senzorskoj mreži temeljenoj na IPv6 protokolu, te kao takav prilagođen svim specifičnostima ovakvog okruženja. To je prepoznato kao problem, te zato ova disertacija donosi rješenje distribuiranog adaptivnog IDS sustava upravo namijenjenog senzorskim mrežama u koje je implementiran IPv6 protokol. Detaljan opis i analiza ovog rješenja dani su u poglavlju 6. Ovo rješenje predstavlja važan dio cjelovitog sigurnosnog okvira namijenjenog IPv6-temeljenim BSM, čiji opis slijedi u poglavlju 5.

5. Sigurnosni okvir za bežične senzorske mreže temeljene na IPv6 protokolu

Ubrzanim širenjem bežičnih senzorskih mreža i porastom broja njihovih mogućih aplikacija u velikoj mjeri raste i svijest o njihovim sigurnosnim aspektima. Također, implementacija odgovarajućih sigurnosnih mehanizama pozitivno utječe na povjerenje korisnika u ovu tehnologiju, što otvara mogućnosti njezinoj još široj primjeni. Problematika sigurnosti u bežičnim senzorskim mrežama predstavlja vrlo aktualno i istraživački vrlo aktivno područje.

Bežične senzorske mreže u današnje vrijeme nalaze svoju primjenu u vrlo različitim realnim scenarijima (vojne primjene, industrijske primjene, primjene u poljoprivredi i zaštiti okoliša i sl.), što problematiku sigurnosti u njima čini iznimno kompleksnom. Gotovo svaka od mogućih primjena BSM izložena je različitim vrstama sigurnosnih prijetnji i zahtijeva postizanje različitih razina sigurnosti. Također, implementaciju odgovarajućih sigurnosnih mehanizama u velikoj mjeri otežava vrlo stroga ograničenost u pogledu resursa (ograničen kapacitet napajanja i računalnih resursa senzorskih čvorova). Zbog toga je iznimno teško razviti i implementirati sigurnosno rješenje koje će biti u dovoljnoj mjeri prilagodljivo da može zadovoljiti potrebe korisnika u svim mogućim scenarijima primjene BSM.

Većina istraživanja u području sigurnosti u BSM usmjerena je na pojedinačne sigurnosne prijetnje na pojedinim slojevima unutar slojevitog mrežnog modela. Zbog toga niti jedan od takvih sigurnosnih mehanizama samostalno ne pruža potpunu zaštitu BSM niti krajnjem korisniku jamči odgovarajuću razinu sigurnosti. Postizanje zadovoljavajuće razine sigurnosti zahtijevalo bi implementaciju više različitih sigurnosnih mehanizama čijim bi se zajedničkim djelovanjem ostvarivao željeni cilj. Uključivanje nekoliko različitih, međusobno neovisnih sigurnosnih mehanizama u jednu BSM dodatno otežava njezinu implementaciju, te kasnije održavanje. Zbog toga se jedan dio istraživanja usmjerio ka razvoju integriranih i sveobuhvatnih sigurnosnih okvira *(security framework)* koji bi prožimali sve slojeve slojevitog mrežnog modela [100]. Ovakav sigurnosni okvir u jedinstvenu cjelinu integrira nekolicinu sigurnosnih rješenja, pružajući na taj način sigurnosne usluge krajnjem korisniku [73, 96, 119, 130]. Za sada je većina predloženih rješenja usmjerena na pojedinačne slojeve, a još uvijek ne postoji široko prihvaćeno rješenje sigurnosnog okvira za BSM koje pruža odgovarajuću razinu sigurnosti prožimajući pri tome sve slojeve mrežnog modela. Također,

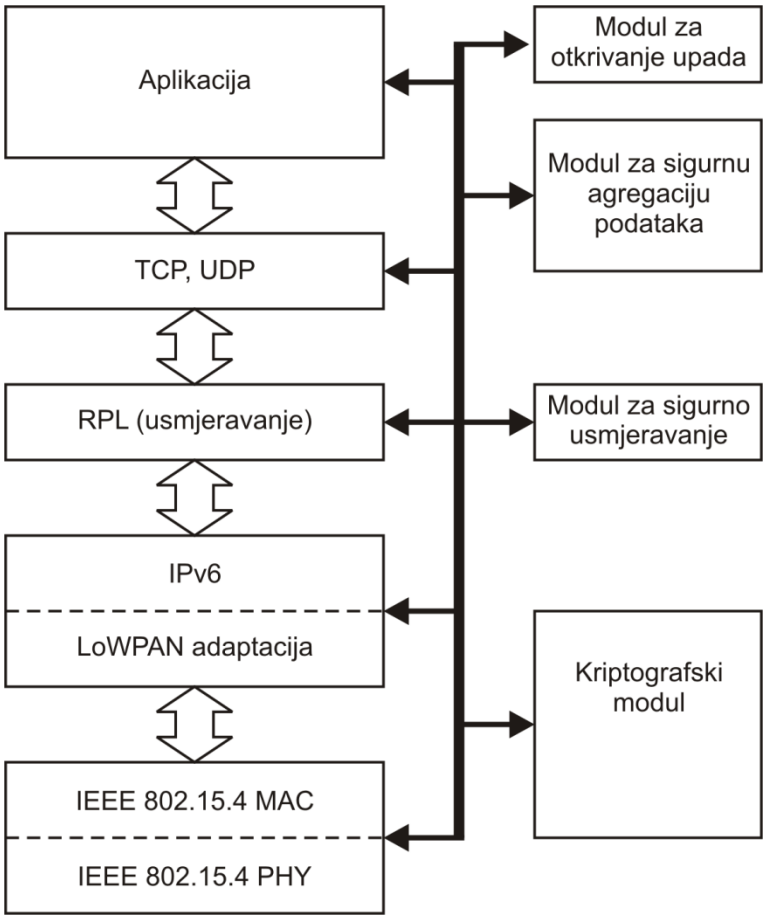
za sada ne postoji prijedlog cjelovitog sigurnosnog okvira koji bi posebno bio usmjeren i orijentiran na BSM u kojima se primjenjuje IPv6 protokol.

Jedinstveni sigurnosni okvir u svakom slučaju treba uključivati sigurnosne mehanizme koji će omogućiti da se u mreži zadovolje temeljne sigurnosne pretpostavke, koje obično podrazumijevaju osiguranje autentičnosti, povjerljivosti, integriteta i dostupnosti informacija i resursa. Sigurnosni okvir treba pružiti mogućnost enkripcije podataka (što također podrazumijeva implementaciju sigurnih mehanizama za upravljanje kriptografskim ključevima – njihovu inicijalnu raspodjelu po čvorovima, međusobnu razmjenu i opoziv u slučaju kompromitacije). Također, potrebno je omogućiti sigurno usmjeravanje podataka kroz mrežu, uz mogućnost pronalaženja višestrukih i alternativnih ruta kako bi se komunikacija neometano nastavila čak i nakon prekida pojedinih ruta uslijed kvara ili kompromitacije čvorova. Sigurnosni okvir svakako treba implementirati odgovarajuće tehnike za sigurnu lokalizaciju čvorova i sigurnu agregaciju podataka. Jednu od najvažnijih komponenata kvalitetnog sigurnosnog okvira čini sustav za otkrivanje zlonamjernog ponašanja pojedinih mrežnih čvorova i detekciju eventualnih napada izvana [99].

Zbog vrlo širokog spektra mogućih primjena bežičnih senzorskih mreža, od kojih svaka ima svoje specifične sigurnosne zahtjeve koji se međusobno mogu značajno razlikovati, sigurnosni okvir koji se primjenjuje u BSM mora biti modularan, kako bi korisnik u konkretnoj situaciji mogao koristiti samo one sigurnosne usluge i funkcije koje su neophodne i čijom primjenom se postiže planirana razina sigurnosti. Zbog toga je dan prijedlog modularnog sigurnosnog okvira koji je primjenjiv u BSM temeljenim na IPv6 protokolu. Potpoglavlja koja slijede detaljnije analiziraju pojedine sigurnosne module iz ovog sigurnosnog okvira, zajedno sa pripadajućim sigurnosnim uslugama i funkcijama koje oni pružaju korisniku. Pri tome se analiziraju i neka postojeća sigurnosna rješenja (namijenjena „klasičnim“ BSM) koja bi se uz odgovarajuću prilagodbu mogla uklopiti unutar jedinstvenog i cjelovitog sigurnosnog okvira namijenjenog IPv6-temeljenim BSM.

Predloženi sigurnosni okvir za IPv6-temeljene BSM čine sljedeći sigurnosni moduli:

- **Kriptografski modul** (kojeg čine modul za kriptiranje i modul za upravljanje kriptografskim ključevima)
- **Modul za sigurno usmjeravanje**
- **Modul za sigurnu agregaciju podataka**
- **Modul za otkrivanje upada i zlonamjernog ponašanja senzorskih čvorova**



Slika 5.1 Sigurnosni okvir za IPv6-temeljene BSM

Na slici 5.1 prikazana je struktura sigurnosnog okvira namijenjenog IPv6-temeljenim BSM i integriranog unutar protokolnog stoga kakav je zastupljen u ovakvim mrežama. Sigurnosni okvir prožima sve slojeve mrežnog modela, pri čemu su svi njegovi blokovi međusobno povezani i integrirani u jedinstvenu cjelinu koja će krajnjem korisniku omogućiti postizanje željene razine sigurnosti. Detaljniji opis strukture i funkcije pojedinačnih modula iz sigurnosnog okvira dan je u potpoglavljima koja slijede. Također, u njima je dan i pregled nekih postojećih sigurnosnih prijedloga i rješenja iz klasičnih BSM koja bi se uz odgovarajuće modifikacije i prilagodbe mogla u budućnosti primijeniti u IPv6-temeljenim BSM i uklopiti u predloženi sigurnosni okvir.

Predloženi sigurnosni okvir nastoji zadovoljiti nekolicinu osnovnih zahtjeva koje bi trebalo zadovoljavati svako kvalitetno sigurnosno rješenje:

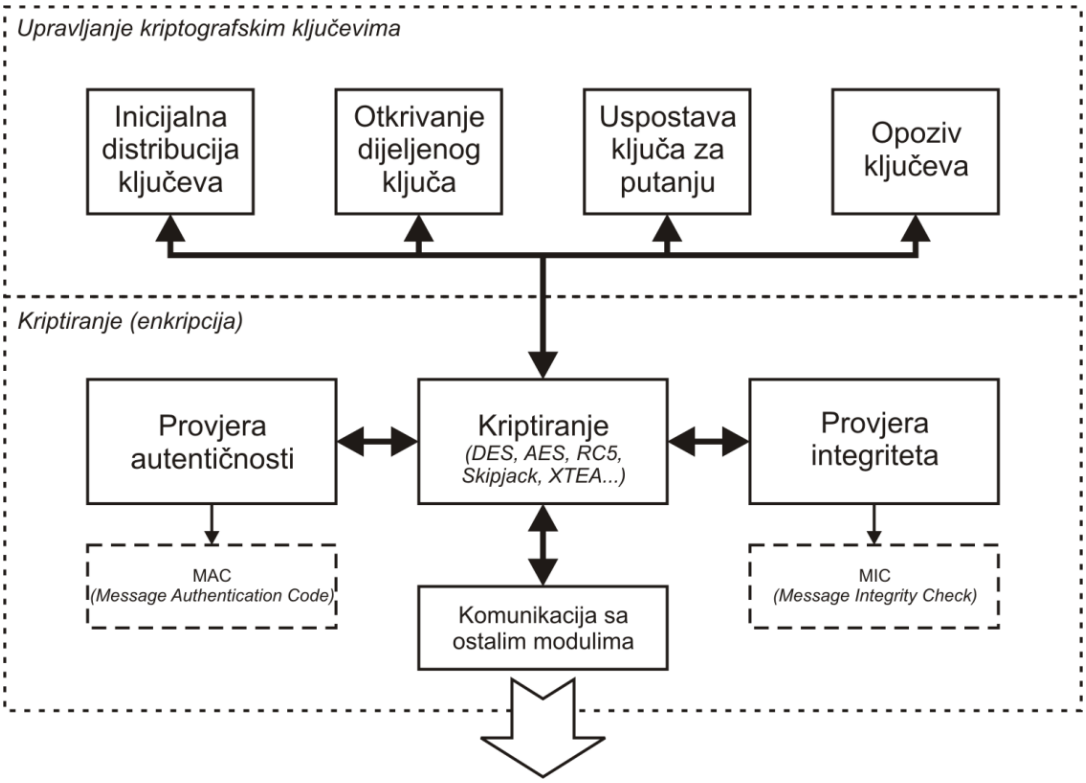
- **Fleksibilnost:** sigurnosni okvir podržava različite sigurnosne usluge i funkcije, no njihova uporaba nije nametnuta niti obvezujuća, nego se korisniku ostavlja mogućnost izbora sigurnosnih usluga ovisno o konkretnoj aplikaciji senzorske mreže
- **Skalabilnost:** dodavanje novih ili uklanjanje postojećih čvorova ne smije imati nikakav utjecaj na funkcioniranje sigurnosnih usluga unutar definiranog sigurnosnog okvira, niti značajnije utjecati na raspoložive mrežne resurse
- **Transparentnost:** pružanje sigurnosnih usluga treba biti transparentno ostalim komponentama ili uslugama
- **Malo zauzeće resursa:** sigurnosne usluge koje pruža sigurnosni okvir trebaju što ekonomičnije koristiti ograničene resurse senzorskih čvorova
- **Otpornost na kompromitaciju čvorova:** eventualna kompromitacija pojedinih čvorova ne smije onemogućiti komunikaciju i pružanje sigurnosnih usluga u ostatku mreže
- **Jednostavnost:** integracija sigurnosnih usluga sa drugim servisima ili komponentama treba unositi što manju količinu dodatnog prometa u mrežu

5.1. Kriptografski modul

U bežičnim senzorskim mrežama se unutar mreže (na pojedinačnim senzorskim čvorovima) odvijaju postupci procesiranja i agregacije podataka prilikom njihovog prijenosa do krajnjeg odredišta (bazne stanice). Postupci obrade i agregacije podataka od velikog su značaja za postizanje energetski učinkovitog prikupljanja informacija iz senzorskog polja i njihovog prijenosa do krajnjeg odredišta. Zbog toga su ovi postupci u senzorskim mrežama neizostavni. Međutim, ovi postupci podrazumijevaju mogućnost pristupa podatkovnim paketima i eventualnu modifikaciju njihovog sadržaja od strane intermedijarnih čvorova (čvorova koji se nalaze na putanji između izvorišnog čvora i krajnjeg odredišta podatkovnog paketa). Kako bi pristup bio moguć, u senzorskim mrežama nije prikladno koristiti sigurnosne mehanizme „s kraja na kraj“ *(end-to-end)*, kakvi su česti u konvencionalnim mrežama (npr. SSL, SSH).

U senzorskoj mreži nužno je intermedijarnim čvorovima omogućiti provjeru autentičnosti i integriteta podatkovnih paketa, što također ne bi bilo moguće primjenom *end-to-end* sigurnosnih mehanizama. Zbog toga je u bežičnoj senzorskoj mreži potrebno implementirati transparentnije sigurnosne mehanizme koji će omogućavati enkripciju podataka i upravljanje kriptografskim ključevima. Budući da se u senzorskim mrežama većina komunikacije odvija od velikog broja perifernih čvorova ka središnjem čvoru (baznoj stanici) gotovo je nemoguće predinstalirati i naknadno osvježavati kriptografske ključeve za svaki pojedini par čvorova. Također, kriptografske metode temeljene na javnom ključu *(public key cryptography)* koje su vrlo raširene u konvencionalnim mrežama u pravilu se smatraju neprikladnim za BSM zbog prevelikih procesorskih zahtjeva (izuzetak u posljednje vrijeme predstavljaju kriptografske metode temeljene na eliptičnim krivuljama - *ECC, Elliptic Curve Cryptography)*. Zbog toga je u bežičnoj senzorskoj mreži (ukoliko se u njoj primjenjuje neka od kriptografskih metoda temeljenih na tajnim ključevima) potrebno implementirati odgovarajući sigurnosni mehanizam (protokol) za sigurno upravljanje ključevima *(secure key management)*. Pri tome ovaj mehanizam mora biti fleksibilan i skalabilan, kako bi omogućio naknadno dodavanje novih čvorova u mrežu [53].

Za sve zadaće vezane uz enkripciju podataka i upravljanje kriptografskim ključevima unutar sigurnosnog okvira namijenjenog IPv6-temeljenim BSM zadužen je kriptografski modul (slika 5.2).



Slika 5.2 Kriptografski modul sigurnosnog okvira

Kriptografski modul čine dva podmodula:

- **Podmodul za kriptiranje (enkripciju)** - osigurava povjerljivost, autentičnost i integritet podataka
- **Podmodul za upravljanje kriptografskim ključevima** - omogućava sigurnu distribuciju, uspostavu i opoziv kriptografskih ključeva

Detaljniji opis strukture i funkcije ovih podmodula dan je u potpoglavljima 5.1.1. i 5.1.2.

5.1.1. Podmodul za kriptiranje (enkripciju)

Podmodul za kriptiranje podataka treba osigurati povjerljivost (tajnost) podataka *(confidentiality)*, njihovu autentičnost *(authentication)* i integritet *(integrity)*. Zbog toga se ovaj podmodul sastoji od tri osnovna bloka:

- Blok za provjeru autentičnosti (osigurava autentičnost podataka)

- Blok za provjeru integriteta (osigurava integritet podataka)
- Blok za enkripciju (osigurava tajnost podataka)

Tajnost podataka postiže se primjenom neke od metoda njihove enkripcije. Za bežične senzorske mreže trenutačno se prikladnijim pokazuju metode simetrične enkripcije (temeljene na tajnom ključu) zbog njihove manje zahtjevnosti po pitanju računalnih i energetskih resursa, iako određena istraživanja ukazuju na mogućnost primjene i metoda asimetrične enkripcije u BSM. S daljnjim napretkom razvoja hardvera za BSM (povećanje brzine uz smanjenje potrošnje i cijene) za očekivati je sve veća zastupljenost asimetričnih kriptografskih metoda. Od metoda simetrične enkripcije u BSM je moguće koristiti slijedne šifre *(stream ciphers)*, poput RC4, blok šifre *(block ciphers)*, kao što su DES, AES, RC5 i *Skipjack*, ili *hash* tehnike (SHA-1, MD5). Iako neka istraživanja pokazuju da slijedne šifre u određenim slučajevima daju nešto bolje performanse nego blok šifre (npr. RC4 u usporedbi sa RC5), za primjenu u BSM najprikladnije i najraširenije su blok šifre. Razlog tome je što se blok šifre mogu koristiti i za enkripciju i za autentifikaciju, što omogućava optimizaciju programskog koda i smanjuje memorijske zahtjeve [36].

Postupak autentifikacije podataka omogućava odredišnom čvoru da provjeri je li izvorišni čvor doista onaj koji se navodi, odnosno da otkrije eventualno ubacivanje lažnih podataka u mrežu od strane treće (neovlaštene) osobe. To se najčešće postiže uporabom koda za ovjeru poruke *(MAC, Message Authentication Code)*. MAC kod se izračunava na temelju podataka koji se šalju i tajnog ključa (koji je poznat pošiljatelju i primatelju) i šalje zajedno sa porukom. Ukoliko odredišni čvor dobije paket sa ispravnim MAC kodom, on zaključuje da je doista poslan s legitimnog izvora i da nije modificiran tijekom prijenosa.

Najraširenija shema izračunavanja koda za ovjeru poruke je CBC-MAC shema *(Cipher Block Chaining Message Authentication Code)*. Ova shema podrazumijeva uporabu neke blok šifre za enkripciju niza blokova podataka, pri čemu se posljednji enkriptirani blok uzima kao MAC kod. Istraživanje [11] pokazuje da je CBC-MAC shema sigurna za poruke fiksne duljine, dok se pokazala nesigurnom za poruke varijabilne duljine. Zbog toga se poruka mora nadopunjavati kako bi joj ukupna duljina predstavljala višekratnik duljine osnovnog bloka za šifriranje, što zapravo zahtijeva transmisiju dodatnih bitova, a to se u BSM može značajnije odraziti na potrošnju energije. Zbog toga neki protokoli u BSM mogu koristiti i drugačije načine djelovanja blok šifri, kao što su primjerice OCB *(Offset Codebook Mode)* i CTR *(Counter Mode)*, kod kojih je duljina šifrirane poruke jednaka duljini otvorenog teksta [93].

Primjenom kriptografskih metoda u mreži potrebno je osigurati da neovlaštena osoba ne može doći do sadržaja otvorenog teksta čak i u slučaju da posjeduje nekoliko različitih šifrata za isti otvoreni tekst (do kojih bi mogla doći praćenjem mrežnog prometa, odnosno „prisluškivanjem“). To se najčešće postiže tako da se kao inicijalizacijski vektor *(IV, Initialization Vector)* za kriptografsku funkciju koristi slučajna *(random)* vrijednost ili brojač. Na taj način se postiže da čak i prilikom slanja iste poruke šifrat uvijek bude različit. Međutim, u tom slučaju se i inicijalizacijski vektor mora slati zajedno sa podacima, što u BSM povećava zahtjeve za resursima. Slanje inicijalizacijskog vektora sa svakim paketom može se izbjeći ukoliko se kao IV koristi dijeljeni brojač *(counter)* na izvorišnom i odredišnom čvoru. Međutim, ovakav pristup podrazumijeva vremensku sinkronizaciju između mrežnih čvorova, što u BSM sa velikim brojem čvorova i ograničenim resursima nije lako postići.

Kvalitetan sigurnosni okvir treba korisniku pružiti mogućnost da izabere koje su mu od navedenih sigurnosnih usluga doista potrebne, budući da svaka od njih zahtijeva odgovarajuće resurse. Na taj način korisnik može izabrati koje sigurnosne usluge će koristiti, što prvenstveno ovisi o konkretnoj primjeni BSM (realna potreba za sigurnosnim uslugama u velikoj mjeri ovisi o konkretnoj primjeni BSM). Tako, primjerice, korisnik može zahtijevati provjeru autentičnosti, a da mu nije nužno potrebno osiguravati tajnost podataka. Time se postiže fleksibilnost sustava i mogućnost njegove prilagodbe različitim aplikacijama, pri čemu korisnik pronalazi kompromis između očekivane razine sigurnosti i performansi senzorske mreže.

U IPv6 temeljenim BSM viši slojevi zamijenjeni su odgovarajućim adaptacijskim slojem (6LoWPAN) i mrežnim slojem na kojem se primjenjuje IPv6 protokol. Međutim, ova činjenica ne sprječava da se na fizikalnom sloju ne primjene sigurnosni mehanizmi podržani od strane samog IEEE 802.15.4 standarda. Sigurnosne usluge koje standard pruža uključuju metode za uspostavu i razmjenu ključeva, zaštitu podatkovnih okvira i upravljanje uređajima. Za enkripciju se koristi standard AES *(Advanced Encryption Standard)* sa 128-bitnim ključevima. Primjena sigurnosnih mehanizama za enkripciju na fizikalnom sloju isključivo omogućava osiguravanje poruka koje se prenose preko pojedinačnih linkova. Za osiguranje poruka koje se prenose kroz više skokova nužno je primijeniti sigurnosne mehanizme na višim slojevima. Integritet poruke osigurava se dodavanjem MIC koda *(Message Integrity Code)* na kraj paketa, iza enkriptiranog dijela.

U proteklih nekoliko godina pojavila se nekolicina sigurnosnih protokola i arhitektura namijenjenih klasičnim BSM koji pokušavaju implementirati sigurnosne usluge (najčešće na sloju podatkovnog linka) nastojeći pomoću njih osigurati povjerljivost, integritet i autentičnost podataka. Ova sigurnosna rješenja se ne mogu izravno primijeniti u BSM temeljenim na IPv6 protokolu, no uz eventualnu prilagodbu u budućnosti mogu naći svoje mjesto unutar sigurnosnog okvira namijenjenog IPv6-temeljenim BSM. Zbog toga je važno ukratko spomenuti najvažnija i najraširenija sigurnosna rješenja namijenjena „klasičnim“ BSM.

Prva, najstarija i najpoznatija sigurnosna arhitektura namijenjena bežičnim senzorskim mrežama bila je SPINS arhitektura *(Security Protocols for Sensor Networks)* [72]. SPINS arhitektura optimizirana je za okruženja sa ograničenim resursima (poput BSM) i čine je dva osnovna dijela: SNEP *(Sensor Network Encryption Protocol)* i μTESLA *(micro Timed, Efficient, Streaming, Loss-tolerant Authentication Protocol).*

SNEP protokol osigurava povjerljivost podataka, pruža mehanizam za autentifikaciju i onemogućava zlouporabe ponovljenim slanjem podataka *(replay protection)* tj. vodi računa o starosti podataka koji se šalju *(data freshness).* Ove sigurnosne usluge SNEP implementira primjenom simetrične kriptografije, pri čemu se za šifriranje i dešifriranje koristi RC5 kriptografska funkcija [92]. Za konstrukciju koda za ovjeru poruke (MAC kod) koristi se CBC-MAC shema uz uporabu RC5 blok šifre. Semantička sigurnost (koja jamči da napadač ne može doći do otvorenog teksta čak i ukoliko dođe u posjed nekoliko šifrata istog otvorenog teksta) postiže se implementacijom dijeljenog brojača između predajnika i prijemnika koji se koristi kao inicijalizacijski vektor za blok šifru. Pri tome ostaju problemi sinkronizacije među čvorovima i pokretanje postupka resinkronizacije u slučaju gubitka pojedinih paketa.

μTESLA protokol omogućava utvrđivanje autentičnosti prilikom razašiljanja poruka *(broadcast)* u bežičnoj senzorskoj mreži. Osiguranje autentičnosti prilikom razašiljanja poruka zahtijeva asimetrične kriptografske mehanizme koji su zbog svoje prevelike zahtjevnosti za resursima neprikladni za senzorske mreže. Protokol μTESLA ovaj problem rješava uvođenjem asimetrije vremenski pomaknutim otkrivanjem simetričnih ključeva. Pri tome je također neophodna vremenska sinkronizacija između bazne stanice i čvorova, gdje svaki čvor mora znati kolika je gornja granica dozvoljene sinkronizacijske pogreške. Prilikom slanja paketa bazna stanica izračunava MAC kod pomoću ključa koji je u tom trenutku tajan. Kada čvor primi paket on provjerava je li taj ključ već objavljen (na temelju sinkronizacijskih

informacija i vremenskog rasporeda objave ključeva). Kada čvor utvrdi da ključ još nije objavljen on pretpostavlja da napadač nije mogao izmijeniti paket prilikom prijenosa i pohranjuje paket u međuspremnik. U trenutku objave ključeva bazna stanica svima razašilje ključ za verifikaciju, i čvorovi mogu provjeriti ispravnost ključa. Ukoliko je ključ ispravan čvor ga koristi za provjeru autentičnosti pohranjenog paketa.

TinySec sigurnosna arhitektura predstavljena je 2004. godine i predstavlja prvu u potpunosti implementiranu sigurnosnu arhitekturu sloja podatkovnog linka namijenjenu klasičnim BSM [49]. TinySec arhitektura implementirana je unutar TinyOS operativnog sustava namijenjenog bežičnim senzorskim mrežama. Sigurnosne usluge koje ova arhitektura pruža su: osiguranje tajnosti, autentičnosti i integriteta poruke i semantička sigurnost. Paketi se osiguravaju tako što se enkriptiraju pomoću grupnog ključa kojeg dijele senzorski čvorovi i izračunava se MAC kod za cijeli paket (uključujući i zaglavlje). Arhitektura omogućava dva načina rada: autentifikacija sa enkripcijom i samo autentifikacija (uobičajeni način rada – podatkovni dio paketa se ne enkriptira, već se paketu samo dodaje MAC kod). Ova arhitektura ne uključuje mehanizam distribucije ključeva, koji je potrebno implementirati kao zasebnu cjelinu. U praksi se obično koristi jedan ključ „ručno“ programiran na senzorske čvorove prije njihovog raspoređivanja. Kao kriptografski algoritam za enkripciju i izračunavanje MAC koda primjenjuje se Skipjack blok šifra u CBC modu *(Cipher Block Chaining)*, uz uporabu 80-bitnog ključa.

SenSec arhitektura slična je TinySec arhitekturi, uz uvođenje nekih izmjena. Za razliku od TinySec arhitekture (na temelju koje je nastala) SenSec podržava isključivo način rada koji uključuje i autentifikaciju i enkripciju. Za šifriranje se koristi nešto naprednija varijanta Skipjack šifre, tzv. Skipjack-X. SenSec arhitektura također implementira napredniji mehanizam upravljanja ključevima, koji uključuje tri razine ključeva: globalni ključ *(global key)*, klasterski ključ *(cluster key)* i senzorski ključ *(sensor key)*. Kao i kod SenSec arhitekture, ovi ključevi se generiraju i učitavaju na senzorske čvorove prije njihovog raspoređivanja.

Još jedna sigurnosna arhitektura namijenjena radu sa TinyOS operativnim sustavom jest MiniSec arhitektura [61]. MiniSec osigurava tajnost i autentičnost poruka i pruža mehanizam zaštite od napada ponovljenim slanjem paketa *(replay attack)*. Podržava dva načina rada, za *unicast* komunikaciju među senzorskim čvorovima (MiniSec-U) i za *broadcast* komunikaciju

(MiniSec-B). U oba načina rada za enkripciju i autentifikaciju koristi se Skipjack šifra u OCB načinu rada.

Pokušaj implementacije kriptografskih metoda temeljenih na javnom ključu u bežične senzorske mreže rezultirao je nastankom TinyECC arhitekture [59]. TinyECC arhitektura također je namijenjena okruženju TinyOS operativnog sustava i temelji se na eliptičkim krivuljama *(ECC – Elliptic Curve Cryptography)*. Od svih kriptografskih tehnika temeljenih na javnom ključu ECC kriptografija za sada se čini najprikladnijom za primjenu u BSM promatrano sa aspekta potrošnje resursa i razine zaštite koju pruža. Međutim, čak i kod ECC kriptografije potrošnja energije za red veličine je veća od potrošnje u slučaju primjene metoda simetrične kriptografije (temeljene na tajnom ključu).

Sigurnosna platforma ContikiSec dizajnirana je za bežične senzorske mreže temeljene na Contiki operativnom sustavu, te je za sada jedinstvena kao takva, budući da su preostale poznatije sigurnosne platforme za BSM orijentirane uglavnom na TinyOS operativni sustav. Sam operativni sustav Contiki ne pruža sigurnosne usluge (omogućava jedino provjeru integriteta primjenom CRC-16 cikličke provjere redundancije). Zbog toga ContikiSec platforma pokušava implementirati sigurnosne usluge unutar Contiki okruženja. ContikiSec arhitektura je konfigurabilnog dizajna i od sigurnosnih usluga omogućava osiguranje tajnosti, autentičnosti i integriteta podataka, te semantičku sigurnost, pokušavajući pri tome pronaći kompromis između potrošnje energije i postizanja željene razine sigurnosti [14, 15].

Prilikom dizajna ContikiSec arhitekture razmatrana je nekolicina najpoznatijih simetričnih blok šifri: AES *(Advanced Encryption Standard)*, RC5, *Skipjack*, *Triple-DES (Data Encryption Standard)*, *Twofish* i XTEA *(Extended Tiny Encryption Algorithm)*. Iscrpna analiza i testiranje rezultirali su zaključkom da je u ovom trenutku za primjenu u BSM najprikladnija AES blok šifra, koja predstavlja najbolji kompromis između razine sigurnosti koju pruža i količine resursa koje pri tome troši. Također, analizirano je i nekoliko modova rada kriptografskog algoritma: CBC-CS *(Cipher Block Chaining – Ciphertext Stealing)*, CMAC *(Cipher-based Message Authentication Code)* i OCB *(Offset Codebook Mode)*. Najučinkovitijim, a time i najprikladnijim za primjenu u BSM, pokazao se OCB mod rada, koji osigurava povjerljivost i autentičnost podataka.

ContikiSec arhitektura podržava tri sigurnosna moda rada: ContikiSec-Enc – mod rada koji samo osigurava povjerljivost podataka *(confidentiality-only)*, ContikiSec-Auth - mod rada koji samo osigurava autentičnost *(authentication-only)*, i ContikiSec-AE – mod rada koji

osigurava i povjerljivost i autentičnost *(authentication with encryption)*. Ovakav modularni dizajn omogućava prilagodbu ContikiSec arhitekture različitim aplikacijama koje imaju različite sigurnosne zahtjeve. U modovima rada u kojima se vrši enkripcija podataka primjenjuje se inicijalizacijski vektor (IV) duljine 2 okteta. Duljina inicijalizacijskog vektora izravno utječe na razinu sigurnosti, ali i potrošnju energije. Dulji inicijalizacijski vektor povećava sigurnost enkripcije, ali i povećava utrošak energije budući da se on prenosi u svakom paketu. Analiza je pokazala da duljina inicijalizacijskog vektora od 2 okteta predstavlja najbolji kompromis između razine sigurnosti i potrošnje energije. Inicijalizacijski vektor kreira se pomoću pseudoslučajnih brojeva, pri čemu se kao inicijalizacijska vrijednost za generator slučajnih brojeva koristi identifikator čvora. Na taj način na svakom čvoru generator slučajnih brojeva biva inicijaliziran drugačijom vrijednošću. Podatkovni dio paketa enkriptira se korištenjem AES šifre u CBC-CS modu rada. Pri tome se podrazumijeva da je prilikom inicijalizacije svakom čvoru dodijeljen jedinstveni 128-bitni ključ (pohranjen je u RAM memoriju). Također, svakom paketu dodaje se i kontrolna suma *(checksum)* duljine 2 okteta. Na taj način za svaki paket osigurani su povjerljivost i integritet (ContikiSec-Enc način rada).

ContikiSec-Auth način rada namijenjen je aplikacijama kod kojih je važno osigurati autentičnost (tj. sa sigurnošću znati tko je pravi izvor pojedinog paketa), a kod kojih osiguranje tajnosti podataka nije presudno. Operativni sustav Contiki implementira 16-bitnu CRC funkciju *(Cyclic Redundancy Check)* za zaštitu integriteta podataka izračunavanjem 16-bitne kontrolne sume. Međutim, ova kontrolna suma dizajnirana je s ciljem detekcije slučajnih modifikacija podataka (uslijed pogreške prilikom prijenosa), dok MAC kod *(Message Authentication Code)* ima za cilj otkriti i namjerno neautorizirano modificiranje podataka. Zato se kod ContikiSec-Auth načina rada iz paketa uklanja kontrolna suma i umjesto nje stavlja MAC kod. Za generiranje MAC koda primjenjuje se CMAC algoritam uz primjenu AES šifre. ContikiSec-AE pruža najvišu razinu sigurnosti koja uključuje osiguranje povjerljivosti, autentičnosti i integriteta podataka. Koristi se OCB algoritam uz primjenu AES šifre temeljene na jedinstvenom 128-bitnom tajnom ključu za potrebe enkripcije i autentifikacije. Primjena ContikiSec-AE načina rada povećava paket za 4 dodatna okteta.

U bežičnoj senzorskoj mreži najveći dio energije utroši se prilikom bežičnog prijenosa podataka. Količina energije koja se utroši prilikom dodatnog procesiranja podataka zbog dodatnih kriptografskih funkcija bitno je manja od količine energije koja se utroši na prijenos dodatnih okteta koji u tom slučaju nastaju. Budući da ContikiSec-Enc i ContikiSec-Auth

načini rada dodaju paketu dva okteta nešto su manje energetski zahtjevni od ContikiSec-AE načina rada, koji paketu dodaje 4 okteta. Pokazalo se da primjena ContikiSec-AE načina rada povećava potrošnju energije za oko 15%, u slučaju da su podatkovni dijelovi paketa veličine 40 okteta.

ContikiSec sigurnosna arhitektura za sada je jedina sigurnosna arhitektura posebno razvijena za BSM temeljene na Contiki operativnom sustavu. Ova arhitektura je modularna (omogućava tri različita moda rada) i konfigurabilna, te pruža sigurnosne usluge povjerljivosti, autentičnosti i integriteta podataka. Budući da je razvijena za Contiki operativni sustav, ona predstavlja i najprikladnije rješenje koje bi se moglo implementirati u BSM temeljenu na IPv6 protokolu (u kojoj se također kao operativni sustav koristi Contiki). Polazeći od ContikiSec arhitekture uz odgovarajuću prilagodbu mogla bi se izgraditi prikladna sigurnosna arhitektura namijenjena IPv6-temeljenim BSM koja bi osiguravala autentičnost, integritet i povjerljivost informacija.

Za implementaciju ContikiSec sigurnosne arhitekture u IPv6-temeljene BSM potrebno je napraviti sljedeće prilagodbe:

- Implementirati punu podršku za 6LoWPAN adaptacijski sloj i IPv6 protokol na mrežnom sloju
- Implementirati punu podršku za IPv6 protokolni stog unutar Contiki operativnog sustava (uIPv6)
- Uspostaviti udgovarajuća sučelja (postojeća sučelja nisu adekvatna) prema ostalim modulima iz cjelovitog sigurnosnog okvira radi razmjene informacija i pružanja kriptografskih usluga ostalim modulima
- Razmjenu i upravljanje ključevima prilagoditi okruženju IPv6-temeljene BSM

5.1.2. Podmodul za upravljanje kriptografskim ključevima

Za primjenu u bežičnim senzorskim mrežama najprikladnijim se pokazuju simetrične kriptografske metode temeljene na tajnim ključevima. Pri tome se javlja problem inicijalne raspodjele ključeva (posebice u mrežama sa velikim brojem čvorova) i potreba za mehanizmom koji bi omogućio promjenu ključeva u slučaju njihove kompromitacije [17, 103]. Većina analiziranih sigurnosnih arhitektura oslanja se na tajni ključ koji je pojedinim

čvorovima pridijeljen prilikom uspostave mreže. Ovakav pristup se pokazuje kao problematičan u slučaju mreže sa velikim brojem čvorova, budući da je kompromitacijom bilo kojeg čvora ugrožena komunikacija u cjelokupnoj mreži. Zbog toga se u bežične senzorske mreže nastoji implementirati odgovarajuće tehnike za upravljanje ključevima *(key management)* koje bi omogućavale uspostavu, raspodjelu i eventualnu naknadnu revokaciju tajnih kriptografskih ključeva unutar BSM.

Uporaba jednog jedinstvenog tajnog ključa za cjelokupnu mrežu zasigurno je u pogledu računalnih i memorijskih resursa najučinkovitiji pristup. Međutim, ozbiljan nedostatak ovakvog pristupa jest činjenica da u tom slučaju kompromitacija pojedinog senzorskog čvora ujedno znači i kompromitaciju cjelokupne mreže. Drugi pristup, kojim bi se ova situacija izbjegla, jest primjena posebnog (različitog) ključa za svaki par senzorskih čvorova. U tom slučaju kompromitacija pojedinog čvora ne bi kompromitirala mrežu u cijelosti. Međutim, u mreži sa *n* čvorova svaki čvor bi trebao pohraniti *n-1* ključeva za komunikaciju sa preostalim čvorovima, što u slučaju većeg broja čvorova također predstavlja problem, budući da potreban prostor za pohranu ključeva linearno raste s porastom broja mrežnih čvorova. Zbog toga se za primjenu u BSM predlažu sheme upravljanja ključevima koje predstavljaju kompromis između ova dva pristupa.

Budući da je pravilno i sigurno upravljanje ključevima od velike važnosti za BSM, kao drugi podmodul unutar kriptografskog modula sigurnosnog okvira izdvaja se podmodul za upravljanje kriptografskim ključevima. Njega čine tri bloka, od kojih je svaki zadužen za obavljanje po jedne temeljne funkcije:

- **Blok za sigurnu inicijalnu distribuciju ključeva:** osnovna zadaća mu je na siguran način izabrati i pohraniti konačan skup ključeva u memoriju senzorskih čvorova
- **Blok za sigurno otkrivanje dijeljenog ključa *(shared key)*:** funkcija ovog bloka jest otkrivanje ključeva (iz skupa ključeva koji su na raspolaganju) koje će koristiti prilikom međusobne komunikacije određeni parovi čvorova
- **Blok za sigurnu uspostavu ključa za pojedinu putanju *(path key)*:** zadaća ovog bloka jest uspostaviti ključ za određenu putanju između čvorova koji nemaju zajednički dijeljeni ključ
- **Blok za sigurni opoziv ključeva:** funkcija ovog bloka jest opozvati pojedine ključeve u slučaju da dođe do njihove kompromitacije, te ponovno pokrenuti postupak za uspostavu novih kriptografskih ključeva

Kada je riječ o klasičnim BSM, prva shema upravljanja ključevima u BSM predložena je 2002. godine, i predstavlja osnovnu shemu koja je kasnije poslužila kao temelj za daljnja istraživanja i kao temeljna osnova za mnogobrojne varijacije koje su kasnije nastajale [35]. Riječ je o probabilističkoj shemi za upravljanje ključevima koja uključuje tri faze: inicijalna distribucija ključeva *(key pre-distribution),* otkrivanje dijeljenog ključa *(shared-key discovery)* i uspostava ključa za pojedinu putanju *(path key establishment).*

Prilikom inicijalne distribucije ključeva podrazumijeva se postojanje velikog skupa jedinstvenih ključeva *(key pool).* Prilikom inicijalizacije mreže svaki senzorski čvor iz ovog skupa slučajnim odabirom bira i pohranjuje u svoju memoriju konačan broj ključeva. Kada su ključevi sa svojim identifikatorima pohranjeni na senzorske čvorove izabire se određeni broj povjerljivih čvorova koji će obnašati ulogu kontrolera. Kontroleri pohranjuju sve identifikatore ključeva uz identifikatore pripadajućih senzorskih čvorova. Ovakav pristup omogućava da bilo koja dva senzorska čvora dijele zajednički ključ (barem uz posredstvo trećeg čvora) uz željenu (zadanu) vjerojatnost.

U sljedećoj fazi (nakon što je u postupku inicijalizacije svakom čvoru dodijeljen određeni broj ključeva) svaki pojedini par čvorova koji se nalazi unutar dometa radio veze uspostavlja zajednički ključ za međusobnu komunikaciju. Postoji određena vjerojatnost da par čvorova dijeli zajednički ključ, koja ovisi o veličini inicijalnog skupa ključeva, broju senzorskih čvorova i broju ključeva koji pohranjuje svaki čvor. Reguliranjem tih parametara se ova vjerojatnost dovodi na željenu razinu. Ukoliko dijeli zajednički ključ par čvorova će ga koristiti za međusobnu komunikaciju. Informacije o ključevima koje posjeduju čvorovi obično razmjenjuju razašiljanjem identifikatora ključeva. Međutim, u BSM se može dogoditi da neki čvorovi ne dijele zajednički ključ, a žele međusobno komunicirati. Zbog toga treća faza predstavlja uspostavu ključa za pojedinu putanju između čvorova koji ne dijele zajednički ključ. U tom slučaju se promatrani par čvorova oslanja na pomoć trećeg čvora s kojim dijele zajednički ključ, pri čemu se treći čvor zapravo ponaša kao posrednik ili centar za distribuciju ključeva. Čvor posrednik će u tom slučaju kreirati ključ kojeg će izvorni par čvorova koristiti prilikom međusobne komunikacije (ključ se kreira na temelju ključeva koje čvor posrednik dijeli s tim čvorovima).

Ovakva shema upravljanja ključevima je jednostavna i fleksibilna, no nije prikladna za situacije u kojima se zahtijeva iznimno visoka razina sigurnosti. Ne pruža mehanizam autentifikacije prilikom komunikacije između dva čvora, a problematično može biti i

oslanjanje na čvorove-kontrolere, čija kompromitacija može dovesti do kompromitacije mreže u cjelini.

Kako bi se riješili problemi komunikacije u situacijama kada dva čvora ne dijele zajednički ključ, nastale su neke sheme upravljanja ključevima koje zapravo predstavljaju varijaciju prethodno analizirane osnovne sheme. Q-kompozitna slučajna predistribucija ključeva *(Q-composite random key pre-distribution)* predstavlja nadogradnju osnovne sheme. Kod osnovne sheme dva čvora za uspostavu sigurne komunikacije dijele zajednički jedinstveni ključ. Povećanjem broja zajedničkih ključeva između čvorova povećava se i razina sigurnosti mreže, kao i otpornost na kompromitaciju čitave mreže u slučaju kompromitacije pojedinih čvorova. Q-kompozitna shema zahtijeva da dva senzorska čvora za uspostavu linka moraju imati barem q zajedničkih ključeva. Međutim, da bi vjerojatnost moguće uspostave linka između čvorova ostala ista uz povećanje potrebnog broja zajedničkih ključeva q mora se smanjiti inicijalni skup svih mogućih ključeva *(key pool)*. Smanjenje ovog skupa ključeva može imati negativne sigurnosne implikacije, budući da u slučaju relativno malog skupa ključeva napadač može kompromitacijom nekolicine čvorova kompromitirati i razmjerno veliki postotak ključeva. Prema tome, ukoliko se primjenjuje ovakav pristup kao problem se javlja izbor optimalnog broja ključeva q koje dva čvora moraju dijeliti da bi mogli uspostaviti komunikaciju.

Prethodno analizirane sheme upravljanja ključevima podrazumijevaju uniformnu razdiobu vjerojatnosti izbora pojedinih ključeva i pozicije na kojoj će se senzorski čvor naći unutar mreže. Neke kasnije predložene sheme oslanjaju se na neuniformne funkcije gustoće vjerojatnosti *(PDF, probability density functions)*, tako da se već unaprijed može predvidjeti približno područje unutar kojeg će se senzorski čvor nalaziti [29]. Pristup je vrlo sličan osnovnoj shemi, od koje se razlikuje jedino u prvoj fazi. Dok je kod osnovne sheme inicijalni skup ključeva jedinstven, sada se on dijeli na više podskupova kako bi se osiguralo da susjedni podskupovi imaju više zajedničkih ključeva. Budući da je svaki podskup namijenjen senzorskim čvorovima jednog područja, na taj način će se osigurati da bliski senzorski čvorovi imaju više zajedničkih ključeva nego udaljeni (što onda posljedično povećava vjerojatnost mogućeg uspostavljanja sigurne komunikacije). Glavni nedostatak ovog pristupa jest složenost pronalaska optimalnih parametara, poput veličine inicijalnih podskupova, njihovog preklapanja, broja ključeva koji se izabiru i sl.

Neke od predloženih shema za upravljanje ključevima oslanjaju se na hijerarhijsku strukturu senzorske mreže, što je često u suprotnosti sa načelima postizanja potpune distribuiranosti u BSM. Jedna od najpoznatijih shema za upravljanje ključevima koja podrazumijeva hijerarhijsku strukturu BSM jest LEAP [129]. LEAP *(Localized Encryption and Authentication Protocol)* shema koristi četiri različite vrste ključeva: pojedinačni *(individual key)*, grupni *(group key)*, upareni *(pair-wise key)* i klasterski ključ *(cluster key)*.

Pojedinačni ključ *(individual key)* je jedinstveni ključ kojeg svaki senzorski čvor dijeli sa baznom stanicom i koristi se za ostvarivanje sigurne komunikacije među njima. Senzorski čvor ovaj ključ može koristiti i za izračunavanje koda za ovjeru poruke *(MAC, Message Authentication Code)* koju šalje baznoj stanici. Također, bazna stanica koristi ovaj ključ prilikom slanja povjerljivih informacija ka senzorskom čvoru (npr. informacije o kriptografskim ključevima, različita upozorenja i sl.). Grupni ključ *(group key)* je globalno dijeljeni ključ kojeg bazna stanica koristi za enkripciju informacija koje razašilje čitavoj grupi senzorskih čvorova. Klasterski ključ *(cluster key)* je ključ kojeg senzorski čvor dijeli sa svim svojim susjedima, a koristi se za enkripciju poruka koje se razašilju lokalno. Najčešće je riječ o usmjerivačkim i drugim kontrolnim porukama. Upareni ključ *(pair-wise key)* je ključ kojeg senzorski čvor dijeli pojedinačno sa svakim od svojih neposrednih susjeda. Koristi se za komunikaciju pri kojoj je potrebno osigurati autentičnost i privatnost, kao primjerice prilikom distribucije klasterskih ključeva.

Određene sheme za upravljanje ključevima, poput [48], podrazumijevaju da je mreža podijeljena na klastere. Pri tome unutar svakog klastera postoji *gateway*, koji obično raspolaže znatno većim resursima od preostalih čvorova iz klastera. Svaki senzorski čvor posjeduje dva kriptografska ključa (jednog dijeli sa *gateway*-om, a drugog sa baznom stanicom). Glavni nedostatak ovakvog pristupa jest činjenica da eventualna kompromitacija *gateway*-a kompromitira cjelokupnu komunikaciju unutar klastera.

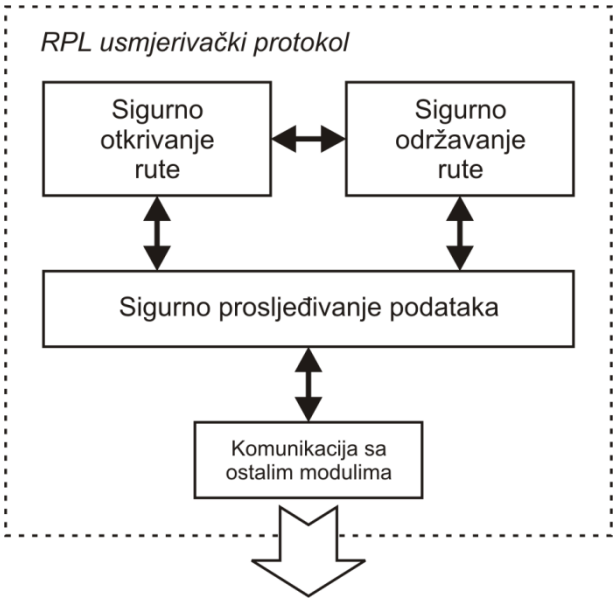
5.2. Modul za sigurno usmjeravanje

Problematika usmjeravanja u bežičnim senzorskim mrežama vrlo je aktualna kroz čitavo razdoblje njihovog razvoja. Vrlo veliki istraživački napori ulažu se u razvoj algoritama i usmjerivačkih protokola prikladnih za primjenu u BSM, što je rezultiralo prijedlogom čitavog

niza različitih usmjerivačkih protokola namijenjenih „klasičnim“ BSM. Međutim, prilikom razvoja velike većine usmjerivačkih protokola za BSM sigurnosnim aspektima nije posvećeno dovoljno pozornosti. Zbog toga većina do sada predloženih usmjerivačkih protokola ne uključuje nikakve sigurnosne mehanizme, već se temelje na pretpostavci da u okruženju BSM nema zlonamjernih aktivnosti, tj. da su svi senzorski čvorovi „prijateljski“ orijentirani i kooperativni [4, 50].

Budući da se BSM u posljednje vrijeme sve više primjenjuju u različitim područjima gdje su sigurnosni aspekti iznimno važni (npr. medicinske i vojne primjene) javlja se svijest o potrebi razvoja sigurnih protokola usmjeravanja, što rezultira prijedlozima usmjerivačkih protokola koji nastoje implementirati odgovarajuće sigurnosne mjere [63]. Siguran usmjerivački protokol mora biti sastavni dio sigurnosnog okvira koji se primjenjuje u BSM, i gotovo je nemoguće načiniti cjelovit sigurnosni okvir koji ne uključuje i siguran protokol usmjeravanja. Zbog toga unutar predloženog sigurnosnog okvira namijenjenog BSM temeljenim na IPv6 protokolu vrlo važan dio predstavlja upravo modul za sigurno usmjeravanje. Ovaj modul temelji se na RPL protokolu (kao jedinom usmjerivačkom protokolu razvijenom upravo za ovakve mreže), te uključuje nekoliko blokova (slika 5.3):

- Blok za sigurno otkrivanje rute *(secure route discovery)*
- Blok za sigurno održavanje rute *(secure route maintenance)*
- Blok za sigurno prosljeđivanje podataka *(secure data forwarding)*



Slika 5.3 Modul za sigurno usmjeravanje

Osnovna zadaća bloka za sigurno otkrivanje rute jest inicijalna uspostava višestrukih ruta između senzorskih čvorova i bazne stanice (primarno), kao i uspostava ruta između pojedinih parova senzorskih čvorova. Blok za sigurno održavanje ruta vodi računa o očuvanju povezivosti u dinamičkom okruženju senzorske mreže, provodeći rekonfiguraciju u slučaju promjene topologije, kvara ili kompromitacije pojedinih čvorova. Na njemu je implementiran i mehanizam za otkrivanje i izbjegavanje usmjerivačkih petlji. Blok za sigurno prosljeđivanje podataka zadužen je za slanje i prijem poruka, vodeći pri tome računa o njihovom redoslijedu i pravilnom izboru sljedećeg čvora sukladno izabranoj putanji ka krajnjem odredištu. Svi ovi blokovi koriste usluge kriptografskog modula, kako bi se primjenom kriptografskih metoda osigurala autentičnost, integritet i povjerljivost podataka i kontrolnih poruka.

U osjetljivom okruženju senzorske mreže jedan od ključnih problema je osigurati pouzdanost *(reliability)* i dostupnost mreže *(availability).* Kako bi se ovi ciljevi zadovoljiti u BSM je potrebno primijeniti višestazno *(multi-path)* usmjeravanje, što podrazumijeva pronalaženje više mogućih ruta od izvora do odredišta. Usmjeravanje koje bi se oslanjalo isključivo na jednu putanju *(single-path routing)* ne bi jamčilo pouzdanost i dostupnost mreže zbog relativno čestih kvarova na linkovima u BSM (uslijed smetnji ili kvarova čvorova).

Usmjeravanje u BSM predstavlja fundamentalnu operaciju čija je osnovna zadaća omogućiti uspostavu komunikacijskih linkova među senzorskim čvorovima i isporuku podatkovnih paketa od izvora do odredišta. Zbog toga ono predstavlja osnovni mrežni

mehanizam na koji se oslanjaju i gotovo svi sigurnosni mehanizmi koje je moguće implementirati u BSM (upravljanje kriptografskim ključevima, otkrivanje zlonamjernih upada, sigurna lokalizacija i agregacija podataka i sl.). Prema tome, već prilikom dizajna usmjerivačkog protokola potrebno je voditi računa o sigurnosnim aspektima kako bi protokol omogućio višestazno usmjeravanje otporno na različite napade uz predviđenu mogućnost oporavka nakon pojave određenih malicioznih aktivnosti.

U praksi se pokazalo da je velik dio napada i zlonamjernih aktivnosti koji se događaju u BSM usmjeren upravo na zlouporabu usmjerivačkih mehanizama. Unatoč različitim metodama koje napadač koristi, većina zlouporaba usmjerivačkih mehanizama usmjerena je ka nekom od sljedećih ciljeva [109]:

- **Zagušenje mreže *(network congestion)*:** napadač namjerno usmjerava veliku količinu prometa ka jednom dijelu mreže, što u tom dijelu izaziva zagušenje (i time onemogućava normalan rad mreže), a može dovesti i do ubrzanog pražnjenja baterija zahvaćenih senzorskih čvorova. Zagušenost mreže će u pravilu izazvati i kašnjenje, koje može pogubno utjecati na neke mrežne mehanizme koji zahtijevaju vremensku sinkronizaciju.
- **Kompromitacija rute *(route compromization)*:** stavljanjem određenog broja čvorova pod svoju kontrolu napadač može kompromitirati uspostavljene rute, i time postići preusmjeravanje prometa, namjerno kreirati usmjerivačke petlje, namjerno kreirati neoptimalne rute, kao i ubacivati vlastite čvorove unutar pojedinih ruta.
- **Iscrpljivanje energetskih resursa *(energy exhaustion)*:** modifikacijom pojedinih ruta napadač namjerno preopterećuje pojedine senzorske čvorove s ciljem pražnjenja njihove baterije.
- **Raščlanjivanje mreže *(network partitioning)*:** napadač nastoji raščlaniti mrežu ometanjem pojedinih njezinih dijelova (uglavnom se radi o ciljanom iscrpljivanju energetskih resursa pojedinih čvorova kako bi se prekinula komunikacija između pojedinih dijelova mreže).
- **Divergencija usmjerivačke baze podataka *(routing database divergence)*:** napadač nastoji onemogućiti konvergenciju usmjerivačkog protokola ka stabilnom stanju, što u mrežu unosi nestabilnost i velike količine kontrolnog prometa, a može dovesti i do njezinog potpunog rušenja

Postupak usmjeravanja u pravilu se odvija kroz tri faze: otkrivanje rute *(route discovery)*, prosljeđivanje podataka *(data forwarding)* i održavanje rute *(route maintenance)*. Svaka od ovih faza izložena je određenim mogućnostima zlouporabe. U početnoj fazi usmjeravanja (fazi otkrivanja rute) napadač nastoji umetnuti vlastite čvorove u mrežu ili umetanjem lažnih informacija utjecati na kreiranje usmjerivačkih tablica. U fazi prosljeđivanja podataka napadač nastoji kompromitirati podatke koji se prenose mrežom, što podrazumijeva neovlašteni pristup sadržaju podatkovnih paketa, kao i namjerno ubacivanje modificiranih paketa u mrežu. Prilikom održavanja rute napadač nastoji slanjem lažnih informacija legitimne mrežne čvorove isključiti iz mreže, budući da modificirane usmjerivačke tablice ne reprezentiraju stvarnu topologiju mreže.

U posljednje vrijeme pojavljuje se sve više usmjerivačkih protokola namijenjenih BSM prilikom čijeg dizajna se u određenoj mjeri vodilo računa i o sigurnosnim aspektima. Članak [109] daje sustavan pregled i po prvi puta kategorizaciju sigurnih protokola usmjeravanja. Sigurni usmjerivački protokoli mogu se razvrstati u tri kategorije, prema primarnom cilju zaštite. Prvu kategoriju predstavljaju protokoli koji isključivo štite mehanizam višestaznog usmjeravanja *(multipath routing protection only)*. Ovi protokoli uključuju samo mehanizme za zaštitu postupka otkrivanja ruta i prosljeđivanja podataka. Drugu skupinu čine protokoli koji su specifično dizajnirani tako da budu otporni na pojedinačnu specifičnu vrstu napada *(attack-specific protocols)*. Treću skupinu čine protokoli koji podržavaju složenije sigurnosne funkcije i zapravo se integriraju u složenije mrežne sigurnosne mehanizme.

Postojeći sigurni protokoli usmjeravanja za BSM u pravilu su namijenjeni klasičnim BSM. Kod bežičnih senzorskih mreža temeljenih na IPv6 protokolu trenutna situacija je bitno lošija, budući da je za sada jedino RPL usmjerivački protokol specijalno namijenjen ovakvoj vrsti mreža. Pozitivna činjenica jest da je u vrijeme nastanka RPL protokola svijest o sigurnosnoj problematici u BSM već bila na dovoljno visokoj razini, pa su paralelno s njegovim razvojem analizirani i njegovi sigurnosni aspekti, te dane odgovarajuće sigurnosne preporuke vezane uz njegovu implementaciju. Zbog toga se RPL protokol trenutno nameće kao jedini usmjerivački protokol koji se može uklopiti u cjeloviti sigurnosni okvir namijenjen BSM temeljenim na IPv6 protokolu.

Radna skupina *Networking* unutar IETF-a *(Internet Engineering Task Force)* izradila je prijedlog sigurnosnog okvira za usmjeravanje u LLN mrežama *(Low Power and Lossy Network)*, koji bi se trebao primijeniti i implementirati unutar RPL usmjerivačkog protokola

namijenjenog takvim mrežama (u ovu skupinu mreža pripadaju i BSM temeljene na IPv6 protokolu). Svrha ovog sigurnosnog okvira jest udovoljiti osnovnim sigurnosnim zahtjevima (povjerljivost, integritet, dostupnost) na razini usmjerivačkog protokola. Iz perspektive protokola usmjeravanja pod osiguranjem povjerljivosti podrazumijeva se zaštita svih usmjerivačkih informacija (uključujući poruke koje se razmjenjuju među susjednim čvorovima radi ažuriranja usmjerivačkih tablica) i njihova nedostupnost neovlaštenoj trećoj osobi. Pod osiguranjem integriteta podrazumijeva se zaštita usmjerivačkih informacija od njihove neovlaštene modifikacije ili zlouporabe. Pri tome se podrazumijeva i osiguranje autentičnosti pošiljatelja i nemogućnost ponovljenog naknadnog slanja istih kontrolnih poruka od strane neovlaštenog entiteta. Osiguranje dostupnosti podrazumijeva da je usluga usmjeravanja i prosljeđivanja paketa kroz mrežu dostupna legalnom korisniku u bilo kojem trenutku kada je to potrebno za normalno funkcioniranje mreže. Modul za sigurno usmjeravanje unutar cjelovitog sigurnosnog okvira za IPv6 temeljene BSM treba zapravo u potpunosti implementirati sigurnosni okvir za usmjeravanje u LLN mrežama, te uvažiti sve njegove sigurnosne preporuke.

U ranijim poglavljima analizirane su prijetnje i napadi kojima je izložen mehanizam usmjeravanja u BSM. Također, spomenute su i odgovarajuće mjere zaštite koje je moguće poduzeti protiv takvih napada, međutim te mjere nisu striktno bile vezane uz protokol usmjeravanja. Budući da sigurni protokol usmjeravanja čini sastavni dio jedinstvenog sigurnosnog okvira, potrebno je posebno analizirati sigurnosne mjere koje je nužno implementirati u sam usmjerivački protokol.

Promatrano sa aspekta povjerljivosti, očuvanje tajnosti usmjerivačkih informacija i informacija o topologiji mreže nije neophodno za sam postupak usmjeravanja niti izravno narušava njegovu funkciju. Međutim, zlonamjerni napadač koji neovlašteno dođe do ovih informacija (npr. prisluškivanjem mrežnog prometa) može ih zlorabiti za pokretanje drugih vrsta napada (tj. napada koji nisu izravno orijentirani na funkciju usmjeravanja u mreži, odnosno na usmjerivački protokol). Prema tome, usmjerivački protokol namijenjen BSM temeljenoj na IPv6 protokolu morao bi omogućiti enkripciju podatkovnog dijela paketa, kao i osigurati privatnost u slučaju da se funkcija usmjeravanja temelji na geografskim informacijama o čvorovima (tj. na informacijama o njihovom prostornom položaju). Poželjno bi bilo da usmjerivački protokol ima podršku za tuneliranje i balansiranje opterećenja.

Očuvanje integriteta usmjerivačkih poruka nužno je za ispravno funkcioniranje usmjerivačkog protokola. Kako bi se zaštitio integritet, usmjerivački protokol mora omogućiti provjeru integriteta poruke (čak i u slučaju da je ona enkriptirana). Također, protokol mora omogućiti provjeru autentičnosti čvorova koji komuniciraju, kao i verificirati ispravan redoslijed poruka. Poželjna je i implementacija mehanizma koji bi provjeravao vrijednosti pojedinih parametara (s ciljem da se utvrdi jesu li unutar očekivanih granica), kao i pratio učestalost pojedinih poruka (kako bi se utvrdilo eventualno odstupanje od uobičajenih vrijednosti).

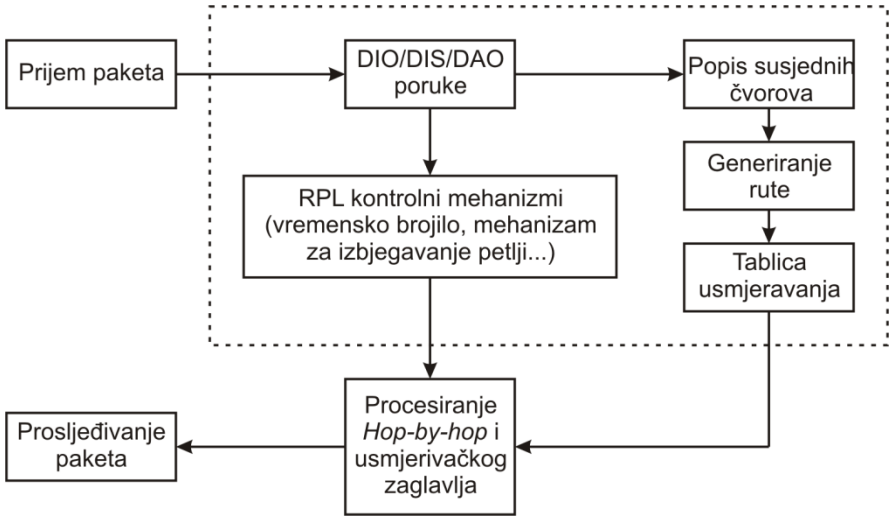
Dostupnost usmjerivačkih informacija izravno je povezana sa dostupnošću cjelokupne mreže. Ukoliko je kompromitirana dostupnost mreže, izravno je narušena dostupnost usmjerivačkih informacija. U potpunosti osigurati dostupnost mreže nije moguće isključivo pomoću sigurnog usmjerivačkog protokola (neophodni su i drugi sigurnosni mehanizmi, odnosno potreban je cjeloviti sigurnosni okvir). Međutim, određene karakteristike usmjerivačkog protokola mogu izravno doprinositi osiguranju dostupnosti mreže. Vjerojatnost da će mreža biti dostupna povećava usmjerivački protokol koji omogućava uspostavu višestrukih putanja između izvora i odredišta, pri čemu podržava slučajni izbor neke od alternativnih putanja. Vjerojatnost dostupnosti mreže može se povećati i limitiranjem količine prometa unutar određenog vremenskog intervala. Poželjno je i senzorske čvorove osigurati od fizičkog pristupa, kako bi se neovlaštenom napadaču onemogućio izravan pristup informacijama pohranjenim na senzorskim čvorovima.

Siguran usmjerivački protokol trebao bi podržavati i odgovarajuću shemu upravljanja kriptografskim ključevima, koja uključuje i mogućnost revokacije i redistribucije ključeva u slučaju kompromitacije. Sigurnosne mjere koje pruža usmjerivački protokol namijenjen BSM mogu se promatrati na dvije razine. Jednu razinu čine mjere koje su izravno implementirane u sam usmjerivački protokol, dok drugu razinu čine mjere koje usmjerivački protokol poziva, a implementirane su na nekom drugom sloju mrežnog modela. U slučaju predloženog modularnog sigurnosnog okvira namijenjenog IPv6-temeljenim BSM modul za sigurno usmjeravanje povezan je sa kriptografskim modulom. Ovi moduli međusobno komuniciraju, pri čemu usmjerivački modul koristi usluge kriptografskog modula za realizaciju usluge sigurnog usmjeravanja. Ovakav pristup prožima sve slojeve mrežnog modela i mehanizam sigurnog usmjeravanja čini sastavnim dijelom jedinstvenog modularnog sigurnosnog okvira. Takav pristup za BSM je značajno prihvatljiviji od pristupa kog kojeg bi sve sigurnosne mjere

bile izravno implementirane unutar samog usmjerivačkog protokola i funkcionirale neovisno o preostalim komponentama jedinstvenog sigurnosnog okvira.

RPL protokol je prvi (i za sada jedini) usmjerivački protokol predložen od radne skupine ROLL *(Routing over Low-power and Lossy Networks)* namijenjen LLN mrežama, i kao takav jedini za sada prikladan za BSM temeljene na IPv6 protokolu. Zbog toga upravo on predstavlja jezgru modula za sigurno usmjeravanje iz cjelovitog sigurnosnog okvira za IPv6-temeljene BSM.

Na slici 5.4 prikazani su podatkovni tokovi kod RPL protokola, pri čemu su vidljive glavne funkcionalne komponente koje mogu biti izložene napadu ili zlouporabi.



Slika 5.4 Podatkovni tokovi kod RPL protokola

Sigurnosne prijetnje usmjerene ka RPL protokolu napadač može realizirati kroz napade na njegove DIO, DIS i DAO poruke, kao i na informacije sadržane u *IPv6 Hop-by-Hop Option* zaglavlju i IPv6 usmjerivačkom zaglavlju *(IPv6 Routing Header)*. Prema tome, sigurnosne mjere implementirane u RPL protokol trebaju omogućiti: očuvanje autentičnosti i integriteta DIO, DIS i DAO poruka, kao i spriječiti njihovu naknadnu retransmisiju od strane napadača [28]. Također, potrebno je osigurati da samo ovlašteni entitet može pristupiti sadržaju ovih poruka. U RPL protokol treba uključiti podesive mehanizme sigurnosti, kako bi se mogao postići kompromis između zahtjeva za resursima i sigurnosnih zahtjeva pojedine aplikacije. RPL protokol bi se trebao oslanjati na neku od simetričnih kriptografskih metoda (temeljenih na tajnim ključevima), pri čemu se podrazumijeva i primjena odgovarajuće sheme za upravljanje ključevima. Usluge kriptiranja i upravljanja kriptografskim ključevima modulu

za usmjeravanje pruža kriptografski modul. Prilikom razmatranja očekivane razine sigurnosti (promatrano iz perspektive aplikacije) potrebno je sagledati funkcije različitih RPL kontrolnih poruka i informacije koje se prenose unutar IPv6 zaglavlja (posebice u zaglavljima koja se procesiraju prilikom svakog skoka). Primjerice, DIO poruke koriste se prilikom izgradnje ruta ka korijenskom čvoru, dok se DAO poruke koriste prilikom izgradnje ruta ka perifernim čvorovima. U nekim aplikacijama smjerovi ruta mogu biti od različitog značaja, pa se za rute ka korijenu i rute ka perifernim čvorovima mogu koristiti različite sigurnosne mjere. Prema tome, poželjno je da sigurnosni mehanizam ugrađen u RPL protokol omogućava podešavanje sigurnosnih svojstava prema različitim tipovima kontrolnih poruka (DIO, DIS, DAO).

U tablici 5.1 pregledno su prikazane preporučene sigurnosne mjere koje implementira modul za sigurno usmjeravanje iz cjelovitog sigurnosnog okvira za IPv6-temeljene BSM. Pri tome su ove mjere razdvojene u dvije skupine: prva skupina uključuje sigurnosne mjere koje su obvezne, dok drugu skupinu čine mjere koje su preporučljive, te se korisniku ostavlja mogućnost izbora sigurnosnih mjera koje će se primijeniti ovisno o konkretnoj aplikaciji senzorske mreže.

TABLICA 5.1 Sigurnosne mjere modula za sigurno usmjeravanje

Obvezne sigurnosne mjere	Preporučene sigurnosne mjere
• Autentifikacija čvorova koji komuniciraju • Enkripcija podatkovnog dijela paketa • Provjera integriteta poruke • Provjera ispravnosti redoslijeda poruka • Primjena višestaznog *(multi-path)* usmjeravanja • Provjera autentičnosti i integriteta DIO, DIS i DAO poruka i onemogućavanje njihove retransmisije	• Osiguranje privatnosti geografskih informacija o čvorovima • Omogućiti tuneliranje prometa između dva dijela mreže (prema potrebi) • Omogućiti balansiranje opterećenja • Podrška za slučajni izbor alternativnih ruta • Limitiranje količine prometa unutar određenog vremenskog intervala • Osiguranje senzorskih čvorova od fizičkog pristupa • Mehanizam za provjeru vrijednosti pojedinih parametara (praćenje odstupanja od očekivanih vrijednosti) • Mehanizam za praćenje učestalosti pojedinih poruka • Omogućiti podešavanje sigurnosnih svojstava prema različitim tipovima kontrolnih poruka (DIO, DIS, DAO)

5.3. Modul za sigurnu agregaciju podataka

U većini praktičnih primjena bežičnih senzorskih mreža podaci sa velikog broja senzorskih čvorova u konačnici se prikupljaju na zajedničkom mjestu – baznoj stanici ili računalu. Kako bi se uštedjelo na potrebnim resursima (prvenstveno energetskim) u većini slučajeva se provodi agregacija podataka na posrednim (intermedijarnim) čvorovima preko kojih podaci putuju od svojeg izvora ka baznoj stanici. Međutim, velika većina sustava i algoritama koji se koriste za agregaciju podataka ne implementira nikakve sigurnosne mjere, te su kao takvi osjetljivi na različite vrste napada. Ranjivost ovakvih sustava može dovesti do ozbiljnih problema, budući da napadač u postupku agregacije može umetnuti lažne informacije, te na taj način u velikoj mjeri utjecati na numeričke vrijednosti pojedinih promatranih parametara koje se prikupljaju na baznoj stanici.

Prilikom agregacije podataka obično se primjenjuje jedna od nekolicine karakterističnih funkcija, najčešće srednja vrijednost prikupljenih podataka, minimalna ili maksimalna vrijednost, ili prebrajanje određene karakteristične vrijednosti. Agregacijom podataka u velikim senzorskim mrežama (kombiniranjem parcijalnih rezultata) značajno se smanjuje potreba za komunikacijom među čvorovima, što u velikoj mjeri štedi energiju i produljuje životni vijek mreže [6].

Za prikupljanje podataka senzorske mreže koriste jedan od dva sustava: sustav temeljen na upitima *(query-based)* i sustav temeljen na događajima *(event-based)*. U sustavu temeljenom na upitima bazna stanica mrežom razašilje upite, na koje senzorski čvorovi odgovaraju slanjem relevantnih informacija. Pri tome se poruke poslane s pojedinačnih čvorova prilikom usmjeravanja ka baznoj stanici agregiraju (združuju), da bi se konačna agregacija prikupljenih podataka dogodila na samoj baznoj stanici. Bazna stanica upite obično razašilje u unaprijed definiranim vremenskim intervalima. U sustavu temeljenom na događajima senzorski čvor šalje podatke baznoj stanici samo u slučaju pojave određenog događaja u njegovoj neposrednoj okolini (okolini koju nadzire).

Napadi orijentirani na mehanizam agregacije podataka obično su orijentirani na ubacivanje lažnih informacija u mrežu (posebice u BSM koje prikupljaju podatke u slučaju pojave određenog događaja, kada napadač često može namjerno izazivati lažni alarm) ili na modifikaciju podataka koji nastaju agregacijom senzorskih očitanja. Napadač to može postići na nekoliko različitih načina. Prvi način je ubacivanje lažnih podataka kako bi se namjerno

izazvala velika pogreška u krajnjem rezultatu procesa agregacije podataka (na baznoj stanici). Drugi pristup podrazumijeva namjerno odbacivanje poruka koje sadrže parcijalno agregirane podatke, što opet u konačnici značajno utječe na krajnji rezultat na baznoj stanici. Nadalje, napadač može u mrežu ubacivati lažna očitanja svojih senzora, kao i falsificirati postupak parcijalne agregacije (ukoliko u njoj sudjeluje).

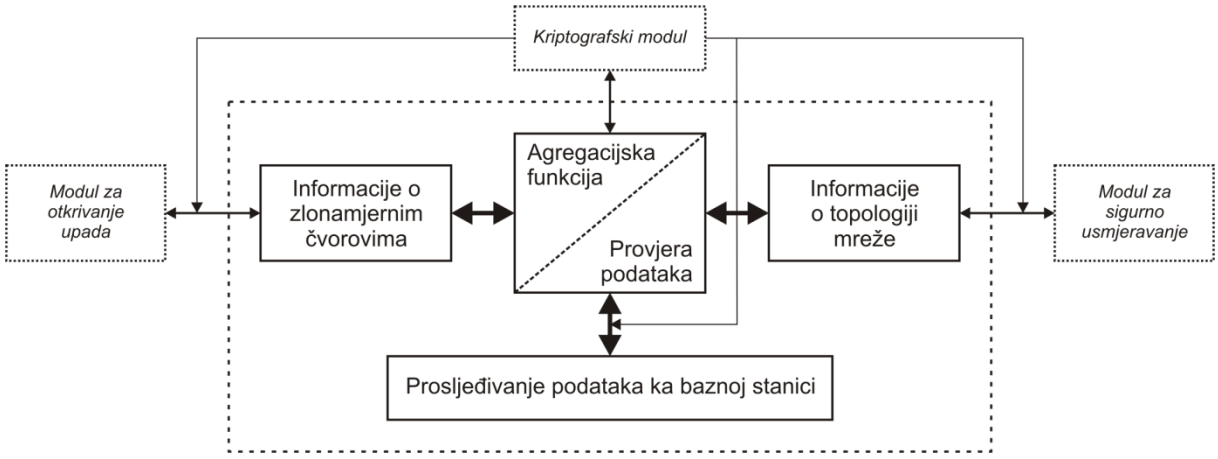
Moguća zlouporaba tehnike za agregaciju podataka u senzorskoj mreži potakla je određene pokušaje pronalaska sigurnijih metoda koje bi se u tu svrhu mogle primijeniti u BSM. Neka predložena rješenja orijentiraju se na mreže u kojima se agregacija podataka obavlja samo na jednom čvoru (baznoj stanici). Pri tome se pokušava pronaći agregacijska funkcija koja će kao rezultat dati ispravnu informaciju čak i u prisustvu nekolicine kompromitiranih čvorova. Ova funkcija se ne može oslanjati na većinsko odlučivanje, budući da bi u slučaju kompromitacije jednog dijela čvorova takva funkcija davala netočne rezultate. Zbog toga se kao veliki problem javlja izbor adekvatne agregacijske funkcije koja bi bila otporna na određeni postotak lažnih podataka (budući da bi bilo puno kompliciranije vršiti pojedinačnu provjeru autentičnosti svakog senzorskog očitanja).

U članku [117] dan je teorijski okvir za modeliranje sigurnosti postupka agregacije podataka. Ovdje se agregacijske funkcije zapravo promatraju kao statistički estimatori, gdje je za niz observacija (senzorskih očitanja) prema poznatoj parametriziranoj razdiobi potrebno pronaći skriveni parametar razdiobe (nije unaprijed specificiran). Kao mjera netočnosti podatka nakon postupka agregacije koristi se RMS pogreška *(root mean square)*, čiji iznos ovisi o broju kompromitiranih čvorova. U slučaju da iznos RMS pogreške sporo raste s porastom broja kompromitiranih čvorova izabrana agregacijska funkcija smatra se otpornom na napade i prikladnom za postupak agregacije. Provedena razmatranja rezultirala su zaključcima da funkcije maksimum, minimum i srednja vrijednost nisu otporne na napade, te kao takve nisu prikladne za obavljanje agregacije podataka u okruženju u kojem je moguća kompromitacija dijela podataka. Funkcija prebrojavanja *(count)* pokazuje se otpornom na napade, dok se kao robusnija zamjena za srednju vrijednost predlaže uporaba funkcije medijan.

Prilikom postupka agregacije poželjno je i ograničiti mogući raspon vrijednosti senzorskih očitanja. Na takav način se napadaču onemogućava ubacivanje lažne vrijednosti koja u jako velikoj mjeri odstupa od očekivanih, i time značajno narušava krajnji rezultat. Također, obično se prije postupka agregacije maksimalna i minimalna vrijednost odbacuju.

U usporedbi sa shemom agregacije koja podrazumijeva postojanje samo jednog čvora agregatora (obično bazna stanica), puno je kompliciranije dizajnirati siguran hijerarhijski protokol za agregaciju, koji podrazumijeva da se postupak agregacije vrši kroz nekoliko faza (na nekoliko čvorova) između krajnjeg čvora i bazne stanice. Pristup koji podrazumijeva hijerarhijsku agregaciju podrazumijeva da mreža mora biti podijeljena na više logičkih cjelina (klastera). Agregacija podataka obavlja se unutar svakog klastera, te se agregirani podatak prosljeđuje dalje, nadređenom čvoru unutar hijerarhije. Nakon što se agregirani podaci iz više klastera prikupe na baznoj stanici provodi se njihova analiza u svrhu pronalaženja sumnjivih (potencijalno malicioznih) podataka. Ukoliko se neki podaci okarakteriziraju sumnjivim, oni se prije finalnog postupka agregacije izbacuju van. Obično se u takvim slučajevima pretpostavlja da je bazna stanica apsolutno sigurna i da ne može biti kompromitirana.

Mehanizam za sigurnu agregaciju podataka u BSM ne može funkcionirati samostalno, nego treba biti uklopljen u jedinstveni sigurnosni okvir, kako bi mogao koristiti usluge drugih sigurnosnih mehanizama implementiranih u BSM. Tako, primjerice, mehanizam za sigurnu agregaciju može prilikom razmjene podataka koristiti mehanizme za autentifikaciju i enkripciju, te usko surađivati sa protokolom za sigurno usmjeravanje prilikom podjele mreže na klastere.



Slika 5.5 Modul za sigurnu agregaciju podataka

Modul za sigurnu agregaciju podataka unutar predloženog sigurnosnog okvira za IPv6-temeljene BSM zadužen je za provedbu agregacije prikupljenih podataka na siguran način (slika 5.5). Budući da je arhitektura cjelokupnog sigurnosnog okvira modularna (kako bi korisnik mogao potrebne sigurnosne mjere prilagoditi konkretnoj mreži u konkretnoj situaciji)

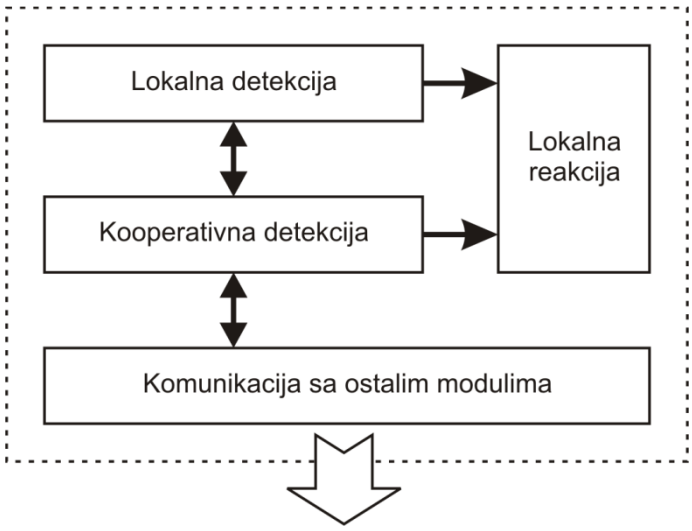
tako i modul za sigurnu agregaciju omogućava korisniku izbor željenih funkcija i parametara. Štoviše, korisniku se ostavlja na izbor hoće li uopće koristiti usluge modula za agregaciju, ili će se svi podaci sa svih senzora prikupljati na baznoj stanici (ovo u velikoj mjeri ovisi o veličini senzorske mreže, kao i o učestalosti prikupljanja novih podataka i njihovoj veličini, a određeno je konkretnom primjenom mreže). Ukoliko se koriste usluge modula za agregaciju podataka korisnik bira agregacijsku funkciju, te definira očekivani raspon vrijednosti senzorskih očitanja. Modul za sigurnu agregaciju koristi usluge preostalih modula iz jedinstvenog sigurnosnog okvira: kriptografskog modula, modula za sigurno usmjeravanje i modula za otkrivanje upada. Usluga kriptografskog modula koristi se za kriptiranje i dekriptiranje podataka prilikom parcijalne agregacije podataka na nekom od čvorova između izvorišnog čvora i bazne stanice. Ukoliko se primjenjuje postupak hijerarhijske agregacije (agregacija kroz nekoliko koraka na nekoliko intermedijarnih čvorova) od modula za sigurno usmjeravanje agregacijski modul dobiva sve potrebne informacije o trenutnoj strukturi i topologiji mreže, kao i o trenutno uspostavljenim rutama ka baznoj stanici. Modul za sigurnu agregaciju komunicira i s modulom za otkrivanje upada i zlonamjernog ponašanja čvorova. Na temelju informacija dobivenih od modula za otkrivanje upada modul za sigurnu agregaciju iz prikupljenog skupa senzorskih podataka može isključiti podatke dobivene od zlonamjernih čvorova, te na taj način spriječiti da oni negativno utječu na krajnji rezultat agregacije.

Za uspješno provođenje postupka agregacije podataka na siguran način, bez negativnog utjecaja pogrešnih senzorskih očitanja, kvara ili kompromitacije čvorova potrebno je uvažiti sljedeće preporuke:

- Pravilno izabrati agregacijsku funkciju, koja će ispravno pratiti niz senzorskih očitanja unutar očekivanog raspona vrijednosti
- Ograničiti mogući raspon vrijednosti očitanja
- Prije postupka agregacije odbaciti maksimalnu i minimalnu vrijednost
- Umjesto srednje vrijednosti koristiti funkciju medijan
- Ne razmatrati očitanja senzorskih čvorova za koje je utvrđeno zlonamjerno ponašanje
- Provjeravati točnost podataka nakon agregacije (primjena RMS funkcije uz analizu brzine rasta pogreške)
- Koristiti kriptografske tehnike prilikom slanja djelomično ili u potpunosti agregiranih podataka (radi očuvanja njihove povjerljivosti i integriteta)

5.4. Modul za otkrivanje upada i zlonamjernog ponašanja senzorskih čvorova

Sustav za otkrivanje upada i zlonamjernog ponašanja postojećih mrežnih čvorova predstavlja jednu od najvažnijih komponenti cjelovitog sigurnosnog okvira, pa tako i sigurnosnog okvira namijenjenog IPv6-temeljenim BSM. Dosadašnji istraživački napori rezultirali su nekolicinom prijedloga ovakvih sustava, što je detaljnije analizirano u poglavlju 4. Međutim, sva dosadašnja predložena rješenja orijentirana su na klasične BSM. S integracijom IPv6 protokola u BSM i pojavom prvih IPv6-temeljenih BSM ukazuje se potreba za razvojem sličnih sustava namijenjenih ovakvoj vrsti mreža. Prepoznavanje ovog problema također je bio jedan od temeljnih motiva za izradu ove disertacije, tako da je kroz nju predložen i razvijen upravo takav jedan sustav. Predloženi sustav je po svojoj prirodi distribuiran, a izvršava se na aplikacijskom sloju slojevitog mrežnog modela. Detaljan opis, analiza i rezultati testiranja predloženog sustava dani su u poglavlju 6. Ovaj sustav integrira se u jedinstveni sigurnosni okvir namijenjen IPv6-temeljenim BSM kao modul za otkrivanje upada i zlonamjernog ponašanja senzorskih čvorova. Modul za otkrivanje upada čine dva osnovna podmodula: modul za lokalnu detekciju i modul za kooperativnu detekciju (slika 5.6). Detaljnija struktura i opis funkcionalnosti predloženog rješenja dani su u poglavlju 6.



Slika 5.6 Modul za otkrivanje upada

Neke osnovne preporuke koje treba zadovoljavati modul za otkrivanje upada uklopljen u cjeloviti sigurnosni okvir su:

- Minimalna potrošnja strogo ograničenih resursa senzorskih čvorova
- Distribuirana arhitektura koja sustavu omogućava nastavak rada čak i u slučaju kvara ili kompromitacije određenog broja senzorskih čvorova
- Puna podrška za IPv6 protokol u okruženju bežične senzorske mreže
- Minimalno narušavanje performansi mreže
- Visok postotak ispravnosti detekcije zlonamjernog ponašanja (unatoč okruženju sklonom učestalim kvarovima, smetnjama i gubicima podatkovnih paketa koji nisu prouzročeni zlonamjernom aktivnošću)
- Potpuna integriranost u cjeloviti sigurnosni okvir, koja podrazumijeva komunikaciju i suradnju sa preostalim modulima iz sigurnosnog okvira

Predloženi sustav za otkrivanje upada u najvećoj mogućoj mjeri nastoji zadovoljiti sve navedene preporuke, što je vidljivo iz rezultata njegove detaljne analize koji su dani u poglavlju 6.

Implementacija pojedinačnih sigurnosnih mehanizama često nije dovoljna za prevenciju i otkrivanje eventualnih napada ili zlouporaba koje se mogu pojaviti unutar senzorske mreže. Zahtijevana i očekivana razina sigurnosti u BSM mogu se postići tek kroz sinergiju više različitih sigurnosnih mehanizama objedinjenih unutar zajedničkog i cjelovitog sigurnosnog okvira koji prožima sve slojeve mrežnog modela.

6. Distribuirani adaptivni sustav za otkrivanje zlonamjernog ponašanja senzorskih čvorova u BSM temeljenoj na IPv6 protokolu

Prethodna poglavlja analiziraju problematiku prelaska sa stare verzije IP protokola (IPv4) na novu, znatno napredniju i poboljšanu verziju 6 (IPv6). Također, razmatra se problematika implementacije IPv6 protokola u bežične senzorske mreže, kao vrlo specifičnu podvrstu bežičnih mreža sa vrlo strogim ograničenjima koja ih u velikoj mjeri razlikuju od drugih vrsta bežičnih mreža. Pri ovim razmatranjima naglasak je stavljen na sigurnosne aspekte i sigurnosne mehanizme. Također, daje se i prijedlog cjelovitog sigurnosnog okvira namijenjenog bežičnim senzorskim mrežama temeljenim na IPv6 protokolu.

Problematika sigurnosti i implementacija sigurnosnih mehanizama u bežičnim senzorskim mrežama temeljenim na IPv6 protokolu do danas nije na adekvatan način riješena. S druge strane, pitanje sigurnosti u mreži vrlo je bitan čimbenik koji u velikoj mjeri utječe na njezinu praktičnu uporabljivost i proširenje mogućih područja primjene. U pogledu sigurnosti brojna otvorena pitanja i neriješeni problemi postoje i u „klasičnim“ bežičnim senzorskim mrežama, a posebice u onima temeljenim na IPv6 protokolu.

Brojni su problemi koji se javljaju u takvim mrežama, a koji imaju izravan utjecaj na problematiku sigurnosti. Neki od karakterističnih problema su:

- Ograničenost resursa, velik broj čvorova, niska propusnost linkova i mali datagrami (što implicira nužnost svođenja komunikacije na minimum i prijenos što manje količine podataka)
- Ograničeni resursi onemogućavaju uporabu IPsec protokola i tradicionalnih kriptografskih metoda (npr. kriptografije javnog ključa)
- Potreba za sigurnosnim rješenjima na drugom sloju
- Mnogobrojne mogućnosti napada (aktivni i pasivni, interni i eksterni tipovi napada)
- Brojne sigurnosne prijetnje: fizički napad, uskraćivanje ili iscrpljivanje resursa, napadi na mehanizme usmjeravanja, *sinkhole*, *sybil*, *wormhole* napadi...
- Problematika upravljanja kriptografskim ključevima: inicijalizacija, revokacija ključeva, detekcija kompromitacije ključeva, dinamičko dodavanje novih čvorova...

- Neprimjenjivost postojećih sigurnosnih rješenja iz MANET ili „klasičnih“ bežičnih senzorskih mreža (zbog IPv6 protokola)
- Pojava novih ranjivosti i prijetnji specifično vezanih uz IPv6 protokol (zbog novih mrežnih mehanizama, primjerice postupka otkrivanja susjednih čvorova)

Iz niza navedenih problema posebno se izdvaja problematika razvoja IDS sustava (za otkrivanje napada i zlonamjernih čvorova) koji bi bio primjenjiv na bežične senzorske mreže temeljene na IPv6 protokolu, budući da za sada ne postoji niti jedno adekvatno rješenje koje je posebno prilagođeno i namijenjeno ovakvom okruženju. Razvoj ovakvog sustava mora podrazumijevati poboljšanje postojećih metoda i njihovu prilagodbu za mogućnost primjene u ovakvim mrežama. S obzirom na vrlo stroga ograničenja raspoloživih resursa potrebno je izvršiti optimizaciju predloženog rješenja u pogledu energetskih zahtjeva i zahtjeva za računalnim resursima (memorija i CPU). Potrebno je omogućiti detekciju različitih tipova napada karakterističnih za ovakve mreže, pri čemu sustav treba biti distribuiran i decentraliziran, uz toleranciju na kvarove pojedinih čvorova. Također, potrebno je provesti detaljna testiranja ovakvog sustava, provesti simulaciju njegovog rada, te implementirati ga u realnom okruženju. IDS sustav namijenjen IPv6-temeljenoj BSM integrira se kao važan modul unutar cjelovitog modularnog sigurnosnog okvira namijenjenog ovakvim mrežama.

6.1. Zahtjevi koje sustav treba zadovoljiti

U različitim vrstama komunikacijskih mreža, pa tako i u bežičnim senzorskim mrežama, postoje različite metode koje se mogu primijeniti kako bi se mreža zaštitila od različitih vrsta napada (npr. enkripcija podataka, sigurni protokoli usmjeravanja i sl.). Primjena ovakvih metoda u BSM onemogućava određenoj kategoriji napadača pristup podacima unutar mreže i narušavanje njezinog normalnog rada. Međutim, uvijek postoji određena kategorija „jakih“ napadača koji su takve mehanizme u stanju zaobići (pogotovo kod BSM, kada napadač često raspolaže znatno većim resursima od tipičnog senzorskog čvora). Zbog toga vrlo važan sigurnosni mehanizam predstavlja sustav za otkrivanje neovlaštenih upada *(IDS, Intrusion Detection System)*, koji je u stanju detektirati pokušaj neovlaštenog napadača da zlorabi sigurnosne ranjivosti koje postoje u mreži.

Sustavi za otkrivanje neovlaštenih upada namijenjeni bežičnim senzorskim mrežama zbog specifičnosti ove vrste mreža još uvijek predstavljaju slabo istraženo područje. Ipak, ovo područje u posljednje vrijeme privlači sve veće zanimanje istraživačke zajednice. Kao specifičan problem izdvajaju se bežične senzorske mreže temeljene na IPv6 protokolu. Prisutan je trend implementacije IPv6 protokola u BSM kako bi se one što lakše i učinkovitije integrirale u globalnu mrežu. Međutim, za sada još ne postoji sustav koji bi detektirao upade i zlonamjerno ponašanje senzorskih čvorova posebno prilagođen za BSM temeljene na IPv6 protokolu.

Sustav za otkrivanje zlonamjernih aktivnosti u BSM temeljenim na IPv6 protokolu mora zadovoljiti vrlo slične opće kriterije kao i u „klasičnim“ BSM. Sustav mora osigurati automatizirani mehanizam koji će identificirati izvor napada (zlonamjerni mrežni čvor), te generirati odgovarajući alarm kako bi se o tome informirao ostatak mreže (ponekad i mrežni administrator) radi poduzimanja odgovarajućih preventivnih akcija. Pri tome se pod napadom može podrazumijevati svaka akcija usmjerena protiv informacija, računalnih ili komunikacijskih resursa u BSM. Napadač može za napad koristiti svoje vlastite (eksterne) resurse (napad „izvana“) ili zlorabiti postojeće mrežne čvorove zaobilazeći legitimne ovlasti (napad „iznutra“). Važno je napomenuti da sustav za otkrivanje upada nije u mogućnosti spriječiti pokušaje napada (to niti nije njegova zadaća), nego ih u slučaju pojave detektirati i poduzeti odgovarajuću reakciju.

Kako bi sustav mogao detektirati napad on mora biti u stanju razlučiti razliku između normalnih (legitimnih) aktivnosti u mreži i onih abnormalnih, koje mogu indicirati da je u mreži prisutna maliciozna aktivnost. Ovo je vrlo ozbiljan problem, budući da uzorci legitimnog ponašanja u mreži često mogu biti nejasni i nepredvidljivi, posebice u složenijim mrežama sa velikim brojem čvorova. Za razlučivanje i klasifikaciju ovih aktivnosti najčešće se koristi jedna od tri tehnike: detekcija zlouporabe *(misuse detection)*, detekcija anomalija *(anomaly detection)* i detekcija na temelju specifikacije *(specification-based detection)*, koja predstavlja svojevrsnu kombinaciju prethodne dvije.

Kod tehnike otkrivanja upada detekcijom zlouporabe trenutne aktivnosti („ponašanje“) u mreži uspoređuju se sa uzorcima ponašanja koji odgovaraju malicioznim aktivnostima („potpisi“ napada, *signatures*). Zbog toga se često ova metoda naziva detekcijom temeljenom na potpisima *(signature-based detection)*. Nedostatak ove metode je mogućnost otkrivanja isključivo onih zlonamjernih aktivnosti za koje postoji pohranjen odgovarajući „potpis“.

Tehnika detekcije anomalija umjesto na „potpise“ napada orijentirana je na analizu „normalnog“ ponašanja mreže. Sustav najprije definira što podrazumijeva „normalno“ ponašanje (najčešće učenjem kroz odgovarajući vremenski period). Potom statistički značajnija odstupanja od ovog uzorka klasificira kao moguće zlonamjerne aktivnosti. Prednost ovakvog pristupa je mogućnost detekcije novih vrsta napada, a glavni nedostatak nešto veći broj lažnih alarma (budući da će i neka legitimna odstupanja od uobičajenog ponašanja mreže biti najčešće prepoznata kao zlonamjerna). Tehnika detekcije na temelju specifikacije kombinira svojstva prethodne dvije tehnike. Također se temelji na detekciji odstupanja od normalnog ponašanja mreže. Međutim, do uzorka normalnog ponašanja u ovom slučaju sustav ne dolazi „učenjem“, nego postoje „ručno“ definirane specifikacije koje opisuju normalno ponašanje. Sustav analizira ponašanje mreže na temelju ovih zadanih specifikacija. Na taj način će se izbjeći česta pojava lažnih alarma, a istovremeno će sustav biti u stanju detektirati i neke nove napade. Također, velika prednost ovakvog pristupa je njegova manja zahtjevnost u pogledu resursa, što ga od tri navedena pristupa čini najprikladnijim za primjenu u bežičnim senzorskim mrežama. Zbog toga je ovaj pristup izabran za implementaciju u sustav za detekciju zlonamjernog ponašanja u BSM temeljenim na IPv6 protokolu. Važno je napomenuti da se specifikacije koje definiraju normalno ponašanje moraju formulirati posebno za svaku konkretnu implementaciju mreže. Zbog iznimno velike raznolikosti bežičnih senzorskih mreža, ovisno o njihovoj strukturi i aplikaciji, nije moguće definirati „univerzalne“ specifikacije koje bi zadovoljavale sve mreže. Zato njihovi parametri obavezno moraju biti prilagodljivi i konfigurabilni, kako bi se mogli prilagoditi i optimizirati za konkretnu mrežu. Definiranje i formulacija ovih specifikacija nije nimalo jednostavan zadatak, budući da brojni utjecaji iz okoline, kao i unutrašnji faktori (npr. napunjenost baterije) značajno utječu na rad mreže i uzorak njezinog „normalnog ponašanja“.

Kao što je ranije rečeno, u pogledu arhitekture razlikuju se dvije vrste sustava za otkrivanje neovlaštenih upada: HIDS *(host-based IDS)* i NIDS *(network-based IDS)*. HIDS sustav orijentiran je na jedno računalo, odnosno jedan mrežni čvor (u kontekstu BSM to bi bio jedan bežični senzorski čvor). Sve odluke donose se na temelju podataka prikupljenih sa tog mrežnog čvora, i nemoguće je detektirati napade usmjerene na cjelokupnu mrežu. Već je iz toga jasno da ovakva arhitektura nije prikladna za bežične senzorske mreže, koje su po svojoj prirodi potpuno distribuirane.

NIDS sustav kao izvor informacija koristi mrežni promet (analizira mrežne pakete). U žičnim mrežama mrežni promet je moguće analizirati na specifičnim mrežnim čvorištima na

kojima se promet koncentrira (preklopnici, usmjerivači, *gateway*-i). U bežičnoj senzorskoj mreži ne postoje ovakve specifične točke pogodne za analizu mrežnog prometa, budući da je mreža u potpunosti distribuirana i da svaki senzorski čvor može obavljati funkciju usmjeravanja mrežnog prometa.

Zbog distribuirane prirode bežične senzorske mreže potrebno je posebno planirati raspored IDS modula (agenata). Kao najprikladnije rješenje nameće se implementacija identičnih IDS modula na svaki senzorski čvor unutar BSM. Ovi moduli trebaju međusobno komunicirati i surađivati prilikom odlučivanja, što znači da se sustav mora temeljiti na kooperativnim algoritmima, i pri tome trošiti što je moguće manje resursa (računalnih, komunikacijskih i energetskih). Upravo na ovakvom načelu zasnovan je i IDS sustav namijenjen BSM temeljenim na IPv6 protokolu.

Drugi mogući pristup primjenjiv u BSM podrazumijeva hijerarhijsku strukturu IDS sustava. Kod ovakvog pristupa IDS moduli postavljeni na senzorske čvorove nisu svi međusobno jednaki. Postoje moduli više razine koji se postavljaju na nekolicinu čvorova (obično se radi o čvorovima koji raspolažu i nešto većim resursima), te moduli niže razine koji se implementiraju na ostale čvorove.

Budući da su BSM uglavnom u potpunosti distribuirane strukture, prirodno je da se i postupak odlučivanja o karakterizaciji određenog događaja zlonamjernim (malicioznim) mora provoditi kooperativno, kroz suradnju susjednih senzorskih čvorova. Svaki čvor pojedinačno nadzire svoje susjedne čvorove (čvorove koji su mu unutar dometa radio primopredajnika). Nakon što senzorski čvor detektira zlonamjerno ponašanje svojeg susjeda on pokreće kooperativni postupak otkrivanja upada zajedno sa preostalim susjedima. Pri tome se konačna odluka najčešće donosi većinskim odlučivanjem. Slična načela odlučivanja primjenjivala su se i u bežičnim ad hoc mrežama, kao i u „klasičnim“ BSM.

Kompromitirani senzorski čvor može svojim susjedima slati lažne (falsificirane) podatke kako bi prikrio svoju malicioznu aktivnost, ili čak za nelegalno ponašanje „optužio“ neki drugi legitimni senzorski čvor. Ovu činjenicu potrebno je uzeti u obzir prilikom razrade mehanizma za kooperativno odlučivanje. Prema tome, temeljna pretpostavka mora biti da se niti jedan senzorski čvor ne može smatrati apsolutno povjerljivim (sigurnim). Međutim, napadač nije u mogućnosti lako preuzeti kontrolu nad velikim brojem čvorova iz određenog područja. Zbog toga se sa velikom vjerojatnošću većina čvorova iz određenog područja može smatrati povjerljivim (nekompromitiranim), dok se tek manji dio čvorova smatra

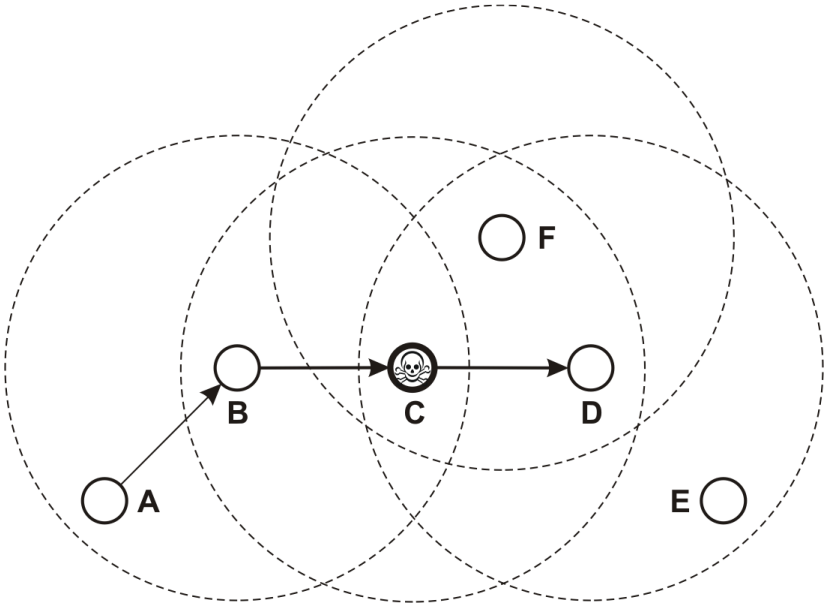
kompromitiranim. Zahvaljujući tome moguće je sa dovoljnom pouzdanošću primijeniti kooperativne mehanizme odlučivanja temeljene na većinskom odlučivanju. Ovakav pristup primijenjen je i u IDS sustavu namijenjenom IPv6-temeljenim BSM.

Alternativa distribuiranom odlučivanju jest sustav u kojem postoji određeni broj čvorova koji neovisno jedan o drugom samostalno provode postupak odlučivanja na temelju podataka prikupljenih od susjednih čvorova. Prednost ovakvog sustava je u njegovoj jednostavnosti i manjoj potrošnji resursa (kod izvršavanja kooperativnih algoritama odlučivanja velik dio energije troši se na komunikaciju između čvorova prilikom razmjene informacija). Veliki nedostatak ovakvog sustava jest činjenica da napadač može onesposobiti (kompromitirati) nekog od čvorova koji su zaduženi za odlučivanje, te na taj način u potpunosti ukloniti zaštitu sa jednog dijela mreže. Također, čvorovi koji donose odluku troše značajno više resursa od ostalih (budući da obavljaju procesiranje prikupljenih informacija), što dovodi do ubrzanog pražnjenja baterije (stoga je poželjno da se čvorovi u ovoj ulozi dinamički izmjenjuju kako bi se izbalansirala ukupna potrošnja).

Implementacija mrežno orijentiranog, distribuiranog adaptivnog IDS sustava u BSM temeljenu na IPv6 protokolu podrazumijeva da mrežni čvorovi moraju pratiti i nadzirati promet u mreži. Kako je mreža distribuirane prirode, ne postoje neke karakteristične točke na kojima je to moguće učiniti nego tu zadaću mora obavljati svaki čvor. Najpogodnija metoda koja se može u tu svrhu iskoristiti, a poznata je još iz bežičnih ad hoc mreža i klasičnih BSM, jest tzv. *watchdog* tehnika.

Watchdog tehnika temelji se na činjenici da je komunikacija u BSM bežična i da su senzorski čvorovi prostorno relativno gusto raspoređeni, tako da uvijek postoji više senzorskih čvorova koji su međusobno bliski (unutar dometa radio veze). To znači da svaki paket koji se bežičnim putem u mreži prenosi od izvora do odredišta nije dostupan samo izvorišnom i odredišnom čvoru, nego ga mogu primiti i svi ostali njima bliski čvorovi (koji su u dometu). U slučaju normalne komunikacije senzorski čvorovi odbacuju pakete koji dolaze do njihovog mrežnog sučelja, a nisu njima namijenjeni. Međutim, prilikom implementacije IDS sustava upravo ovi paketi predstavljaju glavni izvor informacija na ulazu u sustav. U tom slučaju aktivni IDS modul pokrenut na senzorskom čvoru „osluškuje“ pakete koje šalju njegovi susjedi i na taj način prikuplja određene informacije koje zapravo predstavljaju ulazni parametar u proces distribuiranog odlučivanja o karakterizaciji ponašanja nekog mrežnog čvora.

Sljedeći primjer ilustrira neke situacije koje se mogu dogoditi u praksi, kada senzorski čvor ne može zaključiti što se dogodilo na susjednom čvoru, ili čak može donijeti pogrešan zaključak (slika 6.1).



Slika 6.1 Watchdog tehnika - primjer moguće pogreške

Pretpostavka je da čvor A šalje paket čvoru D kroz više skokova, preko čvorova B i C (putanja A – B – C – D). Također, pretpostavka je da je čvor C kompromitiran, te da selektivno odbacuje pakete i ne prosljeđuje ih ka čvoru D. Čvor B nakon što proslijedi paket čvoru C nadzire čvor C, odnosno promatra prosljeđuje li čvor C paket dalje ka čvoru D (tj. čvor B radi kao *watchdog*). Moguće su sljedeće situacije:

- Čvor C prosljeđuje paket čvoru D, no u isto vrijeme čvor A šalje paket čvoru B. U tom slučaju nastaje kolizija na čvoru B. Čvor B ne može odrediti koji paket je izazvao koliziju, pa prema tome ne može zaključiti kako se ponaša čvor C.
- Čvor C prosljeđuje paket čvoru D, dok u isto vrijeme čvor E započinje sa slanjem paketa. To izaziva koliziju na čvoru D, koju čvor B ne može detektirati budući da mu je čvor E izvan dometa. Čvor B zaključuje kako je čvor C uspješno proslijedio paket čvoru D, što zapravo nije točno.
- Čvor C prosljeđuje paket čvoru D, dok u isto vrijeme čvor D započinje sa emitiranjem. Tada dolazi do kolizije na čvoru D. Čvor B opet pogrešno zaključuje da je čvor C uspješno proslijedio paket čvoru D.

Navedene situacije zorno ilustriraju da za uspješno otkrivanje zlonamjernog ponašanja nekog čvora nikako nije dovoljan samo jedan *watchdog*. Zbog toga IDS sustav za IPv6-temeljene BSM prikuplja informacije od više *watchdog* čvorova iz okruženja, pri čemu čvorovi kooperativno donose krajnje zaključke.

Za promatranje cjelokupnog stanja na linku između dva čvora (npr. čvor C i čvor D iz prethodnog primjera) nije dovoljno da se samo jedan od njih nalazi u dometu *watchdog* čvora. U tom slučaju poželjno je da *watchdog* čvor bude čvor kojemu su oba promatrana čvora unutar dometa (tj. da su mu u dometu oba kraja linka kojeg nadzire). Tako bi, primjerice, čvor F mogao biti *watchdog* za kompletnu komunikaciju između čvorova C i D.

Na prvi pogled bi se moglo pretpostaviti da će praćenje mrežnog prometa pomoću *watchdog* čvorova drastično povećati potrošnju energije, budući da čvorovi „slušaju“ sav mrežni promet koji im je unutar dometa. Na sreću, to u praksi nije tako. Razlog tome je činjenica da u većini radiokomunikacijskih sustava koji se primjenjuju u današnjim senzorskim mrežama senzorski čvorovi ionako primaju pakete koje razašilju njihovi susjedi. Senzorski čvor ne može „unaprijed“ znati kome je paket namijenjen sve dok ga ne primi i ne provjeri odredišnu adresu. Prema tome, dodatni utrošak energije odlazi samo na dodatno procesiranje paketa, u ovom slučaju onih koji su adresirani na neke od susjednih čvorova (radiokomunikacijski dio, koji je inače najveći potrošač energije, ne zahtijeva u ovom slučaju nikakvu dodatnu potrošnju).

Prethodna razmatranja pokazuju da je najprikladnije rješenje za IDS sustav u BSM rješenje koje se temelji na međusobnoj suradnji senzorskih čvorova u postupku otkrivanja napada. Osim toga, postoje još neki dodatni zahtjevi i kriteriji koje IDS sustav mora zadovoljavati kako bi bio prikladan za implementaciju u senzorsku mrežu. Osnovni zahtjevi su sljedeći:

- **Distribuiranost**

  Sve aktivnosti IDS sustava (uključujući prikupljanje podataka, njihovu analizu, donošenje odluke i reakciju na otkriveni napad) trebaju biti u potpunosti distribuirane i temeljiti se na kooperativnim algoritmima i međusobnoj suradnji senzorskih čvorova. Primjenom distribuiranog rješenja u senzorskoj mreži postiže se i balansiranje opterećenja, te se na taj način resursi ravnomjernije troše.

- **Nepostojanje povjerljivih čvorova**

  Temeljna pretpostavka distribuiranog IDS sustava jest da se niti jedan mrežni čvor ne može smatrati apsolutno sigurnim niti povjerljivim. U senzorskim mrežama postoji veliki broj čvorova koji su u većini slučajeva vrlo slabo zaštićeni od fizičkog pristupa, te je stoga relativno lako kompromitirati bilo kojeg od njih (za razliku od primjerice žičnih mreža, u kojima napadač puno teže može ostvariti fizički pristup mrežnim uređajima). Prema tome, distribuirani IDS sustav mora pretpostaviti moguću kompromitaciju bilo kojeg čvora, i niti jedan se ne može smatrati apsolutno povjerljivim.

- **Lokalna analiza**

  Distribuirani IDS sustav za BSM mora operirati sa lokalno prikupljenim podacima (ne postoje centralizirana mjesta, osim bazne stanice, na kojima će se prikupljati podaci iz cjelokupne mreže). Također, sustav mora ostati funkcionalan i u slučaju da su mu na raspolaganju samo parcijalni podaci, dok dio podataka nedostaje (npr. nedostaju podaci sa onesposobljenih ili ometanih čvorova).

- **Minimalizacija potrošnje resursa**

  Moduli distribuiranog IDS sustava izvršavaju se na svakom senzorskom čvoru. Zbog toga njihova potrošnja resursa mora biti svedena na najmanju moguću mjeru. Također, prilikom razrade kooperativnog algoritma potrebno je međusobnu komunikaciju između čvorova i količinu podataka koju razmjenjuju što je moguće više reducirati, budući da primopredajnici u BSM troše najviše energije (utrošak energije za bežični prijenos jednog bita informacije je i do 1000 puta veći od energije potrebne za njegovo procesiranje). Treba uzeti u obzir i vrlo malu propusnost linkova kao i njihovu nestabilnost (česta pojava smetnji, pogrešaka prilikom prijenosa i potpunih prekida linkova). Zato komunikacija između IDS modula ne smije oduzeti prevelik dio kapaciteta linkova.

- **Mogućnost proširenja (dodavanja novih čvorova)**

  Budući da senzorska mreža predstavlja dinamičko okruženje u kojem se često javlja potreba za dodavanjem novih čvorova, IDS sustav mora podržavati mogućnost proširenja mreže. Također, bitno je da IDS bude u stanju razlikovati legitimno proširenje mreže (dodavanje novih čvorova) od određenih vrsta zlonamjernih aktivnosti (napada).

- **Sigurnost samog IDS sustava**

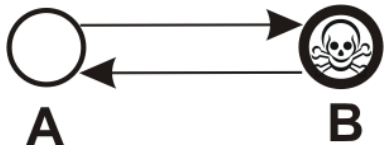
  IDS sustav sam po sebi (odnosno IDS moduli implementirani na senzorske čvorove) mora biti otporan na evenualne napade i kompromitaciju. Postoji realna opasnost da napadač kompromitira i preuzme kontrolu nad nekolicinom senzorskih čvorova, a samim time da preuzme kontrolu i nad IDS modulima (agentima) koji postoje na tim čvorovima. Ovakva situacija (barem dok je broj kompromitiranih čvorova ispod neke kritične vrijednosti) ne bi smjela onesposobiti cijeli IDS sustav i onemogućiti njegov rad. Unatoč kompromitaciji određenog broja agenata sustav mora sačuvati svoju funkcionalnost.

6.2. Problem otkrivanja upada i uvjeti njegovog rješavanja

Problem otkrivanja upada uključuje detekciju da je određeni senzorski čvor u mreži napadnut, kao i identifikaciju izvora napada. Pri tome se problem otkrivanja upada *(IDP, Intrusion Detection Problem)* zapravo svodi na pronalaženje algoritma koji mora zadovoljiti sljedeća svojstva:

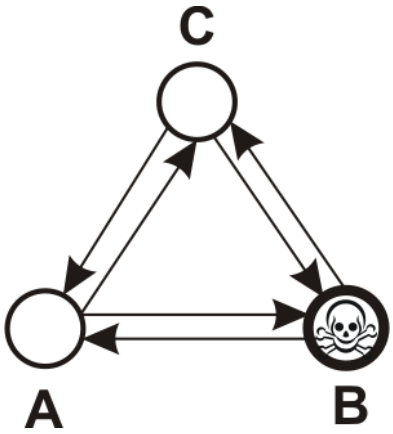
- Ukoliko legitimni čvor ukaže na potencijalno zlonamjerno ponašanje nekog drugog čvora, tada se taj legitimni čvor pridružuje skupu čvorova koji su aktivirali alarm, a potencijalno zlonamjerni čvor karakterizira se kao izvor napada.
- Ukoliko se napad događa, tada će nakon nekog konačnog vremenskog intervala svi legitimni čvorovi iz promatranog skupa ukazati na moguće zlonamjerno ponašanje nekog čvora.

Osnovna ideja kod kooperativnog mehanizma otkrivanja upada jest međusobna razmjena izlaznih informacija lokalnih IDS agenata (modula). Moduli međusobno razmjenjuju podatke o potencijalno zlonamjernim čvorovima, čime se sužava skup „sumnjivih“ čvorova (čvorova koji potencijalno predstavljaju izvor napada). Pretpostavka je da senzorski čvorovi do informacije o mogućim napadačima mogu doći isključivo pomoću IDS modula.



Slika 6.2 Problem otkrivanja upada - primjer dva čvora

Najjednostavniji mogući slučaj je situacija u kojoj postoje samo dva čvora (slika 6.2). Čvor A sumnja da je izvor napada čvor B (što je po pretpostavci točno). U tom slučaju čvor B može namjerno lažno tvrditi da je napadač čvor A. Međutim, budući da čvor A implicitno za sebe zna da nije zlonamjeran, on će ignorirati tvrdnju čvora B i indicirati čvor B kao napadača, te na taj način riješiti problem otkrivanja upada (IDP).



Slika 6.3 Problem otkrivanja upada - primjer tri čvora

Nešto složeniji slučaj je situacija u kojoj postoje tri čvora koji se međusobno sumnjiče za napad (svaki čvor sumnjiči preostala dva, pri čemu je po pretpostavci čvor B zlonamjeran). U tom slučaju se svaki čvor u skupu sumnjivih čvorova pojavljuje dva puta. Zbog toga čvor A (koji za sebe implicitno zna da nije napadač) ne može razlučiti koji je od preostala dva čvora (B ili C) doista zlonamjeran. U ovom slučaju nemoguće je razriješiti problem otkrivanja upada.

Nakon analize prethodna dva primjera nameće se pitanje o rješivosti problema otkrivanja upada u određenim situacijama. Općenito, za rješivost problema otkrivanja upada mogu postojati nužni uvjeti i dovoljni uvjeti. Uvjet je dovoljan ukoliko njegova točnost implicira da postoji algoritam koji rješava problem otkrivanja upada. Uvjet je nužan ako (i samo ako)

postojanje algoritma za rješavanje problema otkrivanja upada implicira da je taj uvjet zadovoljen (točan).

Neka je:

$S = \{s_1, s_2, \dots, s_n\}$ - skup svih senzorskih čvorova u mreži (ukupno *n*)

N(s) – skup svih susjednih čvorova za čvor *s* (tj. skup svih čvorova koji su u dometu radio primopredajnika čvora *s* i s kojima on može izravno komunicirati), uz pretpostavku da u pogledu susjedstva vrijedi simetrija: $s \in N(s') \Rightarrow s' \in N(s)$

D(s) – skup osumnjičenih čvorova u susjedstvu čvora *s*, tj. skup čvorova koje je čvor *s* okarakterizirao kao potencijalno zlonamjerne (budući da su osumnjičeni čvorovi susjedi čvora *s* vrijedi da je $D(s) \subseteq N(s)$

Veličina skupa *D(s)* ovisi o kvaliteti i principu rada IDS modula na senzorskom čvoru *s*. Ukoliko je $|D(s)| = 1$ senzorski čvor *s* uspješno je identificirao zlonamjerni mrežni čvor. Radi pojednostavljenja, pretpostavlja se da u mreži postoji najviše jedan zlonamjerni čvor. Pomoćna funkcija *napadac(s)* daje logičku istinu ukoliko je čvor *s* zlonamjeran, u protivnom daje logičku neistinu, a funkcija *legitiman(s)* daje logičku istinu ukoliko je čvor *s* legitiman.

U mreži su formalno zadovoljena sljedeća svojstva:

- Ako IDS modul na legitimnom mrežnom čvoru *s* formira i objavi skup osumnjičenih čvorova *D(s)* iz njegovog susjedstva, tada se izvor napada (zlonamjerni čvor) nalazi u tom skupu, tj vrijedi sljedeće:

$$\exists s' \in D(s): napadac(s') = true \tag{6.1}$$

- ako je u mreži prisutan zlonamjerni čvor (koji aktivno izvodi napad) nakon isteka konačnog vremenskog intervala neki od legitimnih čvorova *s* formirat će skup osumnjičenih čvorova *D(s)*
- legitimni čvorovi mogu osumnjičiti samo svoje susjedne čvorove:

$$\forall s \in S: legitiman(s) = true \Rightarrow D(s) \subseteq N(s) \tag{6.2}$$

Ako je IDS modul (agent) na čvoru *s* formirao i objavio skup osumnjičenih čvorova *D(s)* tada je čvor *s* „alarmirani čvor“. Skup svih alarmiranih čvorova označen je sa *A(s)*. Pri tome je važno napomenuti da zlonamjerni čvorovi mogu, ali ne moraju pripadati skupu alarmiranih

čvorova, što ovisi o strategiji koju je napadač izabrao. Zlonamjerni čvor će pripadati ovome skupu ukoliko i on objavi skup osumnjičenih čvorova lažno optužujući svoje susjede za zlonamjerno ponašanje. Također, ne moraju nužno svi susjedi zlonamjernog čvora pripadati skupu alarmiranih čvorova, budući da se može dogoditi da neki čvorovi ne uspiju detektirati zlonamjerno ponašanje napadača u svojem susjedstvu. Mogući broj zlonamjernih čvorova u mreži radi pojednostavljenja problema ograničava se na 1.

Za rješavanje problema otkrivanja upada (IDP) postoje dva glavna uvjeta:

- Uvjet otkrivanja upada *(IDC, Intrusion Detection Condition)*
- Uvjeti susjedstva *(NC, Neighborhood Conditions)*

6.2.1. Uvjet otkrivanja upada (IDC)

Uvjet otkrivanja upada (IDC) zapravo predstavlja poopćenje prethodno analiziranog primjera sa tri čvora koji se međusobno sumnjiče za napad. Ukoliko postoji skup sumnjivih čvorova za neki legitimni čvor iz mreže koji je strukturalno identičan skupu sumnjivih čvorova za stvarni izvor napada, problem općenito nije rješiv. Zbog toga je uvjet za otkrivanje napadača da niti jedan drugi čvor nema identičan skup sumnjivih čvorova kao napadač. Ovaj uvjet predstavlja dovoljan uvjet za otkrivanje upada.

Neka je za čvor *s* definiran skup *AN(s)* kao „skup alarmiranih susjeda“:

$$AN(s) = \{t \mid A(t) \wedge t \in N(s)\} \tag{6.3}$$

Neka je definiran skup alarmiranih susjeda od čvora *p* u odnosu na čvor *q*:

$$\widetilde{AN}(p,q) = AN(p) \setminus \{q\} \tag{6.4}$$

Tada se uvjet otkrivanja upada (IDC) formalno može zapisati kao:

$$\forall p,q \in S: napadac(q) = true \Rightarrow \widetilde{AN}(p,q) \neq \widetilde{AN}(q,p), \tag{6.5}$$

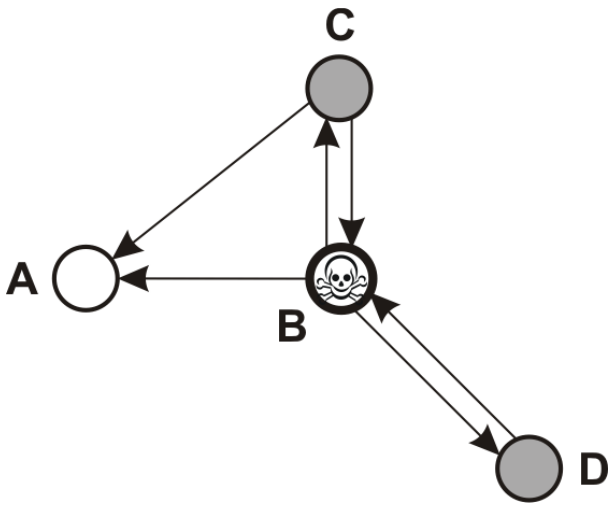
a za slučaj da čvorovi *p* i *q* nisu susjedi, izraz se pojednostavljuje:

$$\forall p,q \in S: napadac(q) = true \Rightarrow AN(p) \neq AN(q) \tag{6.6}$$

Svi alarmirani čvorovi međusobno razmjenjuju svoje skupove osumnjičenih čvorova (zahvaljujući IDS agentu koji se izvršava na svakom čvoru). Zbog polazne pretpostavke da postoji najviše jedan zlonamjerni čvor, razmjena ovih informacija će u svakom slučaju biti moguća. Također, potrebno je voditi računa da napadač također može alarmirati svoje susjede i slati im lažne popise osumnjičenih čvorova. Napadač će biti uvršten u listu sumnjivih čvorova svakog legitimnog čvora. Budući da niti jedan legitimni čvor nema identične susjede kao napadač, neće se pojaviti na listi sumnjivih čvorova više puta nego napadač, te će napadača biti moguće identificirati. Situacija se komplicira ukoliko se neki od čvorova na listama sumnjivih čvorova pojavljuju jednaki broj puta (ako, primjerice, napadač lažno optuži neke od svojih susjeda za zlonamjerno ponašanje i stavi ih na popis osumnjičenih čvorova). Neka je čvor *B* napadač, a čvor *A* (*A*≠*B*) čvor kojeg jednak broj preostalih čvorova sumnjiči za napad (tj. čvorovi *A* i *B* se jednaki broj puta pojavljuju na popisima sumnjivih čvorova). Postavlja se pitanje na koji način će neki treći čvor *C* razlučiti koji je od ova dva čvora (*A* ili *B*) zlonamjeran. U trivijalnom slučaju, ukoliko je *C*=*A*, on implicitno za sebe zna da je legitiman, te otkriva čvor *B* kao napadača. Ukoliko svi legitimni čvorovi „sumnjaju“ na čvor *A* uvjet IDC ne bi bio zadovoljen. Prema tome, mora postojati neki čvor *D* koji će sumnjičiti čvor *B*, a neće sumnjičiti čvor *A*. Dakle, za čvor *D* vrijedi: $A \notin D(D) \wedge B \in D(D)$. Slijedi da je čvor *B* alarmiran i $A \in D(B)$, budući da je broj čvorova koji sumnjiče čvor *a* jednak broju čvorova koji sumnjiče čvor *B*. Sada čvor *C* treba odlučiti koji od ovih čvorova (*B* ili *D*) „laže“ u svojim tvrdnjama.

Potrebno je utvrditi postoji li alarmirani čvor *E* koji nije susjed od čvora *D*. Kada bi svi alarmirani čvorovi bili susjedi od čvora *D*, tada bi čvorovi *B* i *D* imali iste skupove alarmiranih susjeda jedan u odnosu na drugog, što bi bilo kontradiktorno uvjetu otkrivanja upada (IDC). Prema tome čvor *c* treba utvrditi koji od čvorova (*B* ili *D*) nije susjed nekog od alarmiranih čvorova, što je moguće budući da čvorovi znaju koji su im susjedi udaljeni dva koraka. Taj čvor mora biti legitiman, a onda se preostali čvor identificira kao napadač.

Sljedeći primjer ilustrira uvjet za otkrivanje upada (IDC) (slika 6.4):



Slika 6.4 Uvjet otkrivanja upada - primjer

Čvorovi C i D su legitimni čvorovi koji su alarmirani. Čvor A je također legitiman, ali nije alarmiran. Strelicama je označeno koji čvorovi se nalaze na popisu osumnjičenih čvorova, pa prema tome vrijedi:

$$D(A) = \emptyset; \quad D(B) = \{A, C, D\}; \quad D(C) = \{A, B\}; \quad D(D) = \{B\} \tag{6.7}$$

U ovom slučaju IDC uvjet je zadovoljen, budući da vrijede sljedeće relacije:

$$\widetilde{AN}(A, B) = \emptyset; \quad \widetilde{AN}(B, A) = \{D\} \tag{6.8}$$

$$\widetilde{AN}(C, B) = \{A\}; \quad \widetilde{AN}(B, C) = \{A, D\} \tag{6.9}$$

$$\widetilde{AN}(D, B) = \emptyset; \quad \widetilde{AN}(B, D) = \{A\} \tag{6.10}$$

Čvor A prikupio je po dva „glasa“ za svaki od čvorova B i C. Prema tome, lažna su sumnjičenja od strane čvora B ili čvora D. Međutim, budući da čvorovi C i D nisu susjedi, čvor C ne može biti napadač, pa se ispravno zaključuje da je napadač čvor B.

6.2.2. Uvjeti susjedstva (NC)

Budući da IDC uvjet predstavlja dovoljan uvjet (ne i nužan) za rješavanje problema otkrivanja upada (IDP) može postojati situacija u kojoj ovaj uvjet nije zadovoljen, a problem

je ipak rješiv. Uvjeti susjedstva (NC) predstavljaju drugi dovoljan uvjet za rješivost problema otkrivanja upada, neovisno o ispunjenosti uvjeta IDC.

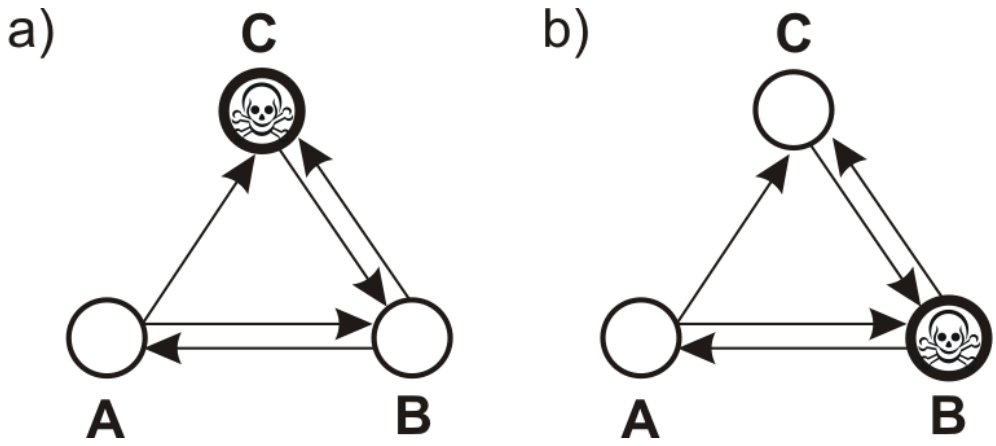
Uvjeti susjedstva (NC) zapravo se sastoje od dva uvjeta:

- NC1: Svi čvorovi koji su susjedni zlonamjernom čvoru su alarmirani.
- NC2: Ako su dva ili više čvorova osumnjičeni od strane većine čvorova, tada svi legitimni čvorovi koji su osumnjičeni od strane većine čvorova imaju i susjede koji nisu alarmirani.

Ukoliko su uvjeti susjedstva zadovoljeni, problem otkrivanja upada je rješiv. Pretpostavka je da svi alarmirani čvorovi razmjenjuju popise osumnjičenih čvorova. Ukoliko je samo jedan čvor osumnjičen od strane većine čvorova, onda je taj čvor zlonamjeran, budući da su svi njegovi susjedni čvorovi alarmirani (NC1). Ukoliko ima dva ili više čvorova koji su osumnjičeni od strane većine, čvorovi iz skupa alarmiranih čvorova trebaju odrediti koji od ovih čvorova imaju susjede koji nisu alarmirani. Prema uvjetu NC2 jedino zlonamjerni čvor nema susjeda koji nisu alarmirani.

Za rješivost problema otkrivanja upada (IDP) u bežičnoj senzorskoj mreži bilo koji od dva uvjeta (IDC ili NC) treba biti zadovoljen. Prema tome, problem otkrivanja upada (IDP) u senzorskoj mreži može se riješiti deterministčkim algoritmom ako i samo ako je zadovoljen uvjet otkrivanja upada (IDC) ili uvjeti susjedstva (NC).

Sljedeći primjer pokazuje da se problem otkrivanja upada ne može riješiti deterministčkim algoritmom ukoliko niti jedan od ovih uvjeta nije zadovoljen.



Slika 6.5 Rješivost problema otkrivanja upada

Na slici 6.5(a) čvor A za zlonamjerno ponašanje sumnjiči čvorove B i C, čvor B sumnjiči čvorove A i C, a čvor C (koji je zapravo zlonamjeran) sumnjiči čvor B.

$$D(A) = \{B, C\}; \quad D(B) = \{A, C\}; \quad D(C) = \{B\} \tag{6.11}$$

$$\widetilde{AN}(A, C) = \widetilde{AN}(C, A) = \{B\} \tag{6.12}$$

U ovom slučaju uvjet otkrivanja upada (IDC) nije zadovoljen, kao niti uvjet NC (zbog neispunjenja poduvjeta NC2). Deterministički algoritam bi u slučaju da je problem rješiv trebao zlonamjernim okarakterizirati čvor C. Međutim, promatrano sa strane algoritma prethodno analizirana situacija potpuno je identična situaciji prikazanoj na slici 6.5(b). U situaciji prikazanoj na slici 6.5(b) zlonamjerni čvor je čvor B (dok topologija mreže i liste sumnjivih čvorova ostaju nepromijenjene). Ne postoje nikakve dodatne informacije koje bi algoritmu omogućile da razluči ove dvije situacije, i prema tome ispravno zlonamjernim okarakterizira čvor C u prvom, a čvor B u drugom slučaju. Prema tome, problem otkrivanja upada nije rješiv, odnosno ne postoji deterministički algoritam kojim bi se on mogao u ovom slučaju riješiti.

6.3. Platforma za implementaciju distribuiranog adaptivnog sustava

Bežične senzorske mreže sastoje se od velikog broja bežičnih čvorova koji su vrlo ograničeni u pogledu računalnih i energetskih resursa. Potrebe za malim dimenzijama i niskom proizvodnom cijenom senzorskih čvorova unaprijed limitiraju njihovu kompleksnost. Tipični senzorski čvorovi u današnje vrijeme opremljeni su 8-bitnim mikrokontrolerom, veličina memorije za pohranu programskog koda je tipično reda veličine 100 kB, dok je količina radne memorije (RAM) reda veličine 20 kB. Ovakvo okruženje zahtijeva implementaciju odgovarajućeg operativnog sustava koji neće biti zahtjevan za resurse („lagan“, *lightweight*). Također, operativni sustav namijenjen ovakvom okruženju svakako treba podržavati dinamičko daljinsko reprogramiranje uređaja.

Jedan od trenutačno najpopularnijih operativnih sustava namijenjenih ovakvom ograničenom okruženju jest Contiki [32]. Contiki podržava dinamičko reprogramiranje čvorova. Jezgra (kernel) operativnog sustava Contiki je upravljana događajima *(event-driven)*,

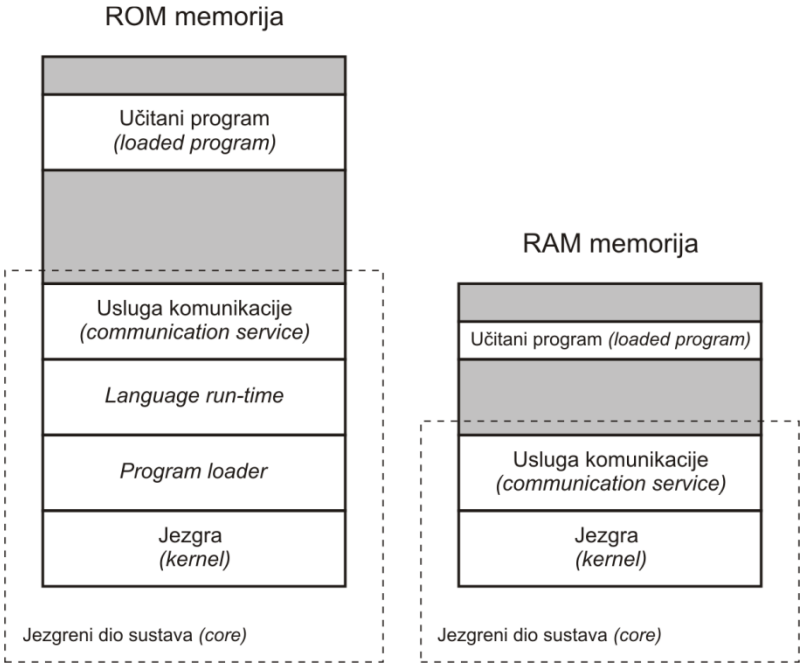
ali sustav podržava i višenitnost *(multi-threading)*. Višenitnost je implementirana kao dodatna biblioteka koja se povezuje s programima koji to eksplicitno zahtijevaju.

Implementacija operativnog sustava Contiki izvedena je u programskom jeziku C, i prilagođena je za većinu arhitektura mikrokontrolera koji se trenutno primjenjuju u bežičnim senzorskim mrežama. Većina drugih operativnih sustava za ugrađene *(embedded)* sustave zahtijeva prijenos kompletne binarne slike cijelog sustava prilikom programiranja pojedinačnih uređaja. Za razliku od njih, Contiki omogućava dinamičko učitavanje i brisanje pojedinačnih aplikacija ili servisa bez prekida rada sustava. Također, pojedinačna aplikacija znatno je manja od slike cjelokupnog sustava i zahtijeva puno manje energije za njezin prijenos kroz bežičnu mrežu (što je vrlo značajno za BSM).

U području bežičnih senzorskih mreža postoji vrlo veliki broj različitih platformi, sa različitim mikrokontrolerima, skupovima senzora i komunikacijskim podsustavima. Zbog takve raznolikosti važno je bilo kreirati zajedničku softversku infrastrukturu (u vidu ugrađenog operativnog sustava) koja je portabilna i može se izvršavati na svim ovim platformama. Razvojem jedinstvenog operativnog sustava u velikoj mjeri olakšava se i ubrzava razvoj aplikacija i povećava se fleksibilnost, odnosno omogućava izvršavanje aplikacija na različitim platformama, kao i interoperabilnost između različitih platformi na kojima je prisutan isti operativni sustav. Jedan od najranijih operativnih sustava namijenjenih bežičnim senzorskim mrežama koji udovoljava ovim zahtjevima bio je TinyOS, koji je ujedno postao i najrašireniji operativni sustav u BSM. TinyOS koristi posebni programski jezik (izveden iz programskog jezika C) za kreiranje sustava koji se sastoji od manjih komponenata koje se statički povezuju sa jezgrom (kernelom) formirajući tako kompletnu sliku *(image)* sustava. U tom slučaju nakon povezivanja modifikacija sustava nije moguća. Operativni sustav Contiki, kao noviji sustav od TinyOS-a, u određenim segmentima je napredniji i donosi neke novosti. Nasuprot TinyOS-u, Contiki osigurava dinamičku strukturu koja omogućava aplikacijama i upravljačkim programima zamjenu prilikom izvršavanja (bez potrebe za prekidanjem rada sustava i potrebe za ponovnim pokretanjem postupka povezivanja).

Contiki operativni sustav (slika 6.6) sastoji se od jezgre sustava *(kernel)*, biblioteka *(libraries)*, modula za učitavanje programa *(program loader)* i skupa procesa *(processes)*. Proces može biti aplikacija ili servis *(service)*. Pri tome servis implementira određenu funkcionalnost koju koristi nekolicina aplikacijskih procesa. Contiki podržava dinamičku

izmjenu svih procesa (i aplikacija i servisa). Komunikacija između procesa odvija se kroz kernel. Kernel ne osigurava poseban sloj za apstrakciju hardvera *(HAL, Hardware Abstraction Layer)*, nego omogućava izravnu komunikaciju sa hardverom.



Slika 6.6 Struktura Contiki operativnog sustava

Contiki sustav obuhvaća jezgreni dio sustava *(core)* i učitane programe *(loaded programs)* (particioniranje se radi prilikom prevođenja). Jezgreni dio prevodi se u jedinstvenu binarnu sliku koja se pohranjuje na uređaje prije njihovog puštanja u rad i obično se nakon toga više ne modificira. Programi se u sustav učitavaju pomoću modula za učitavanje programa i moguće ih je naknadno modificirati (putem bežične komunikacije ili izravnim priključivanjem memorijskog uređaja, poput EEPROM-a).

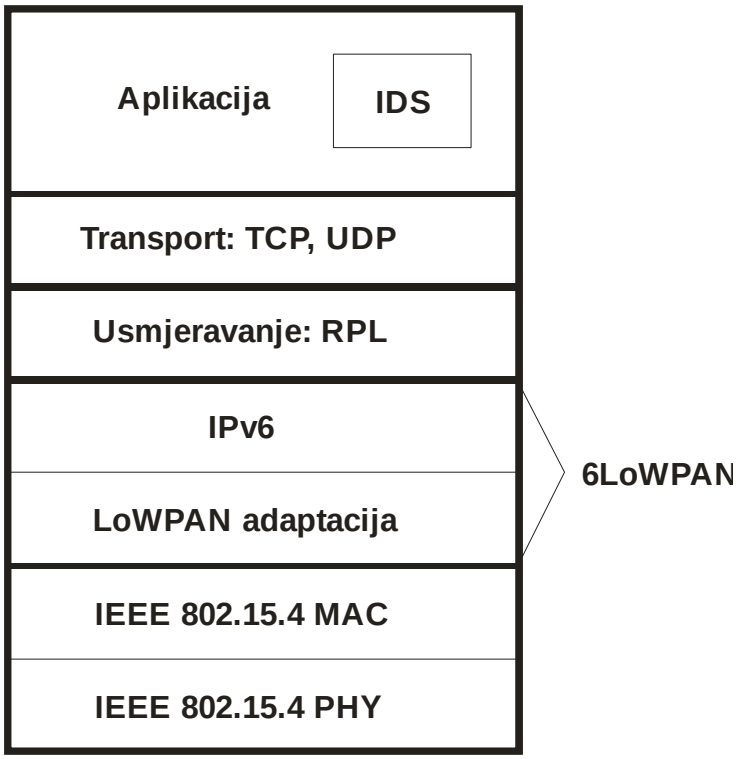
Operativni sustav Contiki predstavlja prvi operativni sustav prikladan za senzorske mreže u koji je implementirana podrška za IP protokol. Najprije se radilo o podršci za IPv4 verziju protokola, da bi kasnije u sustav bila implementirana i podrška za IPv6 protokol (nakon što je specificiran 6LoWPAN adaptacijski sloj). Nakon što je implementirana podrška za IPv6 unutar Contiki OS-a uslijedila je i implementacija podrške za RPL usmjerivački protokol, pri čemu je ContikiOS bio prvi OS sa podrškom za RPL. Zbog svega spomenutog upravo je ContikiOS izabran kao platforma za implementaciju distribuiranog adaptivnog sustava za otkrivanje zlonamjernog ponašanja senzorskih čvorova u IPv6-temeljenoj BSM [31, 34, 114].

Razvoj i testiranje bilo kakvog sustava namijenjenog senzorskim mrežama uvelike je olakšano i ubrzano ukoliko postoji mogućnost njegove simulacije. Simulacijski postupak omogućava provjeru ponašanja sustava i uklanjanje eventualnih pogrešaka prije njegove stvarne implementacije. Postupak testiranja se time značajno ubrzava, a testiranje pojedinih scenarija u realnom okruženju često bi iziskivalo znatno dulje vrijeme i velika materijalna sredstva. Na žalost, postojeći mrežni simulatori (kada se govori o simulaciji BSM) u mogućnosti su istovremeno simulirati samo pojedinu razinu sustava. Za potrebe simulacije predloženog rješenja korišten je simulator COOJA [71]. Ovaj simulator u potpunosti podržava Contiki operativni sustav, te omogućava simulaciju kroz više razina, od razine strojnog koda do razine operativnog sustava, pa je zbog toga izabran kao prikladan za simulaciju ponašanja predloženog sustava.

6.4. Distribuirani adaptivni sustav za otkrivanje zlonamjernih čvorova

Predloženi sustav za otkrivanje zlonamjernih (malicioznih) čvorova u BSM temeljenim na IPv6 protokolu predstavlja u potpunosti distribuirano rješenje. Sustav se temelji na kolaborativnim algoritmima i ne oslanja se na nikakvu središnju infrastrukturu. Sustav predviđa implementaciju IDS agenta (modula) na svaki čvor u bežičnoj senzorskoj mreži. Glavni zadatak ovog agenta jest praćenje ponašanja susjednih čvorova (čvorova koji se nalaze unutar dometa radio primopredajnika) i sudjelovanje u postupku kolektivnog odlučivanja.

Algoritam koji je implementiran unutar IDS agenta (na svakom senzorskom čvoru) izvršava se neovisno od primarne aplikacije senzorske mreže i nadzire komunikaciju unutar ograničenog dometa radio primopredajnika. Sustav je u potpunosti prilagođen protokolnom stogu koji se primjenjuje u bežičnoj senzorskoj mreži temeljenoj na IPv6 protokolu (slika 6.7). Jezgra IDS agenta izvršava se na aplikacijskom sloju. Kao protokol transportnog sloja primjenjuje se UDP protokol, dok se kao protokol usmjeravanja koristi RPL protokol, kao prvi protokol namijenjen senzorskim mrežama sa podrškom za IPv6. Radi kompresije IPv6 zaglavlja primjenjuje se 6LoWPAN adaptacijski sloj, koji omogućava učinkovit prijenos IPv6 paketa kroz mrežu čiji je fizikalni sloj sukladan IEEE 802.15.4 standardu.



Slika 6.7 IDS agent unutar protokolnog stoga

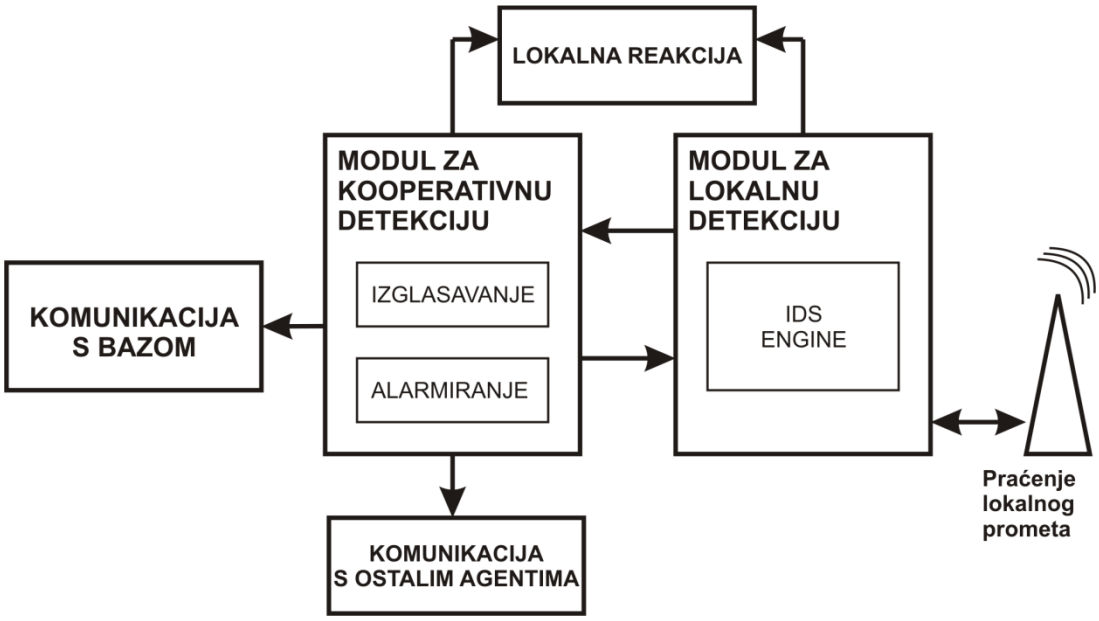
Funkcionalnost IDS agenta moguće je razložiti na tri osnovne komponente:

- **Nadzor mreže:** podrazumijeva prikupljanje odgovarajućih informacija na temelju praćenja i nadzora mrežnog prometa u svojem neposrednom susjedstvu
- **Odlučivanje:** podrazumijeva postupak kolektivnog odlučivanja na temelju informacija prikupljenih međusobnom komunikacijom i kolaboracijom agenata
- **Reakcija:** podrazumijeva poduzimanje odgovarajuće akcije u slučaju da se u mreži detektira zlonamjerno ponašanje određenog senzorskog čvora

Svaki čvor nakon što je proslijedio paket „osluškuje“ ponašanje svojih susjeda, odnosno provjerava hoće li susjedni čvor paket proslijediti dalje (*watchdog* pristup). Neprosljeđivanje paketa može biti indikacija zlonamjernog ponašanja, no to nije uvijek nužno, budući da u nestabilnom okruženju senzorske mreže čitav niz faktora može prouzročiti da paket ne stigne na svoje odredište (npr. kolizija, kvarovi čvorova i sl.).

Zbog toga se unutar sustava definira određeni vremenski interval unutar kojega IDS modul prati količinu (broj) odbačenih podatkovnih paketa na susjednim čvorovima. Ovaj vremenski interval predstavlja promjenjivi i prilagodljivi parametar koji se može prilagoditi

konkretnoj situaciji. Također se definira dozvoljena granica *(threshold)* koju broj odbačenih paketa unutar promatranog vremenskog intervala ne bi smio prijeći. Prelazak ove granice karakterizira se kao moguće zlonamjerno ponašanje i čvor se dodaje na popis „sumnjivih“ čvorova. Dozvoljena granica je također promjenjivi parametar koji ovisi o konkretnoj situaciji. Zbog velike raznolikosti senzorskih mreža u pogledu broja i gustoće čvorova, kapaciteta linkova i količine podataka koja se njima prenosi, nije moguće izabrati univerzalne vrijednosti ovih parametara (koje bi bile prikladne za sve moguće BSM) nego ih je potrebno prilagoditi za svaki konkretan slučaj. Predloženi sustav kao osnovno načelo otkrivanja upada koristi detekciju na temelju predefiniranih specifikacija *(specification-based detection)*. Ovakav pristup pokazuje se pogodnim za primjenu u BSM, budući da bi drugačiji pristupi bili bitno zahtjevniji u pogledu potrebnih resursa (koji su zapravo vrlo strogo ograničeni). Slika 6.8 prikazuje strukturu IDS sustava namijenjenog IPv6-temeljenoj BSM.



Slika 6.8 Struktura IDS sustava za BSM

IDS agenta čine dva glavna modula: modul za lokalnu detekciju i modul za kooperativnu detekciju. Ovi moduli međusobno su povezani i zajednički sudjeluju u postupku otkrivanja zlonamjernog ponašanja senzorskih čvorova. Također, povezani su i sa modulima za praćenje lokalnog prometa te modulima za komunikaciju (sa bazom i ostalim agentima). Komunikacijski moduli neophodni su za izgradnju distribuiranog sustava, budući da se funkcioniranje sustava temelji na međusobnoj suradnji više IDS agenata.

Modul za praćenje lokalnog prometa predstavlja važan dio sustava, budući da se upravo pomoću ovog modula prikupljaju informacije koje se unutar sustava obrađuju, te se na temelju rezultata analize ovih informacija odlučuje o karakterizaciji ponašanja pojedinih senzorskih čvorova. Ulaznu informaciju u sustav predstavljaju podaci o komunikacijskoj aktivnosti susjednih čvorova pojedinog senzorskog čvora (tj. čvorova koji mu se nalaze unutar dometa radio veze).

Modul za lokalnu reakciju aktivira se nakon što je otkriven napad ili zlonamjerno ponašanje nekog senzorskog čvora. Njegova zadaća je poduzeti prikladnu akciju kao odgovor na detektirani napad. U slučaju da je zlonamjerno ponašanje otkriveno potrebno je o tome obavijestiti preostale čvorove i baznu stanicu, kako bi se kompromitirane čvorove moglo isključiti iz mreže, što obično podrazumijeva ažuriranje ruta za usmjeravanje da bi se kompromitirani čvorovi prilikom usmjeravanja zaobišli. Ukoliko se u mreži primjenjuju neke od kriptografskih metoda potrebno je provesti i postupak ažuriranja kriptografskih materijala (ključeva) kako ne bi bio kompromitiran nastavak komunikacije. Lokalna reakcija na otkriveni napad može biti izravna, što podrazumijeva da će kompromitirani čvor odmah biti isključen sa svih ruta (tj. promatrani čvor više neće prosljeđivati promet kompromitiranom susjedu). Neizravna reakcija podrazumijeva samo informiranje bazne stanice i preostalih mrežnih čvorova.

6.4.1. Modul za lokalnu detekciju

Modul za lokalnu detekciju povezan je sa modulom za praćenje lokalnog prometa, od kojeg dobiva informacije na temelju kojih provodi lokalno odlučivanje. Ovaj modul analizira prikupljene informacije, te na temelju prethodno definiranih pravila kreira listu osumnjičenih čvorova i alarmira preostale susjedne čvorove. Prema tome, aktivnost modula za lokalnu detekciju rezultira skupom „osumnjičenih“ čvorova, u kojem se može naći jedan ili više njegovih susjednih čvorova. Svaki čvor generira listu čvorova iz svojeg susjedstva koji su „sumnjivi“ (tj. čije se ponašanje potencijalno može okarakterizirati kao maliciozno). Također, u predloženom sustavu se za svaki čvor koji se nađe na ovom popisu procjenjuje i vjerojatnost da je čvor maliciozan.

Vjerojatnost da je susjedni čvor zlonamjeran (maliciozan) procjenjuje se na temelju broja proslijeđenih i odbačenih paketa unutar promatranog vremenskog intervala. Svaki čvor *s* procjenjuje vjerojatnost zlonamjernog ponašanja svojih susjeda na sljedeći način:

$$p_m(i) = 1 - \frac{n_f(i)}{n_r(i)}, \quad \forall i \in N(s) \tag{6.13}$$

gdje je: $p_m(i)$ – vjerojatnost zlonamjernog ponašanja susjednog čvora

$n_r(i)$ – broj paketa koje je susjedni čvor primio

$n_f(i)$ – broj paketa koje je susjedni čvor proslijedio

Ukoliko je vjerojatnost zlonamjernosti $p_m(i)$ za neki čvor *i* koji je susjed čvora *s* veća od unaprijed definirane granične vrijednosti, čvor *s* će čvora *i* uvrstiti na svoj popis osumnjičenih čvorova *D(s)*, kojeg će razmijeniti sa preostalim čvorovima (zajedno sa pripadajućim procijenjenim vjerojatnostima zlonamjernog ponašanja svojih susjeda).

Liste osumnjičenih čvorova senzorski čvorovi razašilju svojim susjedima, te ih na taj način razmjenjuju. Nakon razmjene alarmnih poruka (koje sadrže popise osumnjičenih čvorova i procijenjene vjerojatnosti zlonamjernog ponašanja), tj. nakon što svi senzorski čvorovi prikupe alarmne poruke od preostalih čvorova aktivira se modul za kooperativnu detekciju koji će na temelju prikupljenih podataka donijeti konačnu odluku o karakteru ponašanja osumnjičenih čvorova (tj. za osumnjičene čvorove procijeniti vjerojatnost njihovog zlonamjernog ponašanja). Trivijalni slučaj predstavlja situacija u kojoj neki senzorski čvor na svojem popisu osumnjičenih čvorova ima samo jednog susjeda za kojeg je procijenjena vjerojatnost malicioznog ponašanja jednaka 1. U tom slučaju modul za lokalnu detekciju izravno aktivira modul za lokalnu reakciju i komunikacijske module, bez potrebe da se provodi metoda kooperativne detekcije.

Algoritam po kojem funkcionira modul za lokalnu detekciju:

POČETAK

Postavi *broj čvorova* ***N****;*

Postavi *interval promatranja* ***Tp****;*

Postavi *graničnu vjerojatnost* ***Pgr****;*

Postavi *vektor brojača primljenih paketa* ***Nr[N]*** *na nulu;*

Postavi *vektor brojača proslijeđenih paketa* ***Nf[N]*** *na nulu;*

Postavi *vektor procijenjenih vjerojatnosti* ***Pm[N]*** *na nulu;*

Postavi *popis osumnjičenih čvorova* ***D[N]*** *na nulu;*

Postavi *tajmer* ***T*** *na vrijednost Tp;*

Sve dok *ne istekne tajmer T*

*Pročitaj poruku iz ulaznog međuspremnika (****src_adr****,* ***dst_adr****);*

Za svaki *susjedni čvor (i=1 do n)*

Ako *je* ***src_adr*** *= adresa[i]* ***onda*** *Nf[i]++;*

Ako *je* ***dst_adr*** *= adresa[i]* ***onda*** *Nr[i]++;*

Za svaki *susjedni čvor (i=1 do n)*

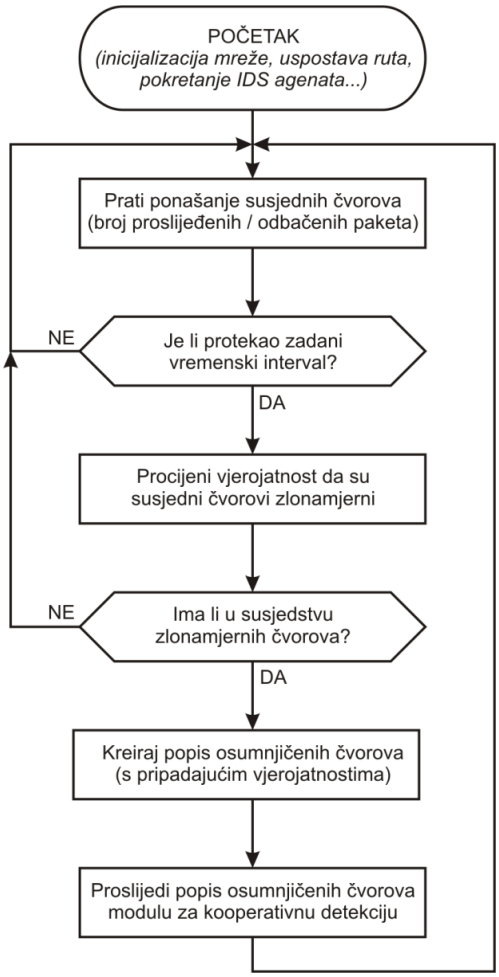
*Pm[i] = (1-Nf[i]/Nr[i])*100;*

Ako *je Pm[i] > Pgr* ***onda*** *D[i] = Pm[i];*

Ako *je Pm[i] = 100* ***onda*** *zlonamjeran = adresa[i];*

Proslijedi popis osumnjičenih čvorova D[N] modulu za kooperativnu detekciju;

KRAJ



Slika 6.9 Modul za lokalnu detekciju

Grafički prikaz algoritma modula za lokalnu detekciju dan je na slici 6.9.

6.4.2. Modul za kooperativnu detekciju

Glavna zadaća modula za kooperativnu detekciju jest donošenje konačne odluke o karakteru ponašanja „sumnjivih“ senzorskih čvorova. Modul ovu odluku ne donosi samostalno, nego u suradnji (kooperativno) sa preostalim modulima (modulima na preostalim čvorovima). Odluka se donosi nakon izvršavanja kooperativnog algoritma unutar kojeg se većinskim odlučivanjem odlučuje o karakteru ponašanja čvorova sa popisa osumnjičenih čvorova.

Ulazne informacije u postupak odlučivanja predstavljaju popisi sumnjivih čvorova koji su prikupljeni od svih mrežnih čvorova. Ovi popisi osim skupa sumnjivih čvorova za svaki

pojedini čvor sadrže i procijenjenu vjerojatnost malicioznog ponašanja. Na temelju prikupljenih informacija izvršavanjem algoritma unutar modula za kooperativnu detekciju procjenjuje se ukupna vjerojatnost malicioznog ponašanja svih čvorova sa popisa. Unutar sustava definira se donja granica (prag) vjerojatnosti iznad koje će se čvor okarakterizirati kao zlonamjeran, te se protiv njega poduzima odgovarajuća reakcija. Ovaj prag vjerojatnosti fleksibilan je i promjenjiv, te ga se može posebno prilagođavati za svaku pojedinu mrežu, ili je moguće mijenjati njegovu vrijednost unutar iste mreže, ovisno o konkretnoj primjeni i situaciji.

Vjerojatnost da je pojedini čvor maliciozan izračunava se na sljedeći način:

$$p_M(s_i) = \frac{1}{n}\sum_{i=1}^{n} p_m(i)\ ,\quad \forall s_i \in S \tag{6.14}$$

gdje $p_M(s_i)$ predstavlja konačnu izračunatu vjerojatnost da je čvor s_i zlonamjeran. Ova vjerojatnost izračunava se kao aritmetička sredina svih procijenjenih vjerojatnosti $p_m(i)$ od strane svih čvorova koji su čvor s_i uvrstili u skup sumnjivih čvorova. Ukoliko u konačnici neka od vjerojatnosti $p_M(s_i)$ prelazi definiranu vrijednost praga, čvor s_i se proglašava zlonamjernim. Ukoliko više procijenjenih vjerojatnosti prelazi vrijednost praga zlonamjernim se proglašava onaj čvor za kojeg je pristiglo više „glasova“ koji prelaze vrijednost praga (tj. čvor za kojeg je više preostalih čvorova procijenilo da je zlonamjeran s vjerojatnošću iznad vrijednosti praga). Ukoliko je broj „glasova“ jednak, zlonamjernim će se okarakterizirati čvor za kojeg je procijenjena najveća vjerojatnost $p_M(s_i)$.

U slučaju da modul za kooperativnu detekciju ponašanje pojedinih mrežnih čvorova okarakterizira kao zlonamjerno, o tome se izvještavaju preostali čvorovi i bazna stanica (putem odgovarajućih komunikacijskih modula), te se zlonamjerni čvorovi isključuju iz mreže tako što se na njihovim susjednim čvorovima aktiviraju moduli za lokalnu reakciju.

Algoritam po kojem funkcionira modul za kooperativnu detekciju:

POČETAK

Preuzmi popis osumnjičenih čvorova D[N] od modula za lokalnu detekciju;

***Postavi** matricu za pohranu primljenih vjerojatnosti **Dtotal[N][N]** (inicijalne vrijednosti -1);*

***Postavi** vektor ukupnih procijenjenih vjerojatnosti **Pmtotal[N]** (inicijalna vrijednost 0);*

***Postavi** vektor „brojač glasova“ **votes[N]**;*

***Postavi** pomoćne varijable **counter**, **maxvotes**, **maxP**;*

Postavi *interval razašiljanja* ***Tbc****;*

Postavi *tajmer* ***T*** *na vrijednost Tbc;*

Sve dok *ne istekne tajmer T*

Postavi poruku D[N] u izlazni međuspremnik;

Razašilji D[N] ostalim čvorovima u mreži;

Pročitaj poruku iz ulaznog međuspremnika (nodeID, D[nodeID]);

Pohrani primljene vjerojatnosti u vektor Dr[N];

i = nodeID;

Za svaki *(j=1 do N)*

Dtotal[i][j] = Dr[i];

Za svaki *(j=1 do N)*

counter = 0;

Za svaki *(i=1 do N)*

Ako *je Dtotal[i][j] != -1* ***onda***

Pmtotal[j] = Pmtotal[j] + Dtotal[i][j];

counter++;

Ako *je Dtotal[i][j] > Pgr* ***onda***

votes[j]++;

Pmtotal[j]=Pmtotal[j]/counter;

maxvotes = 0;

maxP = 0;

counter = 0;

Za svaki *(i=1 do N)*

Ako je votes[i]>maxvotes onda maxvotes=votes[i];

Za svaki *(i=1 do N)*

Ako *je votes[i]=maxvotes* ***onda***

counter++;

zlonamjeran = adresa[i];

Ako *je counter>1* ***onda***

Za svaki *(i=1 do N)*

Ako *je Pmtotal[i] > maxP* ***onda***

maxP = Pmtotal[i];

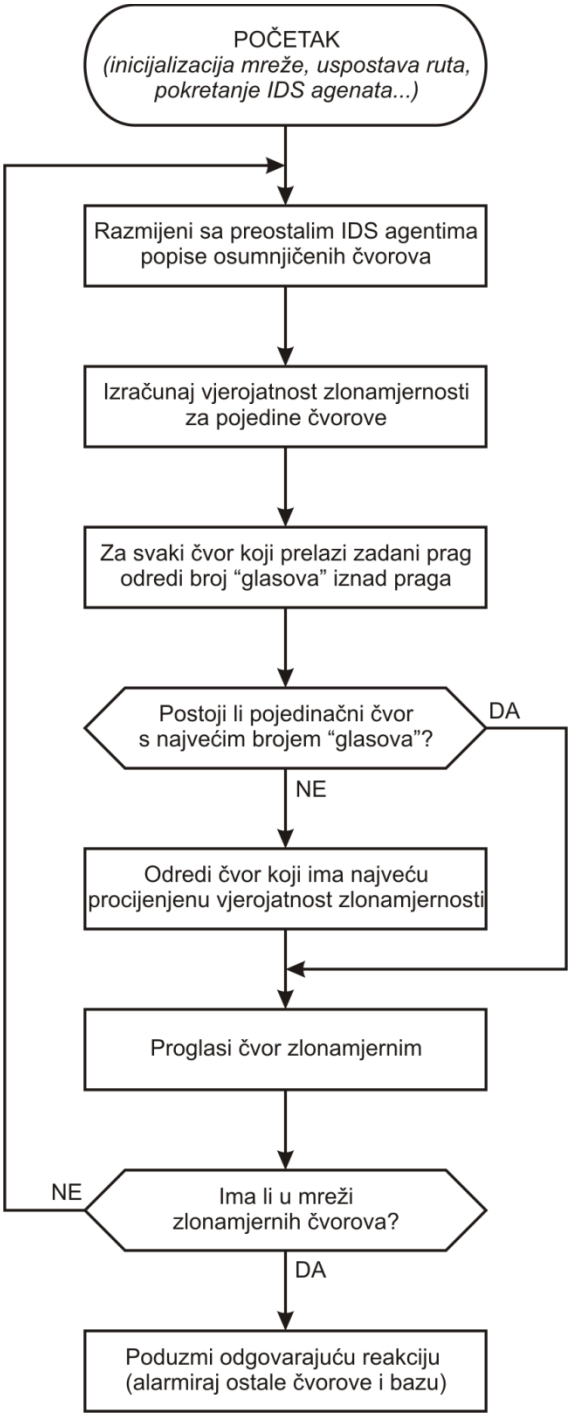
zlonamjeran = adresa[i];

Ako *je zlonamjeran != 0*

Razašilji poruku o identitetu zlonamjernog čvora

KRAJ

Grafički prikaz algoritma modula za kooperativnu detekciju dan je na slici 6.10.



Slika 6.10 Modul za kooperativnu detekciju

6.5. Scenariji za testiranje sustava

Ponašanje predloženog distribuiranog adaptivnog sustava za otkrivanje zlonamjernih čvorova analizira se kroz simulacijski postupak. Sustav je implementiran u nekoliko karakterističnih scenarija koji se susreću u realnim bežičnim senzorskim mrežama. Kroz simulacijski postupak prati se ponašanje predloženog sustava, njegova mogućnost detekcije zlonamjernog ponašanja, kao i njegov utjecaj na funkcioniranje mreže u cjelini (prvenstveno utjecaj na potrošnju mrežnih resursa – napajanja i propusnosti linkova). Kako bi se moglo uvidjeti i analizirati razliku u ponašanju mreže prije i nakon implementacije predloženog sustava najprije je provedena analiza karakterističnih scenarija za implementaciju sustava za otkrivanje upada.

Testiranje performansi predloženog sustava za otkrivanje zlonamjernih čvorova, njegovog utjecaja na normalno funkcioniranje mreže i njegovih mogućnosti detekcije zlonamjernog ponašanja provedeni su kroz nekoliko karakterističnih scenarija i nekoliko različitih topologija mreže.

Sva testiranja provedena su u tri različite mreže. Prva mreža sastoji se od 6 čvorova (5 čvorova i bazna stanica, slika 6.11), druga od 10 čvorova (9 čvorova i bazna stanica, slika 6.36), a treću čini 17 čvorova (16 čvorova i bazna stanica, slika 6.61). Ove tri topologije izabrane su zbog toga što u pogledu razmještaja i broja čvorova pokrivaju veliki broj mogućih praktičnih primjena senzorskih mreža. Ograničavanjem dometa primopredajnika na čvorovima postigla se nužnost komunikacije sa baznom stanicom kroz više skokova (kao i među udaljenim čvorovima unutar mreže). Kako bi se čvorovi što više razlikovali u pogledu broja potrebnih skokova prilikom komunikacije s baznom stanicom, ona u ovim scenarijima nije postavljena u središnjem dijelu, nego na rubu područja koje pokriva bežična senzorska mreža. Domet primopredajnika isti je za sve čvorove u mreži, kao što su im identične i sve ostale karakteristike, pa su simulirane mreže u tom pogledu homogene (na slikama koje prikazuju ove topologije radi preglednosti grafički je prikazan domet za samo jedan čvor). Po ovim karakteristikama simulirane mreže također odgovaraju većini realnih senzorskih mreža. Na svim čvorovima u mreži implementiran je IPv6 protokolni stog, kakav je prikazan i na slici 6.7.

U svakoj od ove tri mreže (sa 6, 10 i 17 čvorova) simulirana su tri različita scenarija. Ovi scenariji međusobno se razlikuju po vjerojatnosti uspješnog slanja i prijema podatkovnih paketa. U prvom simuliranom scenariju (u svakoj od triju simuliranih mreža) vjerojatnost uspješnog slanja i prijema iznosi 100%, pa prema tome prvi scenarij reprezentira „idealan“ slučaj. Međutim, u senzorskim mrežama u praksi vrlo često dolazi do gubitaka podatkovnih paketa zbog smetnji, kvarova čvorova i kolizije, a često je i zlonamjerna (maliciozna) aktivnost uzrokom gubitka dijela podatkovnih paketa. Ovakve situacije važno je razmotriti, budući da gubici paketa i potreba za njihovom retransmisijom izravno utječu na performanse mreže i potrošnju resursa, te otežavaju (u ekstremnim situacijama čak i onemogućavaju) otkrivanje zlonamjernih aktivnosti u mreži. Zato se u sve tri mreže osim „idealnog“ slučaja analiziraju još dva scenarija. U drugom analiziranom scenariju u svim mrežama vjerojatnost uspješnog slanja i prijema paketa iznosi 80%, dok u trećem simuliranom scenariju ova vjerojatnost iznosi 60%.

Za potrebe testiranja performansi najprije je provedena simulacija svih scenarija bez implementiranog IDS sustava (ukupno 9 scenarija, po tri scenarija u svakoj od tri topologije) kako bi se ispitalo „normalno“ ponašanje mreže, bez utjecaja implementiranog IDS sustava na njezin rad. Pri tome senzorski čvorovi prikupljene informacije iz svoje okoline (temperatura, vlažnost, osvijetljenost) periodički (jednom u minuti) šalju baznoj stanici. Kroz sve simulacije promatrano je ponašanje mreže u vremenskom intervalu od jednog sata. U svakom simulacijskom postupku nakon inicijalizacije mreže i uspostave ruta zabilježeni su broj susjeda i broj potrebnih skokova do bazne stanice za svaki čvor (ove vrijednosti u pravilu su vezane za konkretnu topologiju mreže, pa se za istu mrežu značajnije ne mijenjaju za tri različita simulirana scenarija – do manjih promjena može doći ukoliko se zbog gubitaka paketa dogodi rekonfiguracija dijela mreže i izmjena dijelova ruta). Za svaki simulirani scenarij zabilježeni su broj primljenih paketa (promatrano tijekom vremena, kao i ukupno za svaki čvor), broj izgubljenih paketa, ETX metrika (kao pokazatelj potrebnog broja retransmisija na pojedinim linkovima), prosječni radni ciklus primopredajnika (za svaki čvor u mreži), potrošnja energije tijekom vremena, kao i prosječna potrošnja energije za svaki čvor u mreži. Kao referentna hardverska platforma za procjenu potrošnje energije koristi se TelosB platforma, kao jedna od najraširenijih platformi za realizaciju BSM. Ukupna potrošnja senzorskog čvora razlaže se na četiri komponente:

- potrošnja mikroprocesora (CPU)
- potrošnja u niskoenergetskom modu (LPM)

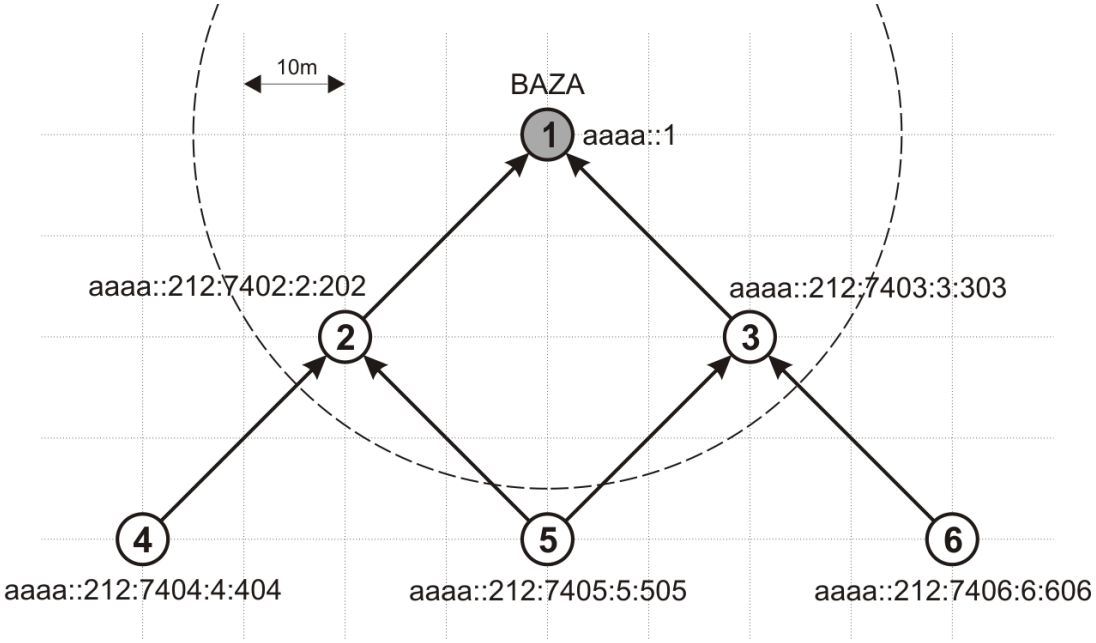
- potrošnja primopredajnika u stanju „slušanja“ *(listen mode)*
- potrošnja primopredajnika u stanju aktivne predaje *(transmit mode)*

Dobiveni rezultati služe za usporedbu sa identičnim scenarijima, ali sa implementiranim IDS sustavom (topologije i svi drugi parametri ostaju nepromijenjeni), kako bi se moglo promotriti na koji način njegova implementacija utječe na „normalan“ rad mreže (tj. narušava li njezine performanse i dovodi li do znatnijeg povećanja potrošnje resursa). Prema tome, nakon implementacije IDS sustava ponovno je provedena simulacija svih 9 karakterističnih slučajeva (po tri scenarija u svakoj od tri mreže).

Osim testiranja performansi predloženog IDS sustava, provedeno je i testiranje njegovih sposobnosti otkrivanja zlonamjernog ponašanja. Testiranje sposobnosti detekcije zlonamjernog ponašanja također je provedeno u 9 različitih prethodno opisanih scenarija (po tri karakteristična scenarija u tri različite mreže), budući da na sposobnost detekcije izravno utječu broj čvorova u mreži, broj susjednih čvorova, kao i broj odbačenih paketa (koji nisu odbačeni namjerno od strane napadača). U svakom od simuliranih scenarija namjerno je postavljen po jedan zlonamjerni čvor koji selektivno prosljeđuje pakete i pri tome odbacuje 80% paketa. Za svaki scenarij razmatrana su po dva slučaja. U jednom slučaju u mreži je prisutan jedan zlonamjerni čvor koji na opisani način selektivno prosljeđuje podatke, a u drugom slučaju taj čvor još k tome za isto lažno „optužuje“ svoje susjede (što je u praksi čest slučaj). Analiziraju se mogućnosti otkrivanja zlonamjernog ponašanja u opisanim situacijama (pri čemu sustav procjenjuje vjerojatnost zlonamjernog ponašanja čvorova), te se na temelju dobivenih rezultata izvode zaključci o utjecaju broja čvorova, količine odbačenih paketa i ponašanja samog zlonamjernog čvora na mogućnost uspješne detekcije zlonamjernog ponašanja.

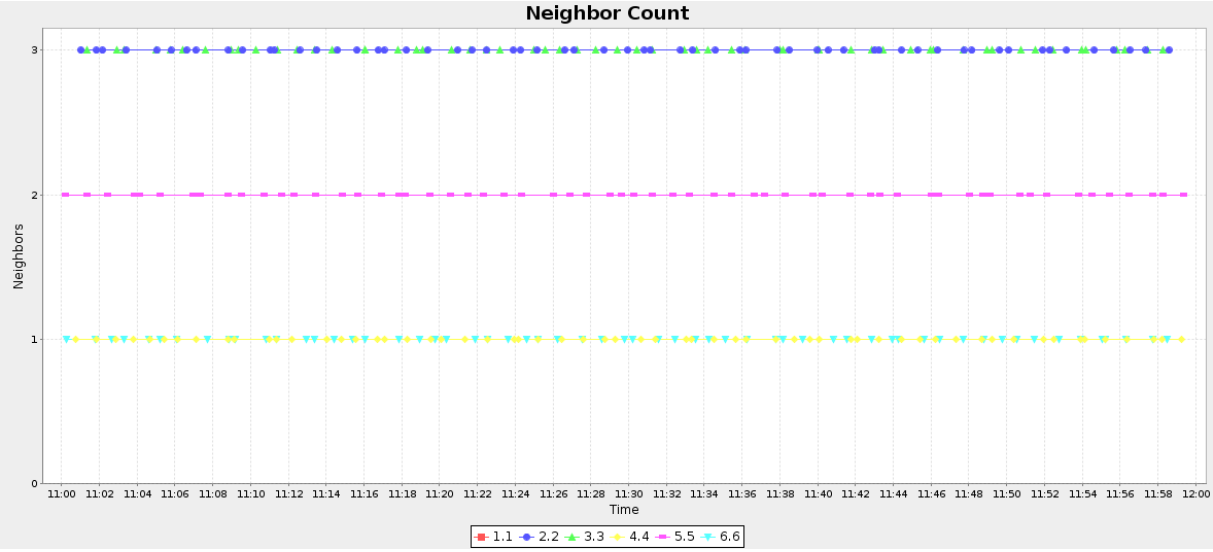
6.5.1. Mreža sa 6 čvorova

Prvi karakteristični scenarij koji je kreiran za potrebe analize i testiranja uključuje 6 čvorova (slika 6.11).



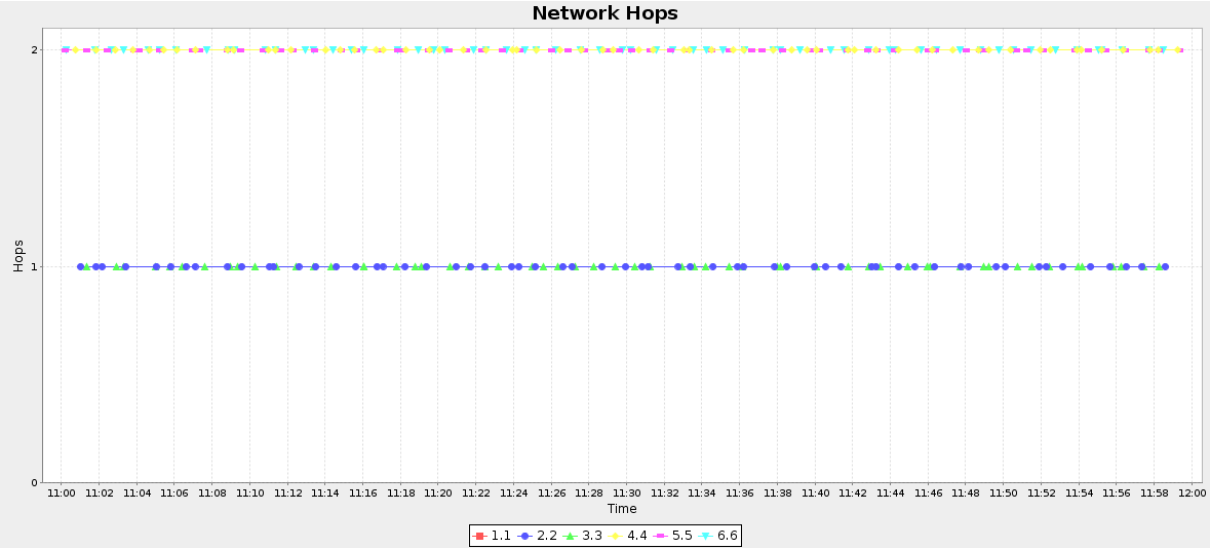
Slika 6.11 Topologija mreže sa 6 čvorova

Čvor 1 predstavlja baznu stanicu, a preostali čvorovi (2-6) su obični senzorski čvorovi. Podjela rastera na slici odgovara udaljenosti od 10 metara. Domet radio primopredajnika postavljen je na 30 metara, dok je područje interferencije postavljeno na 50 metara. Izborom ovih vrijednosti utjecalo se na definiranje topologije mreže i uspostavu ruta ka baznoj stanici, budući da od dometa primopredajnika ovisi koji će čvorovi biti u stanju izravno komunicirati. U prikazanoj mreži bazna stanica je u izravnom dometu čvorovima 2 i 3. Čvoru 4 u dometu je čvor 2, čvoru 6 u dometu je čvor 3, a čvoru 5 u dometu su čvorovi 2 i 3. Slika 6.12 prikazuje broj susjednih čvorova za svaki mrežni čvor.



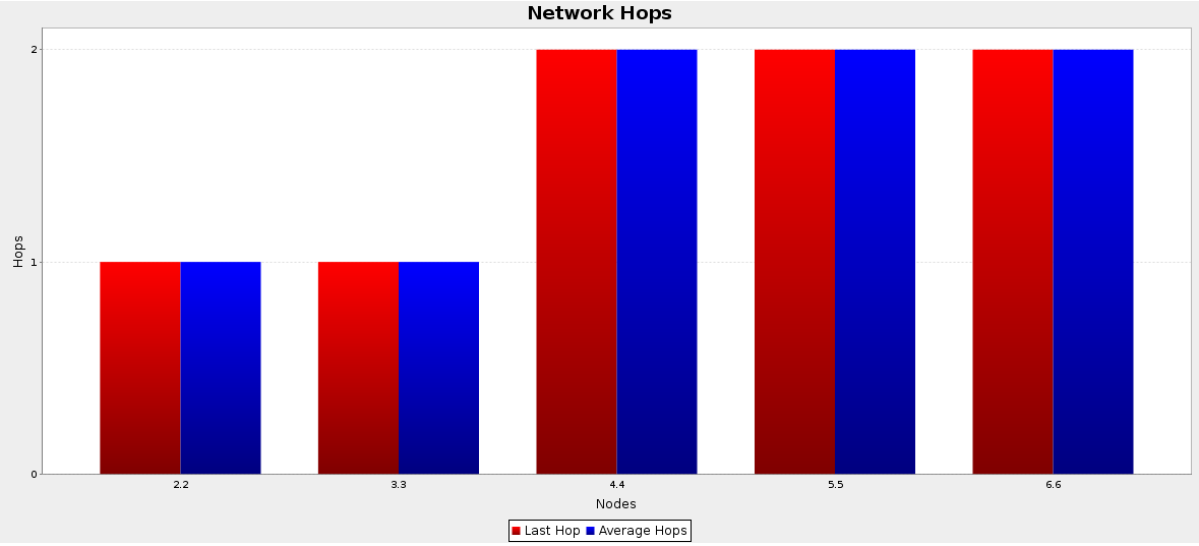
Slika 6.12 Broj susjednih čvorova u mreži sa 6 čvorova

Sa slike 6.12 je vidljivo da čvorovi 4 i 6 imaju po jednog susjeda, čvor 5 ima dva, a čvorovi 2 i 3 imaju po tri susjedna čvora. Prema tome, putanje će od čvorova 4, 5 i 6 do bazne stanice uključivati dva skoka, dok će paketi od čvorova 2 i 3 do bazne stanice stizati u jednom skoku, kao što je prikazano na slici 6.13.



Slika 6.13 Broj skokova do bazne stanice u mreži sa 6 čvorova

Slika 6.14 prikazuje broj skokova za svaki pojedini čvor.

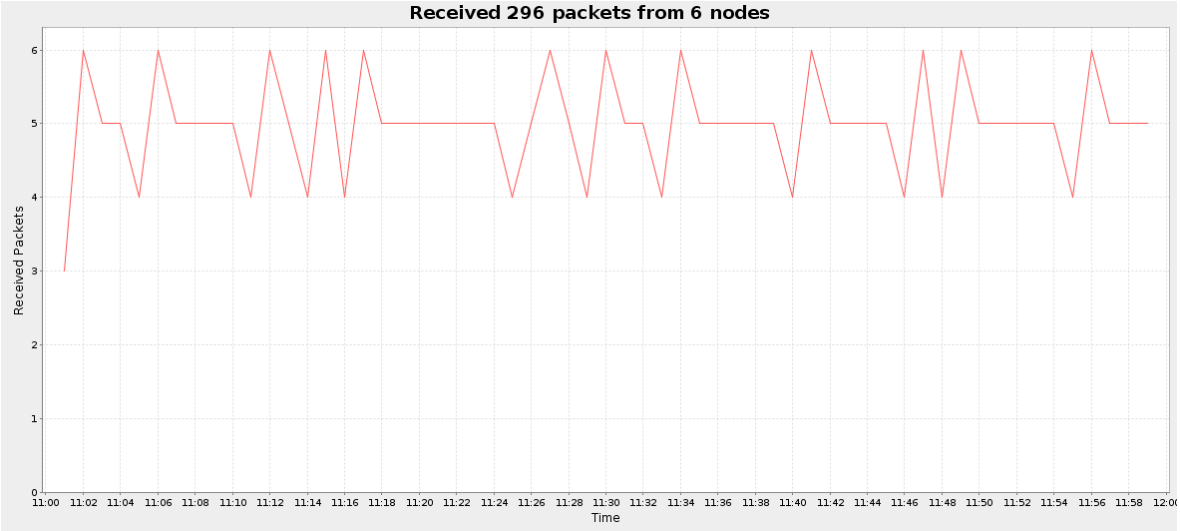


Slika 6.14 Broj skokova za pojedinačne čvorove u mreži sa 6 čvorova

Nakon inicijalizacije mreže svaki čvor periodički (otprilike jednom u minuti) šalje baznoj stanici informacije prikupljene putem svojih senzora (temperatura, vlažnost, osvijetljenost). U pogledu vjerojatnosti ispravnog prijenosa paketa analizirana su tri različita scenarija. U prvom scenariju omjer primljenih i poslanih paketa iznosi 100%, odnosno pretpostavlja se da nema gubitaka paketa prilikom prijenosa (idealan slučaj). U drugom scenariju ovaj omjer iznosi 80%, a u trećem 60%. U svim scenarijima trajanje simulacije postavljeno je na jedan sat.

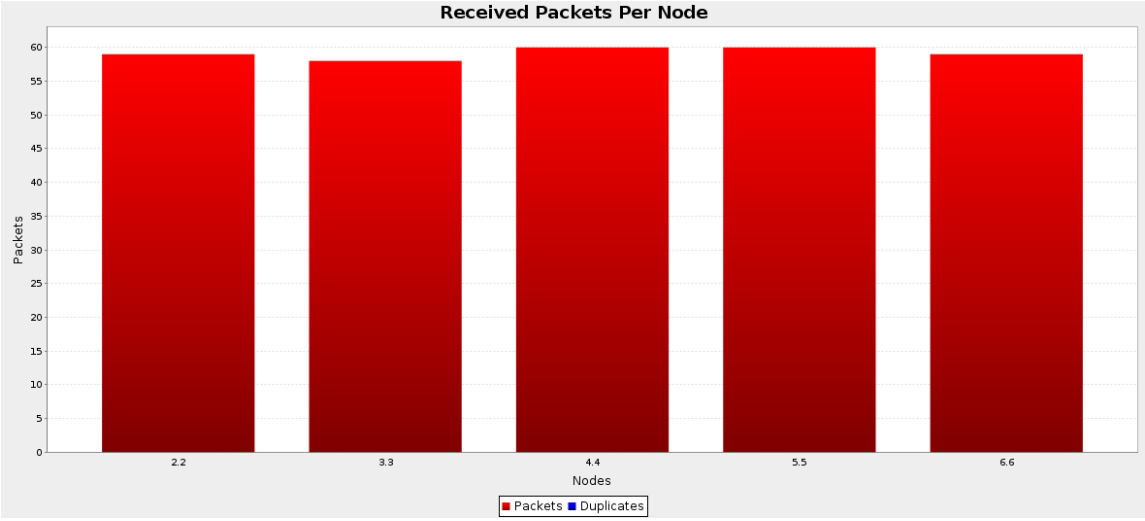
Scenarij 1 (Rx/Tx=100%)

Na slici 6.15 prikazano je kretanje broja primljenih paketa kroz promatrano razdoblje od sat vremena u prvom scenariju u mreži sa 6 čvorova.



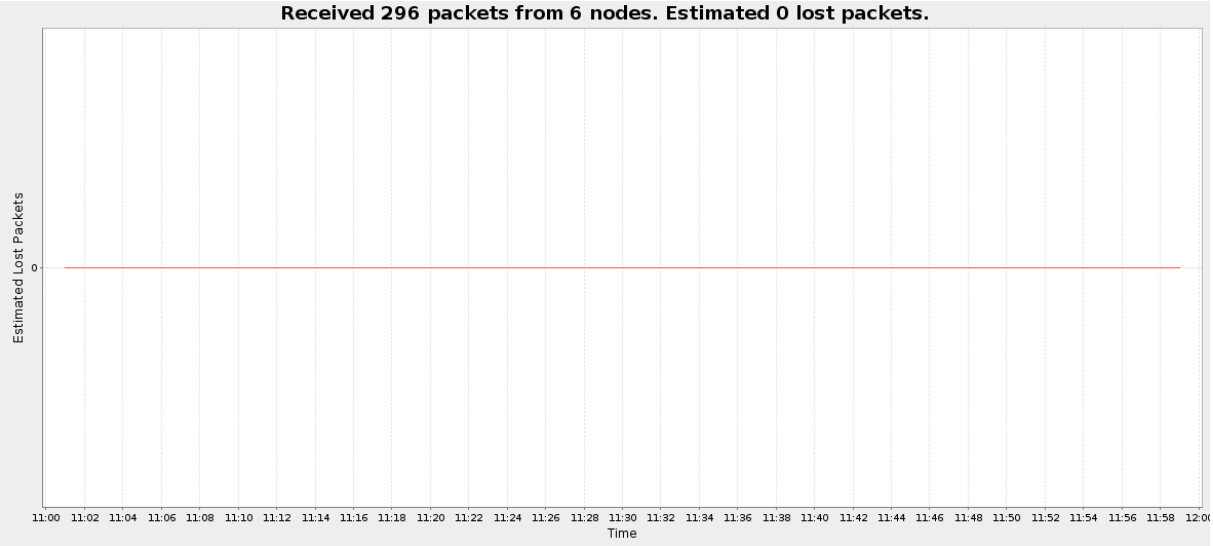
Slika 6.15 Broj primljenih paketa (6 čvorova, scenarij 1, bez IDS-a)

Slika 6.16 prikazuje broj primljenih paketa za svaki pojedinačni čvor.



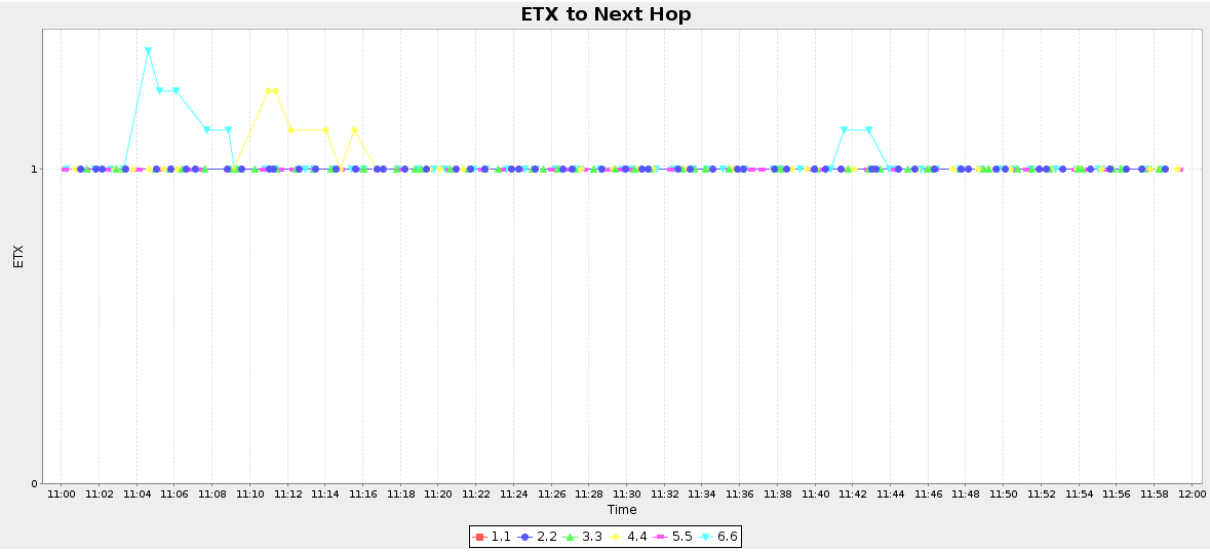
Slika 6.16 Broj primljenih paketa za svaki čvor (6 čvorova, scenarij 1, bez IDS-a)

U promatranom scenariju nije bilo izgubljenih paketa (budući da on reprezentira „idealan slučaj“), što je vidljivo i sa slike 6.17.



Slika 6.17 Izgubljeni paketi (6 čvorova, scenarij 1, bez IDS-a)

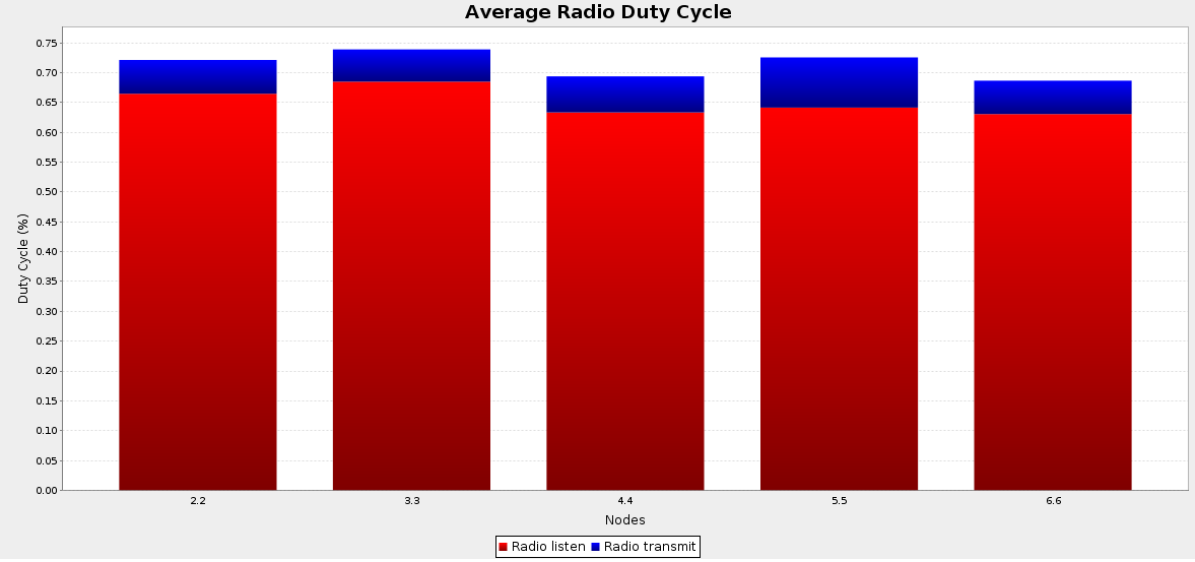
Na slici 6.18 prikazana je ETX vrijednost za pojedinačne čvorove. Ova vrijednost izravno govori o broju pokušaja koji je potreban za uspješno slanje i prijem paketa.



Slika 6.18 ETX metrika (6 čvorova, scenarij 1, bez IDS-a)

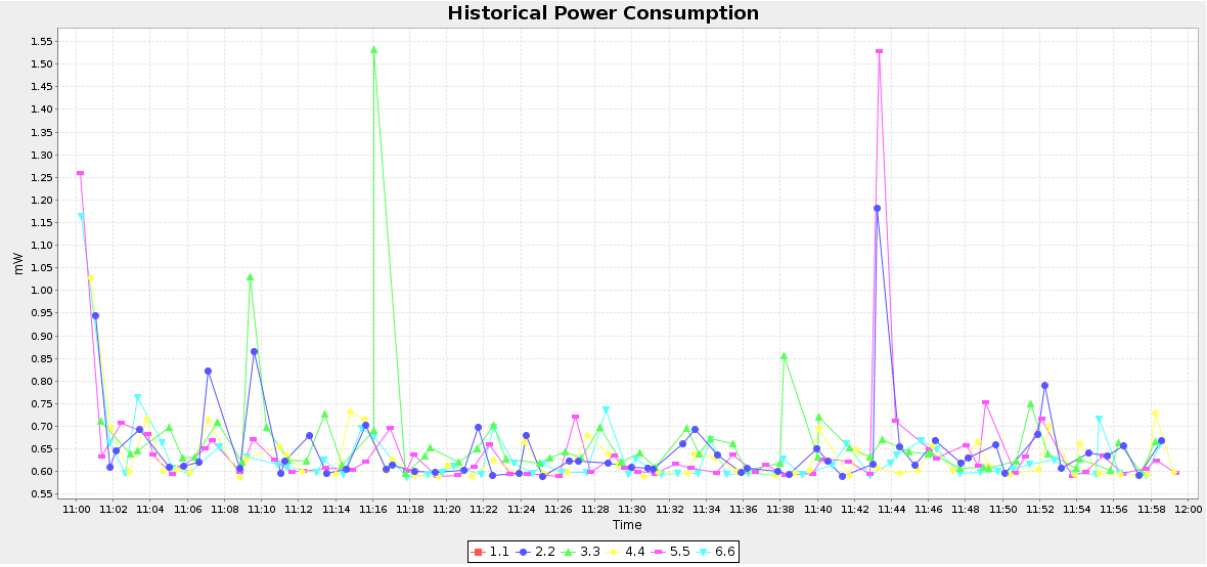
Sa slike je vidljivo da ETX za linkove u promatranom scenariju iznosi 1, što je i očekivano budući da nema gubitaka, pa nema niti potrebe za retransmisijama.

Zanimljivo je promotriti potrošnju energije prilikom normalnog rada mreže. Najveći dio energije troši radio primopredajnik, koji je aktivan u 65-75% vremena (od toga samo manji dio vremena otpada na aktivni prijem ili predaju, dok je u većem dijelu vremena primopredajnik u stanju „slušanja“). Na slici 6.19 prikazan je prosječni radni ciklus *(duty cycle)* za svaki pojedini mrežni čvor.



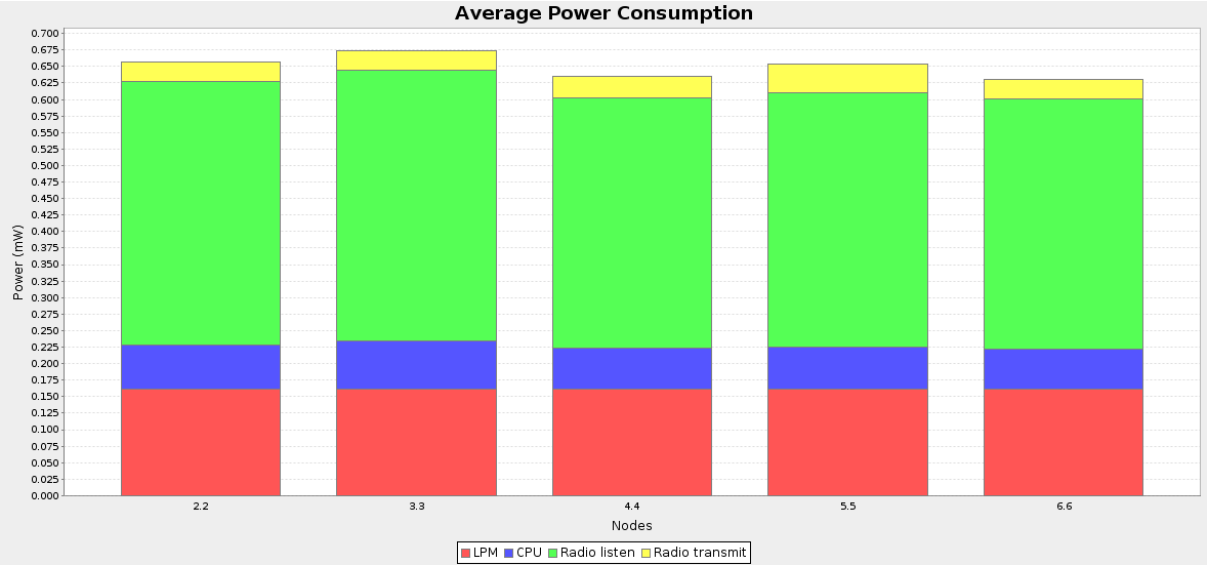
Slika 6.19 Prosječni radni ciklus primopredajnika (6 čvorova, scenarij 1, bez IDS-a)

Dio energije troši računalni dio senzorskog čvora (primarno CPU), dok se najmanje energije troši za vrijeme dok je čvor u niskoenergetskom modu *(Low-Power Mode,* mod „spavanja“). Međutim, u konačnici energija utrošena u niskoenergetskom modu može po apsolutnom iznosu biti i veća od energije koju potroši CPU, budući da senzorski čvorovi u prosjeku provedu značajno više vremena u niskoenergetskom modu nego u aktivnom procesiranju informacija.



Slika 6.20 Potrošnja energije (6 čvorova, scenarij 1, bez IDS-a)

Slika 6.20 prikazuje kretanje potrošnje energije kroz promatrano razdoblje od sat vremena, dok je na slici 6.21 prikazana prosječna potrošnja energije za svaki pojedini čvor u mreži.



Slika 6.21 Prosječna potrošnja energije (6 čvorova, scenarij 1, bez IDS-a)

Sa slike 6.21 vidljivo je da najveći dio energije potroši radio primopredajnik. Također, vidljivo je da je ukupna potrošnja energije čvorova 2 i 3 nešto veća od preostalih čvorova, što

se može objasniti činjenicom da su bliže baznoj stanici, te su služili kao posredni čvorovi pri komunikaciji čvorova 4, 5 i 6 sa baznom stanicom.

U tablici 6.1 su pregledno prikazane vrijednosti dobivene za prvi simulirani scenarij u mreži sa 6 čvorova.

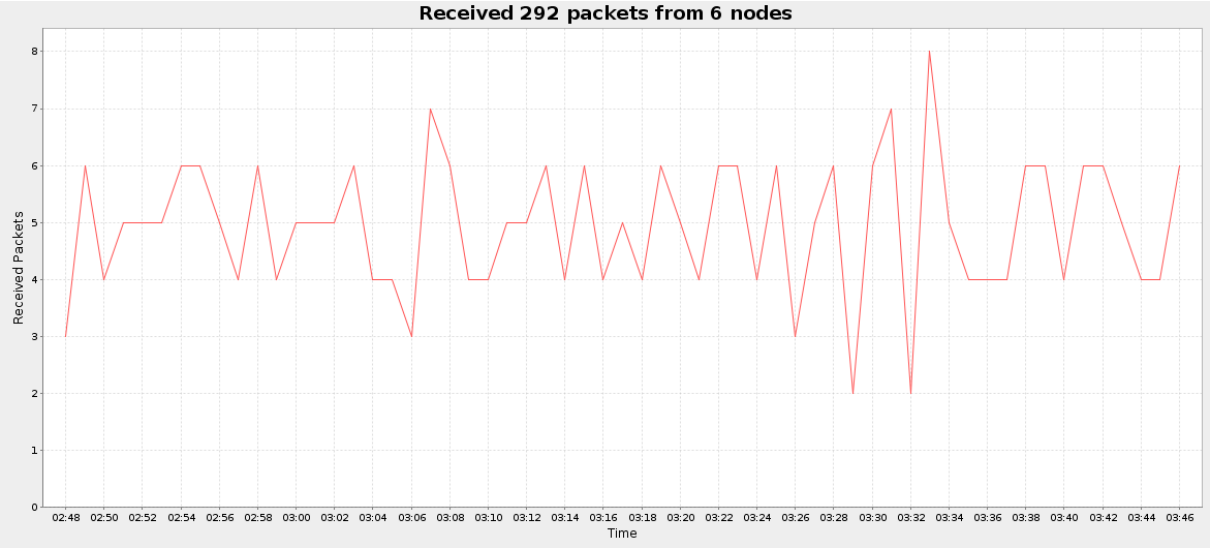
TABLICA 6.1 Mreža sa 6 čvorova, scenarij 1, bez IDS-a

Čvor	Primljeni paketi	Izgubljeni paketi	Skokovi do baze	ETX	Potrošnja energije (mW)					Radni ciklus (%)	
					CPU	LPM	Slušanje	Predaja	Ukupno	Slušanje	Predaja
2	59	0	1	1.000	0.067	0.161	0.399	0.030	0.657	0.665	0.057
3	58	0	1	1.000	0.073	0.161	0.411	0.029	0.674	0.685	0.054
4	60	0	2	1.015	0.061	0.162	0.380	0.032	0.635	0.633	0.060
5	60	0	2	1.000	0.063	0.162	0.385	0.045	0.654	0.641	0.084
6	59	0	2	1.023	0.060	0.162	0.378	0.030	0.630	0.631	0.056
Prosjek	**59.200**	**0.000**	**1.600**	**1.008**	**0.065**	**0.162**	**0.391**	**0.033**	**0.650**	**0.651**	**0.062**

Scenarij 2 (Rx/Tx=80%)

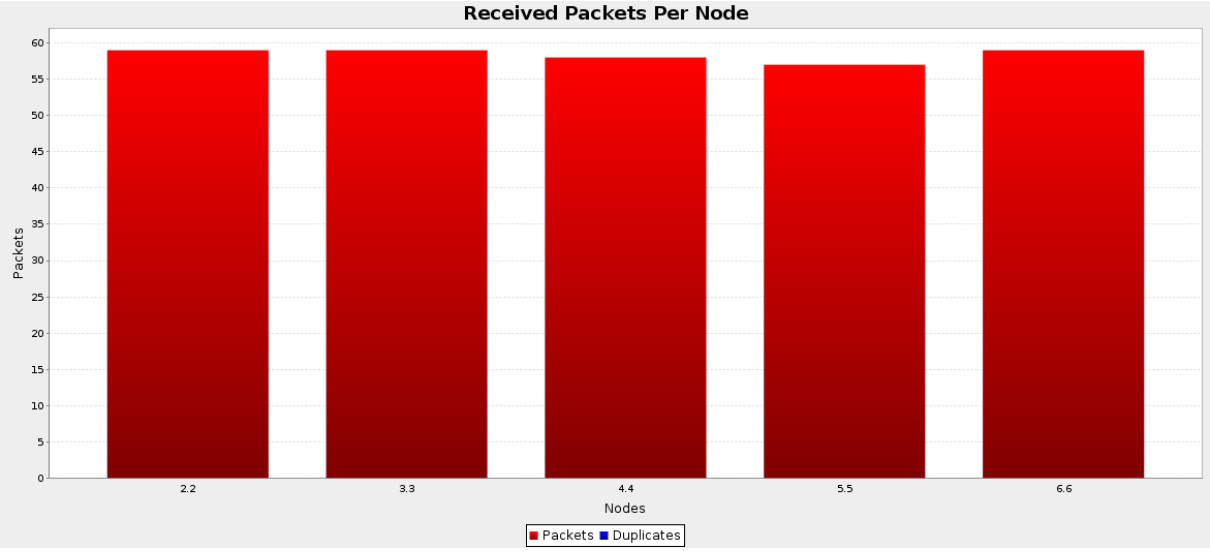
U drugom scenariju koji je analiziran u istoj mreži omjer uspješno primljenih i poslanih paketa postavljen je na 80%. Topologija mreže ostala je ista. Prema tome, situacija u pogledu broja skokova do bazne stanice i broja susjednih čvorova ista je kao u prethodno razmatranom scenariju (slike 6.12, 6.13 i 6.14).

Na slici 6.22 prikazan je broj primljenih paketa u promatranom jednosatnom intervalu.



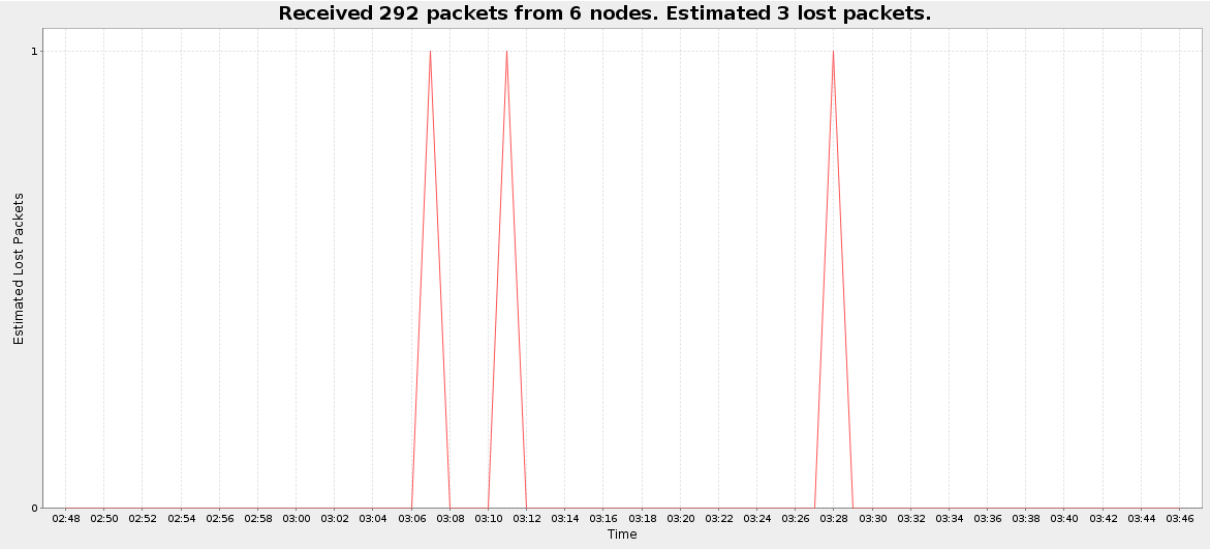
Slika 6.22 Broj primljenih paketa (6 čvorova, scenarij 2, bez IDS-a)

Slika 6.23 prikazuje broj primljenih paketa za svaki pojedinačni čvor.



Slika 6.23 Broj primljenih paketa za svaki čvor (6 čvorova, scenarij 2, bez IDS-a)

U ovom scenariju došlo je i do gubitka određenog broja paketa, što je vidljivo sa slike 6.24.

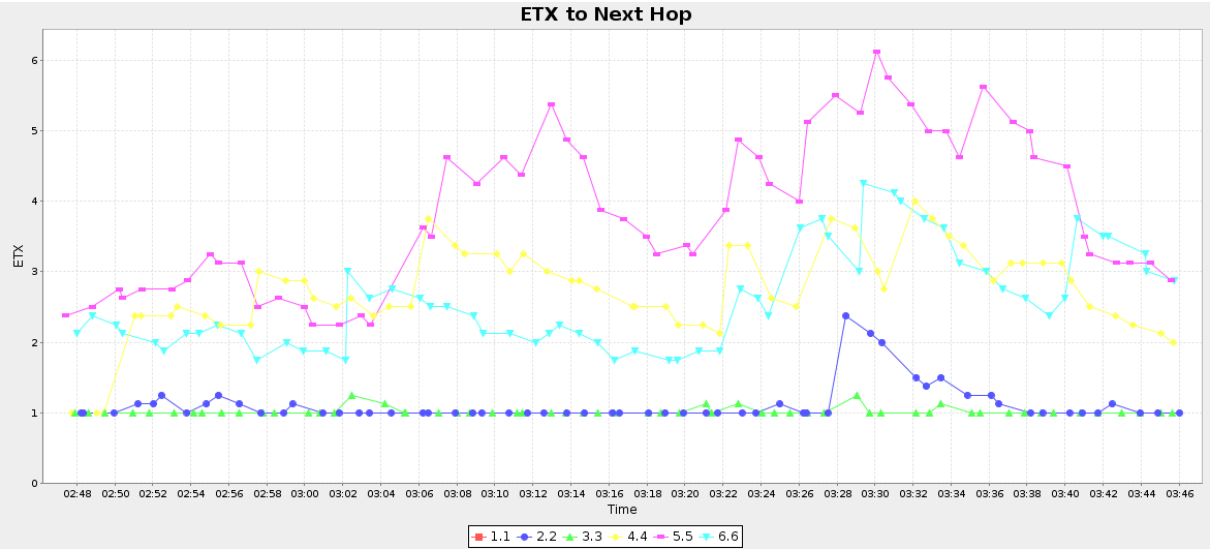


Slika 6.24 Izgubljeni paketi (6 čvorova, scenarij 2, bez IDS-a)

Do gubitka nekoliko paketa došlo je unatoč mehanizmima potvrde i retransmisije. Ipak, vidljivo je da je gubitak razmjerno mali u odnosu na ukupni primljeni broj paketa. Međutim,

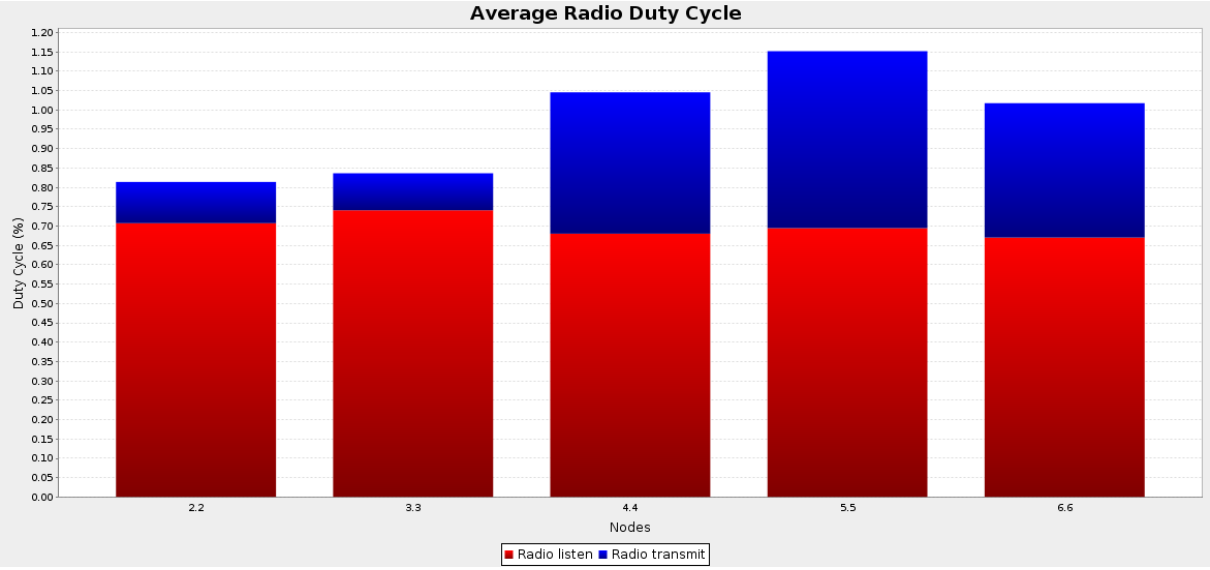
budući da je u ovom scenariju vjerojatnost uspješnog slanja i prijema bila postavljena na 80%, potrebno je analizirati na koji način će potreba za retransmisijom određenih podataka utjecati na ETX metriku, radne cikluse primopredajnika, te potrošnju energije u mreži.

Na slici 6.25 prikazane su ETX vrijednosti za pojedine čvorove u drugom simuliranom scenariju.



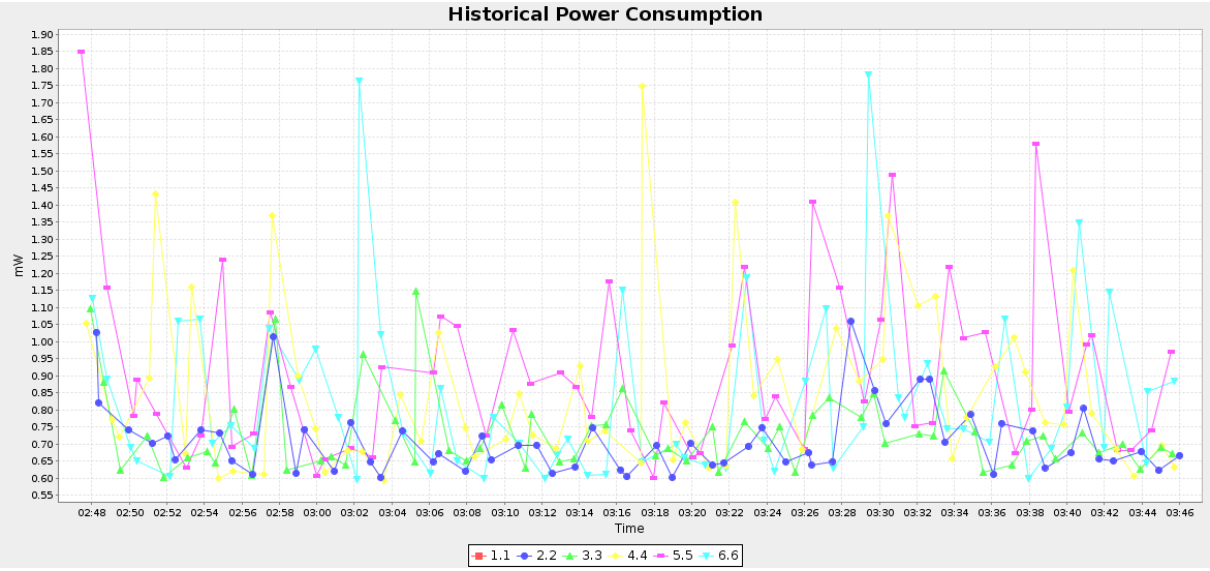
Slika 6.25 ETX metrika (6 čvorova, scenarij 2, bez IDS-a)

Sa slike 6.25 vidljivo je da se ETX vrijednosti za pojedine linkove povećavaju, pogotovo za čvorove udaljenije od bazne stanice (čvorovi 4, 5 i 6). Kao što je ranije rečeno, ETX vrijednost izravno je povezana sa propusnošću linka, odnosno očekivanim brojem pokušaja potrebnim za uspješan prijenos paketa. U prethodnom scenariju, kada je vjerojatnost uspješnog prijema i slanja bila 100% (idealan slučaj), ETX vrijednosti pojedinih linkova bile su 1 (što znači da je za uspješno slanje jednog paketa bio dovoljan jedan pokušaj). U ovom scenariju za uspješno slanje pojedinih paketa (posebice sa udaljenijih čvorova) potrebni su višestruki pokušaji, što se nužno odražava na radne cikluse primopredajnika (slika 6.26).



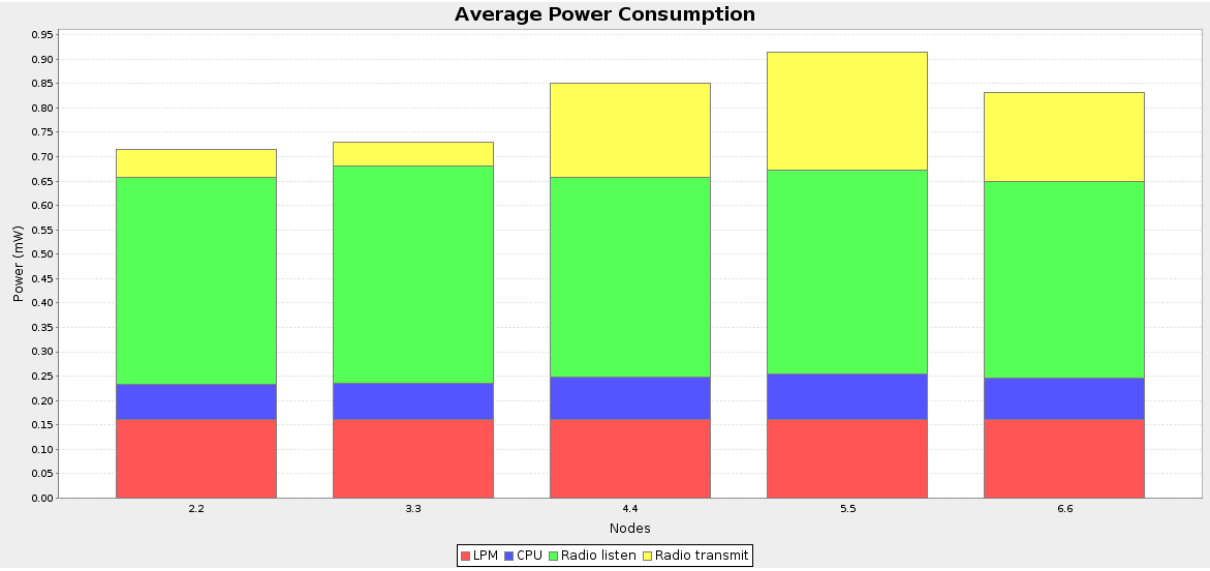
Slika 6.26 Prosječni radni ciklus primopredajnika (6 čvorova, scenarij 2, bez IDS-a)

Na slici 6.26 vidi se da u usporedbi sa idealnim slučajem (slika 6.19) primopredajnici se nalaze znatno dulje u stanju aktivne predaje, osobito na čvorovima udaljenijim od bazne stanice. Budući da je primopredajnik energetski najzahtjevnija komponenta senzorskog čvora, njegova povećana aktivnost nužno se odražava i na ukupnu potrošnju energije u mreži. Na slici 6.27 prikazana je potrošnja energije u mreži sa 6 čvorova za scenarij 2.



Slika 6.27 Potrošnja energije (6 čvorova, scenarij 2, bez IDS-a)

Slika 6.28 prikazuje potrošnju energije za svaki pojedini mrežni čvor u drugom scenariju.



Slika 6.28 Prosječna potrošnja energije (6 čvorova, scenarij 2, bez IDS-a)

Prosječna potrošnja energije za svaki čvor u drugom scenariju povećala se u odnosu na prethodni scenarij. Razlika u potrošnji u odnosu na prethodni scenarij primarno proizlazi iz povećanja potrošnje primopredajnika u stanju aktivne predaje (posebno za čvorove 4, 5 i 6, koji su dva skoka udaljeni od bazne stanice). U scenariju 2 dolazi do gubitka određenog broja paketa (20%), pa je potrebno vršiti njihovu retransmisiju. Zbog toga se predajnici dulje nalaze u stanju aktivne predaje, posebno na udaljenijim čvorovima gdje su gubici izraženiji.

U tablici 6.2 su prikazane dobivene vrijednosti za drugi simulirani scenarij u mreži sa 6 čvorova.

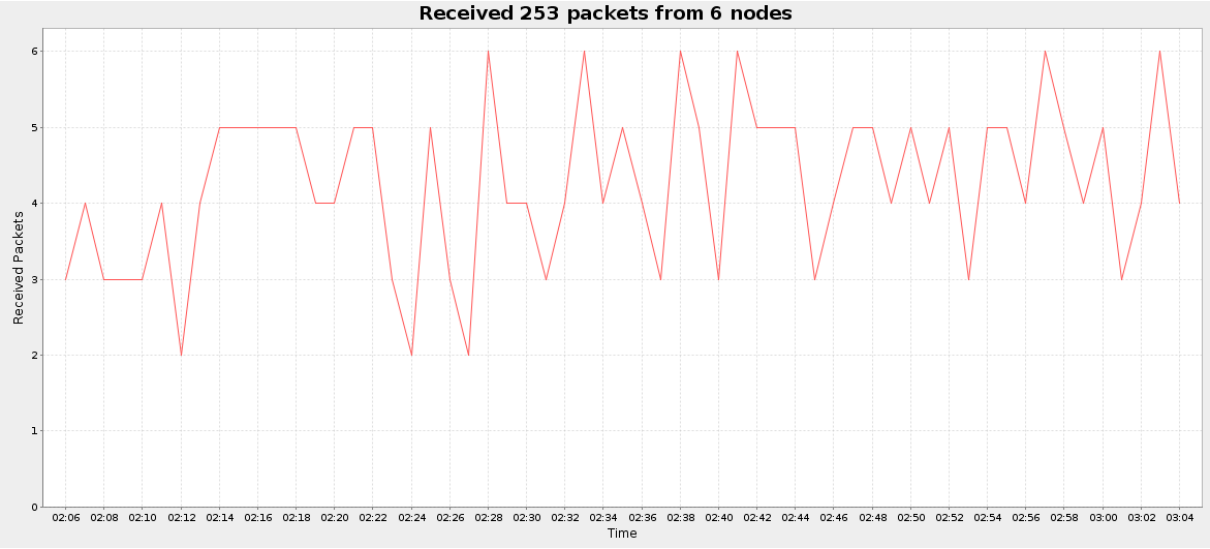
TABLICA 6.2 Mreža sa 6 čvorova, scenarij 2, bez IDS-a

Čvor	Primljeni paketi	Izgubljeni paketi	Skokovi do baze	ETX	Potrošnja energije (mW)					Radni ciklus (%)	
					CPU	LPM	Slušanje	Predaja	Ukupno	Slušanje	Predaja
2	59	0	1	1.117	0.072	0.161	0.424	0.057	0.714	0.707	0.107
3	59	0	1	1.017	0.074	0.161	0.444	0.051	0.731	0.741	0.095
4	58	1	2	2.724	0.088	0.161	0.408	0.194	0.851	0.680	0.365
5	57	2	2	3.842	0.094	0.161	0.417	0.243	0.914	0.694	0.457
6	59	0	2	2.583	0.085	0.161	0.402	0.184	0.833	0.670	0.347
Prosjek	**58.400**	**0.600**	**1.600**	**2.256**	**0.083**	**0.161**	**0.419**	**0.146**	**0.808**	**0.699**	**0.274**

Scenarij 3 (Rx/Tx=60%)

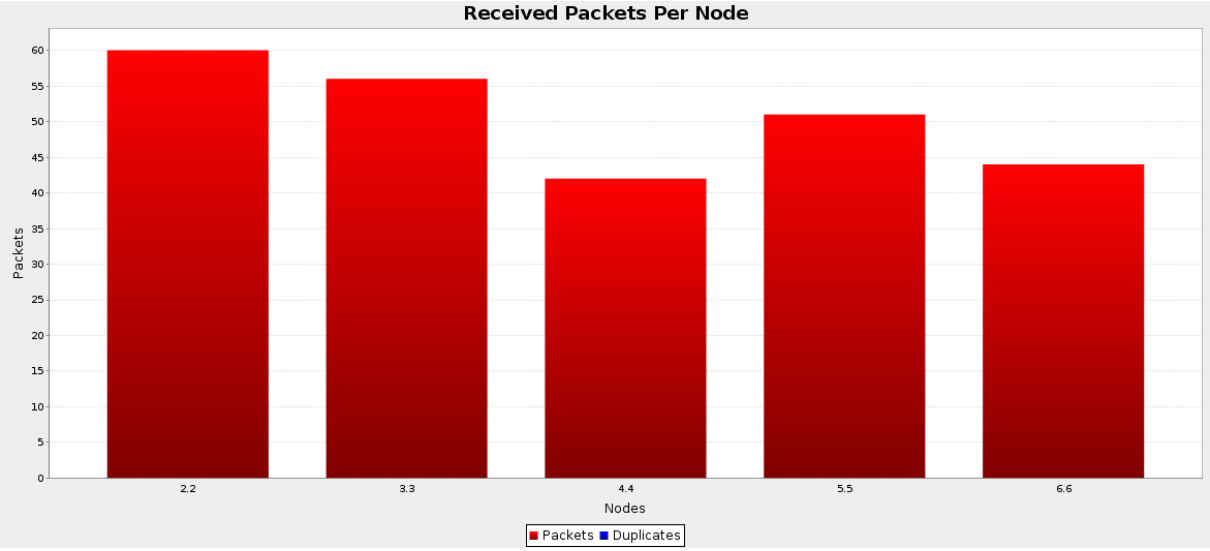
Treći scenarij simuliran u mreži sa 6 čvorova predstavlja scenarij u kojem je vjerojatnost uspješnog prijema i slanja paketa postavljena na 60%. Topologija mreže, kao i broj susjednih čvorova i broj skokova do bazne stanice za pojedine čvorove nisu se promijenili u odnosu na prethodno analizirane scenarije.

Slika 6.29 prikazuje broj primljenih paketa u promatranom intervalu od sat vremena.



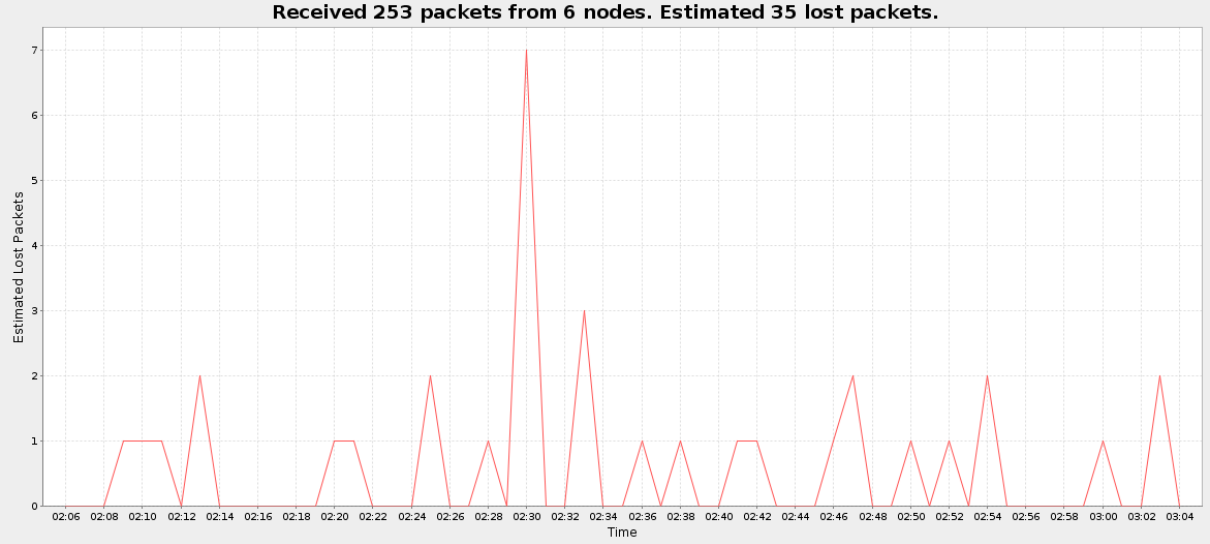
Slika 6.29 Broj primljenih paketa (6 čvorova, scenarij 3, bez IDS-a)

Na slici 6.30 prikazan je broj primljenih paketa za svaki pojedinačni čvor.



Slika 6.30 Broj primljenih paketa za svaki čvor (6 čvorova, scenarij 3, bez IDS-a)

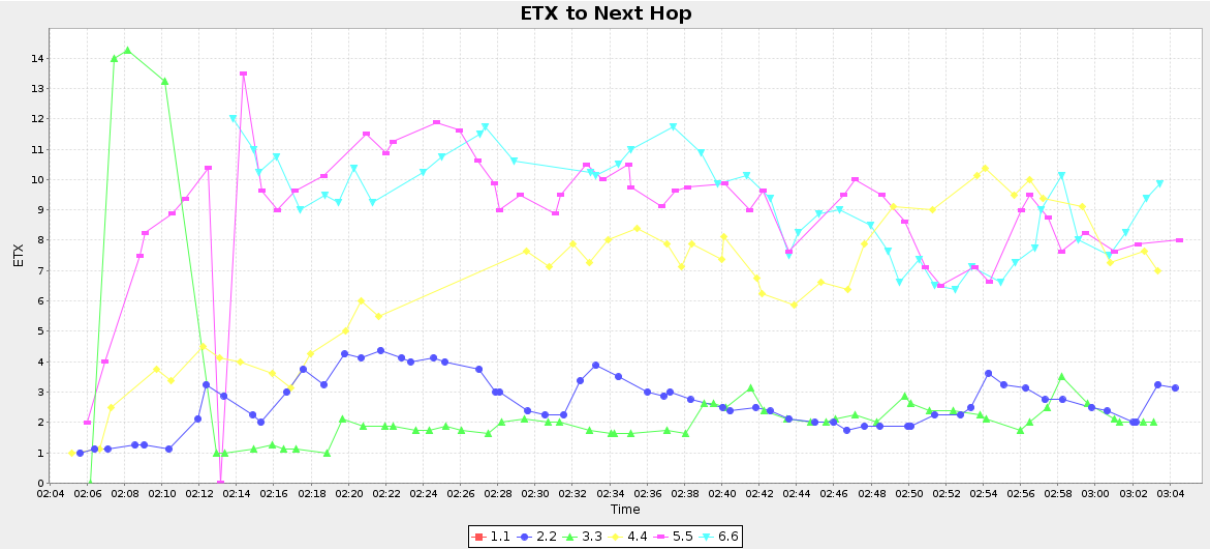
Izgubljeni paketi u scenariju 3 prikazani su na slici 6.31.



Slika 6.31 Izgubljeni paketi (6 čvorova, scenarij 3, bez IDS-a)

U scenariju 3 primjetan je porast broja izgubljenih paketa u odnosu na prethodni scenarij (slika 6.24), što je u skladu s očekivanjima (unatoč mehanizmima potvrde i retransmisije izgubljeno je 35 paketa). Ukoliko se analizira broj primljenih paketa za pojedinačne čvorove, može se zaključiti da je manje paketa pristiglo sa udaljenijih čvorova (čvorovi 4, 5, 6) u odnosu na čvorove u izravnom dometu bazne stanice (čvorovi 2 i 3).

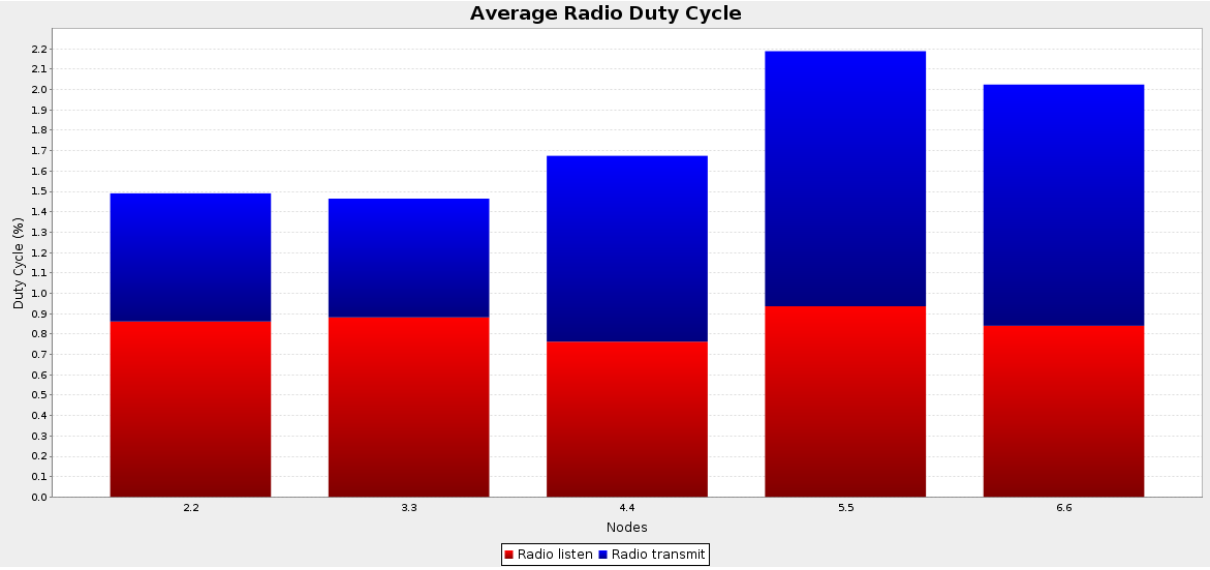
Slika 6.32 prikazuje ETX vrijednosti za pojedine čvorove u trećem scenariju u mreži sa 6 čvorova.



Slika 6.32 ETX metrika (6 čvorova, scenarij 3, bez IDS-a)

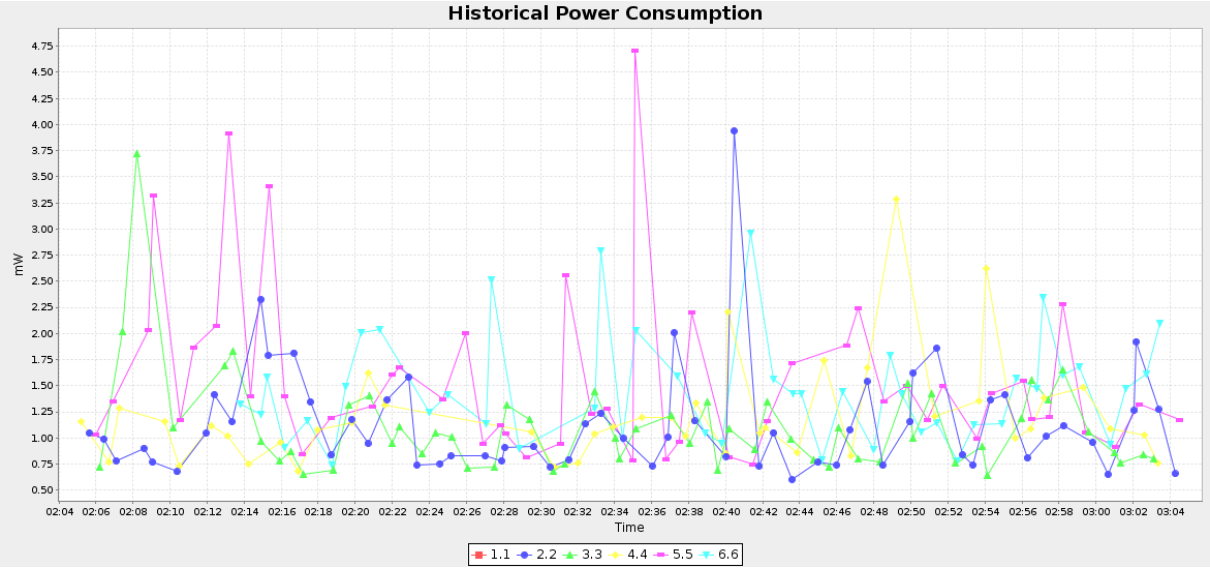
Može se primijetiti da su ETX vrijednosti porasle za sve čvorove u mreži u usporedbi sa scenarijem 2 (slika 6.25). Također, sa slike je vidljivo da su opet ETX vrijednosti veće za udaljenije čvorove (4, 5 i 6) nego za čvorove bliže baznoj stanici (2 i 3). To znači da njima treba više pokušaja za uspješno slanje jednog paketa, pa je otuda i povećani gubitak paketa zabilježen upravo za udaljenije čvorove.

U scenariju 3 zbog povećanih gubitaka paketa dodatno se povećava i potreba za retransmisijom paketa, pa je u odnosu na scenarij 2 (slika 6.26) dodatno povećan udio aktivne predaje u radnom ciklusu radio primopredajnika, što je vidljivo na slici 6.33.



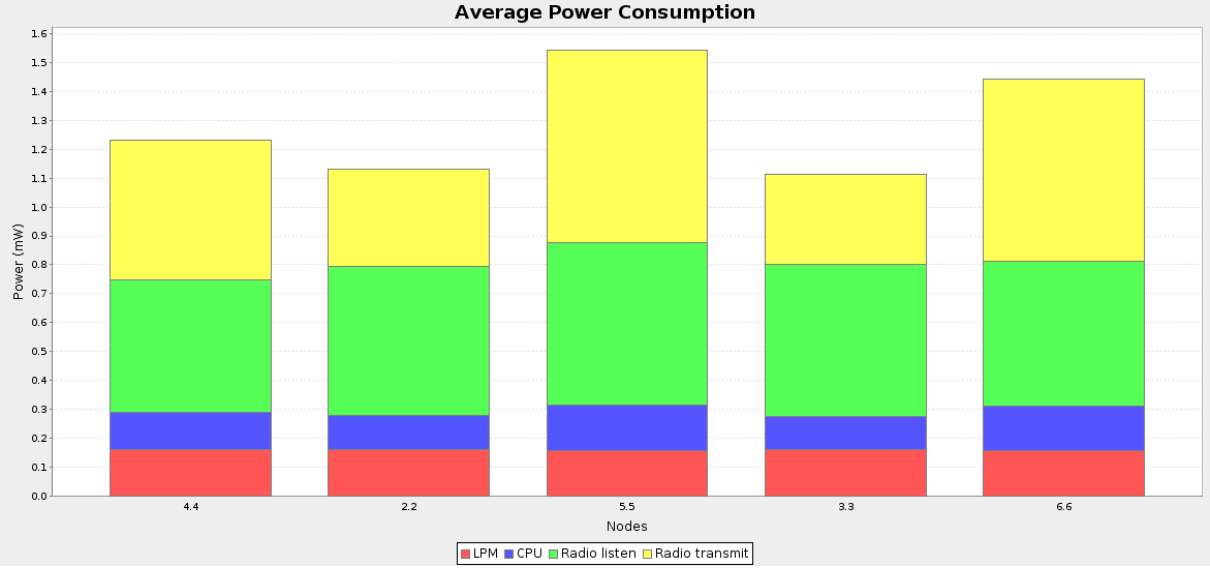
Slika 6.33 Prosječni radni ciklus primopredajnika (6 čvorova, scenarij 3, bez IDS-a)

Slika 6.34 prikazuje potrošnju energije u scenariju 3.



Slika 6.34 Potrošnja energije (6 čvorova, scenarij 3, bez IDS-a)

Na slici 6.35 prikazana je potrošnja energije za svaki pojedinačni čvor.



Slika 6.35 Prosječna potrošnja energije (6 čvorova, scenarij 3, bez IDS-a)

Iz ovih slika vidljivo je da je potrošnja energije u mreži dodatno povećana u odnosu na prethodni slučaj (scenarij 2, slike 6.27 i 6.28), te da još veći dio utrošene energije otpada na potrošnju primopredajnika u stanju aktivne predaje. Dobiveni rezultat u potpunosti je sukladan očekivanjima, budući da je u razmatranom scenariju dodatno povećan gubitak

paketa, što nužno dovodi do povećane potrebe za njihovom retransmisijom. I u ovom razmatranom slučaju potrošnja energije veća je za periferne čvorove, budući da su periferni čvorovi više puta trebali raditi retransmisiju (što je vidljivo i sa slike koja prikazuje ETX metriku u mreži).

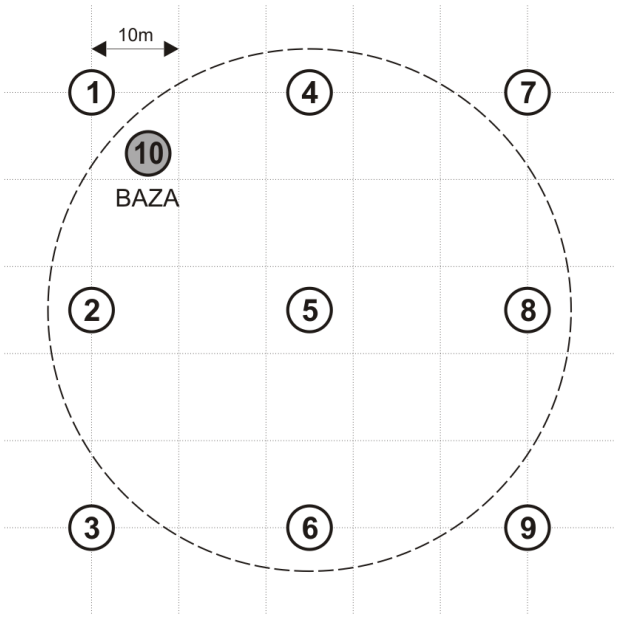
U tablici 6.3 su pregledno prikazane sve dobivene vrijednosti za treći scenarij u mreži sa 6 čvorova.

TABLICA 6.3 Mreža sa 6 čvorova, scenarij 3, bez IDS-a

Čvor	Primljeni paketi	Izgubljeni paketi	Skokovi do baze	ETX	Potrošnja energije (mW)					Radni ciklus	
					CPU	LPM	Slušanje	Predaja	Ukupno	Slušanje	Predaja
2	60	0	1.000	2.671	0.119	0.160	0.517	0.334	1.130	0.861	0.629
3	56	2	1.143	2.583	0.114	0.160	0.529	0.309	1.113	0.882	0.583
4	42	17	2.000	6.542	0.131	0.160	0.457	0.485	1.233	0.762	0.913
5	51	9	2.000	8.897	0.157	0.159	0.562	0.665	1.543	0.937	1.251
6	44	7	2.000	9.264	0.151	0.159	0.504	0.629	1.443	0.840	1.184
Prosjek	**50.600**	**7.000**	**1.629**	**5.991**	**0.135**	**0.159**	**0.514**	**0.484**	**1.292**	**0.857**	**0.912**

6.5.2. Mreža sa 10 čvorova

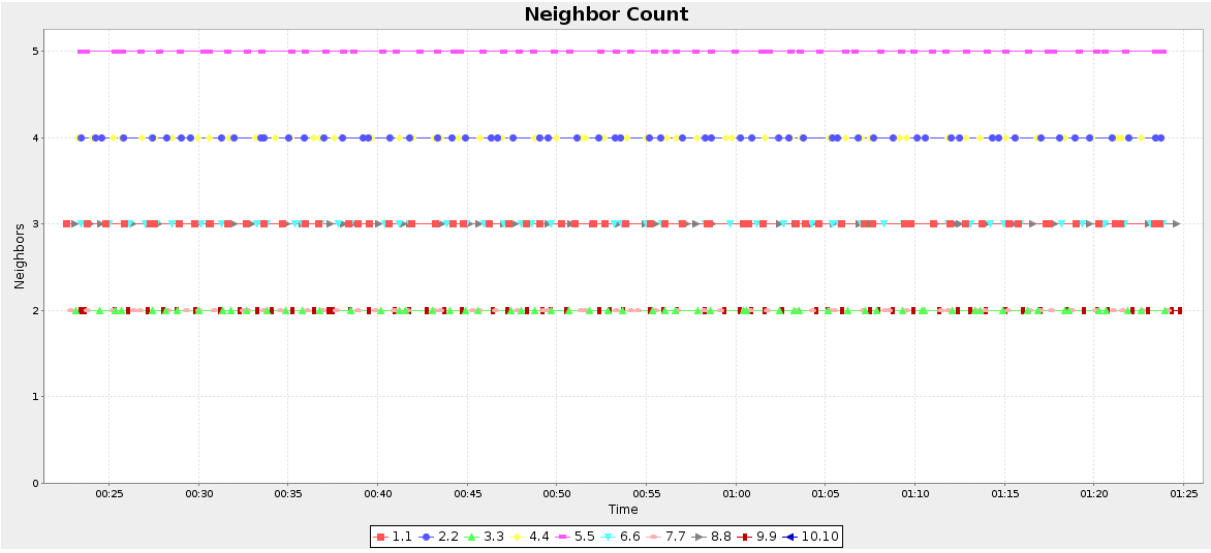
Druga karakteristična mreža koja se koristi za potrebe testiranja sastoji se od 10 čvorova (9 standardnih čvorova i bazna stanica). Topologija mreže prikazana je na slici 6.36.



Slika 6.36 Topologija mreže sa 10 čvorova

Kao i u slučaju mreže sa 6 čvorova, i u slučaju mreže sa 10 čvorova analizirana su tri karakteristična scenarija. Prvi scenarij predstavlja „idealan slučaj“, u kojem je vjerojatnost uspješnog slanja i prijema postavljena na 100%. Druga dva scenarija predstavljaju realnu situaciju u kojoj su ove vrijednosti postavljene na 80% (scenarij 2) i 60% (scenarij 3), analogno prethodno analiziranoj mreži. Čvorovi označeni brojevima 1-9 su standardni čvorovi, dok je čvor 10 bazna stanica.

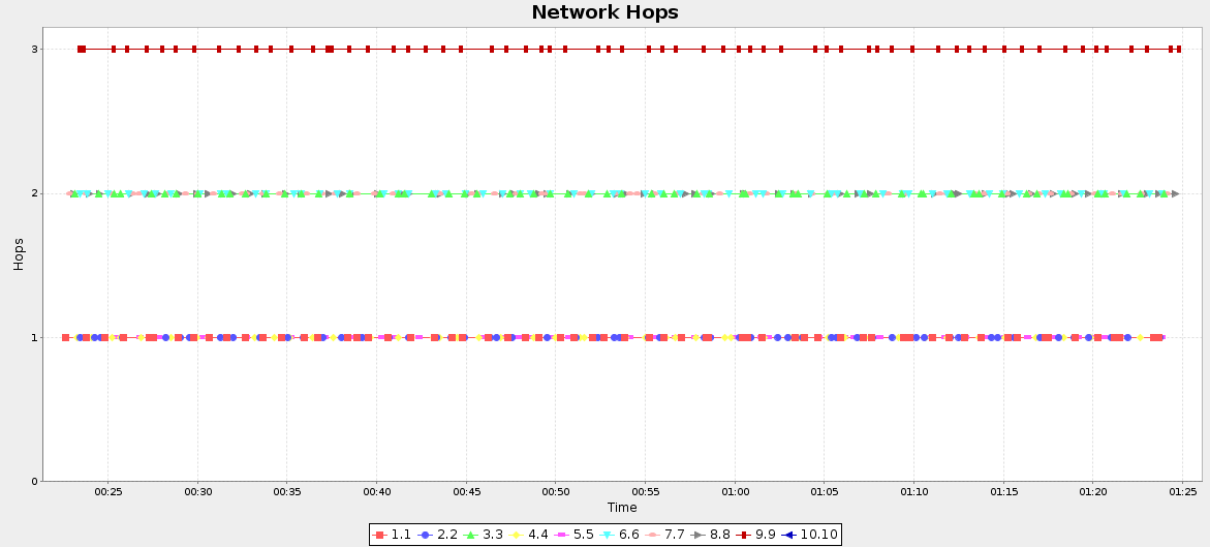
Na slici 6.37 prikazan je broj susjednih čvorova za svaki pojedini čvor u mreži.



Slika 6.37 Broj susjednih čvorova u mreži sa 10 čvorova

Sa slike je vidljivo da u simuliranoj mreži sa 10 čvorova čvorovi imaju od minimalno 2 do maksimalno 5 susjednih čvorova (čvorova koji su im u izravnom dometu). Tako po dva susjedna čvora imaju čvorovi 3, 7 i 9, po 3 susjedna čvora imaju čvorovi 1, 6 i 8, po 4 susjedna čvora imaju čvorovi 2 i 4, do 5 susjeda ima čvor 5.

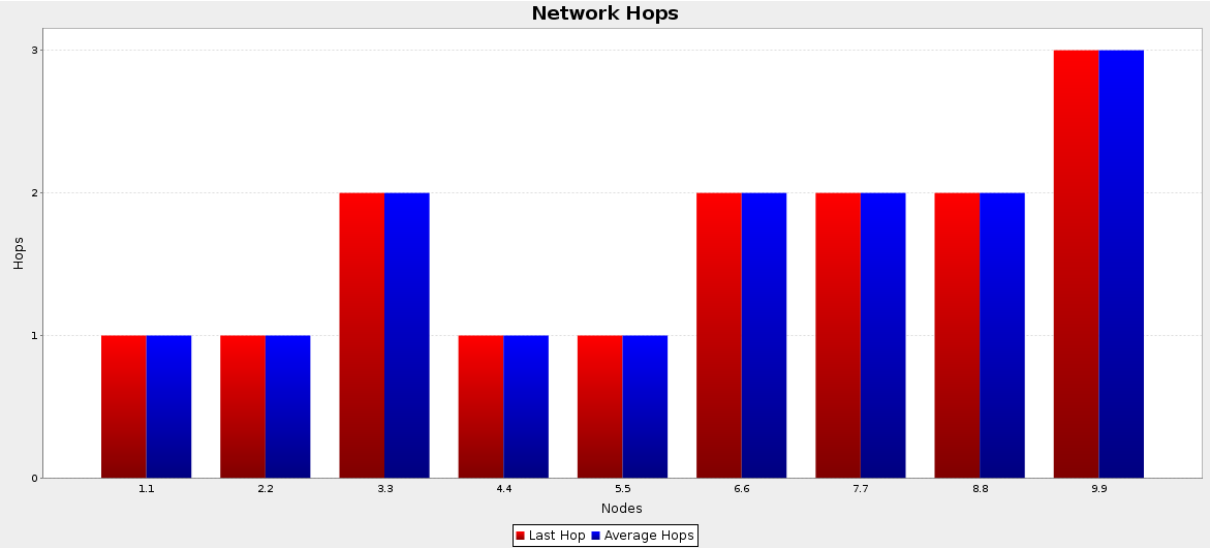
Rasporedom čvorova i dometom primopredajnika (domet 30 metara, područje interferencije 45 metara) uvjetovan je i broj skokova prilikom komunikacije pojedinih čvorova sa baznom stanicom. Na slici 6.38 prikazan je broj skokova do bazne stanice za svaki pojedini čvor.



Slika 6.38 Broj skokova do bazne stanice u mreži sa 10 čvorova

Sa slike je vidljivo da su jedan skok od bazne stanice udaljeni čvorovi 1, 2, 4 i 5, čvorovi 3, 6, 7 i 8 udaljeni su po 2 skoka, dok je čvor 9 tri skoka udaljen od bazne stanice.

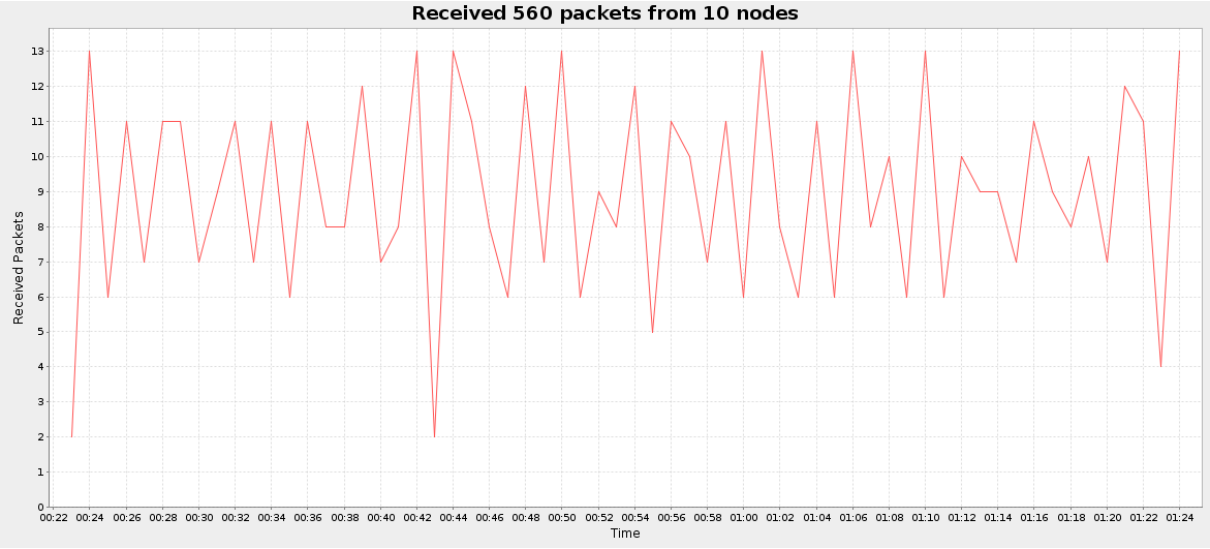
Slika 6.39 prikazuje broj skokova za svaki pojedini čvor.



Slika 6.39 Broj skokova za pojedinačne čvorove u mreži sa 10 čvorova

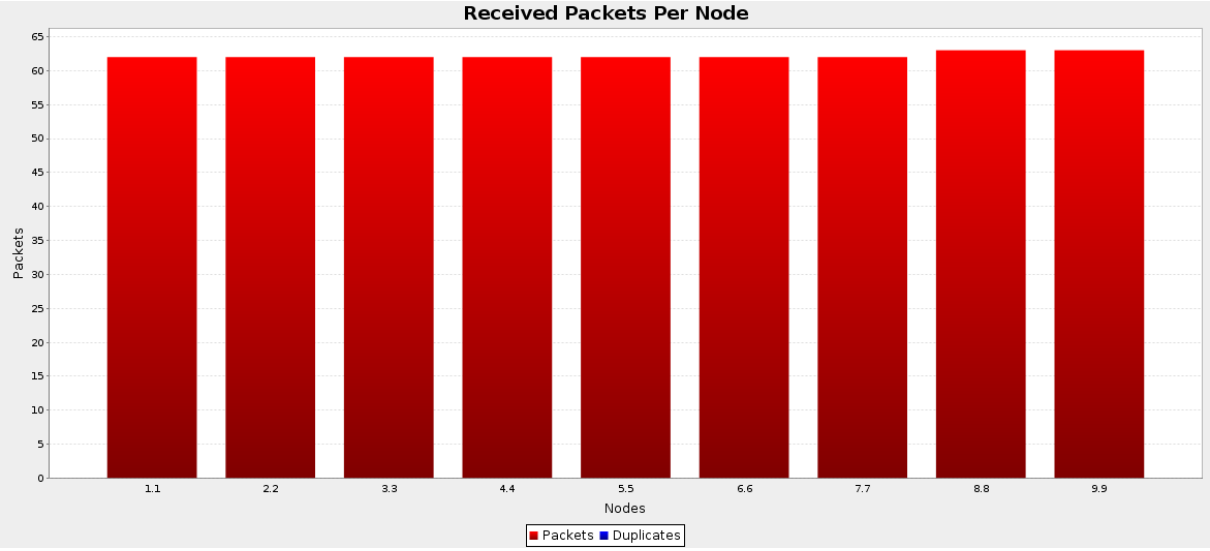
Scenarij 1 (Rx/Tx=100%)

U prvom simuliranom scenariju u mreži sa 10 čvorova vjerojatnost ispravnog slanja i prijema paketa iznosi 100%. Prema tome, izgubljenih paketa nema, a primljeni paketi tijekom promatranog intervala od jednog sata prikazani su na slici 6.40.



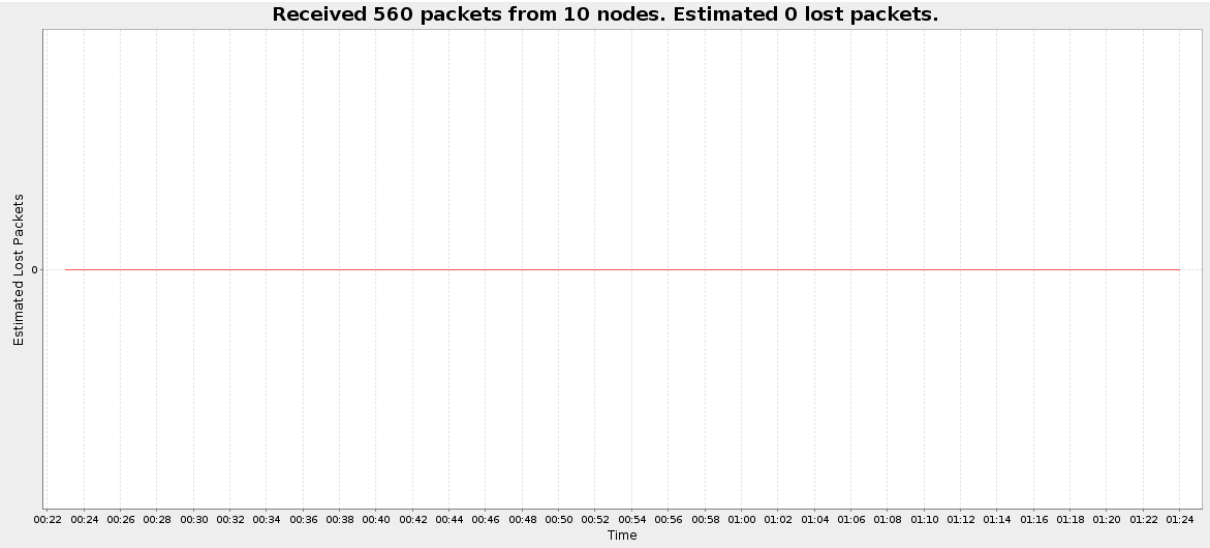
Slika 6.40 Broj primljenih paketa (10 čvorova, scenarij 1, bez IDS-a)

Slika 6.41 prikazuje broj primljenih paketa za svaki pojedini čvor u prvom scenariju.



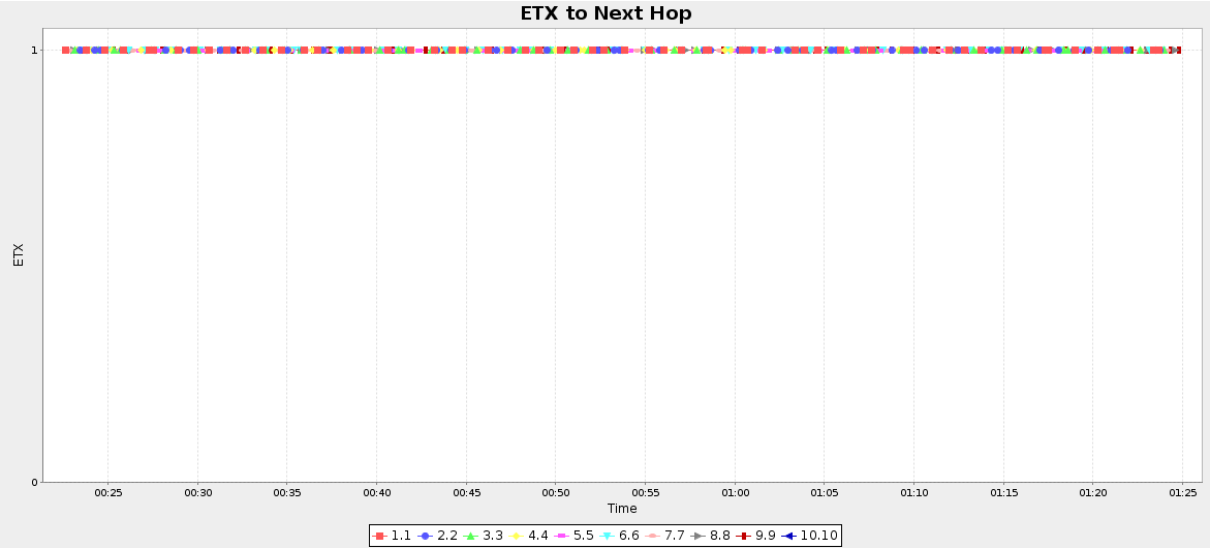
Slika 6.41 Broj primljenih paketa za svaki čvor (10 čvorova, scenarij 1, bez IDS-a)

Prikaz na slici 6.42 potvrđuje da nije bilo izgubljenih paketa.



Slika 6.42 Izgubljeni paketi (10 čvorova, scenarij 1, bez IDS-a)

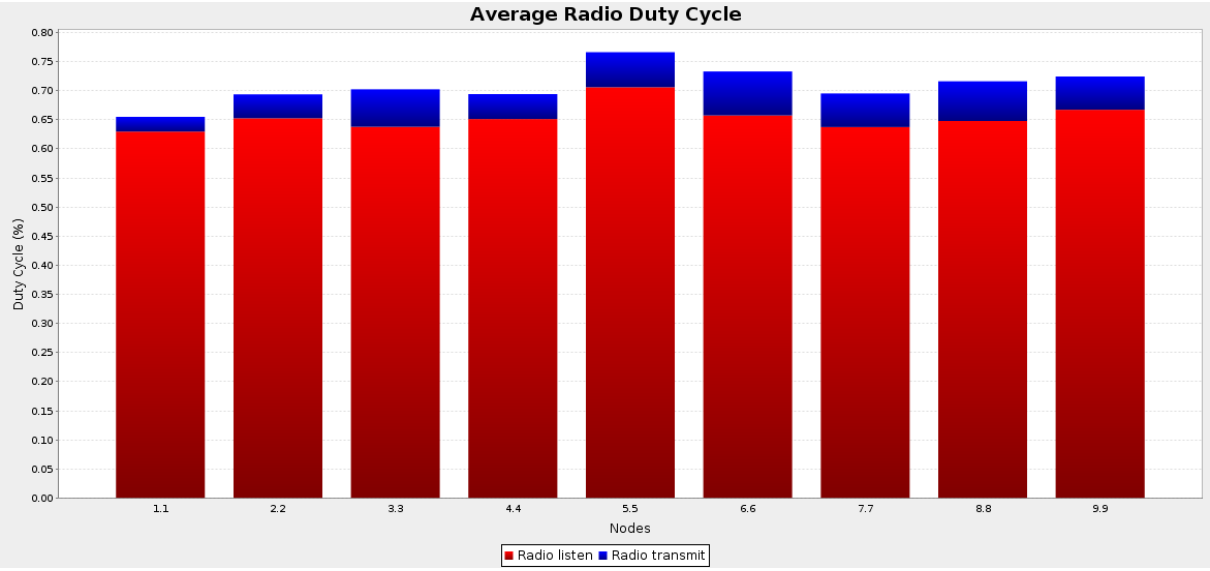
Slika 6.43 prikazuje ETX metriku za prvi scenarij u mreži sa 10 čvorova.



Slika 6.43 ETX metrika (10 čvorova, scenarij 1, bez IDS-a)

Sa slike je vidljivo da ETX vrijednost za sve linkove iznosi 1, što je u skladu sa činjenicom da niti na jednom od linkova u mreži nema gubitka podataka prilikom prijenosa.

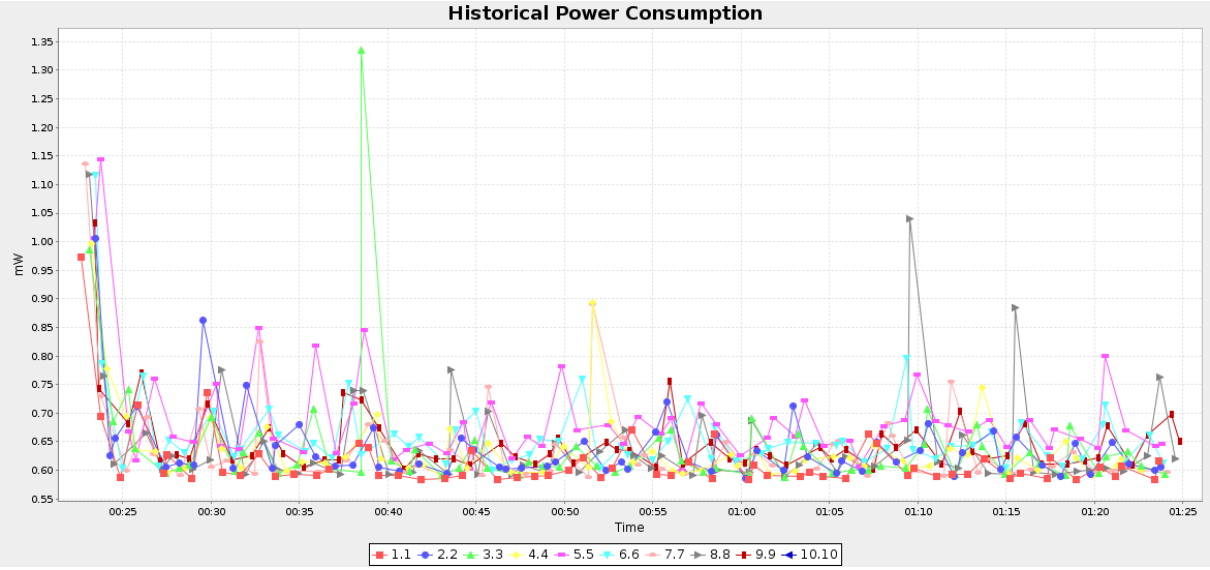
Slika 6.44 prikazuje prosječni radni ciklus primopredajnika u prvom simuliranom scenariju iz mreže sa 10 čvorova.



Slika 6.44 Prosječni radni ciklus primopredajnika (10 čvorova, scenarij 1, bez IDS-a)

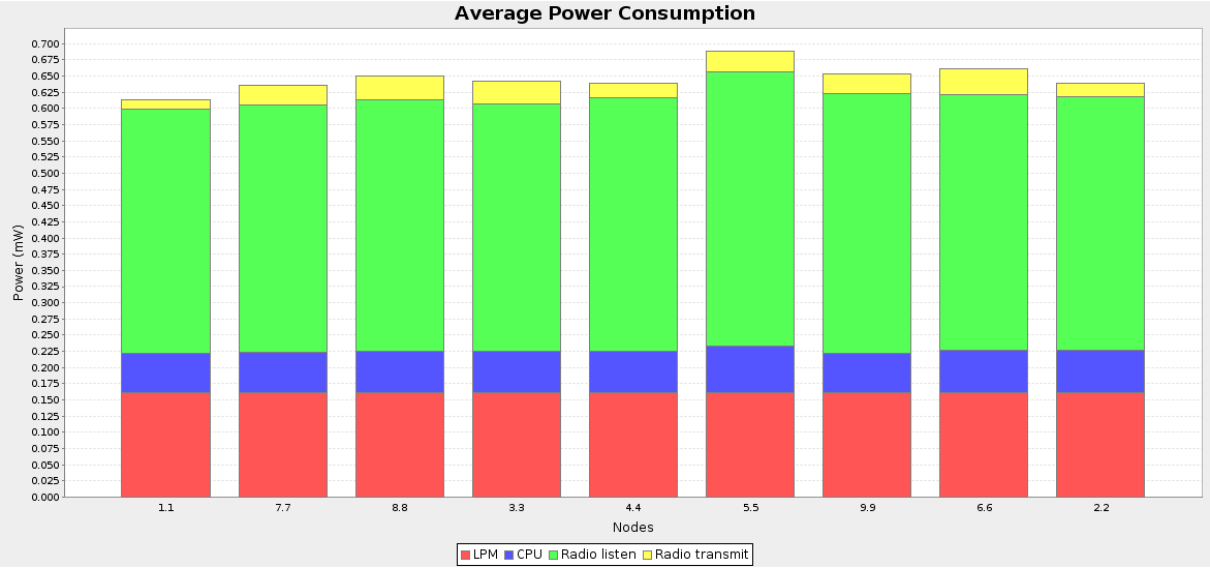
Vidljivo je da za svaki pojedinačni primopredajnik vrijedi da najveći dio njegovog aktivnog perioda otpada na „slušanje“, a tek vrlo mali dio na aktivnu predaju. Očekivano,

nešto veća aktivnost primopredajnika zabilježena je kod čvorova koji imaju više susjednih čvorova. Za očekivati je da će se to odraziti i na potrošnju energije, budući da je primopredajnik energetski najzahtjevnija komponenta u senzorskoj mreži. Slika 6.45 prikazuje kretanje potrošnje energije kroz promatrano jednosatno razdoblje.



Slika 6.45 Potrošnja energije (10 čvorova, scenarij 1, bez IDS-a)

Slika 6.46 prikazuje prosječnu potrošnju energije za svaki pojedini čvor u mreži sa 10 čvorova (prvi simulirani scenarij).



Slika 6.46 Prosječna potrošnja energije (10 čvorova, scenarij 1, bez IDS-a)

Vidljivo je da u strukturi energetske potrošnje za svaki pojedini čvor najveći dio predstavlja potrošnja primopredajnika u stanju „slušanja“. U pogledu ukupne potrošnje pokazuje se da je ona za nijansu veća na središnjim čvorovima (preko kojih prolazi više ruta ka baznoj stanici).

U tablici 6.4 su pregledno prikazane dobivene vrijednosti za prvi simulirani scenarij u mreži sa 10 čvorova.

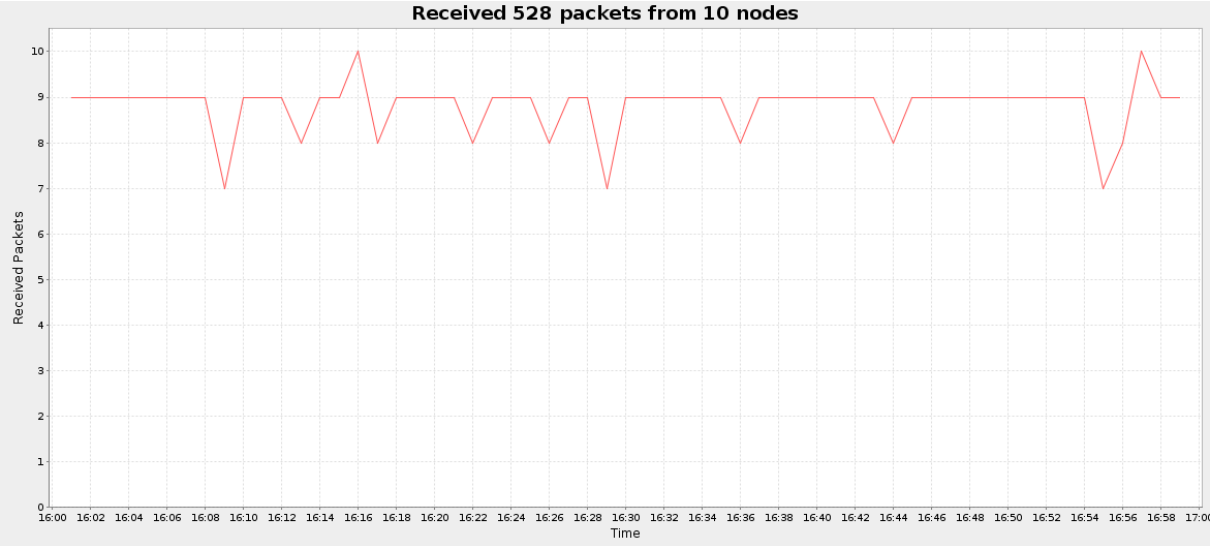
TABLICA 6.4 Mreža sa 10 čvorova, scenarij 1, bez IDS-a

Čvor	Primljeni paketi	Izgubljeni paketi	Skokovi do baze	ETX	Potrošnja energije (mW)					Radni ciklus (%)	
					CPU	LPM	Slušanje	Predaja	Ukupno	Slušanje	Predaja
1	62	0	1.000	1.000	0.060	0.162	0.378	0.013	0.613	0.630	0.025
2	62	0	1.000	1.000	0.065	0.162	0.392	0.022	0.639	0.653	0.041
3	62	0	2.000	1.000	0.063	0.162	0.383	0.034	0.642	0.638	0.064
4	62	0	1.000	1.000	0.064	0.162	0.391	0.023	0.639	0.651	0.043
5	62	0	1.000	1.000	0.072	0.161	0.424	0.032	0.688	0.706	0.060
6	62	0	2.000	1.000	0.066	0.162	0.394	0.040	0.662	0.657	0.076
7	62	0	2.000	1.000	0.062	0.162	0.383	0.031	0.636	0.638	0.058
8	63	0	2.000	1.000	0.064	0.162	0.389	0.036	0.650	0.648	0.068
9	63	0	3.000	1.000	0.061	0.162	0.400	0.030	0.653	0.667	0.057
Prosjek	**62.222**	**0.000**	**1.667**	**1.000**	**0.064**	**0.162**	**0.392**	**0.029**	**0.647**	**0.654**	**0.055**

Scenarij 2 (Rx/Tx=80%)

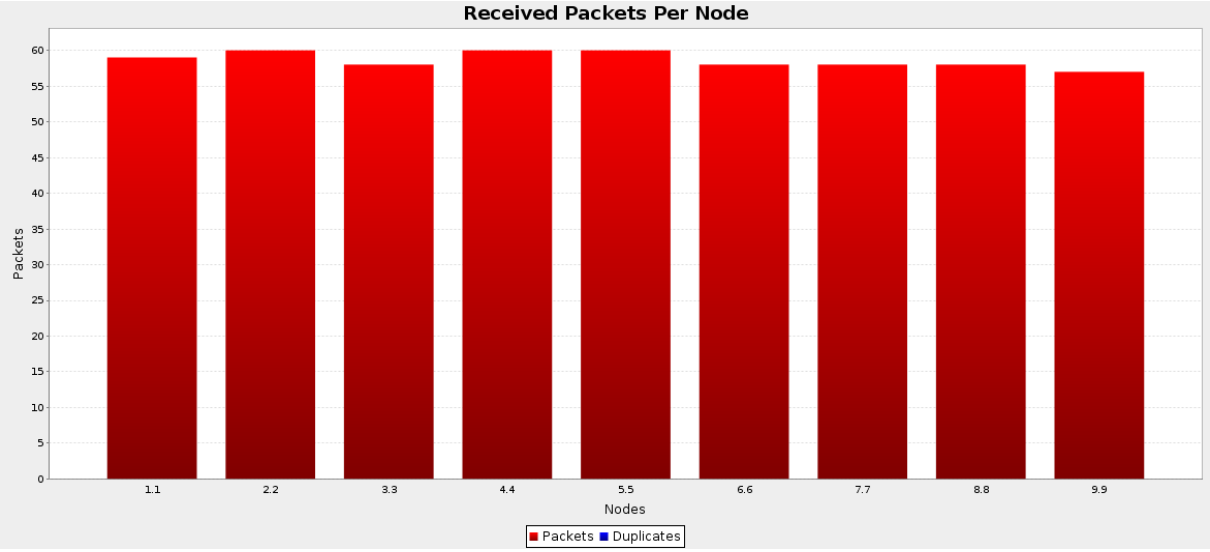
U drugom scenariju razmatranom u mreži sa 10 čvorova vjerojatnost uspješnog slanja i prijema paketa postavljena je na 80% (analogno drugom analiziranom scenariju u mreži sa 6 čvorova). Topologija mreže nije se promijenila u odnosu na prvi scenarij. Broj susjednih čvorova, kao i broj skokova do bazne stanice za svaki pojedini čvor također su nepromijenjeni.

Slika 6.47 prikazuje broj primljenih paketa za drugi scenarij u mreži sa 10 čvorova.



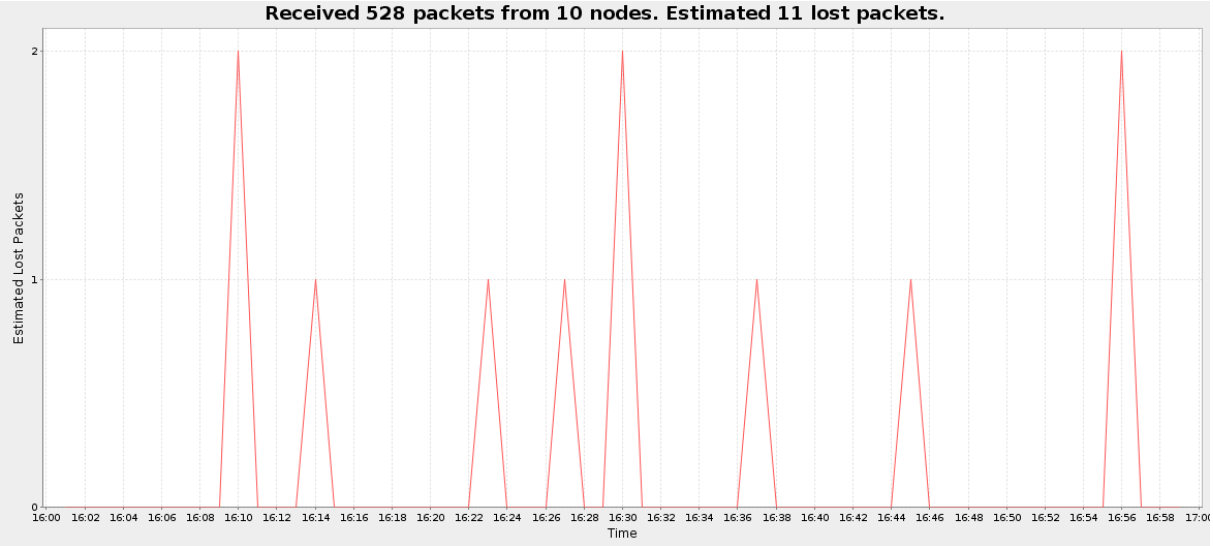
Slika 6.47 Broj primljenih paketa (10 čvorova, scenarij 2, bez IDS-a)

Na slici 6.48 prikazan je broj primljenih paketa od svakog pojedinačnog čvora.



Slika 6.48 Broj primljenih paketa za svaki čvor (10 čvorova, scenarij 2, bez IDS-a)

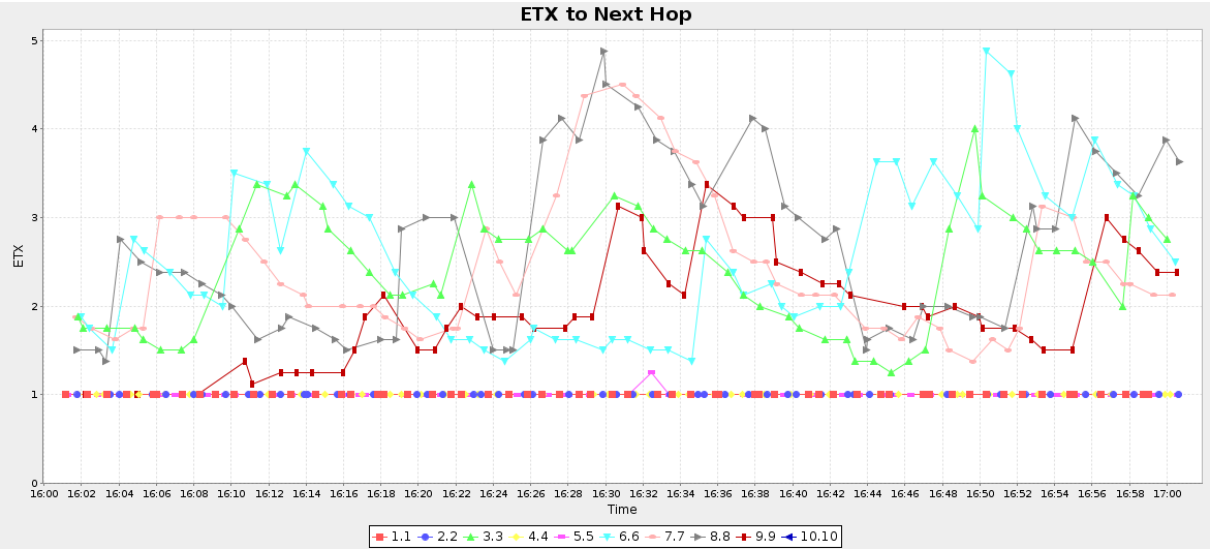
U scenariju 2, očekivano, dolazi i do gubitka pojedinih paketa. Procjena izgubljenih paketa prikazana je na slici 6.49.



Slika 6.49 Izgubljeni paketi (10 čvorova, scenarij 2, bez IDS-a)

Mehanizmi potvrde i retransmisije osigurali su da u ovome scenariju ne dođe do velikog broja izgubljenih paketa. Međutim, za očekivati je da se nužnost retransmisije određenih paketa nužno mora odraziti na potrošnju energije u mreži, kao i na ETX metriku.

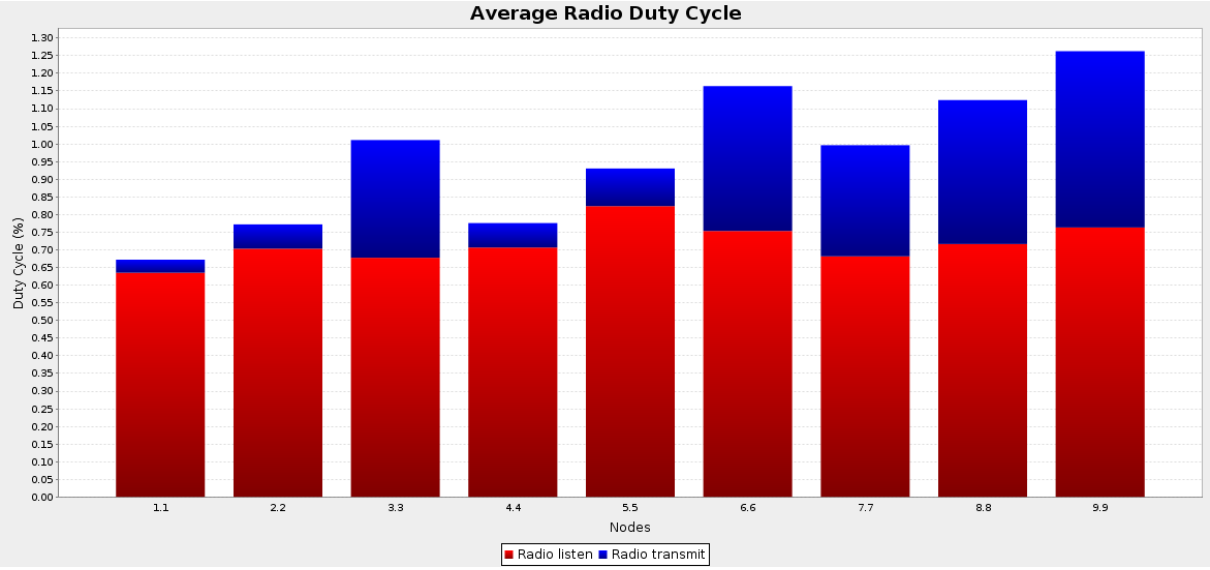
Slika 6.50 prikazuje ETX metriku za drugi simulirani scenarij u mreži sa 10 čvorova.



Slika 6.50 ETX metrika (10 čvorova, scenarij 2, bez IDS-a)

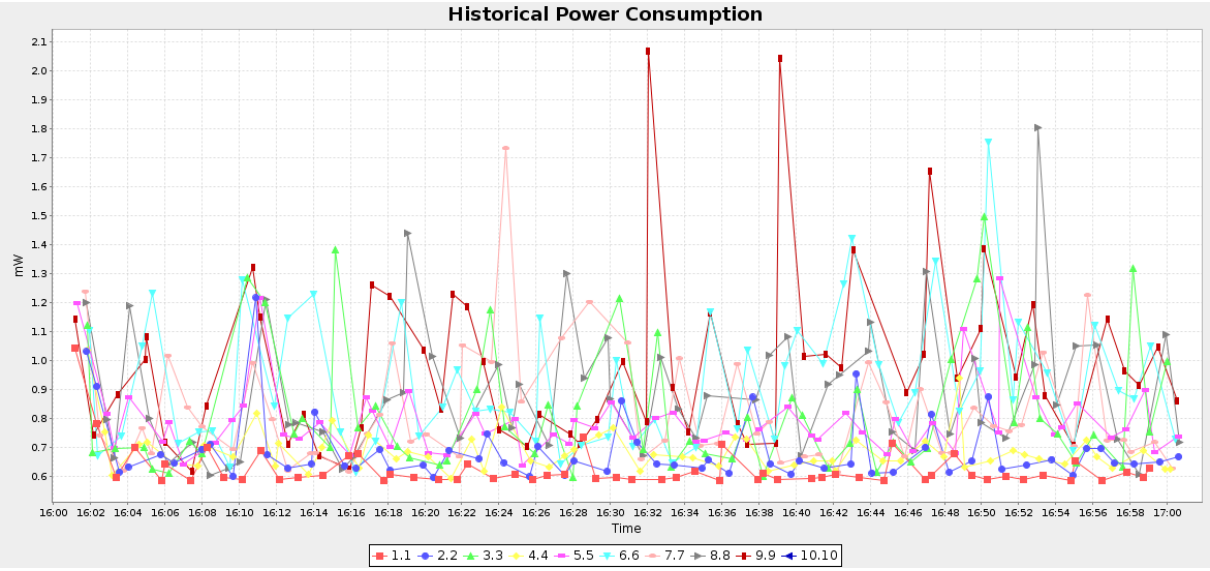
ETX vrijednosti su se povećale, prvenstveno za čvorove udaljenije od bazne stanice, što znači da je na određenim linkovima trebalo više pokušaja za uspješan prijenos poruke.

Potreba za retransmisijom paketa odražava se na radne cikluse primopredajnika (slika 6.51), a time i na potrošnju energije u mreži.



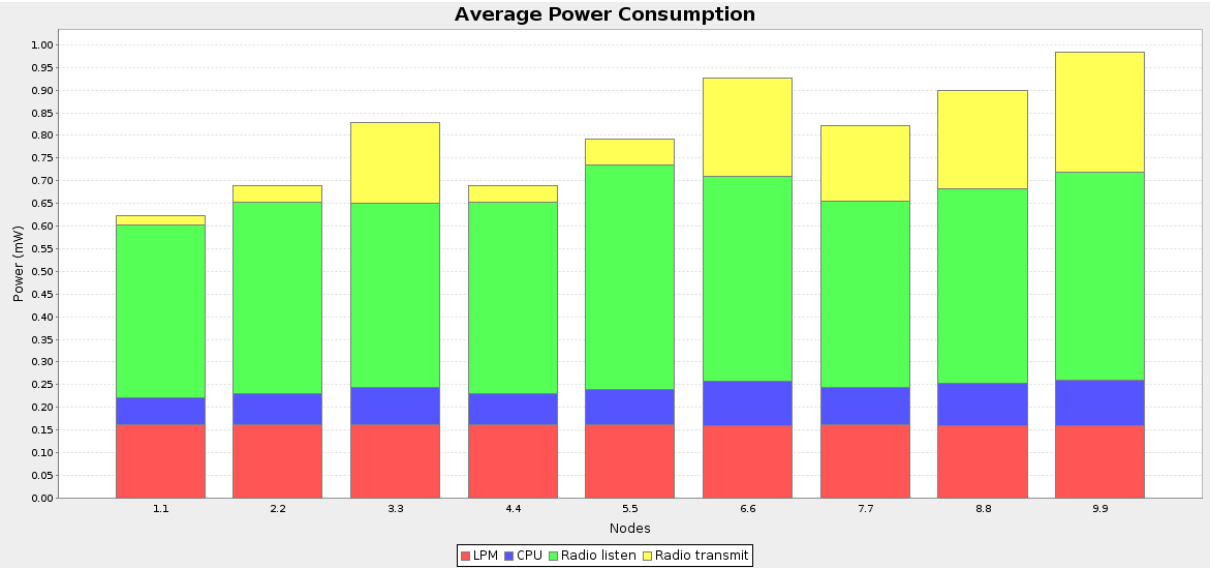
Slika 6.51 Prosječni radni ciklus primopredajnika (10 čvorova, scenarij 2, bez IDS-a)

Sa slike se može primijetiti da se znatno povećao udio vremena koje primopredajnik provodi u stanju aktivnog slanja podataka, posebice za čvorove udaljenije od bazne stanice. Slika 6.52 prikazuje kako se to odražava na potrošnju energije.



Slika 6.52 Potrošnja energije (10 čvorova, scenarij 2, bez IDS-a)

Povećana potrošnja energije u odnosu na prethodni scenarij (slika 6.46) primjećuje se i na slici 6.53, koja prikazuje prosječnu potrošnju energije za svaki pojedinačni čvor.



Slika 6.53 Prosječna potrošnja energije (10 čvorova, scenarij 2, bez IDS-a)

Na slici je vidljivo da se prosječna potrošnja energije povećala u odnosu na prethodni scenarij, prvenstveno na čvorovima koji su udaljeniji od bazne stanice, i to zbog povećane aktivnosti njihovih predajnika radi potrebe za češćim retransmisijama paketa nakon njihovog neuspješnog prijema.

Tablica 6.5 pregledno prikazuje dobivene vrijednosti za drugi simulirani scenarij u mreži sa 10 čvorova.

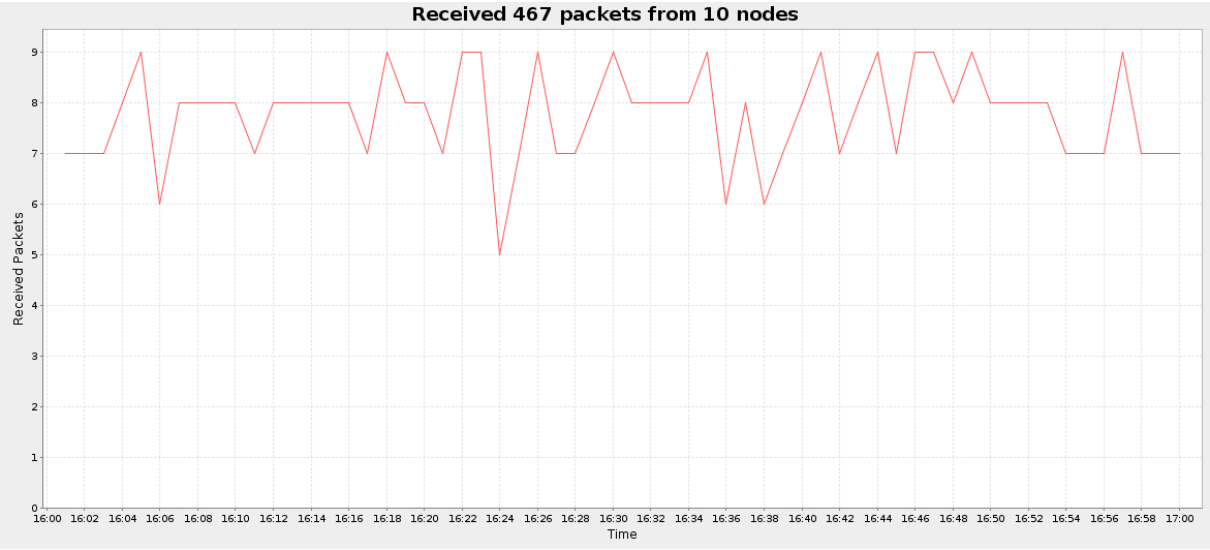
TABLICA 6.5 Mreža sa 10 čvorova, scenarij 2, bez IDS-a

Čvor	Primljeni paketi	Izgubljeni paketi	Skokovi do baze	ETX	Potrošnja energije (mW)					Radni ciklus (%)	
					CPU	LPM	Slušanje	Predaja	Ukupno	Slušanje	Predaja
1	59	0	1.000	1.000	0.060	0.162	0.381	0.020	0.623	0.635	0.037
2	60	0	1.000	1.000	0.068	0.161	0.422	0.037	0.688	0.703	0.069
3	58	2	2.000	2.425	0.084	0.161	0.407	0.177	0.829	0.678	0.333
4	60	0	1.000	1.000	0.068	0.161	0.424	0.037	0.690	0.707	0.069
5	60	0	1.000	1.004	0.079	0.161	0.494	0.057	0.791	0.824	0.107
6	58	2	2.000	2.511	0.096	0.161	0.452	0.218	0.927	0.753	0.410
7	58	2	2.000	2.388	0.084	0.161	0.409	0.167	0.821	0.682	0.315
8	58	2	2.207	2.655	0.093	0.161	0.430	0.217	0.900	0.717	0.408
9	57	3	3.000	1.908	0.100	0.160	0.458	0.265	0.984	0.764	0.499
Prosjek	**58.667**	**1.222**	**1.690**	**1.766**	**0.081**	**0.161**	**0.431**	**0.133**	**0.806**	**0.718**	**0.250**

Scenarij 3 (Rx/Tx=60%)

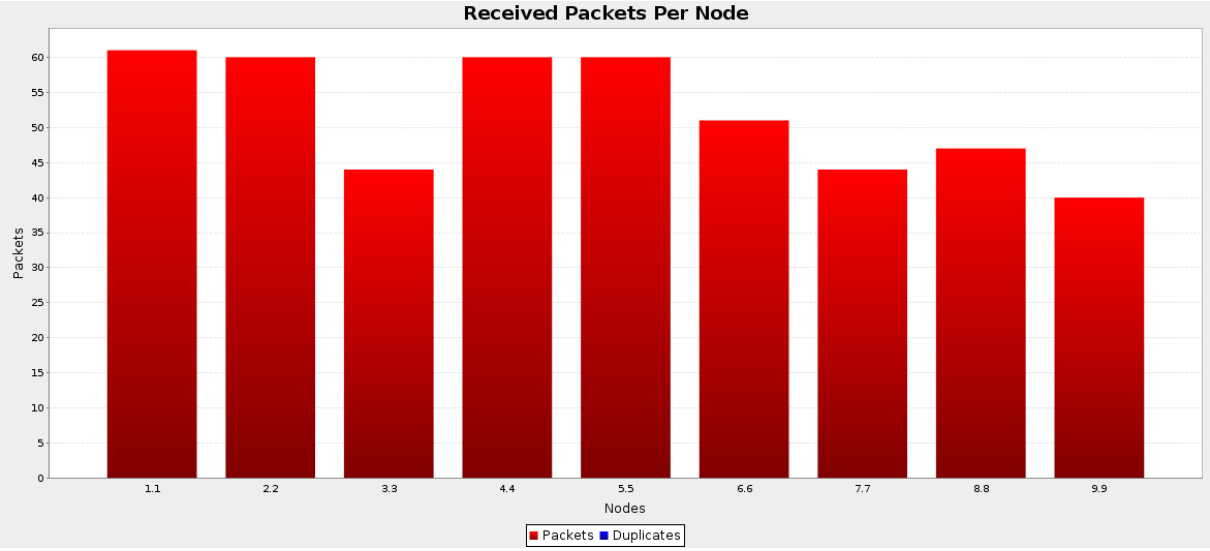
Treći simulirani scenarij u mreži sa 10 čvorova podrazumijeva da je vjerojatnost uspješnog slanja i prijema paketa 60% (analogno trećem scenariju u mreži sa 6 čvorova), dok su preostali parametri mreže (raspored čvorova, učestalost slanja paketa, broj skokova, broj susjednih čvorova) isti kao u prethodna dva scenarija.

Slika 6.54 prikazuje primljeni podatkovni promet u trećem simuliranom scenariju mreže sa 10 čvorova tijekom simuliranog jednosatnog intervala.



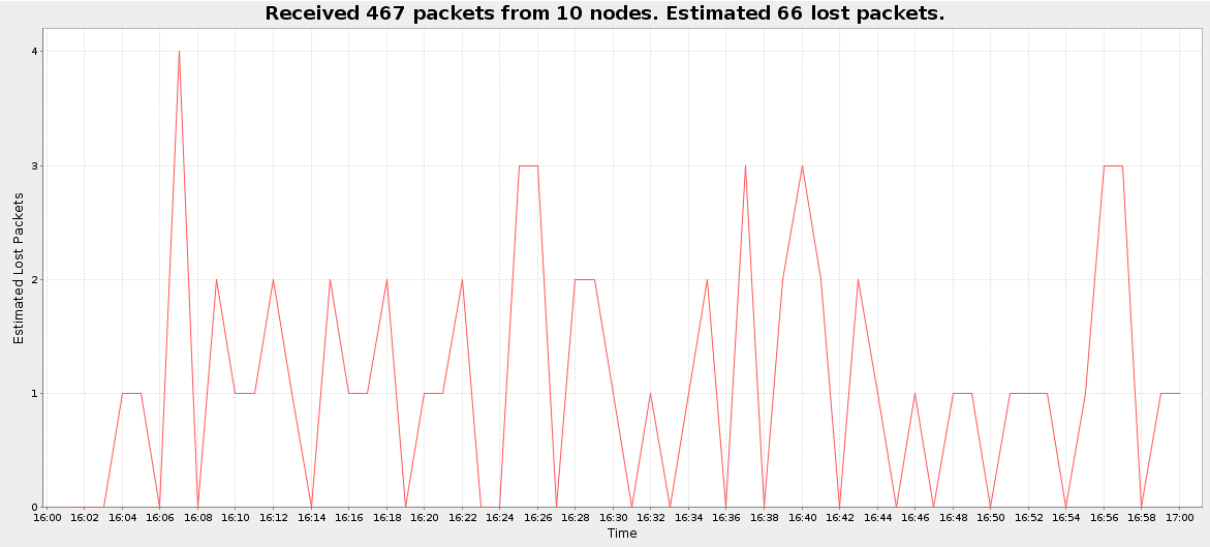
Slika 6.54 Broj primljenih paketa (10 čvorova, scenarij 3, bez IDS-a)

Slika 6.55 prikazuje primljene pakete za svaki pojedini čvor u mreži.



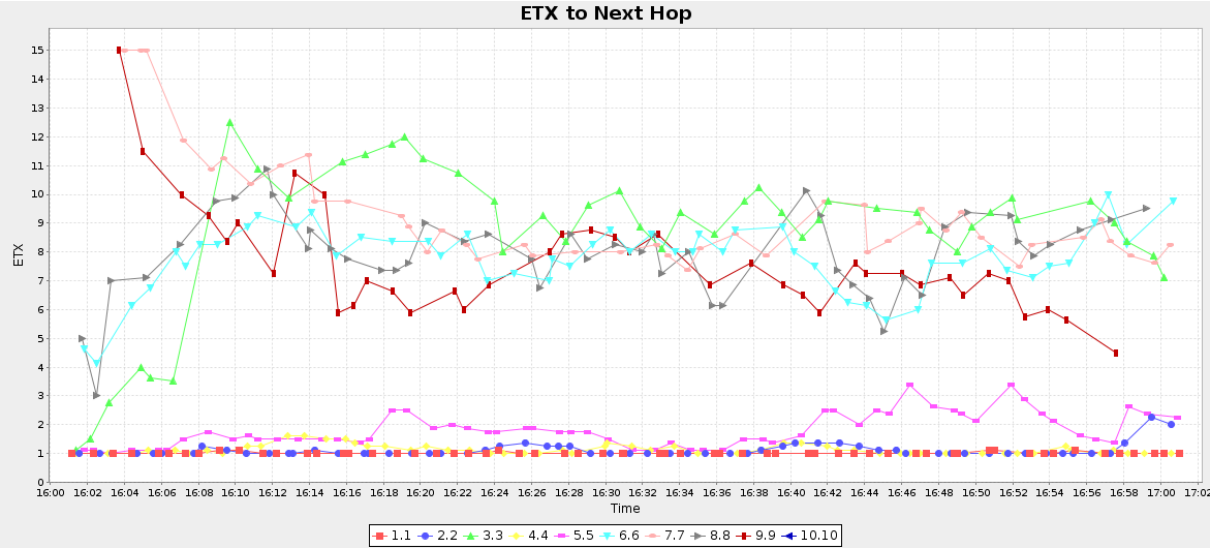
Slika 6.55 Broj primljenih paketa za svaki čvor (10 čvorova, scenarij 3, bez IDS-a)

Može se primijetiti znatno smanjenje broja primljenih paketa u odnosu na prethodni scenarij (slika 6.48), prvenstveno od čvorova koji su udaljeniji od bazne stanice. Na slici 6.56 prikazani su procijenjeni gubici.



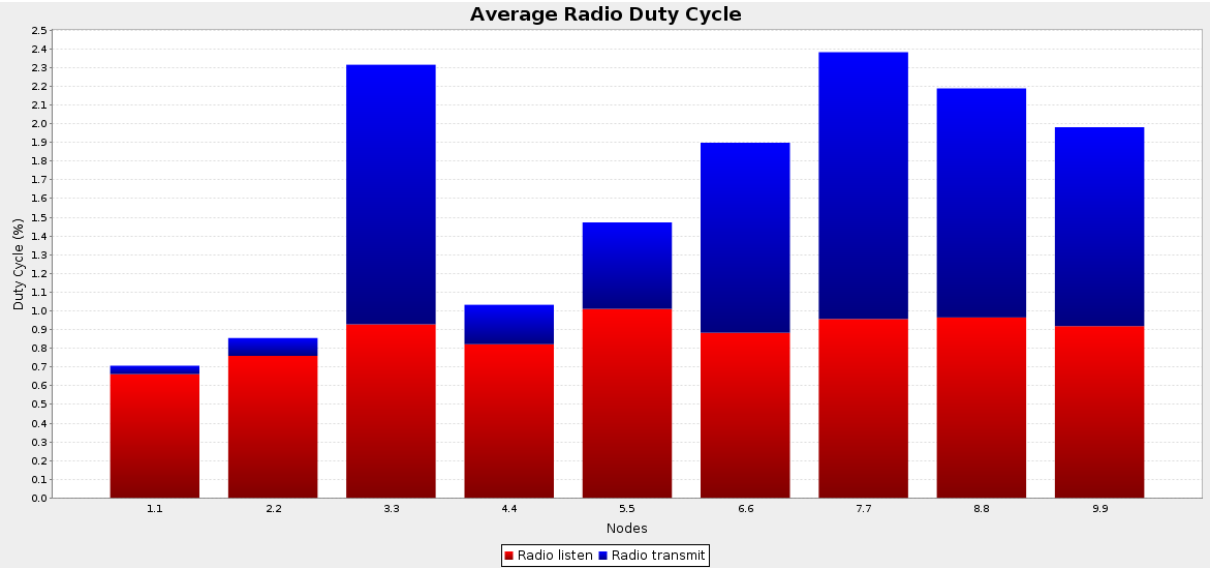
Slika 6.56 Izgubljeni paketi (10 čvorova, scenarij 3, bez IDS-a)

U trećem scenariju čak niti mehanizmi potvrde i retransmisije nisu bili u mogućnosti spriječiti gubitak značajnog broja paketa. Slika 6.57 prikazuje ETX metriku u mreži.



Slika 6.57 ETX metrika (10 čvorova, scenarij 3, bez IDS-a)

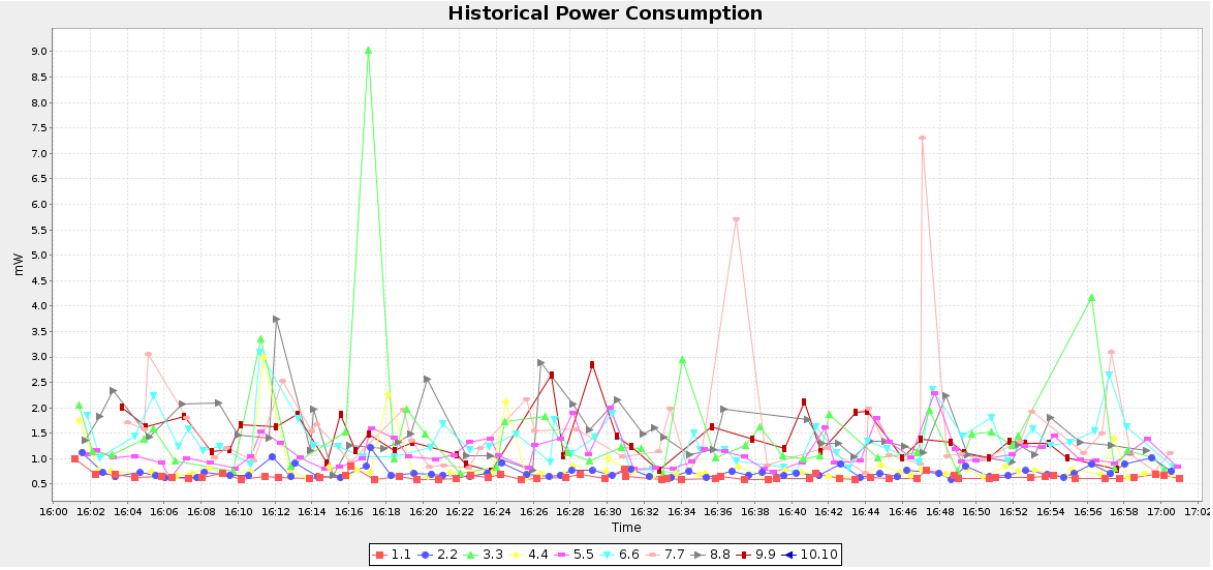
ETX vrijednosti su se povećale u odnosu na prethodni scenarij (slika 6.50), što znači da je za uspješan prijenos paketa potreban još veći broj pokušaja, prvenstveno za udaljenije čvorove.



Slika 6.58 Prosječni radni ciklus primopredajnika (10 čvorova, scenarij 3, bez IDS-a)

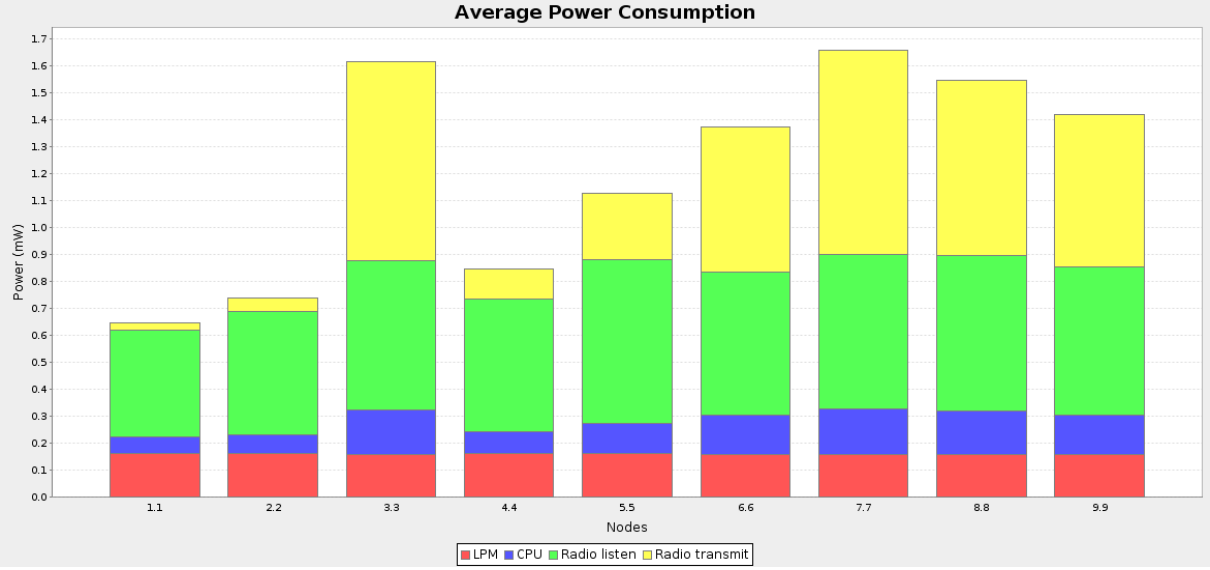
Na slici 6.58, koja prikazuje radne cikluse primopredajnika, vidi se značajno povećanje razdoblja u kojem čvorovi šalju pakete, prvenstveno kod onih udaljenijih (čvorovi 3, 6, 7, 8 i

9). Slika 6.59 prikazuje potrošnju energije tijekom promatranih sat vremena u trećem scenariju.



Slika 6.59 Potrošnja energije (10 čvorova, scenarij 3, bez IDS-a)

Na slici 6.60 prikazana je prosječna potrošnja energije za svaki pojedini čvor u trećem scenariju.



Slika 6.60 Prosječna potrošnja energije (10 čvorova, scenarij 3, bez IDS-a)

Može se primijetiti da ukupna potrošnja energije raste, te po apsolutnom iznosu značajno nadmašuje potrošnju u prethodnom slučaju (slika 6.53). Također, karakteristično je značajno

povećanje potrošnje na udaljenim čvorovima, zbog povećane potrošnje predajnika u opetovanim postupcima slanja izgubljenih paketa.

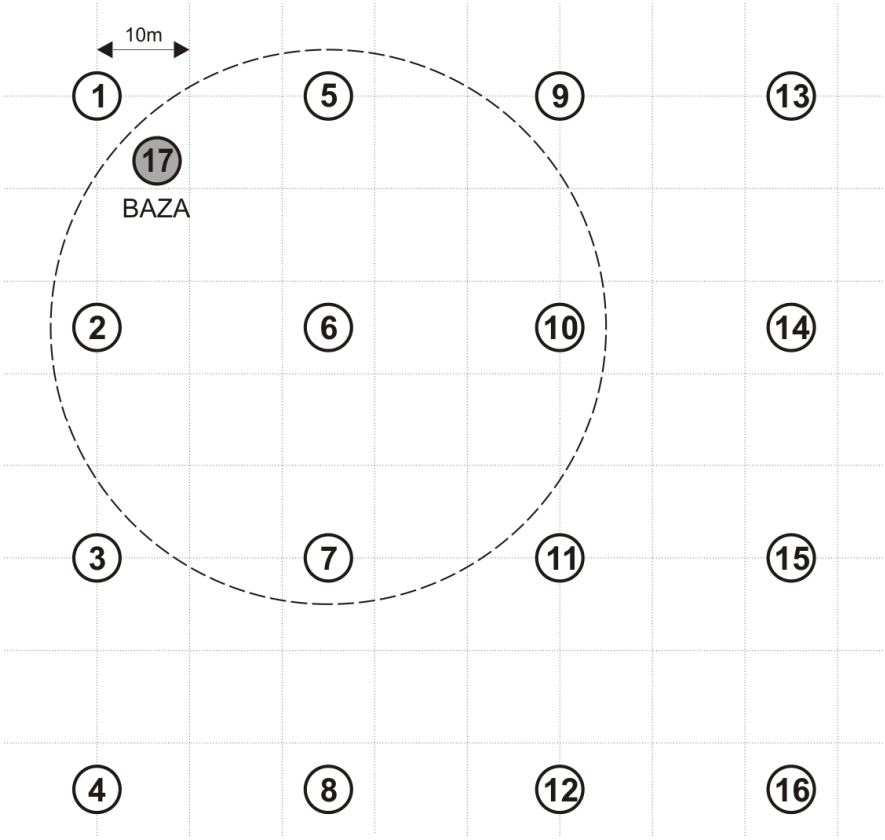
U tablici 6.6 su pregledno prikazane vrijednosti dobivene za treći scenarij u mreži sa 10 čvorova.

TABLICA 6.6 Mreža sa 10 čvorova, scenarij 3, bez IDS-a

Čvor	Primljeni paketi	Izgubljeni paketi	Skokovi do baze	ETX	Potrošnja energije (mW)					Radni ciklus (%)	
					CPU	LPM	Slušanje	Predaja	Ukupno	Slušanje	Predaja
1	61	0	1.000	1.012	0.061	0.162	0.397	0.024	0.644	0.662	0.045
2	60	0	1.000	1.110	0.070	0.161	0.456	0.051	0.738	0.760	0.095
3	44	16	2.136	8.634	0.163	0.159	0.557	0.737	1.615	0.928	1.387
4	60	0	1.000	1.131	0.080	0.161	0.493	0.112	0.846	0.822	0.211
5	60	0	1.000	1.808	0.113	0.160	0.606	0.245	1.125	1.011	0.462
6	51	9	2.000	7.767	0.143	0.159	0.530	0.539	1.371	0.883	1.015
7	44	14	2.068	9.290	0.167	0.158	0.574	0.757	1.657	0.956	1.426
8	47	12	2.021	7.947	0.159	0.159	0.579	0.650	1.547	0.965	1.224
9	40	15	3.000	7.628	0.145	0.159	0.551	0.564	1.419	0.919	1.062
Prosjek	**51.889**	**7.333**	**1.692**	**5.148**	**0.122**	**0.160**	**0.527**	**0.409**	**1.218**	**0.878**	**0.770**

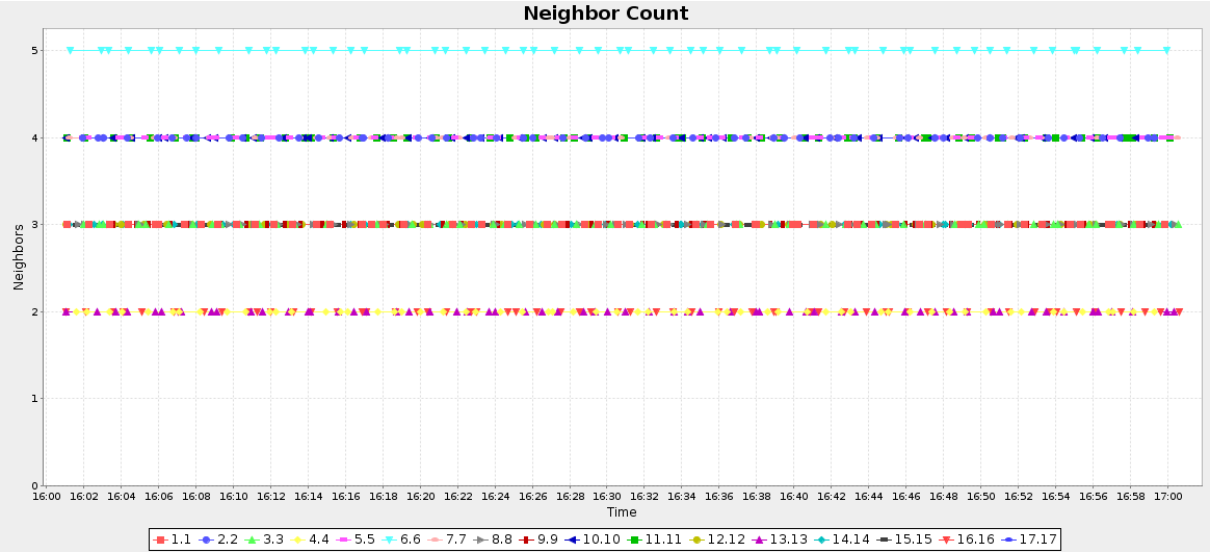
6.5.3. Mreža sa 17 čvorova

Treću analiziranu mrežu čini ukupno 17 čvorova (16 standardnih čvorova i bazna stanica). Topologija mreže prikazana je na slici 6.61. Čvorovi označeni brojevima 1-16 su standardni čvorovi, dok čvor 17 predstavlja baznu stanicu.



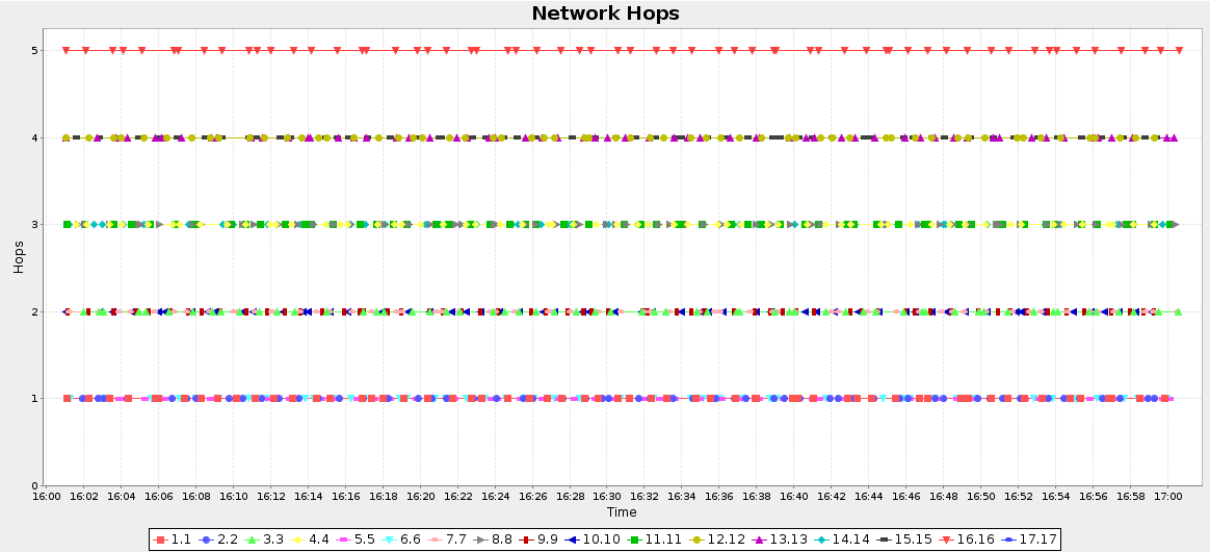
Slika 6.61 Topologija mreže sa 17 čvorova

Kao i u prethodnim slučajevima, i u mreži sa 17 čvorova analizirana su tri karakteristična scenarija koji se međusobno razlikuju po vjerojatnosti uspješnog slanja i prijema paketa. Analogno prethodnim analiziranim mrežama, i u mreži sa 17 čvorova u prvom scenariju ovaj omjer iznosi 100%, u drugom 80%, a u trećem 60%. Slika 6.62 prikazuje broj susjednih čvorova za svaki čvor u mreži.



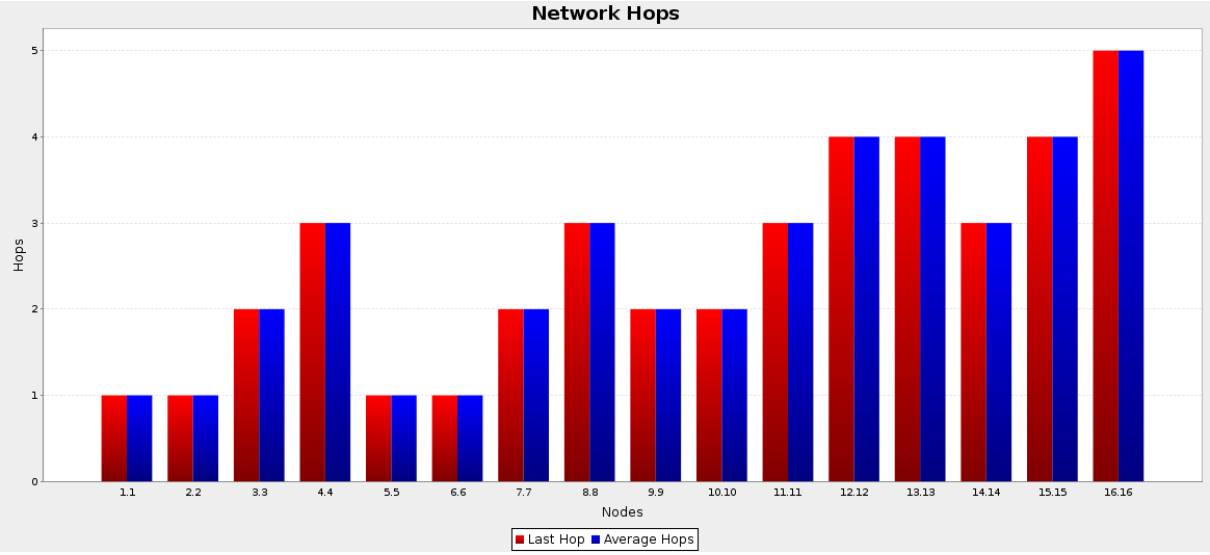
Slika 6.62 Broj susjednih čvorova u mreži sa 17 čvorova

Sa slike je vidljivo da čvorovi u mreži imaju od minimalno 2 do maksimalno 5 susjeda (čvorova koji su im u izravnom dometu). Slika 6.63 prikazuje broj skokova do bazne stanice u mreži sa 17 čvorova.



Slika 6.63 Broj skokova do bazne stanice u mreži sa 17 čvorova

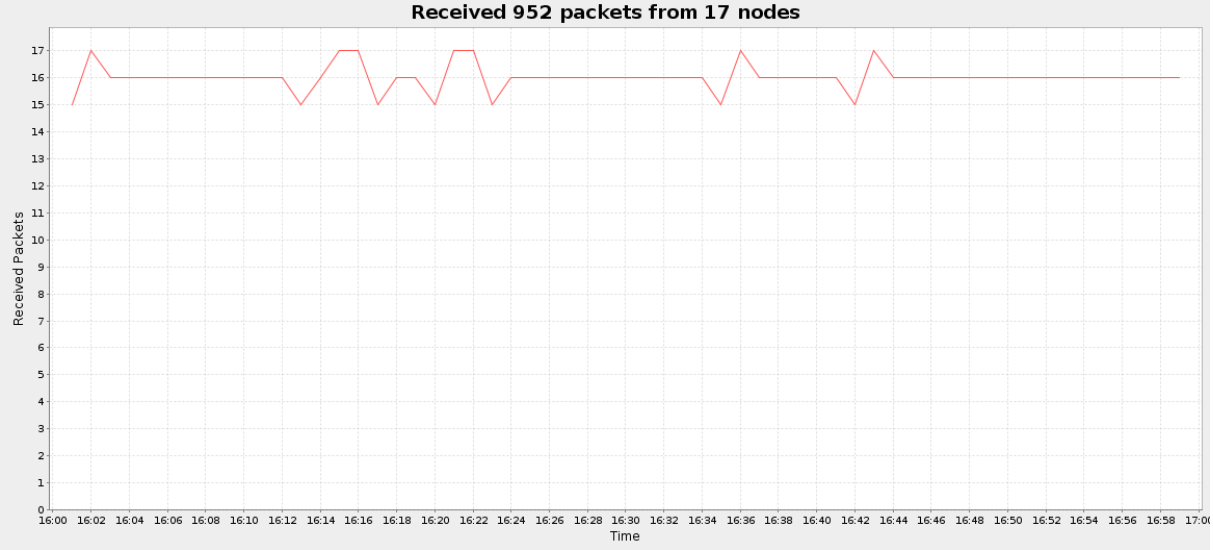
Sa slike je vidljivo da minimalan broj skokova do bazne stanice iznosi 1 (čvorovi 1, 2, 5 i 6 kojima je bazna stanica u izravnom dometu), a maksimalan 5 (za čvor 16, koji je najudaljeniji od bazne stanice). Slika 6.64 prikazuje broj skokova do bazne stanice za svaki pojedini čvor.



Slika 6.64 Broj skokova za pojedinačne čvorove u mreži sa 17 čvorova

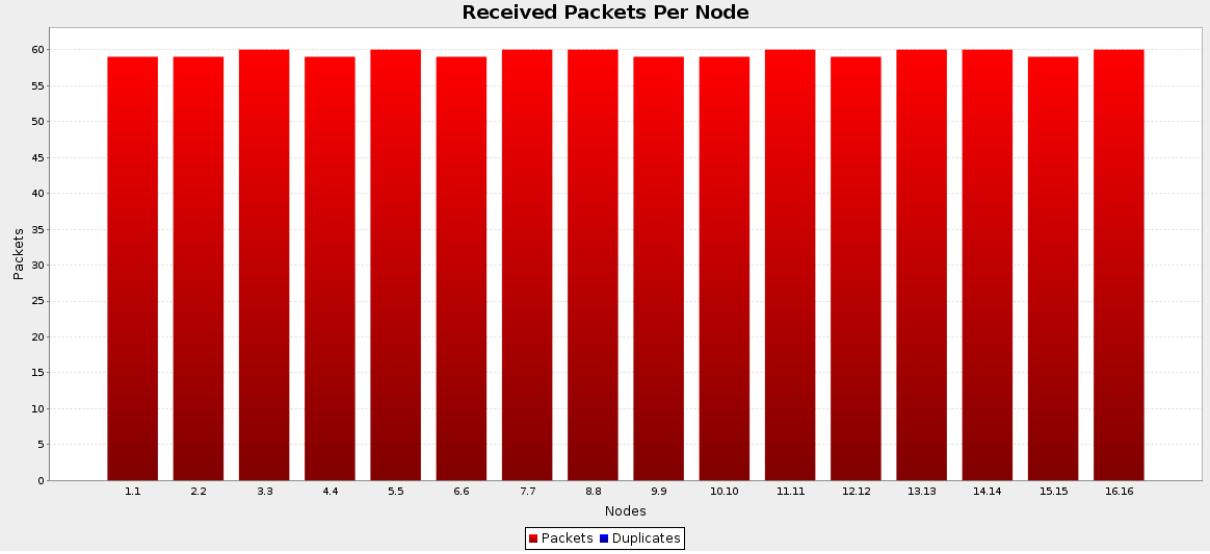
Scenarij 1 (Rx/Tx=100%)

Prvi simulirani scenarij u mreži sa 17 čvorova (analogno prethodnim razmatranjima mreža sa 6 i 9 čvorova) predstavlja „idealan slučaj“ u kojem vjerojatnost ispravnog slanja i prijema paketa iznosi 100%. Slika 6.65 prikazuje primljene pakete za ovaj scenarij tijekom jednog sata.



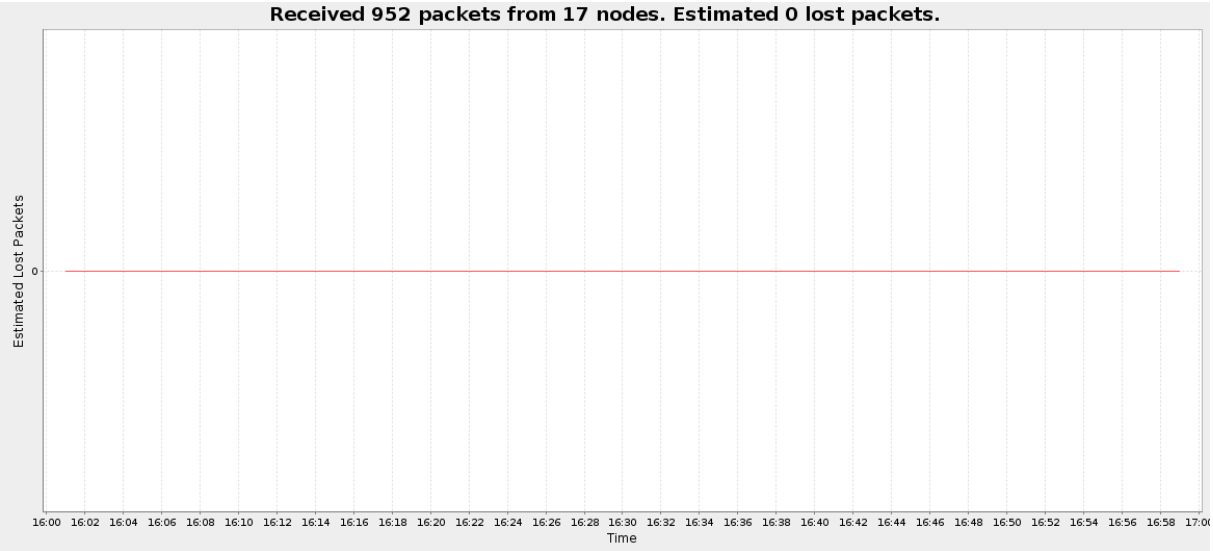
Slika 6.65 Broj primljenih paketa (17 čvorova, scenarij 1, bez IDS-a)

Na slici 6.66 prikazan je broj primljenih paketa za svaki pojedini mrežni čvor.



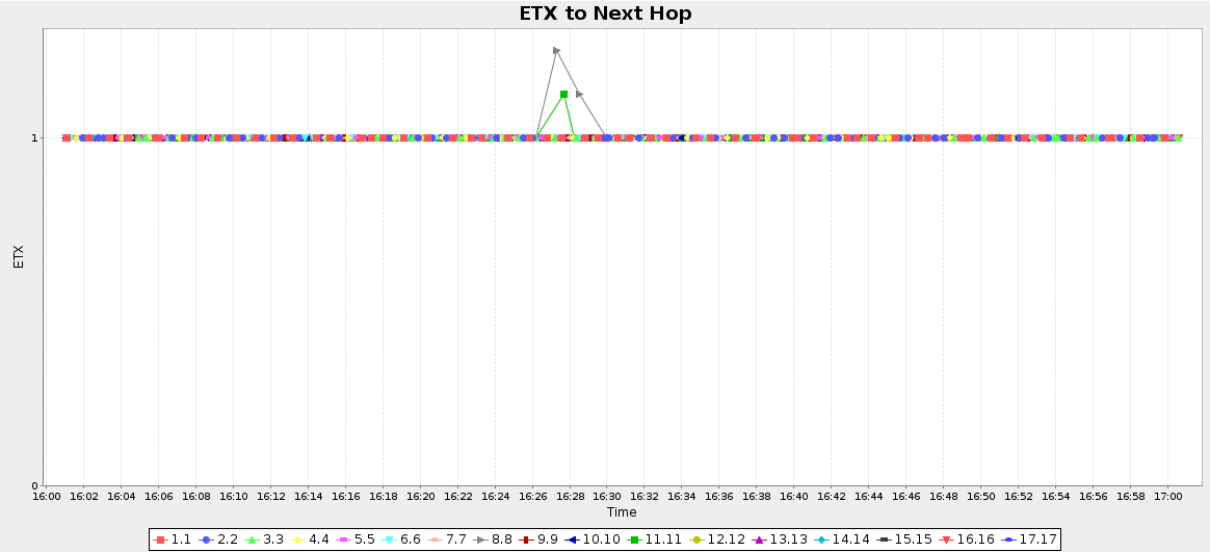
Slika 6.66 Broj primljenih paketa za svaki čvor (17 čvorova, scenarij 1, bez IDS-a)

Budući da se radi o „idealnom slučaju“ svi paketi stižu na svoje odredište i nema izgubljenih paketa (slika 6.67).



Slika 6.67 Izgubljeni paketi (17 čvorova, scenarij 1, bez IDS-a)

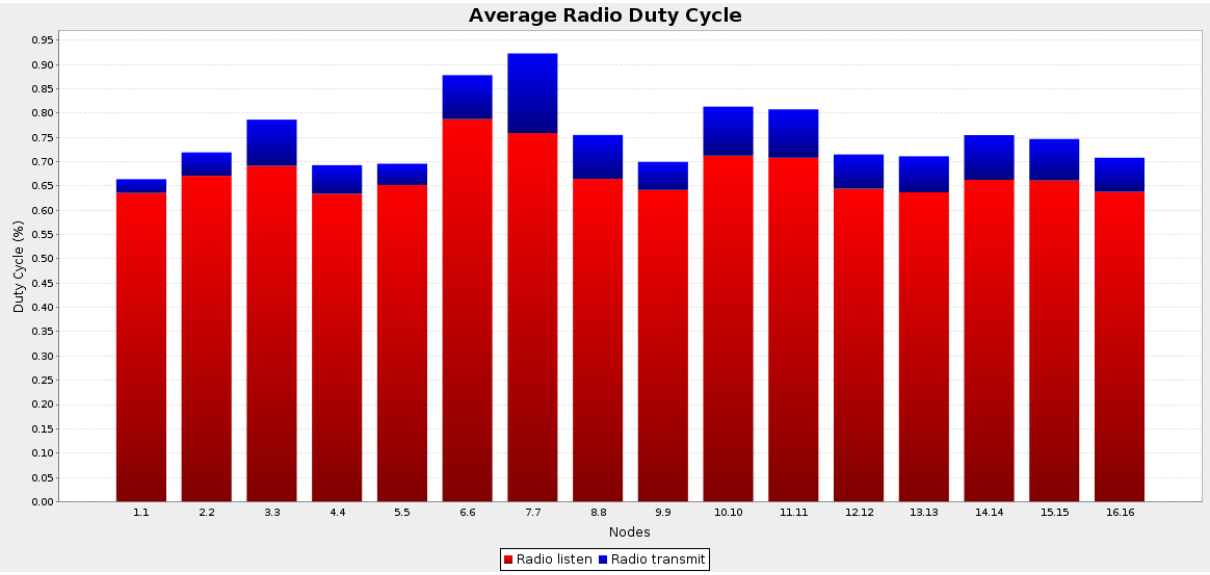
Na slici 6.68 prikazana je ETX metrika za prvi simulirani scenarij u mreži sa 17 čvorova.



Slika 6.68 ETX metrika (17 čvorova, scenarij 1, bez IDS-a)

ETX vrijednost 1 za pojedine linkove znači da na njima nije bilo potrebno vršiti retransmisiju, što je u skladu s očekivanim rezultatima za prvi scenarij.

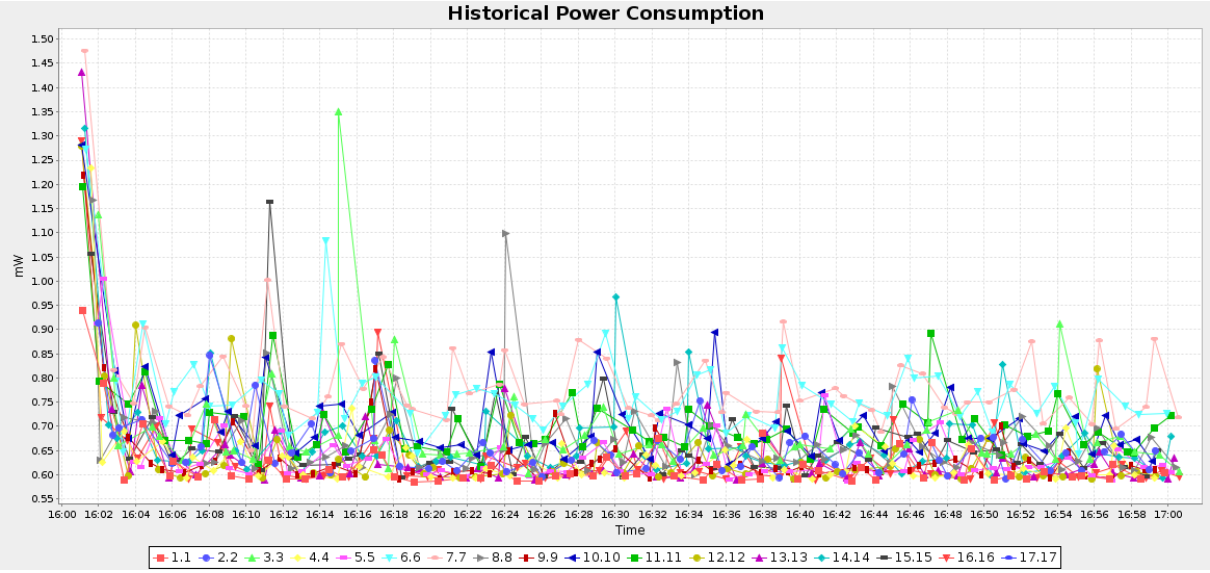
Na slici 6.69 prikazani su radni ciklusi primopredajnika za prvi simulirani scenarij mreže sa 17 čvorova.



Slika 6.69 Prosječni radni ciklus primopredajnika (17 čvorova, scenarij 1, bez IDS-a)

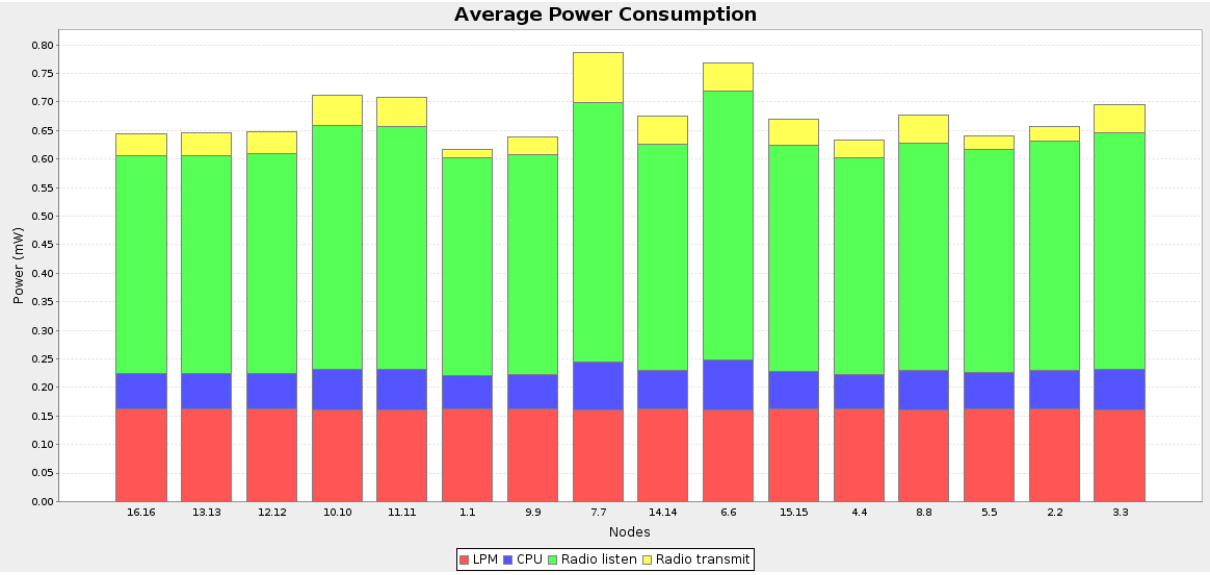
Sa slike se vidi da primopredajnici najveći dio vremena provode u stanju „slušanja“. Nešto veća aktivnost primopredajnika zabilježena je za središnje čvorove, preko kojih prolazi

veći broj ruta od perifernih čvorova ka baznoj stanici. Slika 6.70 prikazuje potrošnju energije u prvom scenariju mreže sa 17 čvorova u promatranom jednosatnom intervalu.



Slika 6.70 Potrošnja energije (17 čvorova, scenarij 1, bez IDS-a)

Na slici 6.71 prikazana je prosječna potrošnja energije za svaki pojedini mrežni čvor.



Slika 6.71 Prosječna potrošnja energije (17 čvorova, scenarij 1, bez IDS-a)

Sa slike je vidljivo da je nešto veća potrošnja energije zabilježena na središnjim čvorovima, i to prvenstveno zbog veće aktivnosti njihovog primopredajnika kao energetski najzahtjevnijeg dijela senzorskog čvora.

U tablici 6.7 su pregledno prikazani rezultati dobiveni simulacijom prvog scenarija u mreži sa 17 čvorova.

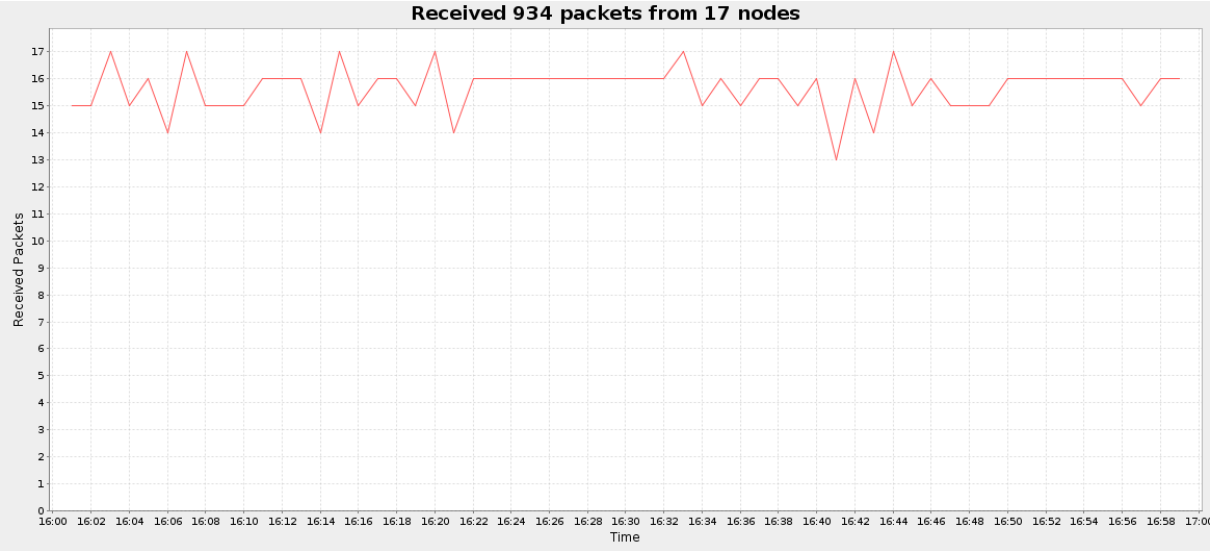
TABLICA 6.7 Mreža sa 17 čvorova, scenarij 1, bez IDS-a

Čvor	Primljeni paketi	Izgubljeni paketi	Skokovi do baze	ETX	Potrošnja energije (mW)					Radni ciklus (%)	
					CPU	LPM	Slušanje	Predaja	Ukupno	Slušanje	Predaja
1	59	0	1.000	1.000	0.060	0.162	0.381	0.015	0.618	0.636	0.028
2	59	0	1.000	1.000	0.068	0.161	0.402	0.026	0.657	0.671	0.048
3	60	0	2.000	1.000	0.070	0.161	0.415	0.050	0.696	0.691	0.095
4	59	0	3.000	1.000	0.061	0.162	0.380	0.031	0.634	0.634	0.059
5	60	0	1.000	1.000	0.064	0.162	0.391	0.023	0.640	0.652	0.044
6	59	0	1.000	1.000	0.087	0.161	0.472	0.048	0.768	0.787	0.091
7	60	0	2.000	1.000	0.083	0.161	0.455	0.087	0.787	0.759	0.164
8	60	0	3.000	1.006	0.069	0.161	0.399	0.048	0.677	0.664	0.091
9	59	0	2.000	1.000	0.062	0.162	0.385	0.031	0.639	0.642	0.058
10	59	0	2.000	1.000	0.070	0.161	0.427	0.054	0.713	0.712	0.101
11	60	0	3.000	1.002	0.070	0.161	0.425	0.053	0.709	0.708	0.099
12	59	0	4.000	1.000	0.062	0.162	0.387	0.037	0.647	0.644	0.070
13	60	0	4.000	1.000	0.063	0.162	0.382	0.039	0.646	0.637	0.074
14	60	0	3.000	1.000	0.068	0.161	0.397	0.049	0.676	0.662	0.092
15	59	0	4.000	1.000	0.067	0.161	0.397	0.045	0.670	0.661	0.085
16	60	0	5.000	1.000	0.062	0.162	0.383	0.037	0.644	0.638	0.070
Prosjek	**59.500**	**0.000**	**2.563**	**1.001**	**0.068**	**0.161**	**0.405**	**0.042**	**0.676**	**0.675**	**0.079**

Scenarij 2 (Rx/Tx=80%)

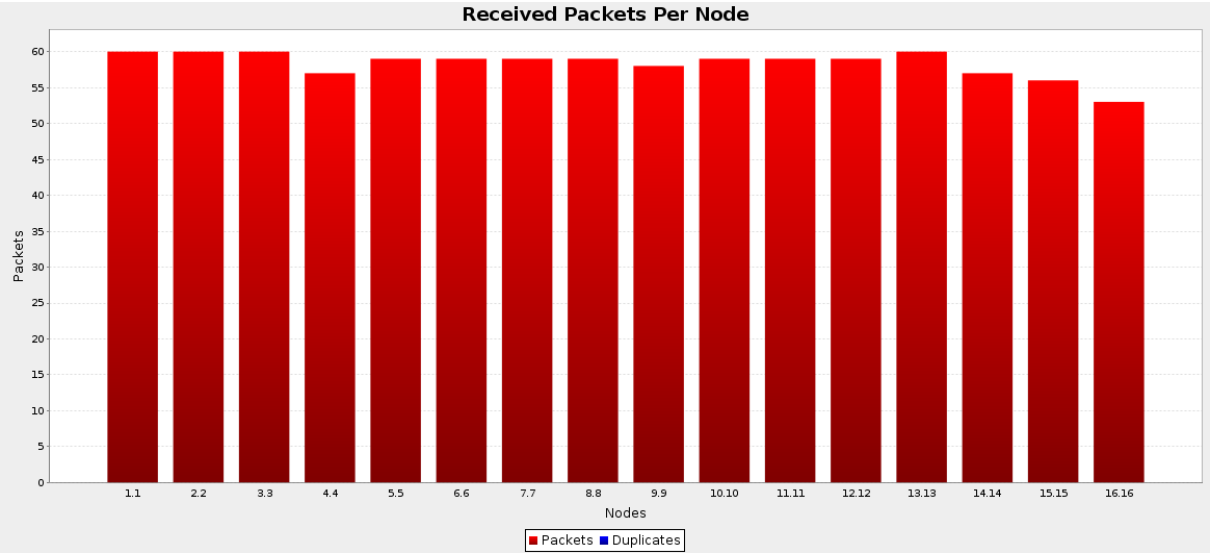
Drugi simulirani scenarij u mreži sa 17 čvorova predstavlja slučaj u kojemu je uspješnost slanja i prijema paketa postavljena na 80%. U pogledu topologije, broja skokova do bazne stanice i broja susjednih čvorova ovaj scenarij ne razlikuje se od prethodnog.

Slika 6.72 prikazuje primljeni promet u drugom simuliranom scenariju u mreži sa 17 čvorova tijekom jednog sata.



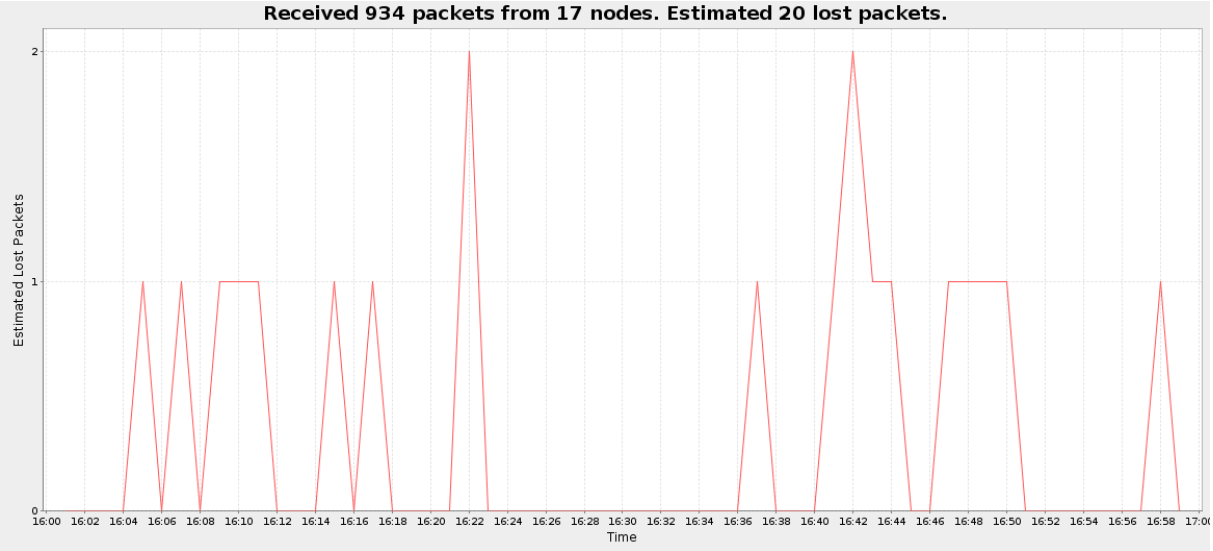
Slika 6.72 Broj primljenih paketa (17 čvorova, scenarij 2, bez IDS-a)

Na slici 6.73 prikazan je primljeni promet za svaki pojedini mrežni čvor.



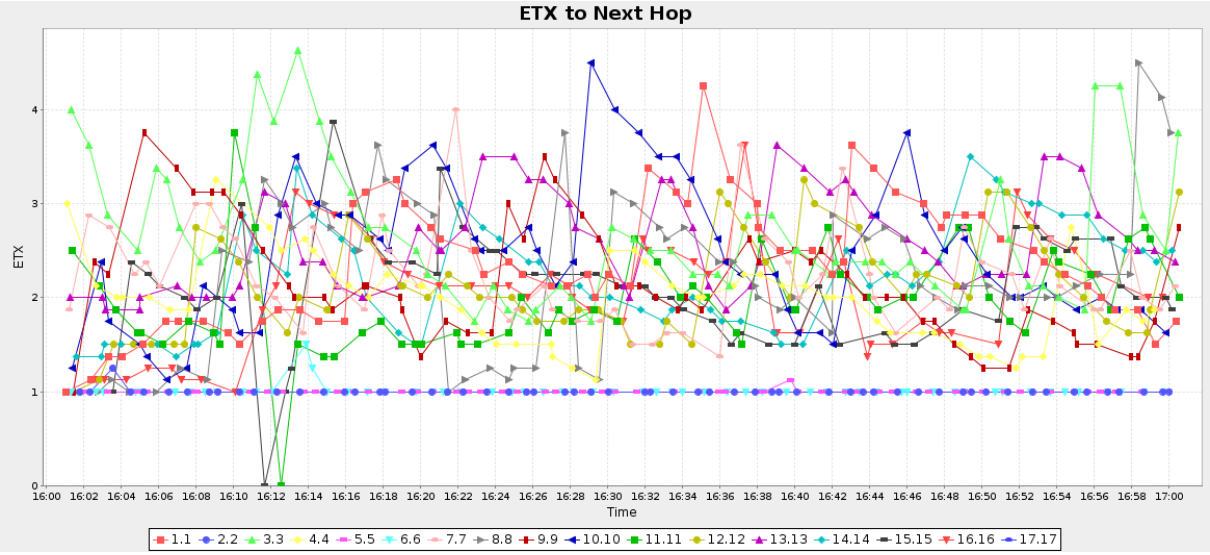
Slika 6.73 Broj primljenih paketa za svaki čvor (17 čvorova, scenarij 2, bez IDS-a)

Slika 6.74 prikazuje procijenjene gubitke paketa.



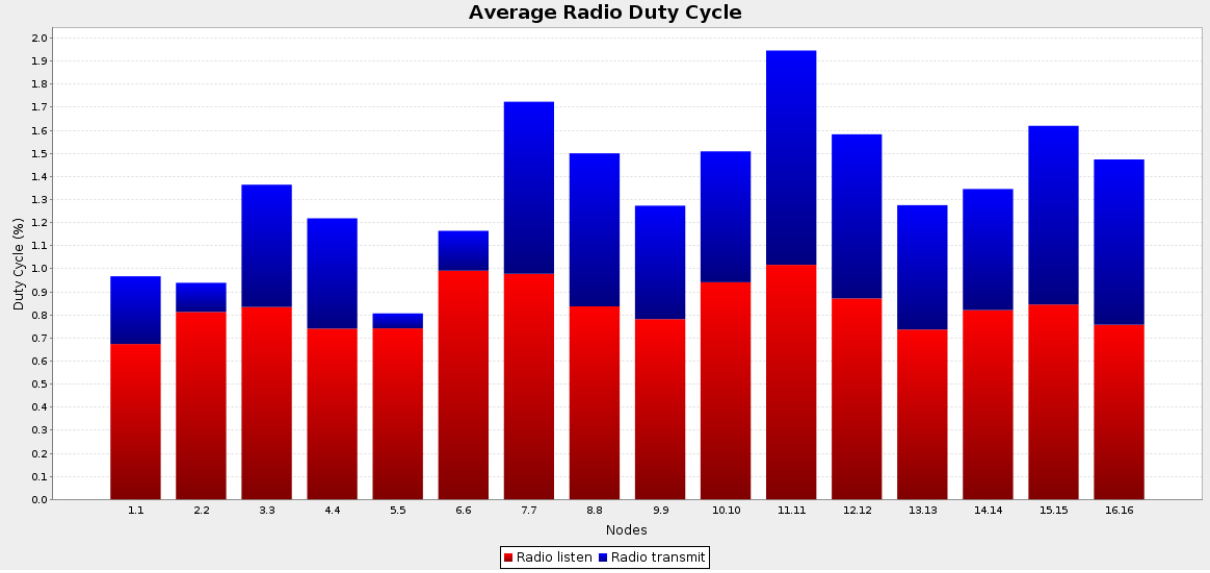
Slika 6.74 Izgubljeni paketi (17 čvorova, scenarij 2, bez IDS-a)

Sa slike je vidljivo da je u drugom scenariju određeni broj paketa ipak izgubljen, unatoč mehanizmima potvrde i retransmisije. Međutim, potreba za retransmisijom određenog broja paketa (zbog gubitaka) odražava se na ETX metriku za pojedine čvorove, te radne cikluse njihovih primopredajnika, a time utječe i na potrošnju energije. Slika 6.75 prikazuje ETX metriku za ovaj scenarij.



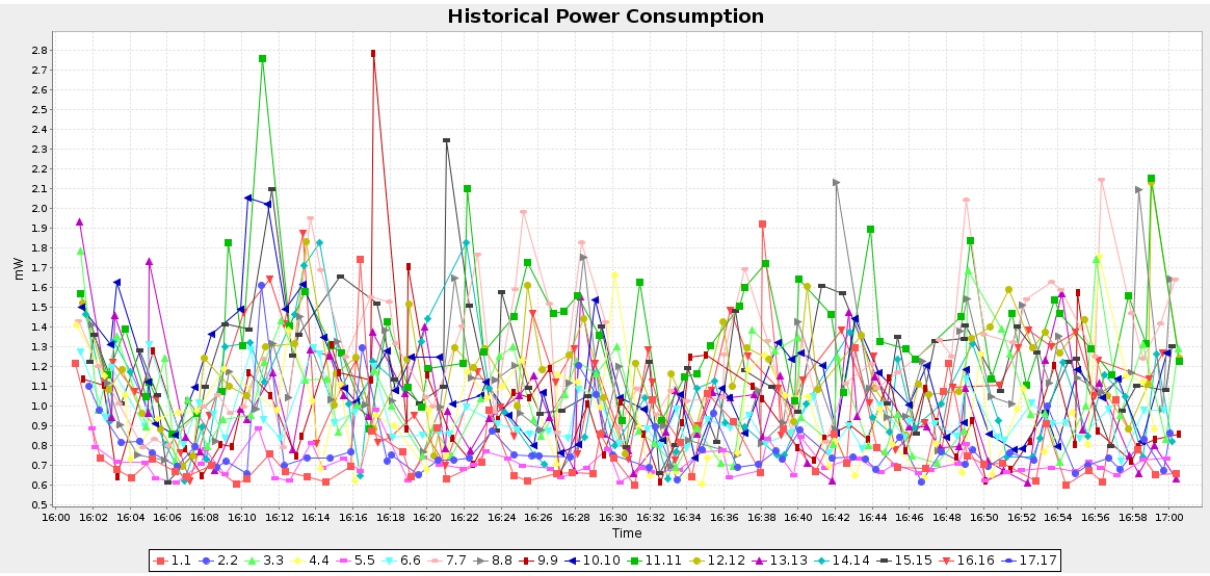
Slika 6.75 ETX metrika (17 čvorova, scenarij 2, bez IDS-a)

Sa slike je vidljivo da se ETX vrijednost povećala za sve čvorove koji nisu u susjedstvu bazne stanice, što znači da je potrebno više pokušaja za uspješno slanje jednog paketa. Na slici 6.76 prikazani su radni ciklusi primopredajnika za sve čvorove u mreži.



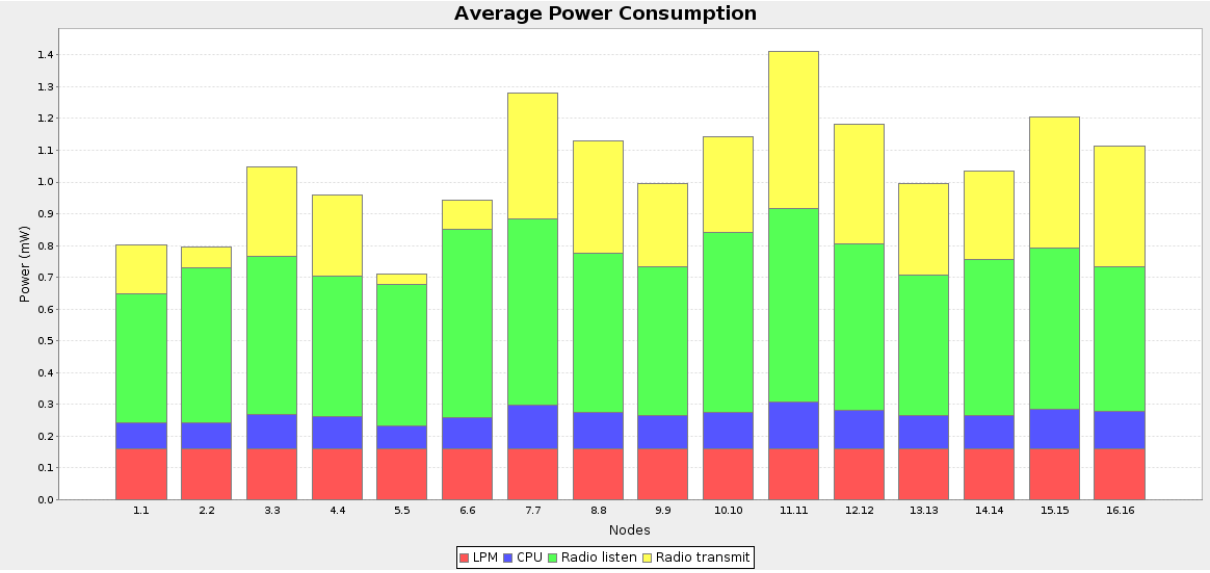
Slika 6.76 Prosječni radni ciklus primopredajnika (17 čvorova, scenarij 2, bez IDS-a)

Na slici je vidljiva povećana aktivnost predajnika na čvorovima udaljenijim od bazne stanice, zbog veće potrebe za retransmisijom izgubljenih paketa. Na slici 6.77 prikazana je potrošnja energije u promatranom intervalu od jednog sata za scenarij 2.



Slika 6.77 Potrošnja energije (17 čvorova, scenarij 2, bez IDS-a)

Na slici 6.78 prikazana je prosječna potrošnja energije za svaki pojedini čvor drugog simuliranog scenarija mreže sa 17 čvorova.



Slika 6.78 Prosječna potrošnja energije (17 čvorova, scenarij 2, bez IDS-a)

Na slici 6.78 je vidljivo povećanje u potrošnji energije u odnosu na prvi scenarij (slika 6.71). Ovo povećanje posebno je izraženo kod čvorova koji su udaljeniji od bazne stanice (zbog povećanog broja potrebnih retransmisija) i kod središnjih čvorova (zbog većeg broja ruta koje preko ovih čvorova povezuju periferne čvorove sa baznom stanicom). Ukupno povećanje potrošnje u najvećoj mjeri proizlazi iz povećanja potrošnje predajnika.

U tablici 6.8 su pregledno prikazani rezultati dobiveni simulacijom drugog scenarija u mreži sa 17 čvorova.

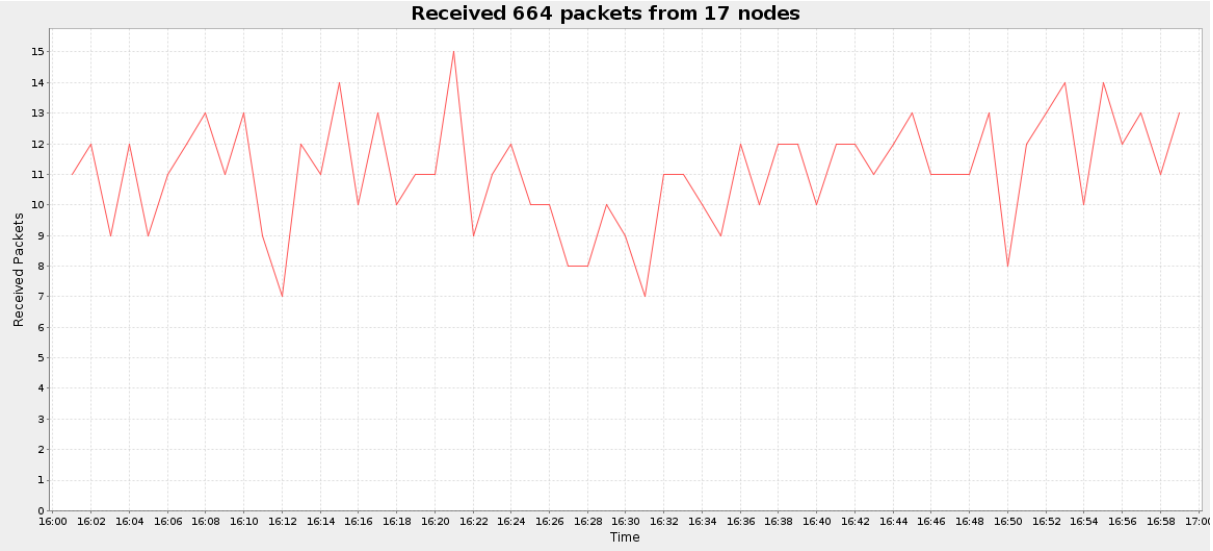
TABLICA 6.8 Mreža sa 17 čvorova, scenarij 2, bez IDS-a

Čvor	Primljeni paketi	Izgubljeni paketi	Skokovi do baze	ETX	Potrošnja energije (mW)					Radni ciklus (%)	
					CPU	LPM	Slušanje	Predaja	Ukupno	Slušanje	Predaja
1	60	0	2.000	2.358	0.082	0.161	0.404	0.156	0.803	0.674	0.294
2	60	0	1.000	1.004	0.081	0.161	0.488	0.067	0.797	0.813	0.126
3	60	0	2.000	2.679	0.106	0.160	0.501	0.282	1.049	0.834	0.530
4	57	2	3.018	1.969	0.100	0.160	0.445	0.254	0.959	0.741	0.478
5	59	0	1.000	1.002	0.071	0.161	0.445	0.035	0.712	0.742	0.065
6	59	0	1.000	1.013	0.097	0.161	0.595	0.092	0.944	0.992	0.173
7	59	1	2.000	2.214	0.138	0.159	0.587	0.396	1.280	0.979	0.745
8	59	1	3.136	2.242	0.115	0.160	0.502	0.352	1.129	0.837	0.663
9	58	2	2.000	2.153	0.105	0.160	0.469	0.261	0.996	0.782	0.492
10	59	0	2.000	2.441	0.115	0.160	0.565	0.301	1.142	0.942	0.567
11	59	1	3.000	1.953	0.149	0.159	0.610	0.493	1.411	1.017	0.928
12	59	1	4.000	2.119	0.122	0.160	0.523	0.377	1.182	0.872	0.711
13	60	0	3.167	2.575	0.105	0.160	0.442	0.286	0.994	0.737	0.539
14	57	3	3.000	2.202	0.104	0.160	0.493	0.279	1.036	0.821	0.525
15	56	4	4.000	2.036	0.126	0.160	0.507	0.411	1.204	0.845	0.774
16	53	5	5.000	2.057	0.118	0.160	0.455	0.380	1.113	0.758	0.716
Prosjek	**58.375**	**1.250**	**2.582**	**2.001**	**0.108**	**0.160**	**0.502**	**0.276**	**1.047**	**0.837**	**0.520**

Scenarij 3 (Rx/Tx=60%)

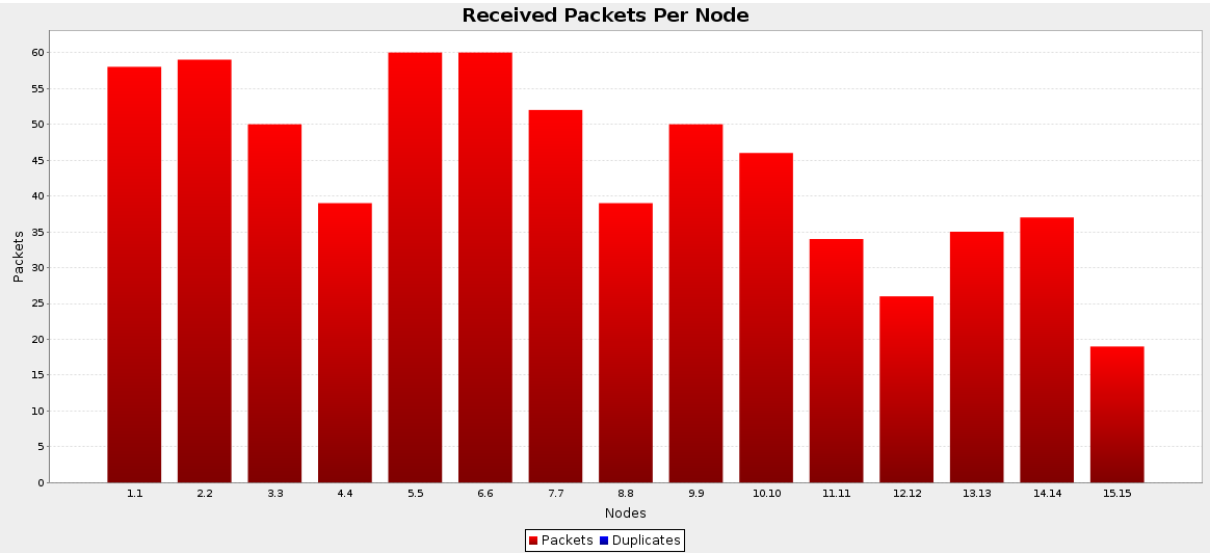
Treći simulirani scenarij u mreži sa 17 čvorova (analogno prethodno analiziranim mrežama) predstavlja scenarij u kojem je vjerojatnost uspješnog prijema i slanja paketa 60%. Po ostalim inicijalnim parametrima ovaj scenarij ne razlikuje se od prethodna dva.

Na slici 6.79 prikazani su primljeni paketi u mreži sa 17 čvorova tijekom promatranog intervala od jednog sata.



Slika 6.79 Broj primljenih paketa (17 čvorova, scenarij 3, bez IDS-a)

Slika 6.80 prikazuje primljeni promet za svaki pojedini čvor u mreži.

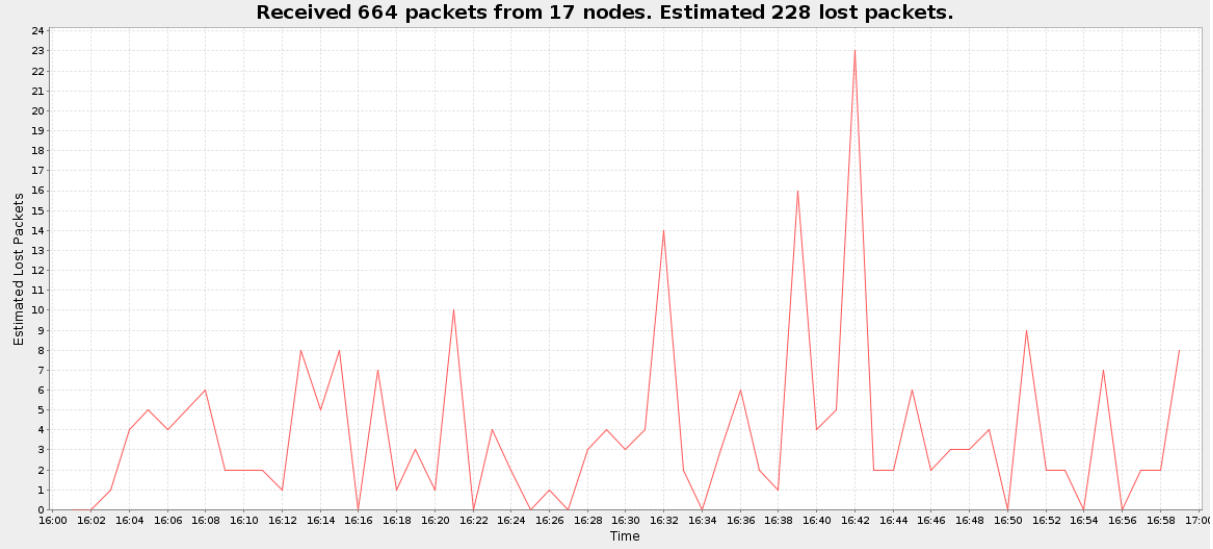


Slika 6.80 Broj primljenih paketa za svaki čvor (17 čvorova, scenarij 3, bez IDS-a)

Sa slike je vidljivo da je broj paketa primljenih od pojedinih čvorova značajno manji nego u prethodnim scenarijima, posebno za čvorove koji su udaljeniji više skokova od bazne stanice. To dovodi do zaključka da su u ovom scenariju gubici paketa značajno izraženi. U

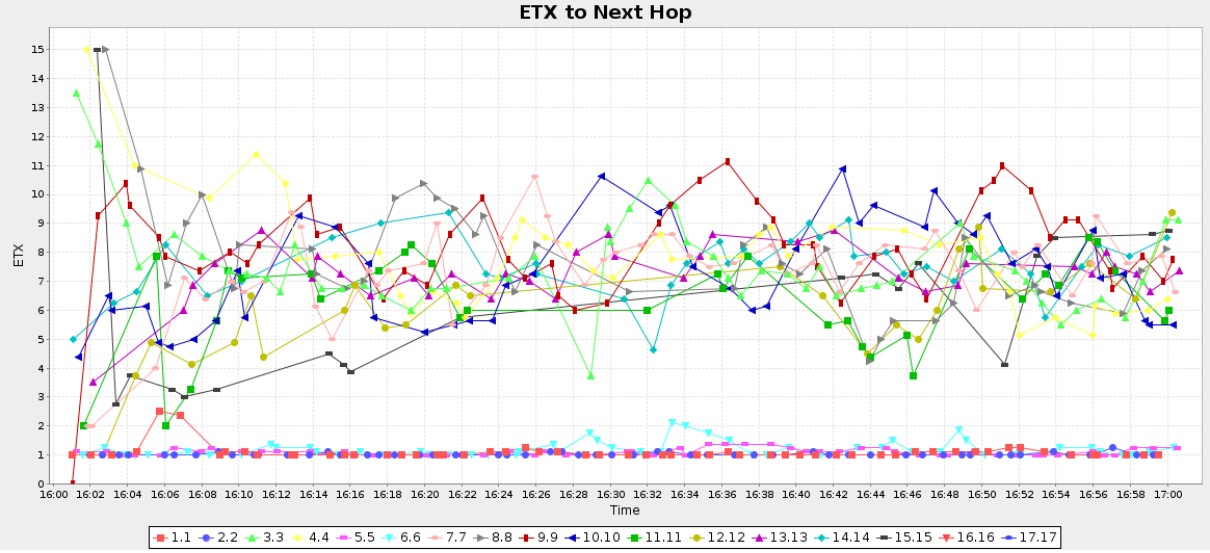
ovom slučaju čak nije bilo moguće uspostaviti normalnu komunikaciju sa najudaljenijim čvorom (čvor 16) zbog prevelikih gubitaka, te je on naprosto „ispao“ iz mreže.

Slika 6.81 prikazuje procjenu gubitaka paketa u mreži.



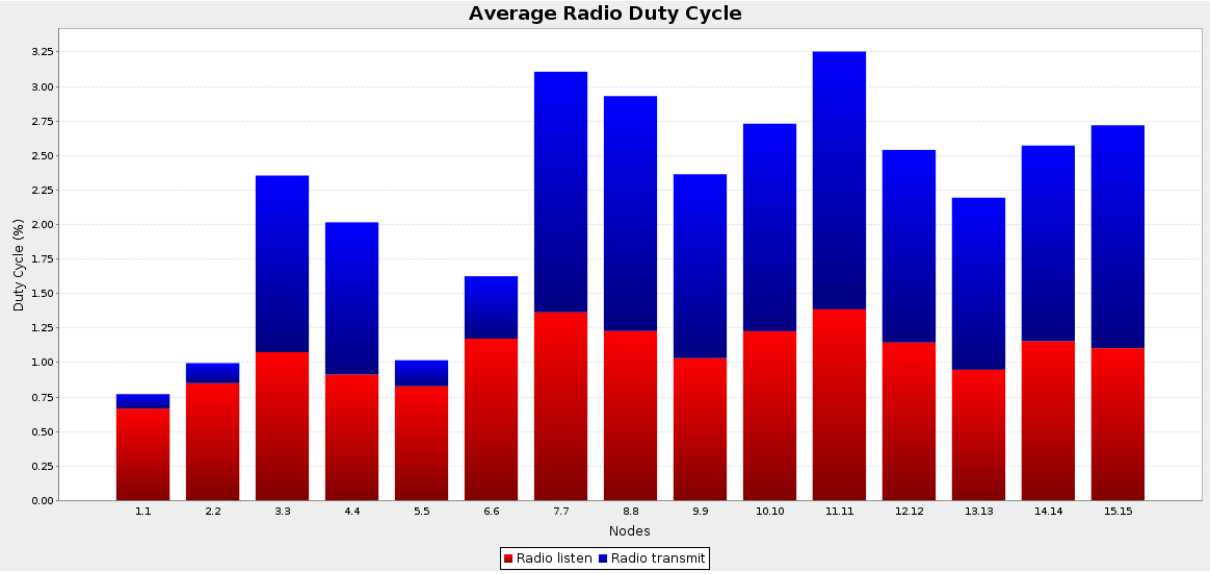
Slika 6.81 Izgubljeni paketi (17 čvorova, scenarij 3, bez IDS-a)

Povećani gubici paketa odražavaju se i na povećanje ETX vrijednosti za pojedine linkove, što je vidljivo na slici 6.82.



Slika 6.82 ETX metrika (17 čvorova, scenarij 3, bez IDS-a)

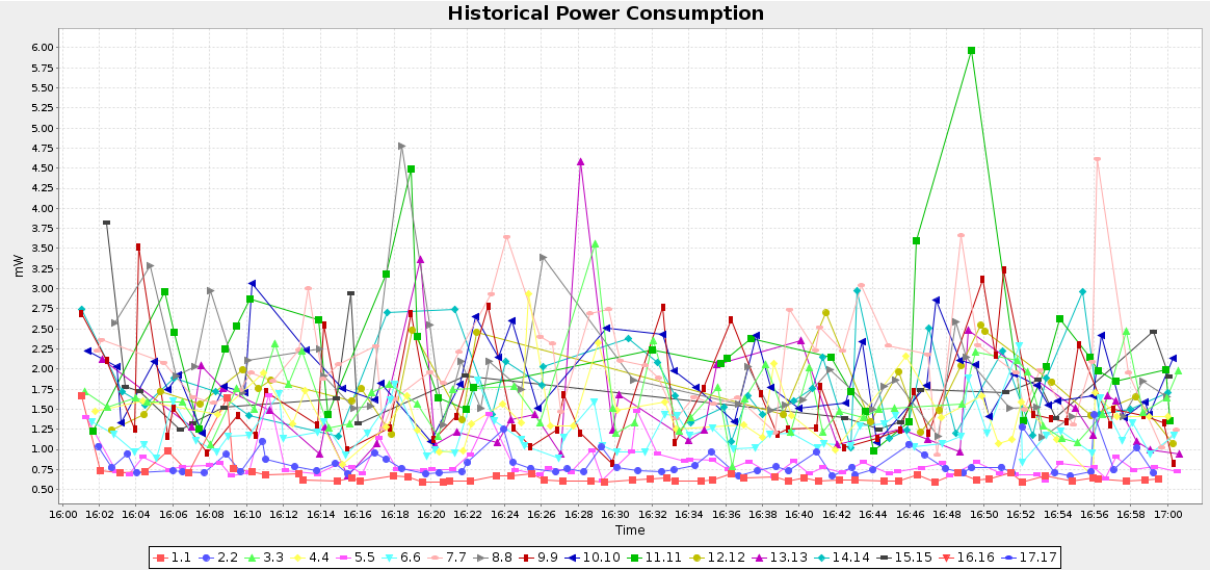
Sa slike je vidljivo dodatno povećanje broja potrebnih retransmisija za uspješno slanje paketa na pojedinim linkovima, što će se značajno odraziti na radni ciklus primopredajnika i potrošnju energije. Slika 6.83 prikazuje radne cikluse primopredajnika pojedinih čvorova u scenariju 3 mreže sa 17 čvorova.



Slika 6.83 Prosječni radni ciklus primopredajnika (17 čvorova, scenarij 3, bez IDS-a)

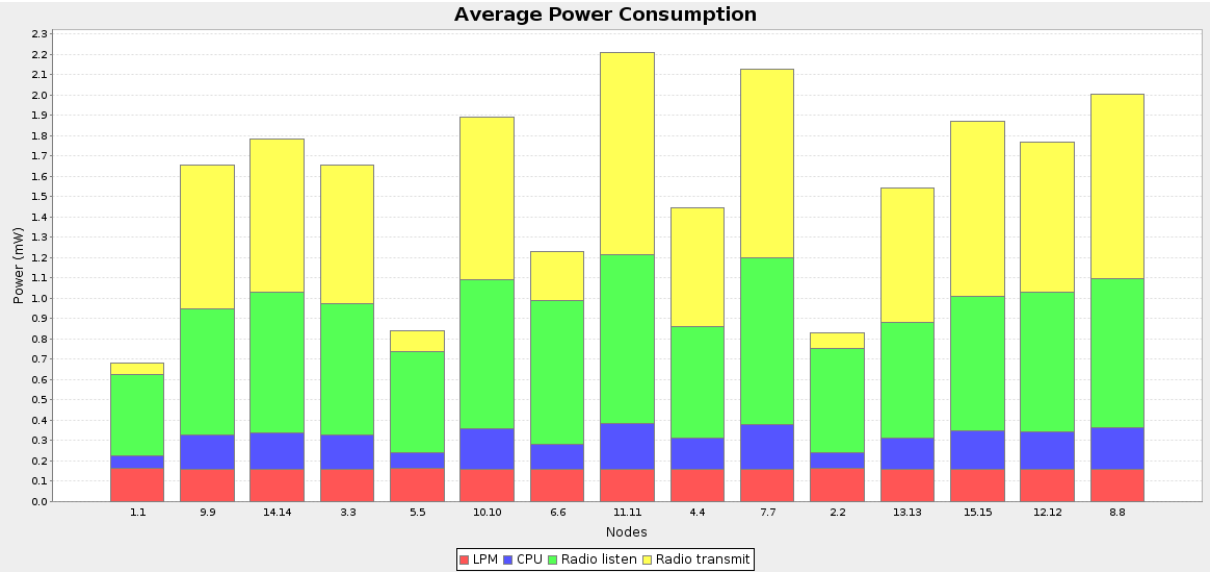
Na slici se može primijetiti značajni porast udjela aktivne predaje u ukupnom radnom ciklusu pojedinih primopredajnika, posebno na udaljenijim čvorovima. Na ovoj slici je također vidljivo da zbog prevelikih gubitaka najudaljeniji čvor (čvor 16) čak niti ne uspijeva ostvariti komunikaciju sa baznom stanicom.

Na slici 6.84 prikazana je potrošnja energije u mreži kroz promatranih sat vremena.



Slika 6.84 Potrošnja energije (17 čvorova, scenarij 3, bez IDS-a)

Slika 6.85 prikazuje prosječnu potrošnju energije za svaki pojedini čvor.



Slika 6.85 Prosječna potrošnja energije (17 čvorova, scenarij 3, bez IDS-a)

Na slici je vidljivo značajno povećanje potrošnje energije po apsolutnom iznosu, kao i značajno povećanje udjela potrošnje predajnika u ukupnoj potrošnji senzorskih čvorova.

U tablici 6.9 su prikazani rezultati dobiveni simulacijom trećeg scenarija u mreži sa 17 čvorova.

TABLICA 6.9 Mreža sa 17 čvorova, scenarij 3, bez IDS-a

Čvor	Primljeni paketi	Izgubljeni paketi	Skokovi do baze	ETX	Potrošnja energije (mW)					Radni ciklus (%)	
					CPU	LPM	Slušanje	Predaja	Ukupno	Slušanje	Predaja
1	58	1	1.103	1.093	0.065	0.162	0.400	0.056	0.683	0.667	0.105
2	59	0	1.000	1.021	0.080	0.161	0.510	0.077	0.829	0.850	0.145
3	50	10	2.020	7.582	0.169	0.158	0.645	0.680	1.653	1.075	1.280
4	39	21	3.000	7.859	0.151	0.159	0.548	0.586	1.444	0.913	1.103
5	60	0	1.000	1.102	0.081	0.161	0.497	0.100	0.839	0.828	0.189
6	60	0	1.000	1.190	0.123	0.160	0.704	0.240	1.227	1.174	0.452
7	52	8	2.077	7.373	0.223	0.157	0.818	0.926	2.124	1.364	1.744
8	39	19	3.103	7.811	0.205	0.157	0.737	0.904	2.003	1.228	1.703
9	50	10	2.020	8.178	0.168	0.158	0.619	0.708	1.653	1.032	1.333
10	46	14	2.043	7.239	0.198	0.157	0.737	0.798	1.891	1.228	1.504
11	34	26	3.000	6.276	0.228	0.157	0.831	0.992	2.208	1.386	1.868
12	26	33	4.077	5.976	0.184	0.158	0.687	0.741	1.770	1.145	1.396
13	35	24	3.000	7.268	0.154	0.159	0.569	0.662	1.543	0.948	1.246
14	37	22	3.054	7.537	0.179	0.158	0.693	0.753	1.783	1.155	1.418
15	19	40	4.000	6.099	0.191	0.158	0.663	0.858	1.869	1.105	1.615
16	0	0	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000
Prosjek	**44.267**	**15.200**	**2.366**	**5.574**	**0.160**	**0.159**	**0.644**	**0.605**	**1.568**	**1.073**	**1.140**

6.6. Rezultati testiranja performansi distribuiranog adaptivnog sustava

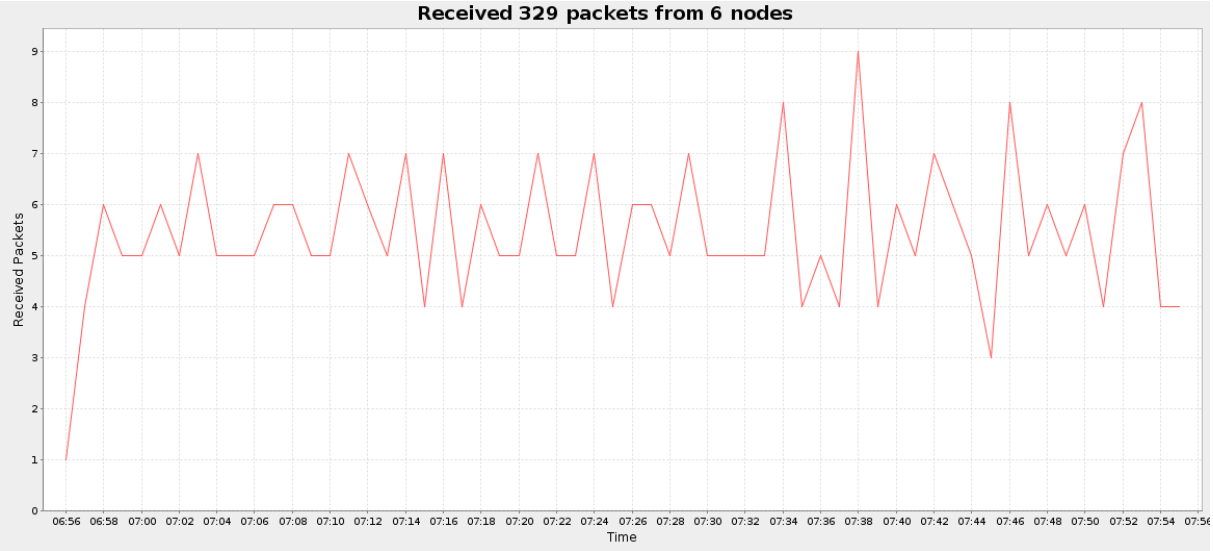
Distribuirani adaptivni sustav za otkrivanje zlonamjernog ponašanja senzorskih čvorova u IPv6-temeljenoj BSM implementiran je u tri različite IPv6-temeljene BSM (mreža sa 6 čvorova, mreža sa 10 čvorova i mreža sa 17 čvorova) za potrebe testiranja njegovog rada i ponašanja u „normalnom“ mrežnom okruženju, kao i analize njegovog utjecaja na normalan rad mreže i potrošnju njezinih resursa. U svakoj od ovih mreža simulirana su tri različita scenarija kakvi se mogu susresti u realnim senzorskim mrežama. Detaljan opis okruženja i scenarija u koje je sustav implementiran dan je u poglavlju 6.5.

6.6.1. IDS sustav implementiran u mrežu sa 6 čvorova

Predloženi IDS sustav najprije je implementiran u mrežu sa 6 čvorova, gdje je provedena analiza njegovog ponašanja u tri različita scenarija (koji su detaljno opisani u poglavlju 6.5.1.). Topologija mreže u potpunosti odgovara slici 6.11. Na svakom mrežnom čvoru implementiran je i izvršava se IDS agent, opisan u poglavlju 6.4. Budući da je topologija ostala nepromijenjena, u pogledu broja susjednih čvorova (slika 6.12) i potrebnog broja skokova do bazne stanice za pojedine čvorove (slika 6.13 i slika 6.14) nema nikakve razlike u odnosu na funkcionalnu IPv6-temeljenu BSM bez implementiranog IDS sustava.

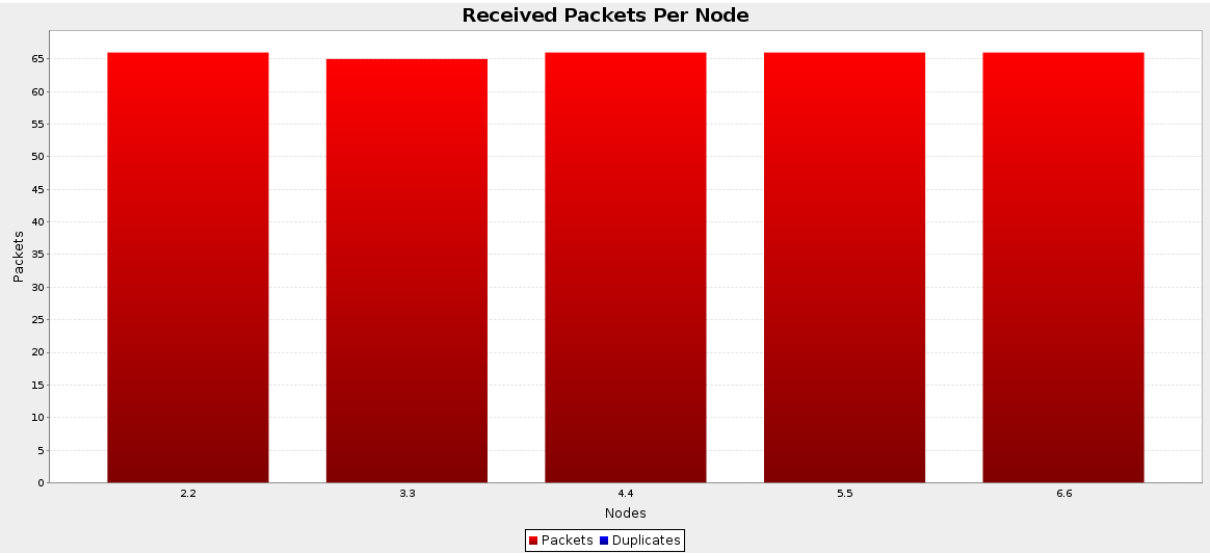
Scenarij 1 (Rx/Tx=100%)

Prvi simulirani scenarij predstavlja idealan slučaj u kojem je pretpostavka da nema gubitaka paketa prilikom prijenosa (vjerojatnost prijema i slanja paketa iznosi 100%). Na slici 6.86 prikazano je kretanje broja primljenih paketa kroz promatrano vremensko razdoblje od jednog sata.



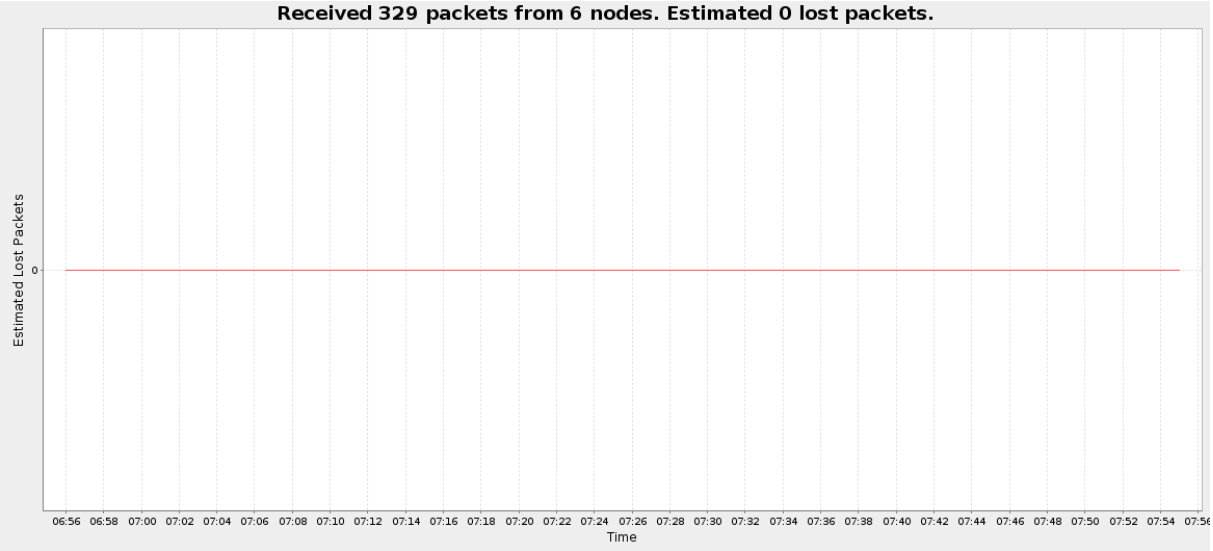
Slika 6.86 Broj primljenih paketa (6 čvorova, scenarij 1, sa IDS-om)

Na slici 6.87 prikazan je broj primljenih paketa za svaki čvor pojedinačno.



Slika 6.87 Broj primljenih paketa za svaki čvor (6 čvorova, scenarij 1, sa IDS-om)

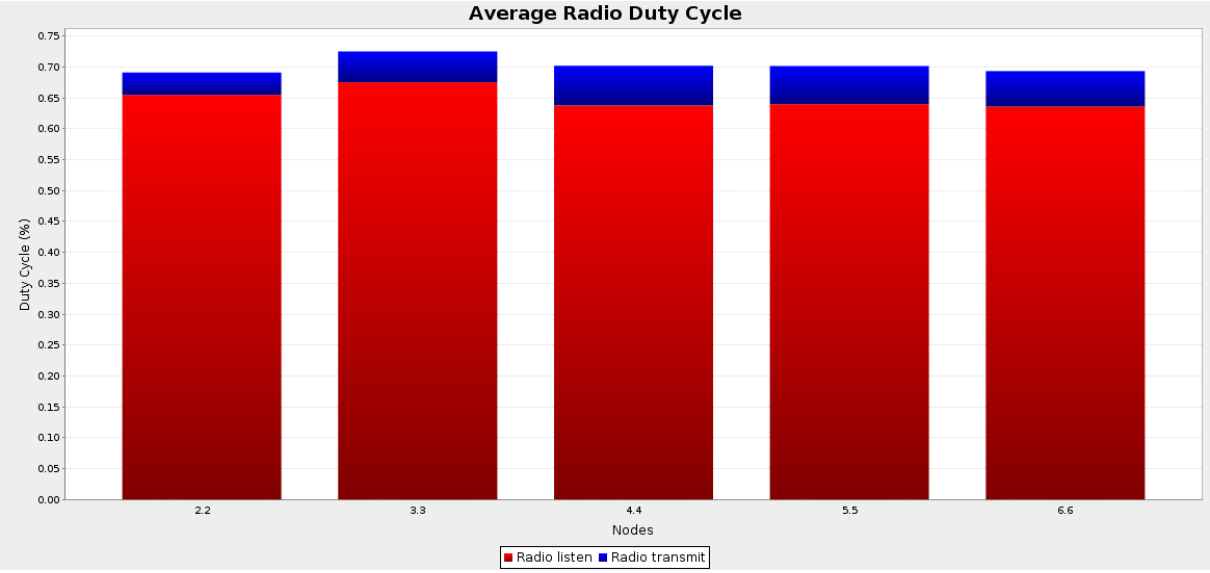
Budući da promatrani scenarij predstavlja „idealan slučaj“ u njemu nema izgubljenih paketa, što je vidljivo sa slike 6.88.



Slika 6.88 Izgubljeni paketi (6 čvorova, scenarij 1, sa IDS-om)

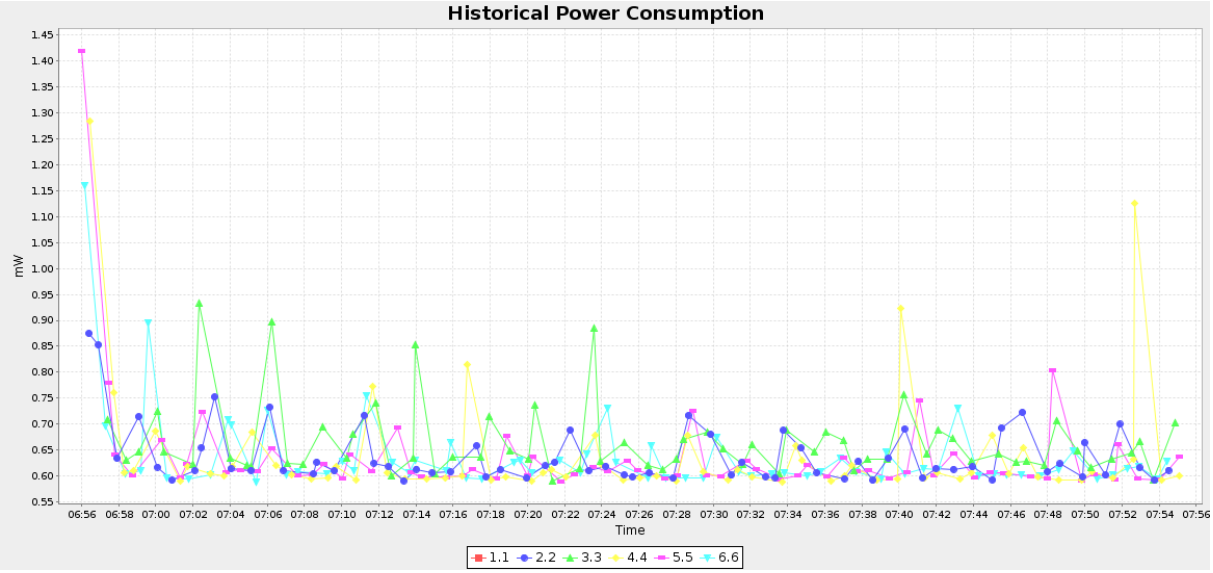
Usporedbom primljenog prometa u slučaju kada je u mrežu implementiran IDS sustav (slike 6.86 i 6.87) i mreže bez IDS sustava (slike 6.15 i 6.16) vidljiv je povećan broj primljenih paketa za svaki pojedinačni čvor. Ovo je u skladu s očekivanjima, budući da IDS agenti međusobno komuniciraju i razmjenjuju poruke, što se u konačnici očituje kao povećanje prometa u mreži. U pogledu ETX vrijednosti za pojedine linkove u mreži nema razlike u odnosu na „normalnu“ mrežu, budući da ona ovisi o očekivanom broju transmisija potrebnih za uspješan prijenos paketa, a ne o količini prometa u mreži.

Zanimljivo je promotriti kako se implementacija IDS agenata odražava na potrošnju energije u usporedbi sa „normalnom“ mrežom (mrežom bez implementiranog IDS sustava). Slika 6.89 prikazuje prosječni radni ciklus za svaki pojedini mrežni čvor.



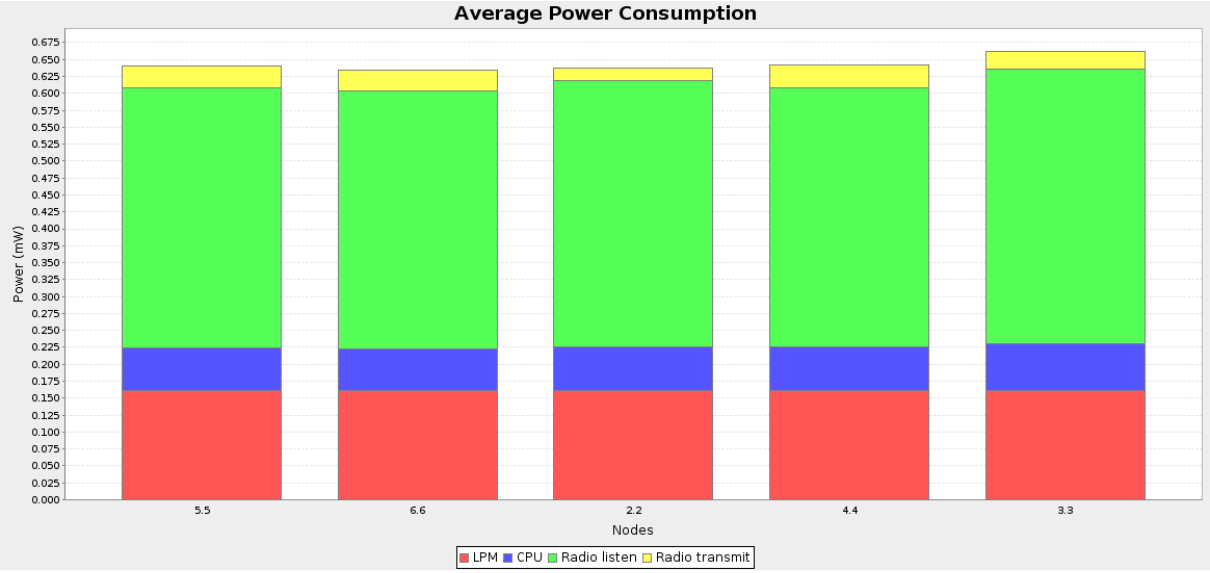
Slika 6.89 Prosječni radni ciklus primopredajnika (6 čvorova, scenarij 1, sa IDS-om)

Slika 6.90 prikazuje vremenski tijek potrošnje energije kroz promatrani interval od sat vremena.



Slika 6.90 Potrošnja energije (6 čvorova, scenarij 1, sa IDS-om)

Na slici 6.91 prikazana je prosječna potrošnja energije za svaki pojedini mrežni čvor u mreži sa 6 čvorova i implementiranim IDS sustavom.



Slika 6.91 Prosječna potrošnja energije (6 čvorova, scenarij 1, sa IDS-om)

Ukoliko se dobiveni rezultati usporede sa istim scenarijem u mreži bez IDS sustava (slike 6.20 i 6.21) vidljivo je da nema značajne razlike u potrošnji energije, što je od velikog značaja budući da su energetski resursi senzorske mreže strogo ograničeni i najčešće nije prihvatljivo u njih implementirati mehanizme koji bi potrošnju energije značajnije povećali. Također, u usporedbi sa „normalnom“ mrežom vidljivo je da niti nakon implementacije IDS sustava nema promjene u pogledu raspodjele potrošnje energije na primopredajnik, CPU i niskoenergetski način rada (i u ovom slučaju najveći dio energije potroši radio primopredajnik).

U tablici 6.10 su pregledno prikazane dobivene vrijednosti za prvi simulirani scenarij u mreži sa 6 čvorova uz implementirani IDS sustav.

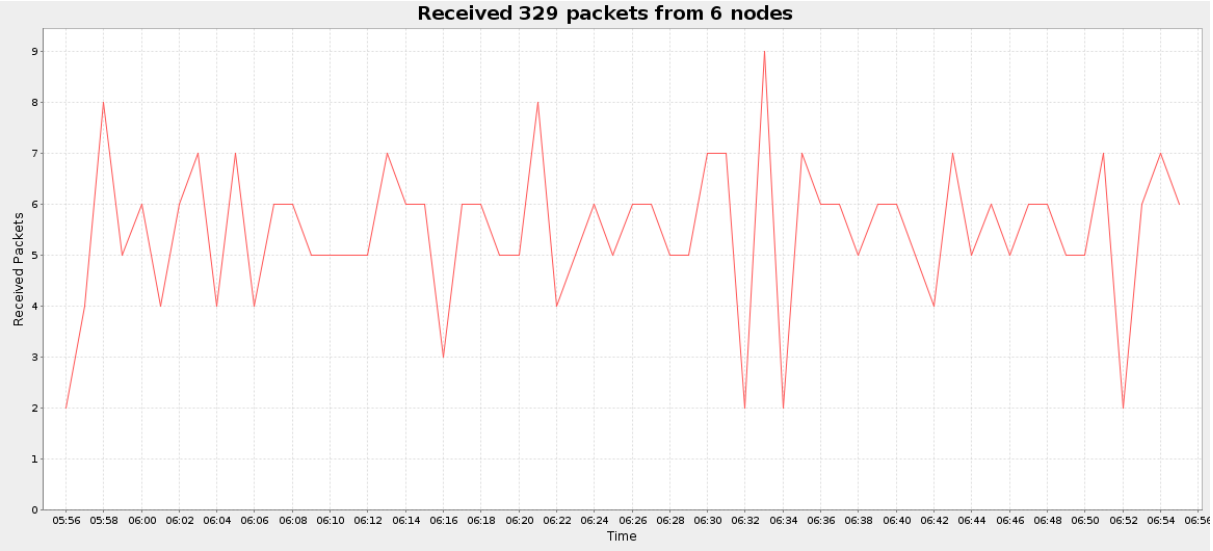
TABLICA 6.10 Mreža sa 6 čvorova, scenarij 1, sa IDS-om

Čvor	Primljeni paketi	Izgubljeni paketi	Skokovi do baze	ETX	Potrošnja energije (mW)					Radni ciklus (%)	
					CPU	LPM	Slušanje	Predaja	Ukupno	Slušanje	Predaja
2	66	0	1.000	1.000	0.064	0.162	0.393	0.019	0.638	0.655	0.036
3	65	0	1.000	1.000	0.069	0.161	0.405	0.027	0.662	0.675	0.050
4	66	0	2.000	1.000	0.064	0.162	0.383	0.034	0.643	0.638	0.064
5	66	0	2.000	1.000	0.062	0.162	0.384	0.033	0.640	0.640	0.062
6	66	0	2.000	1.008	0.061	0.162	0.382	0.030	0.634	0.636	0.057
Prosjek	**65.800**	**0**	**1.600**	**1.002**	**0.064**	**0.162**	**0.389**	**0.029**	**0.643**	**0.649**	**0.054**

Scenarij 2 (Rx/Tx=80%)

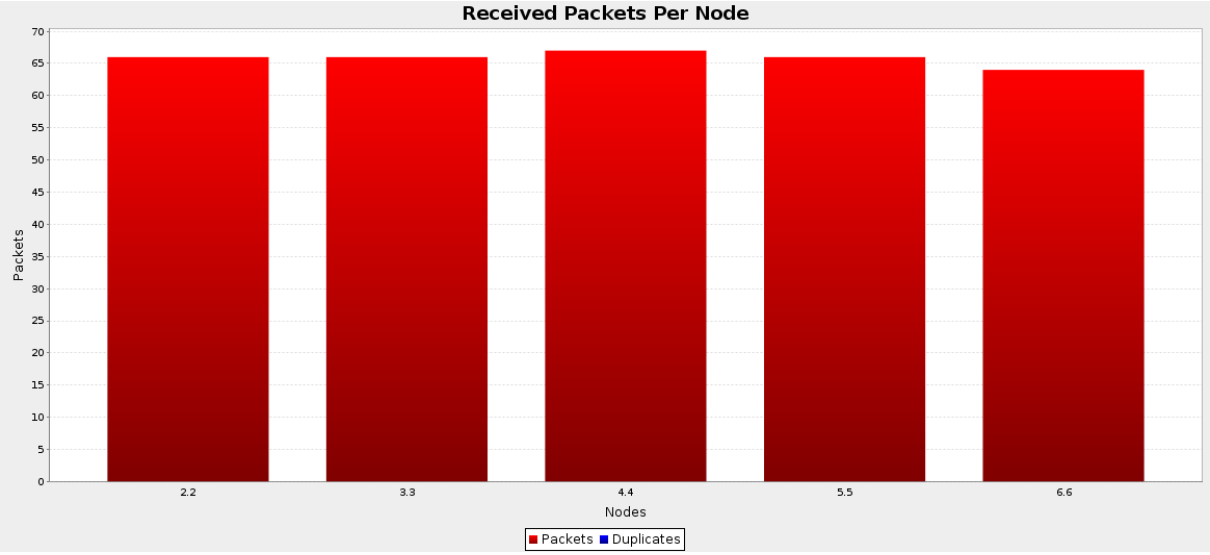
U drugom scenariju analiziranom u istoj mreži omjer uspješno primljenih i poslanih paketa postavljen je na 80% (također uz implementiran IDS sustav). Svi drugi parametri ostaju nepromijenjeni.

Na slici 6.92 prikazan je broj primljenih paketa u mreži u promatranom intervalu od sat vremena.



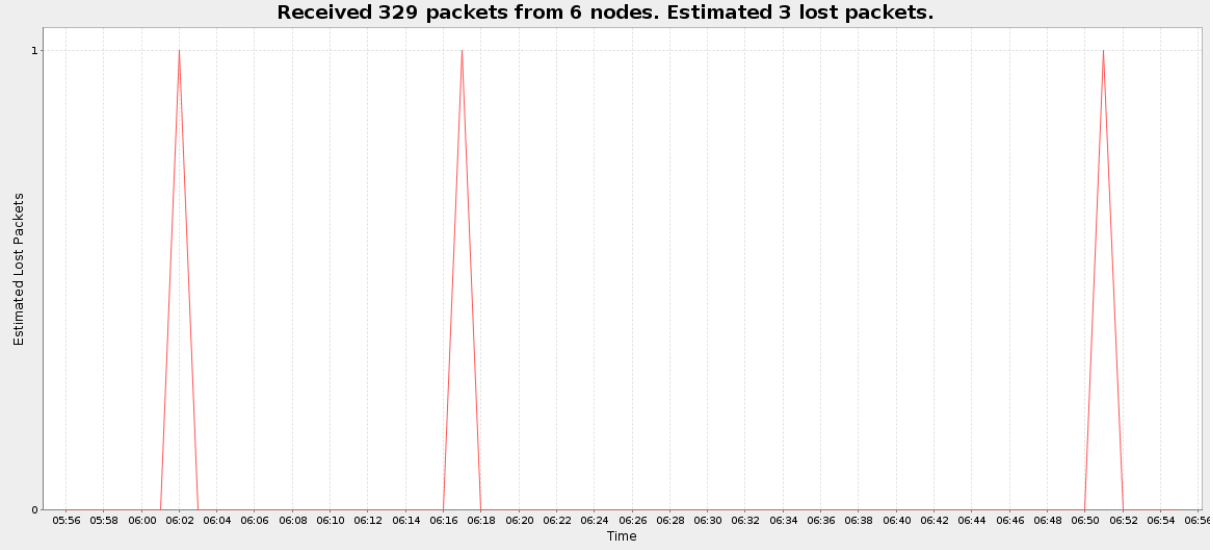
Slika 6.92 Broj primljenih paketa (6 čvorova, scenarij 2, sa IDS-om)

Slika 6.93 prikazuje broj primljenih paketa za svaki pojedinačni čvor.



Slika 6.93 Broj primljenih paketa za svaki čvor (6 čvorova, scenarij 2, sa IDS-om)

U ovom scenariju dolazi i do gubitka određenog broja paketa (unatoč mehanizmu potvrde i retransmisije), što je vidljivo na slici 6.94.

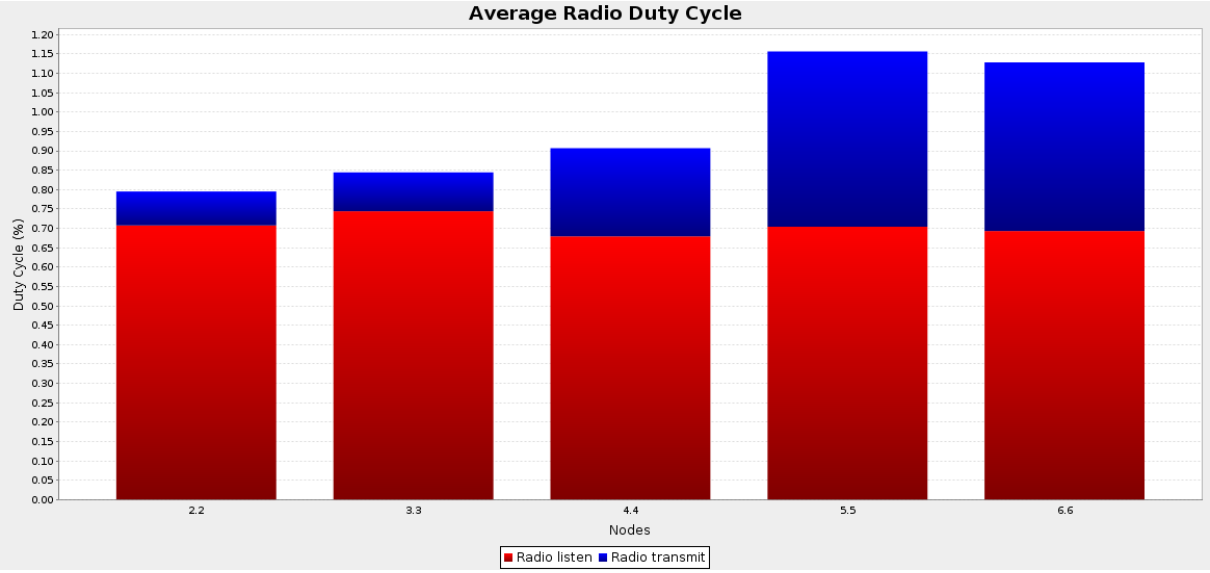


Slika 6.94 Izgubljeni paketi (6 čvorova, scenarij 2, sa IDS-om)

Ukoliko se primljeni promet usporedi sa količinom primljenog prometa u istom scenariju ali bez implementiranog IDS sustava (slike 6.22 i 6.23) primjećuje se povećanje broja primljenih paketa. Ovo povećanje nastaje zbog komunikacije među IDS agentima. Smanjena vjerojatnost uspješnog prijema i slanja paketa (na 80%) utjecala je na ETX vrijednosti za pojedine linkove (ETX vrijednosti se povećavaju), međutim sama implementacija IDS

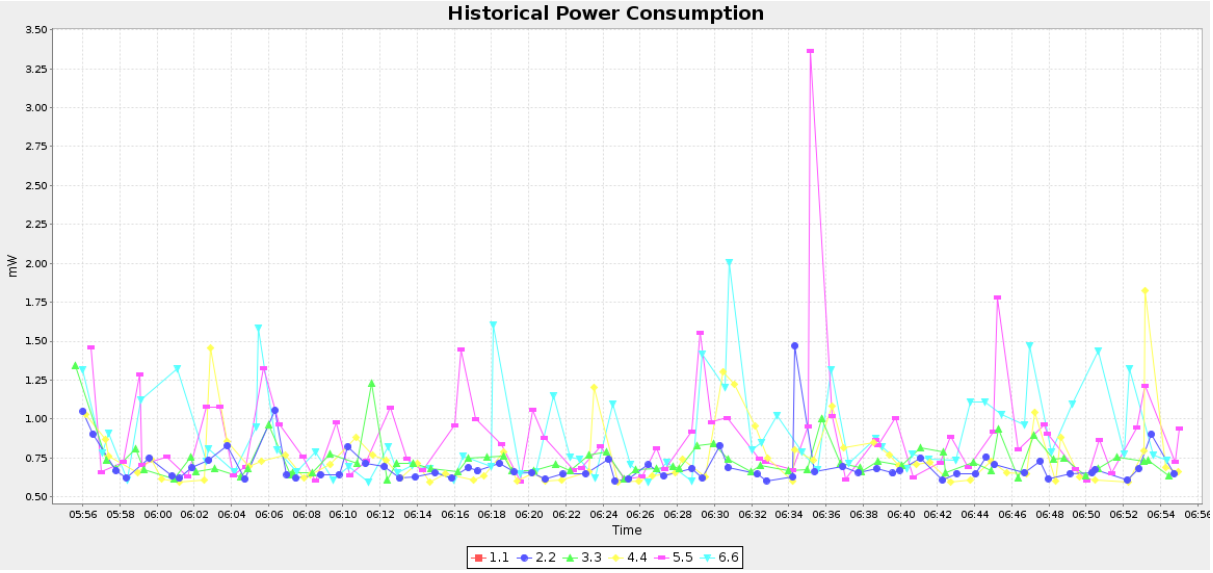
sustava na ovo nema nikakvog utjecaja. Implementacija IDS sustava nije utjecala niti na broj izgubljenih paketa.

Slika 6.95 prikazuje prosječne radne cikluse primopredajnika na svakom pojedinom čvoru.



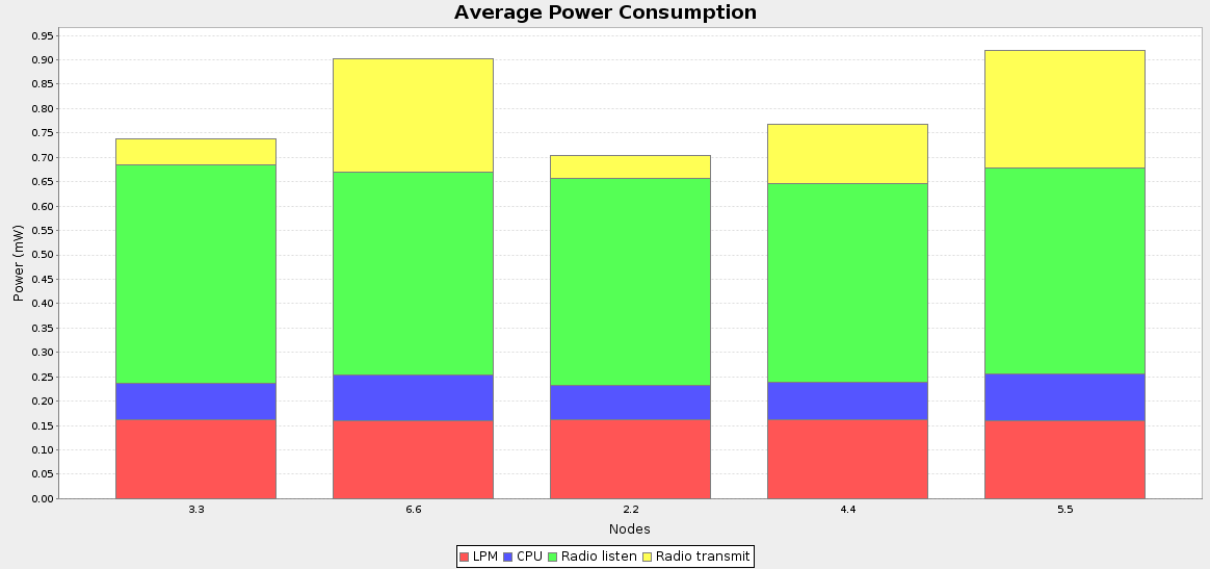
Slika 6.95 Prosječni radni ciklus primopredajnika (6 čvorova, scenarij 2, sa IDS-om)

Slika 6.96 prikazuje potrošnju energije u mreži sa 6 čvorova uz implementirani IDS sustav u scenariju 2.



Slika 6.96 Potrošnja energije (6 čvorova, scenarij 2, sa IDS-om)

Na slici 6.97 prikazana je prosječna potrošnja energije za svaki pojedini čvor.



Slika 6.97 Prosječna potrošnja energije (6 čvorova, scenarij 2, sa IDS-om)

Prosječna potrošnja energije povećana je u odnosu na prethodni scenarij (posebice za čvorove 4, 5 i 6 koji su udaljeniji od bazne stanice) zbog potrebe za retransmisijom određenog broja paketa. Međutim, značajno je primijetiti da nema povećane potrošnje energije u odnosu na isti scenarij, ali bez implementiranog IDS sustava (slika 6.28).

U tablici 6.11 su pregledno prikazane dobivene vrijednosti za drugi scenarij u mreži sa 6 čvorova, uz implementiran IDS sustav.

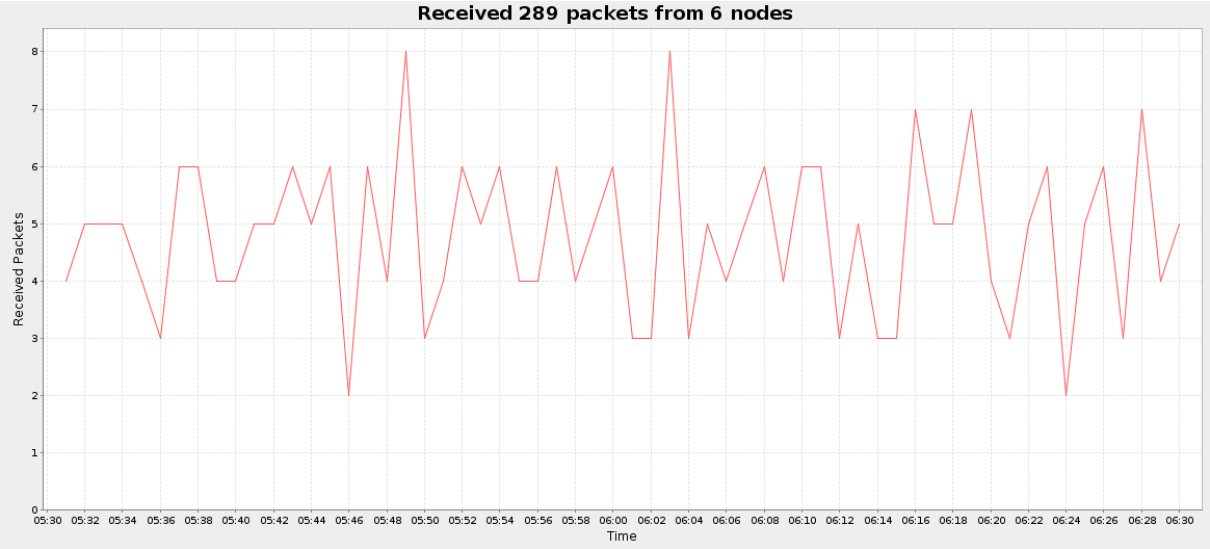
TABLICA 6.11 Mreža sa 6 čvorova, scenarij 2, sa IDS-om

Čvor	Primljeni paketi	Izgubljeni paketi	Skokovi do baze	ETX	Potrošnja energije (mW)					Radni ciklus (%)	
					CPU	LPM	Slušanje	Predaja	Ukupno	Slušanje	Predaja
2	66	0	1.000	1.004	0.071	0.161	0.425	0.046	0.703	0.708	0.087
3	66	0	1.000	1.011	0.076	0.161	0.447	0.053	0.737	0.744	0.100
4	67	0	2.000	1.925	0.078	0.161	0.408	0.121	0.768	0.679	0.228
5	66	1	2.000	3.042	0.096	0.161	0.423	0.240	0.919	0.704	0.452
6	64	2	2.000	3.301	0.094	0.161	0.416	0.231	0.902	0.693	0.435
Prosjek	**65.800**	**0.600**	**1.600**	**2.057**	**0.083**	**0.161**	**0.423**	**0.138**	**0.806**	**0.706**	**0.260**

Scenarij 3 (Rx/Tx=60%)

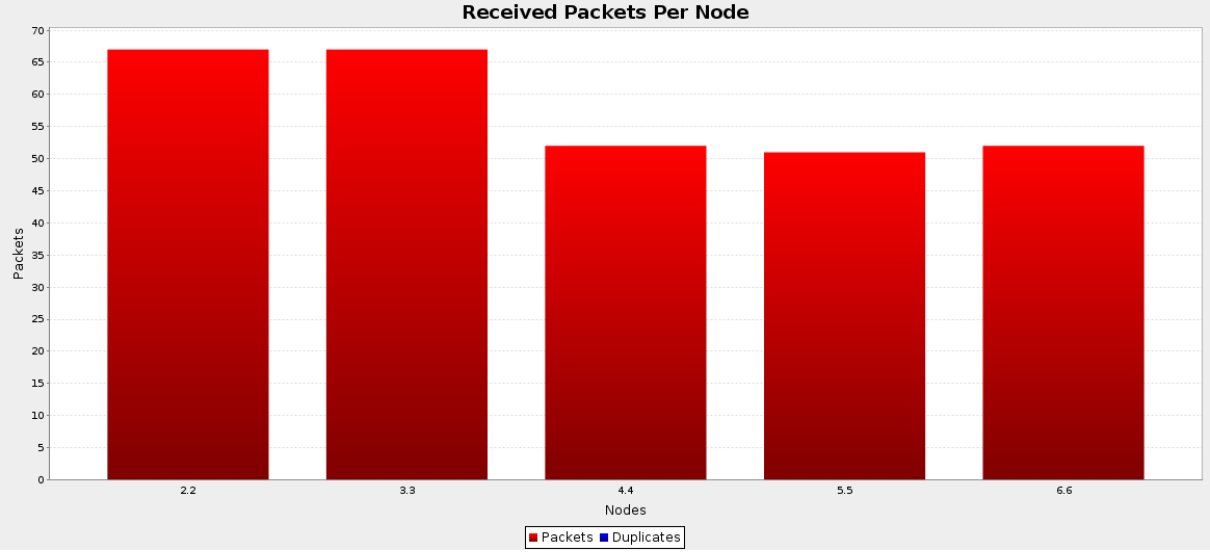
U trećem simuliranom scenariju vjerojatnost uspješnog prijema i slanja paketa u mreži postavljena je na 60% i na svaki mrežni čvor je implementiran IDS agent. Svi ostali parametri identični su kao i u prethodno analiziranim scenarijima.

Slika 6.98 prikazuje broj primljenih paketa u intervalu od sat vremena.



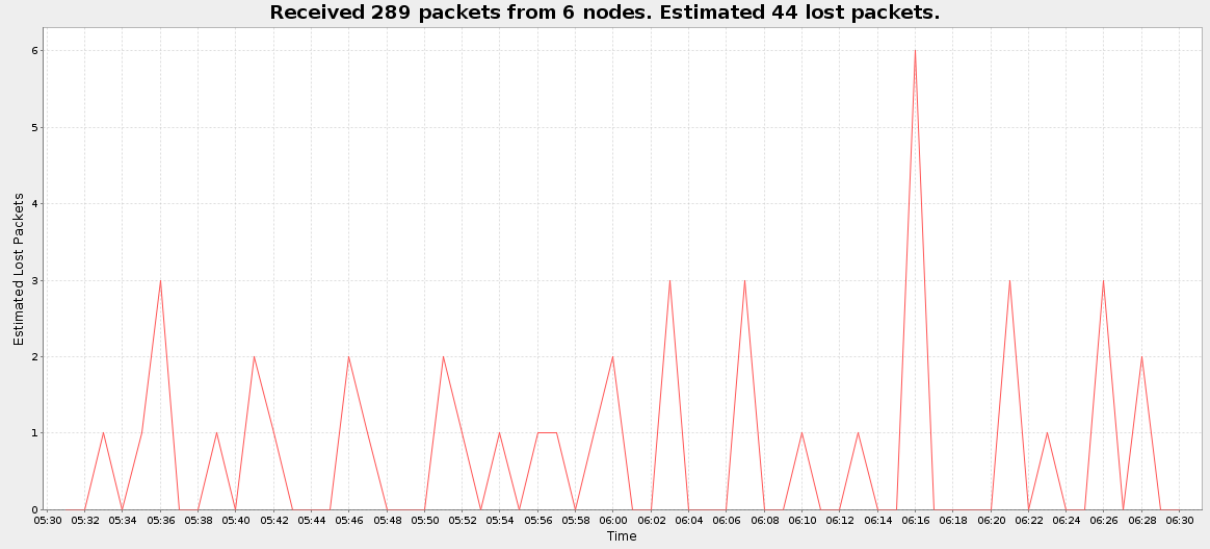
Slika 6.98 Broj primljenih paketa (6 čvorova, scenarij 3, sa IDS-om)

Slika 6.99 prikazuje broj primljenih paketa u trećem scenariju za svaki čvor pojedinačno.



Slika 6.99 Broj primljenih paketa za svaki čvor (6 čvorova, scenarij 3, sa IDS-om)

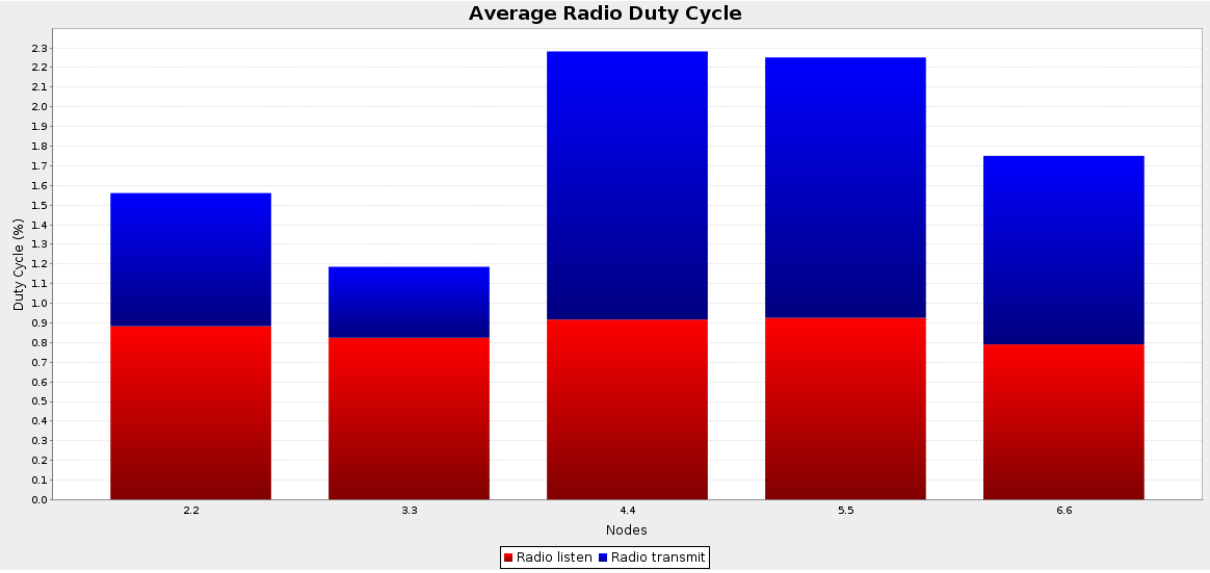
Procjena izgubljenih paketa prikazana je na slici 6.100.



Slika 6.100 Izgubljeni paketi (6 čvorova, scenarij 3, sa IDS-om)

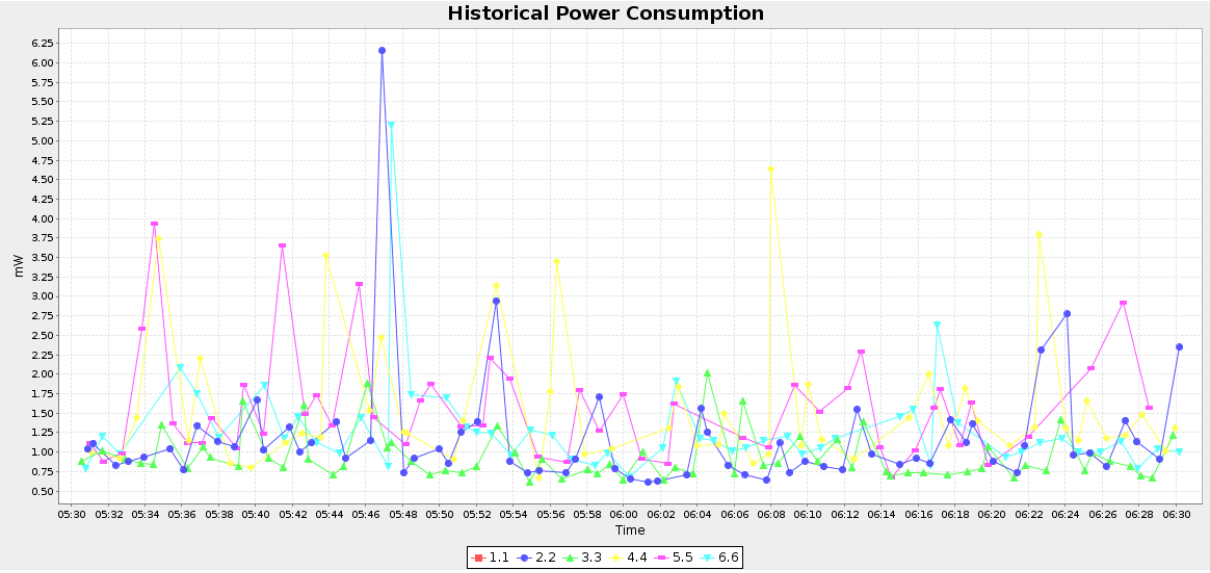
U scenariju 3 broj izgubljenih paketa povećan je u odnosu na scenarij 2, što je očekivano budući da je i vjerojatnost uspješnog slanja i prijema smanjena. Također se primjećuje smanjen broj primljenih paketa sa udaljenijih čvorova (čvorovi 4, 5 i 6). Međutim, u odnosu na isti scenarij bez implementiranog IDS sustava (slike 6.29 i 6.30) primjećuje se povećanje broja primljenih paketa (zbog dodatne komunikacije koju u mrežu uvodi sam IDS sustav).

Na slici 6.101 prikazani su prosječni radni ciklusi primopredajnika na pojedinim čvorovima.



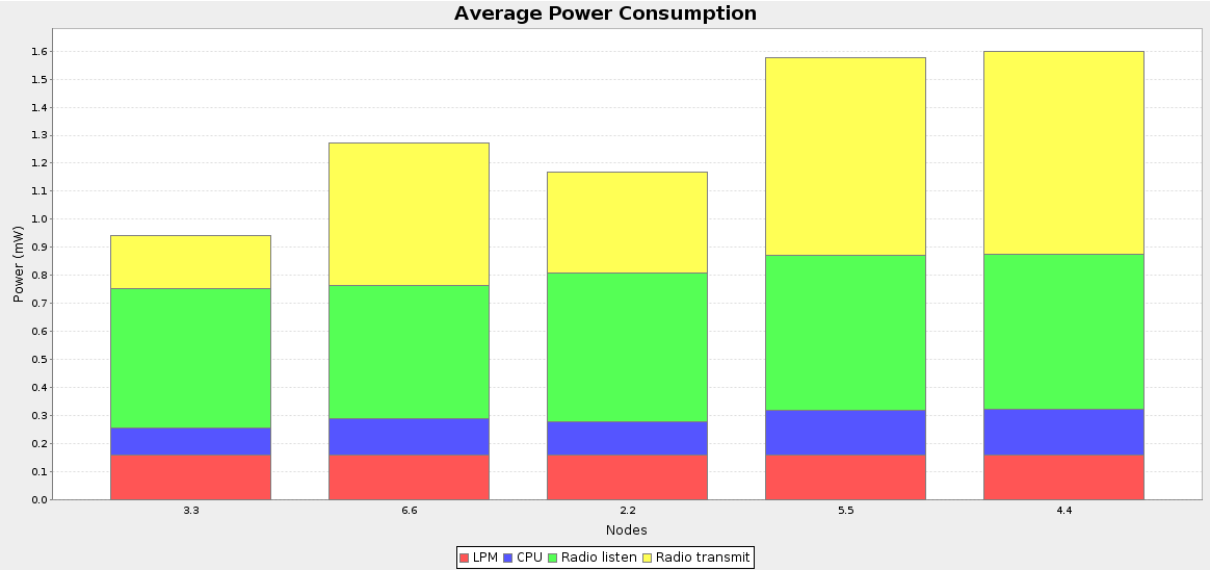
Slika 6.101 Prosječni radni ciklus primopredajnika (6 čvorova, scenarij 3, sa IDS-om)

Na slici 6.102 prikazana je potrošnja energije u trećem scenariju mreže sa 6 čvorova, uz implementiran IDS sustav.



Slika 6.102 Potrošnja energije (6 čvorova, scenarij 3, sa IDS-om)

Slika 6.103 prikazuje prosječnu potrošnju energije za svaki pojedini mrežni čvor.



Slika 6.103 Prosječna potrošnja energije (6 čvorova, scenarij 3, sa IDS-om)

Potrošnja raste u odnosu na prethodni scenarij zbog povećanja potrošnje primopredajnika u stanju aktivne predaje, uslijed potrebe za dodatnim retransmisijama pojedinih paketa. Međutim, u usporedbi sa istim scenarijem bez implementiranog IDS sustava (slike 6.34 i 6.35) nema značajnije promjene u potrošnji energije.

U tablici 6.12 su pregledno prikazane sve dobivene vrijednosti za treći scenarij u mreži sa 6 čvorova, uz implementiran IDS sustav.

TABLICA 6.12 Mreža sa 6 čvorova, scenarij 3, sa IDS-om

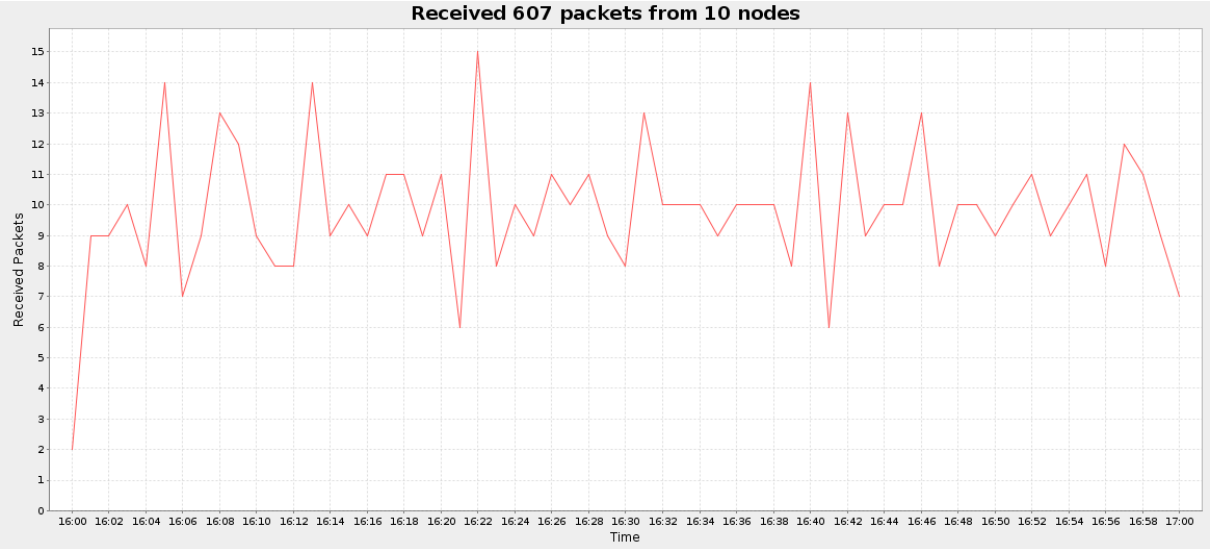
Čvor	Primljeni paketi	Izgubljeni paketi	Skokovi do baze	ETX	Potrošnja energije (mW)					Radni ciklus (%)	
					CPU	LPM	Slušanje	Predaja	Ukupno	Slušanje	Predaja
2	67	0	1.000	2.119	0.120	0.160	0.530	0.360	1.169	0.884	0.677
3	67	0	1.000	1.634	0.096	0.161	0.495	0.192	0.943	0.824	0.362
4	52	15	2.000	8.450	0.165	0.158	0.550	0.725	1.599	0.917	1.365
5	51	14	2.000	8.434	0.159	0.159	0.555	0.704	1.577	0.925	1.326
6	52	15	2.000	8.327	0.129	0.160	0.475	0.509	1.273	0.791	0.959
Prosjek	**57.800**	**8.800**	**1.600**	**5.793**	**0.134**	**0.159**	**0.521**	**0.498**	**1.312**	**0.868**	**0.938**

6.6.2. IDS sustav implementiran u mrežu sa 10 čvorova

Nakon mreže sa 6 čvorova, IDS sustav implementiran je u mrežu sa 10 čvorova. Analiza njegovog ponašanja i utjecaja na mrežu provedena je također kroz tri scenarija (scenariji su detaljnije opisani u poglavlju 6.5.). IDS agent implementiran je na svaki senzorski čvor, a topologija mreže ostala je nepromijenjena u odnosu na mrežu sa 10 čvorova bez IDS sustava (slika 6.36). Budući da je topologija ostala ista, ništa se nije promijenilo u pogledu broja susjednih čvorova i broja potrebnih skokova do bazne stanice u usporedbi sa odgovarajućom mrežom bez implementiranog IDS sustava.

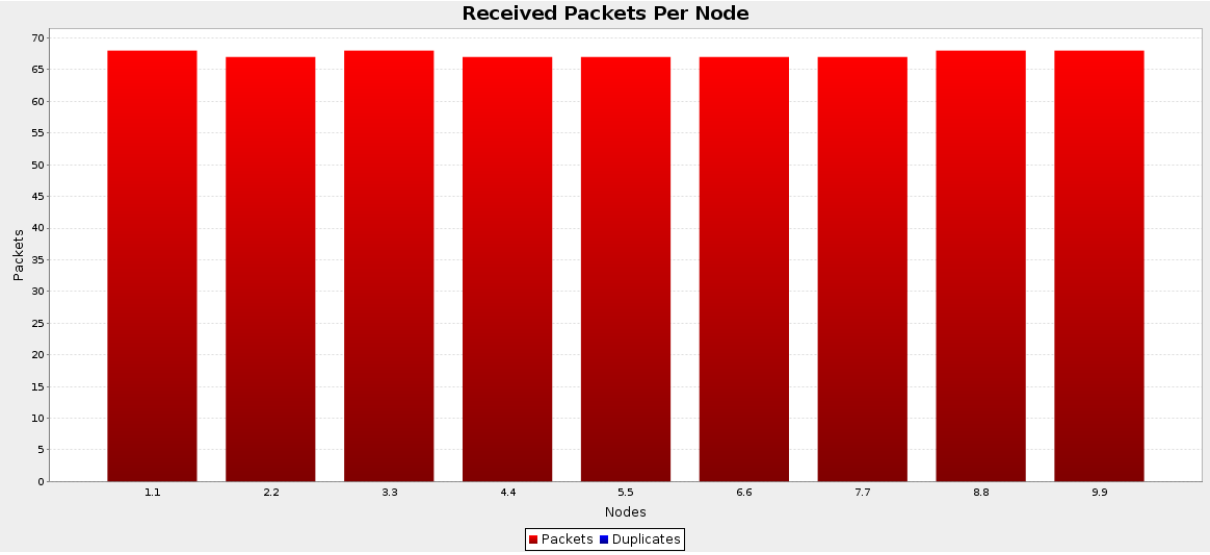
Scenarij 1 (Rx/Tx=100%)

Slika 6.104 predstavlja broj primljenih paketa tijekom jednosatnog intervala u prvom simuliranom scenariju, u kojem je vjerojatnost ispravnog slanja i prijema paketa 100% („idealan slučaj“).



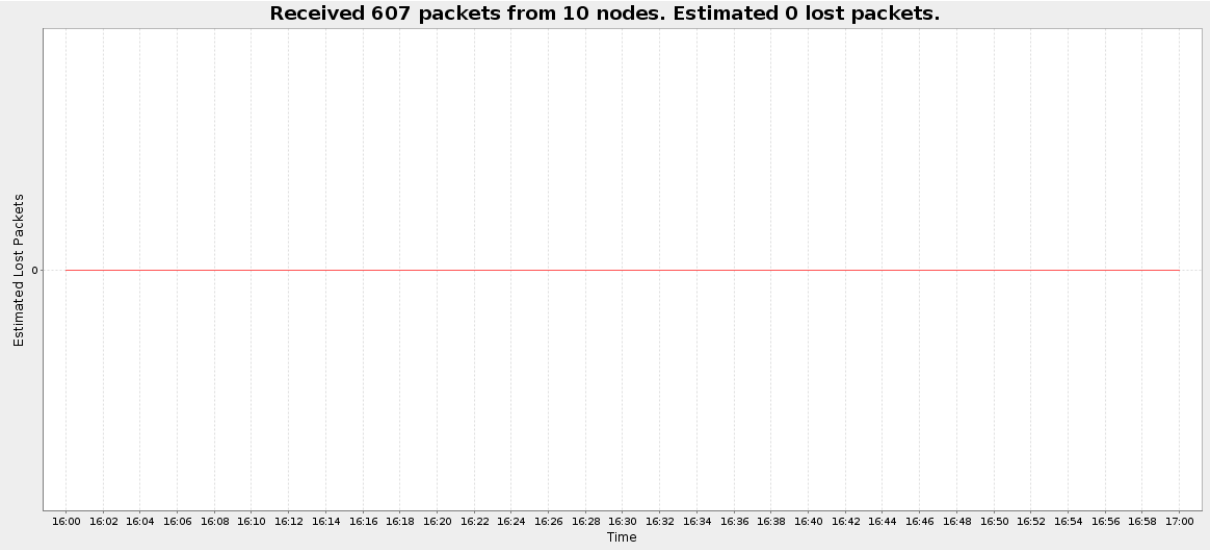
Slika 6.104 Broj primljenih paketa (10 čvorova, scenarij 1, sa IDS-om)

Na slici 6.105 prikazan je broj primljenih paketa za svaki čvor pojedinačno.



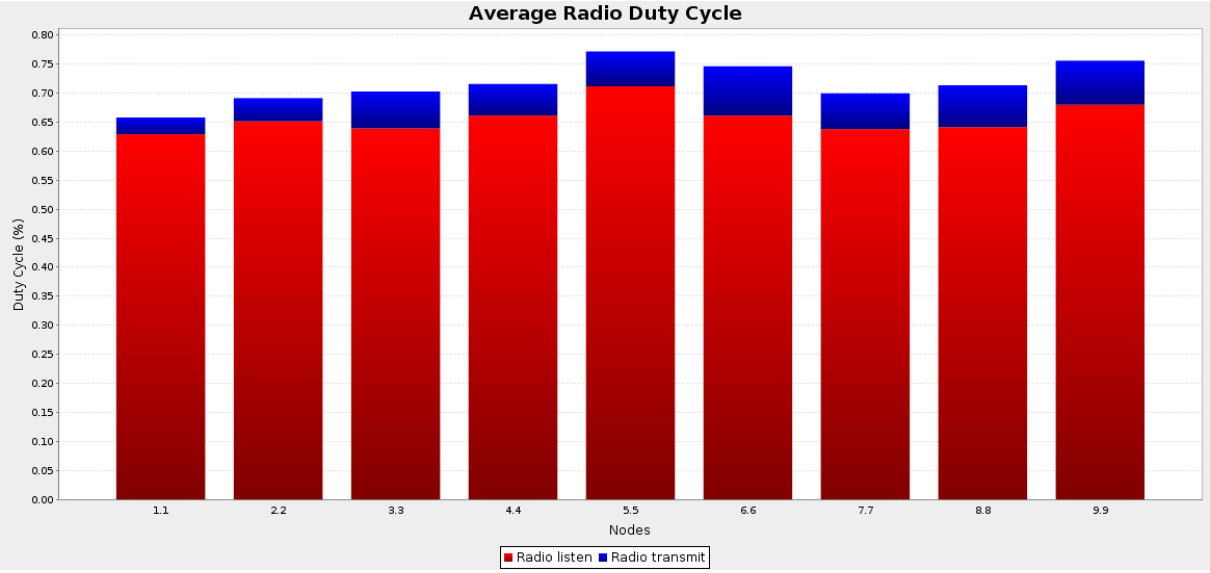
Slika 6.105 Broj primljenih paketa za svaki čvor (10 čvorova, scenarij 1, sa IDS-om)

Na slikama 6.104 i 6.105 vidljivo je povećanje broja primljenih paketa u usporedbi sa istim scenarijem u mreži bez IDS agenata (slike 6.40 i 6.41), zbog toga što agenti svojom komunikacijom unose dodatni promet u mrežu. Kako se radi o „idealnom slučaju“ u ovom scenariju nema izgubljenih paketa, kao što se vidi na slici 6.106.



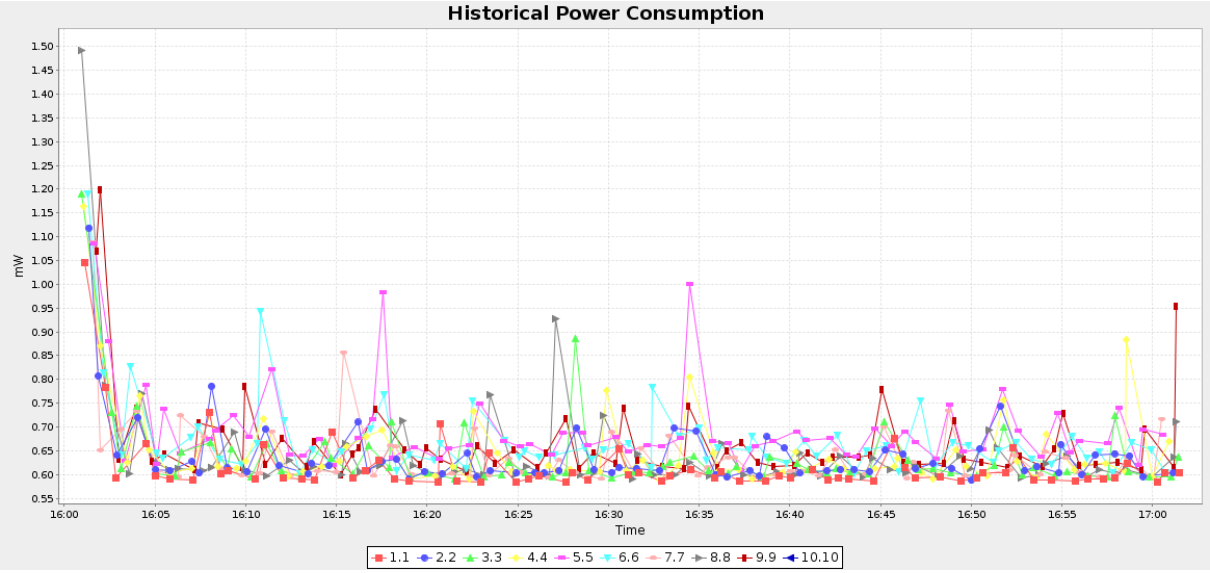
Slika 6.106 Izgubljeni paketi (10 čvorova, scenarij 1, sa IDS-om)

Slika 6.107 prikazuje radne cikluse primopredajnika u prvom scenariju mreže sa 10 čvorova.



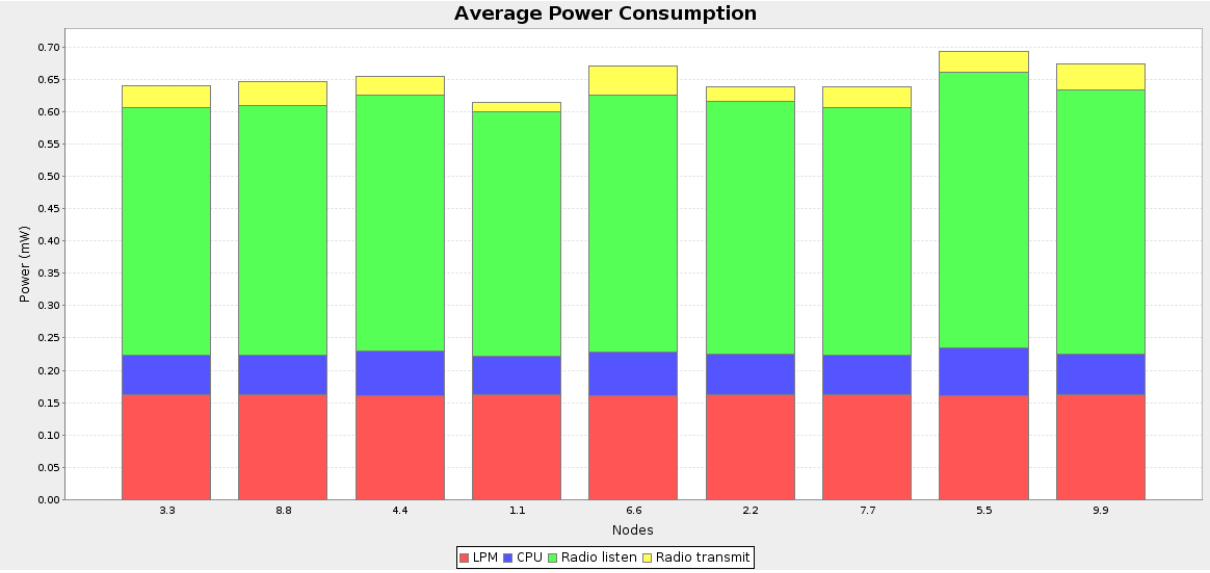
Slika 6.107 Prosječni radni ciklus primopredajnika (10 čvorova, scenarij 1, sa IDS-om)

Slika 6.108 prikazuje potrošnju energije u prvom scenariju mreže sa 10 čvorova, uz implementirani IDS sustav.



Slika 6.108 Potrošnja energije (10 čvorova, scenarij 1, sa IDS-om)

Na slici 6.109 prikazana je prosječna potrošnja energije za svaki pojedini čvor.



Slika 6.109 Prosječna potrošnja energije (10 čvorova, scenarij 1, sa IDS-om)

Moguće je primijetiti da je potrošnja za nijansu veća na središnjim čvorovima, zbog većeg broja ruta koje preko njih vode ka baznoj stanici. Međutim, usporedi li se potrošnja sa ekvivalentnim scenarijem u kojem nije implementiran IDS sustav (slike 6.45 i 6.46), može se zaključiti da njegova implementacija neće dovesti do povećane potrošnje.

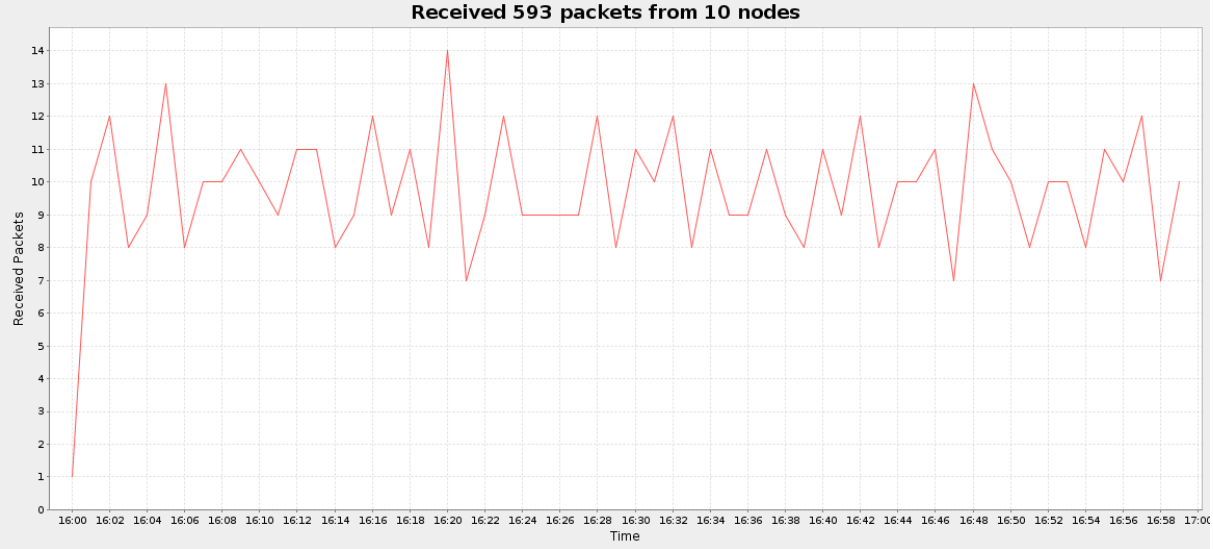
U tablici 6.13 su pregledno prikazane vrijednosti dobivene simulacijom prvog scenarija u mreži sa 10 čvorova uz implementiran IDS sustav.

TABLICA 6.13 Mreža sa 10 čvorova, scenarij 1, sa IDS-om

Čvor	Primljeni paketi	Izgubljeni paketi	Skokovi do baze	ETX	Potrošnja energije (mW)					Radni ciklus (%)	
					CPU	LPM	Slušanje	Predaja	Ukupno	Slušanje	Predaja
1	68	0	1.000	1.000	0.060	0.162	0.377	0.015	0.615	0.629	0.029
2	67	0	1.000	1.000	0.064	0.162	0.391	0.021	0.638	0.651	0.040
3	68	0	2.000	1.000	0.062	0.162	0.383	0.034	0.641	0.639	0.064
4	67	0	1.000	1.000	0.068	0.161	0.397	0.029	0.655	0.661	0.054
5	67	0	1.000	1.000	0.073	0.161	0.427	0.032	0.693	0.711	0.060
6	67	0	2.000	1.000	0.067	0.161	0.397	0.045	0.670	0.661	0.085
7	67	0	2.000	1.000	0.062	0.162	0.383	0.033	0.639	0.638	0.061
8	68	0	2.000	1.000	0.063	0.162	0.385	0.038	0.647	0.641	0.072
9	68	0	3.000	1.000	0.064	0.162	0.408	0.040	0.673	0.680	0.076
Prosjek	**67.444**	**0.000**	**1.667**	**1.000**	**0.065**	**0.162**	**0.394**	**0.032**	**0.652**	**0.657**	**0.060**

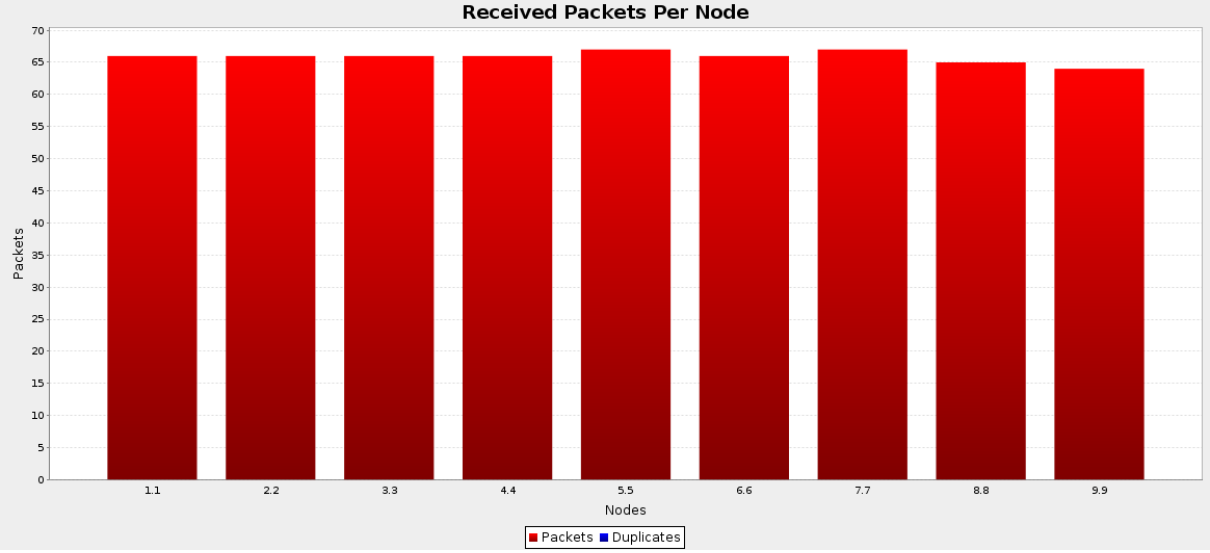
Scenarij 2 (Rx/Tx=80%)

Slika 6.110 prikazuje broj primljenih paketa u mreži sa 10 čvorova u drugom scenariju, u kojem je vjerojatnost uspješnog slanja i prijema 80% (uz implementirane IDS agente na senzorskim čvorovima).



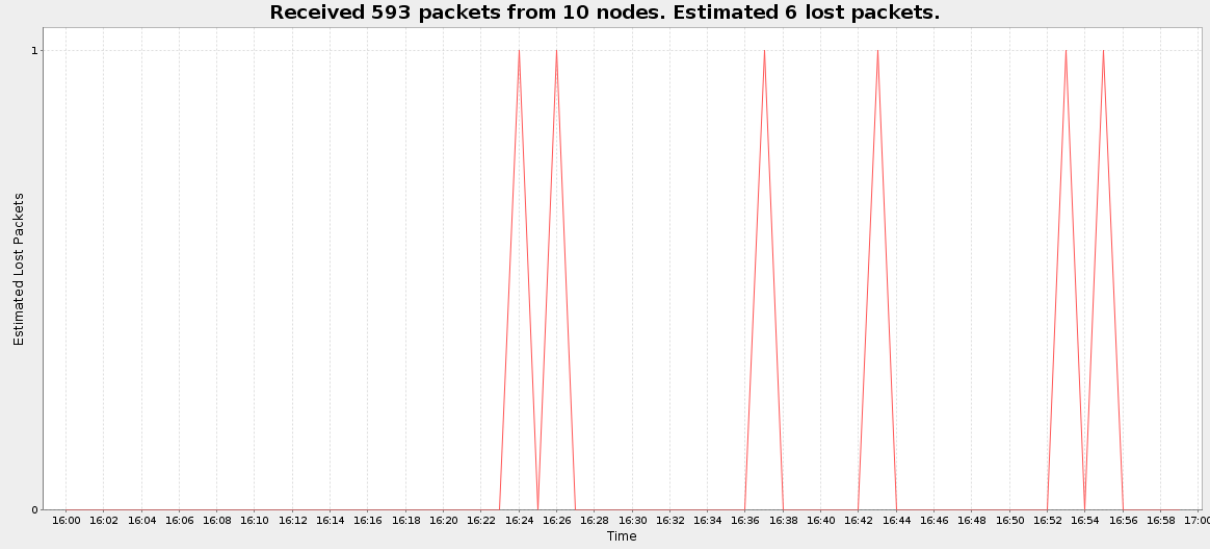
Slika 6.110 Broj primljenih paketa (10 čvorova, scenarij 2, sa IDS-om)

Slika 6.111 prikazuje broj primljenih paketa za svaki pojedinačni čvor.



Slika 6.111 Broj primljenih paketa za svaki čvor (10 čvorova, scenarij 2, sa IDS-om)

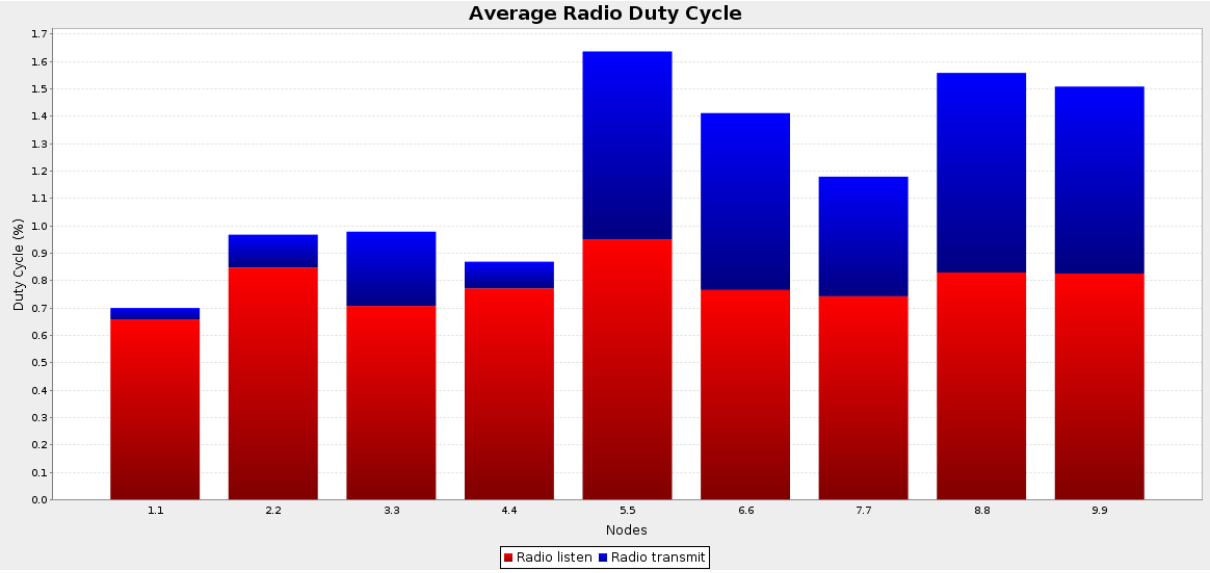
Procijenjeni broj izgubljenih paketa prikazan je na slici 6.112.



Slika 6.112 Izgubljeni paketi (10 čvorova, scenarij 2, sa IDS-om)

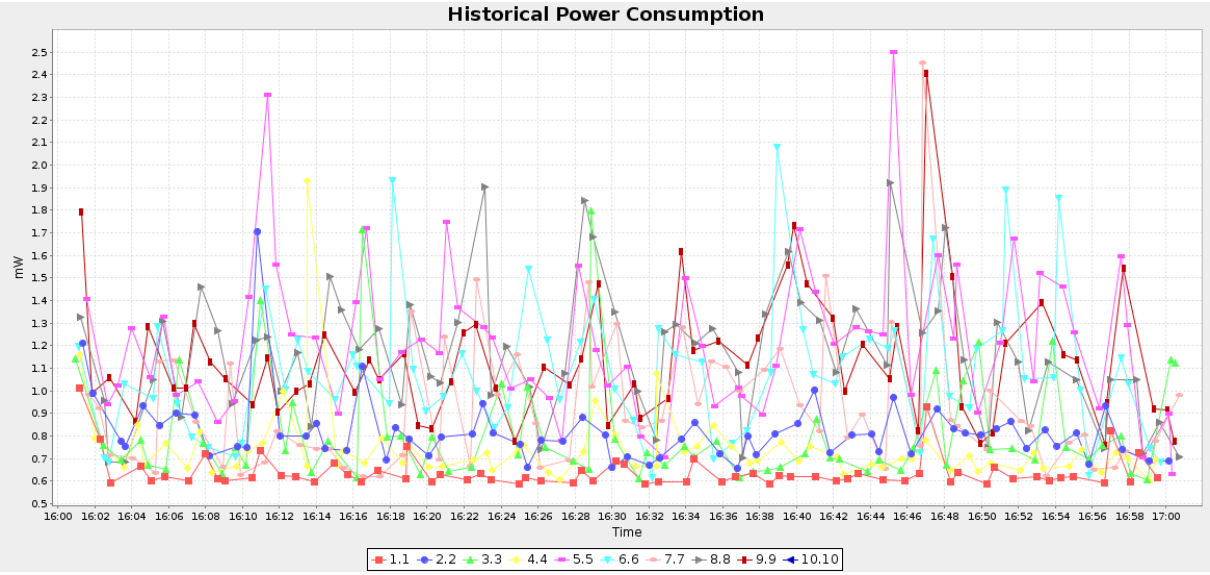
Primjećuje se da je u odnosu na odgovarajući scenarij bez implementiranog IDS sustava (slike 6.47 i 6.48) porastao broj primljenih paketa, što je i očekivano jer se radi o dodatnom prometu zbog komunikacije među IDS agentima. U drugom simuliranom scenariju dolazi i do gubitka određenog broja paketa, što je također očekivano, budući da je vjerojatnost ispravnog slanja i prijema smanjena.

Slika 6.113 prikazuje prosječne radne cikluse primopredajnika u drugom scenariju mreže sa 10 čvorova.



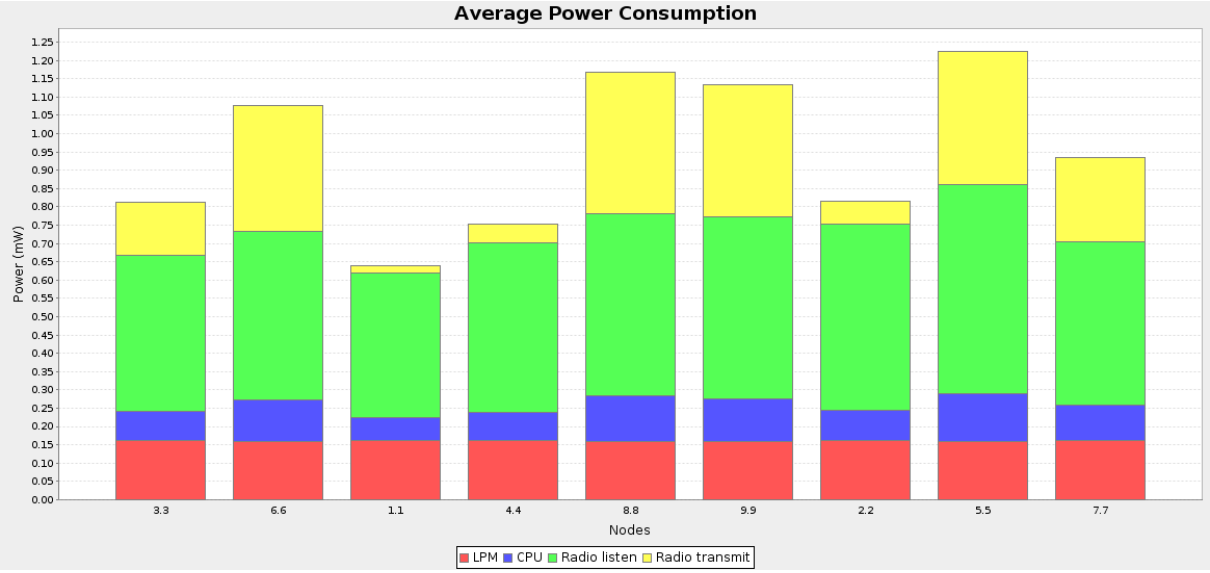
Slika 6.113 Prosječni radni ciklus primopredajnika (10 čvorova, scenarij 2, sa IDS-om)

Slika 6.114 prikazuje potrošnju energije u drugom scenariju mreže sa 10 čvorova.



Slika 6.114 Potrošnja energije (10 čvorova, scenarij 2, sa IDS-om)

Na slici 6.115 prikazana je prosječna potrošnja energije za svaki pojedinačni čvor.



Slika 6.115 Prosječna potrošnja energije (10 čvorova, scenarij 2, sa IDS-om)

Zbog potrebe za povećanom aktivnosti predajnika povećala se i potrošnja energije u odnosu na prethodni scenarij, posebice na udaljenijim čvorovima koji su trebali obavljati češće retransmisije. Međutim, važno je primijetiti da implementacija IDS sustava nije dovela do velikog povećanja potrošnje, što je vidljivo usporedbom rezultata sa ekvivalentnim scenarijem bez IDS sustava (slike 6.52 i 6.53).

U tablici 6.14 su na pregledan način prikazane vrijednosti dobivene za drugi scenarij u mreži sa 10 čvorova.

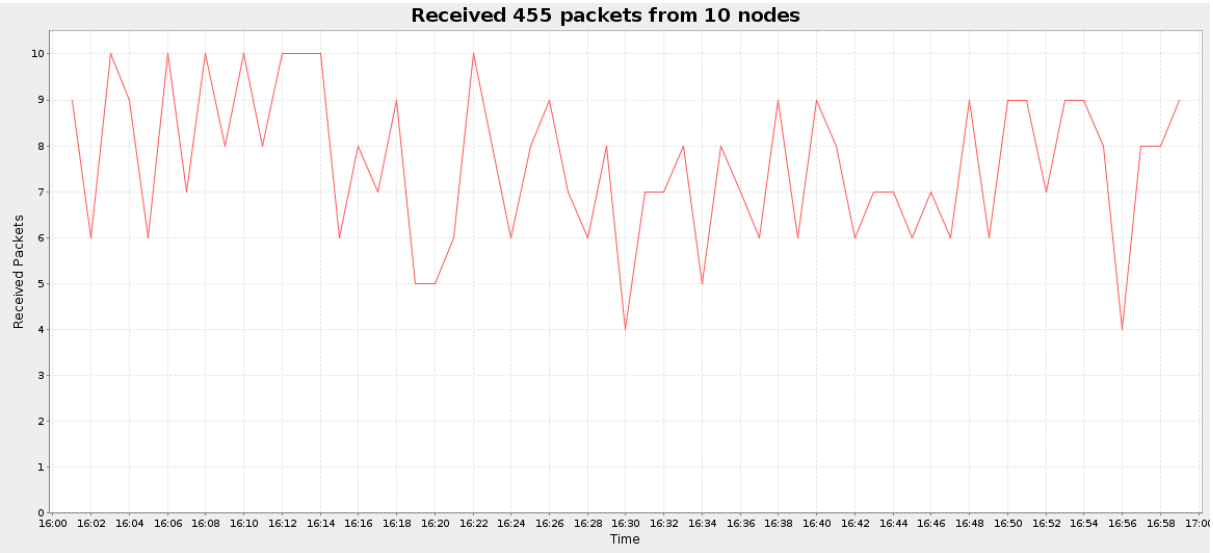
TABLICA 6.14 Mreža sa 10 čvorova, scenarij 2, sa IDS-om

Čvor	Primljeni paketi	Izgubljeni paketi	Skokovi do baze	ETX	Potrošnja energije (mW)					Radni ciklus (%)	
					CPU	LPM	Slušanje	Predaja	Ukupno	Slušanje	Predaja
1	66	0	1.000	1.000	0.061	0.162	0.395	0.022	0.640	0.658	0.042
2	66	0	1.000	1.000	0.083	0.161	0.509	0.064	0.816	0.848	0.120
3	66	1	2.000	2.335	0.082	0.161	0.425	0.144	0.811	0.708	0.271
4	66	0	1.000	1.000	0.077	0.161	0.463	0.052	0.754	0.772	0.097
5	67	0	1.925	2.272	0.130	0.160	0.570	0.364	1.224	0.951	0.686
6	66	0	2.939	2.521	0.113	0.160	0.459	0.343	1.076	0.766	0.646
7	67	0	2.000	2.621	0.097	0.161	0.446	0.232	0.935	0.743	0.437
8	65	2	2.923	2.279	0.123	0.160	0.498	0.387	1.167	0.830	0.729
9	64	3	3.922	2.195	0.116	0.160	0.496	0.363	1.134	0.826	0.683
Prosjek	**65.889**	**0.667**	**2.079**	**1.914**	**0.098**	**0.161**	**0.473**	**0.219**	**0.951**	**0.789**	**0.412**

Scenarij 3 (Rx/Tx=60%)

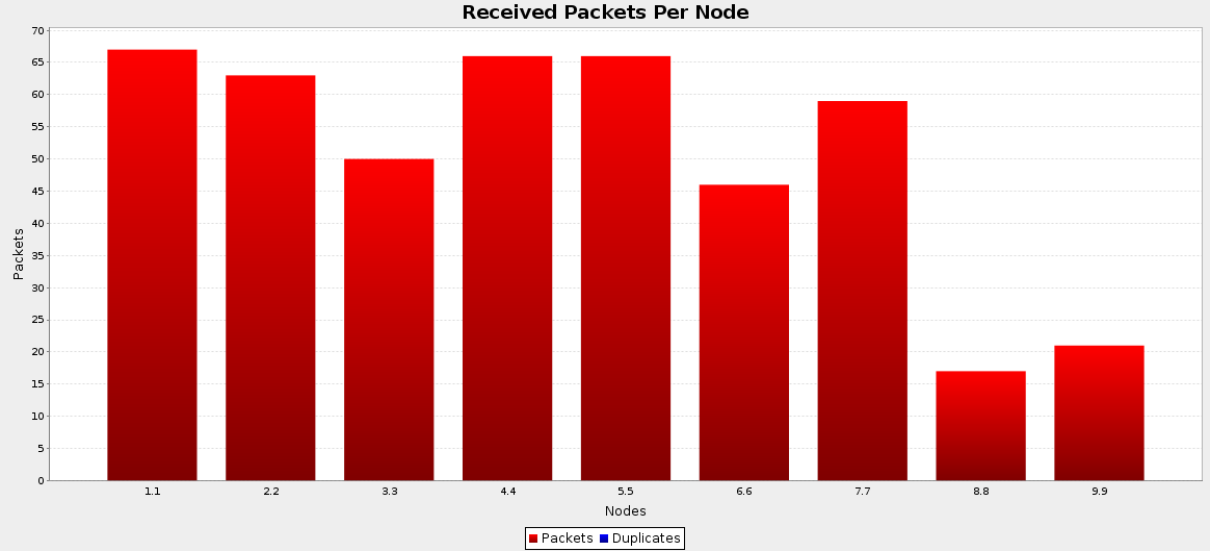
U trećem simuliranom scenariju mreže sa 10 čvorova, analogno simulacijama bez implementiranog IDS-a, vjerojatnost uspješnog slanja i prijema paketa iznosi 60%. Preostali parametri mreže identični su kao i u prethodna dva scenarija.

Na slici 6.116 prikazan je primljeni podatkovni promet tijekom simuliranih sat vremena trećeg scenarija u mreži sa 10 čvorova (uz implementiran IDS).



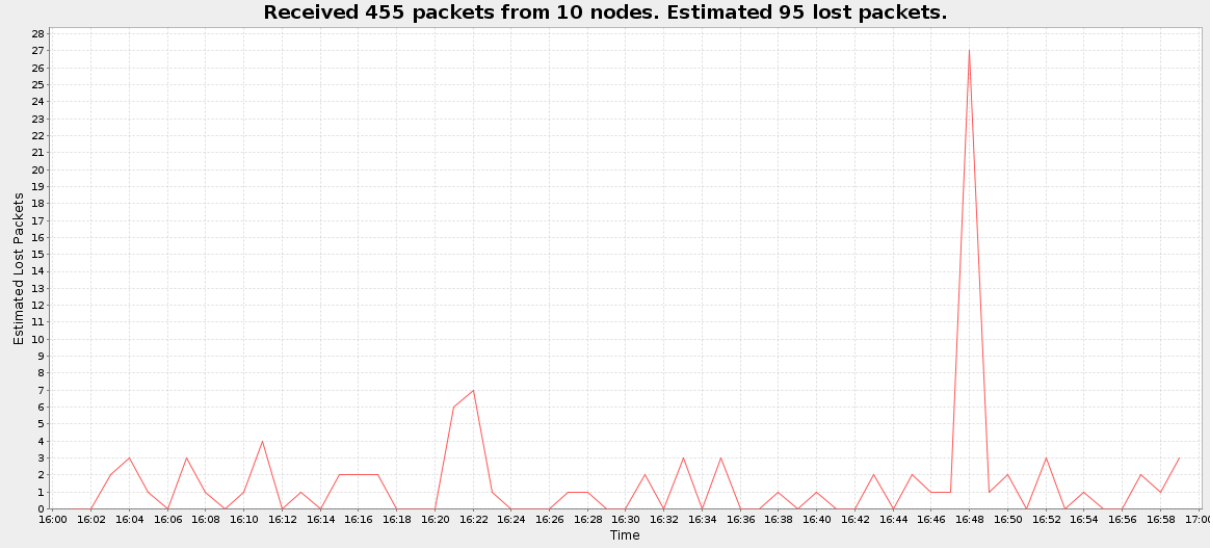
Slika 6.116 Broj primljenih paketa (10 čvorova, scenarij 3, sa IDS-om)

Na slici 6.117 prikazani su primljeni paketi za svaki pojedini čvor u mreži.



Slika 6.117 Broj primljenih paketa za svaki čvor (10 čvorova, scenarij 3, sa IDS-om)

Slika 6.118 prikazuje izgubljene pakete u trećem scenariju mreže sa 10 čvorova.

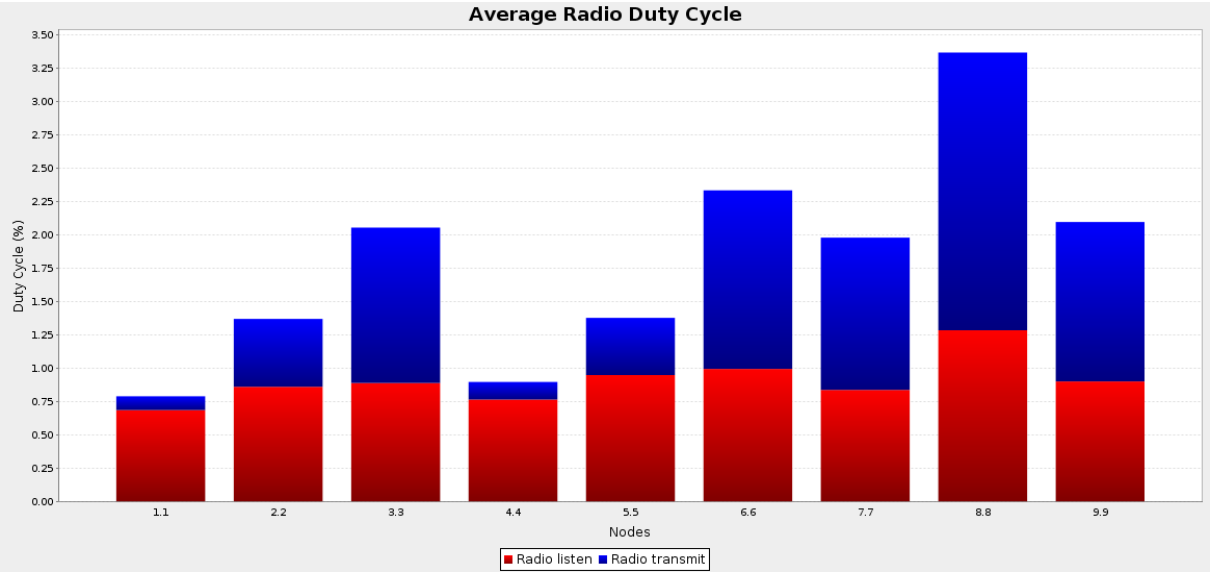


Slika 6.118 Izgubljeni paketi (10 čvorova, scenarij 3, sa IDS-om)

Iz dobivenih prikaza vidljivo je da u trećem scenariju dolazi do znatno većih gubitaka paketa, pa je broj primljenih paketa za neke čvorove osjetno manji u odnosu na prethodne scenarije, posebice za čvorove koji su udaljeniji od bazne stanice. Usporedbom sa ekvivalentnim scenarijem bez implementiranog IDS-a (slike 6.54 i 6.55) vidljivo je da je za

čvorove bliže baznoj stanici broj primljenih paketa veći (jer na njima gubici nisu značajno izraženi, a postoje dodatni paketi nastali komunikacijom IDS agenata), dok je za udaljene čvorove broj primljenih paketa manji, zbog većih gubitaka.

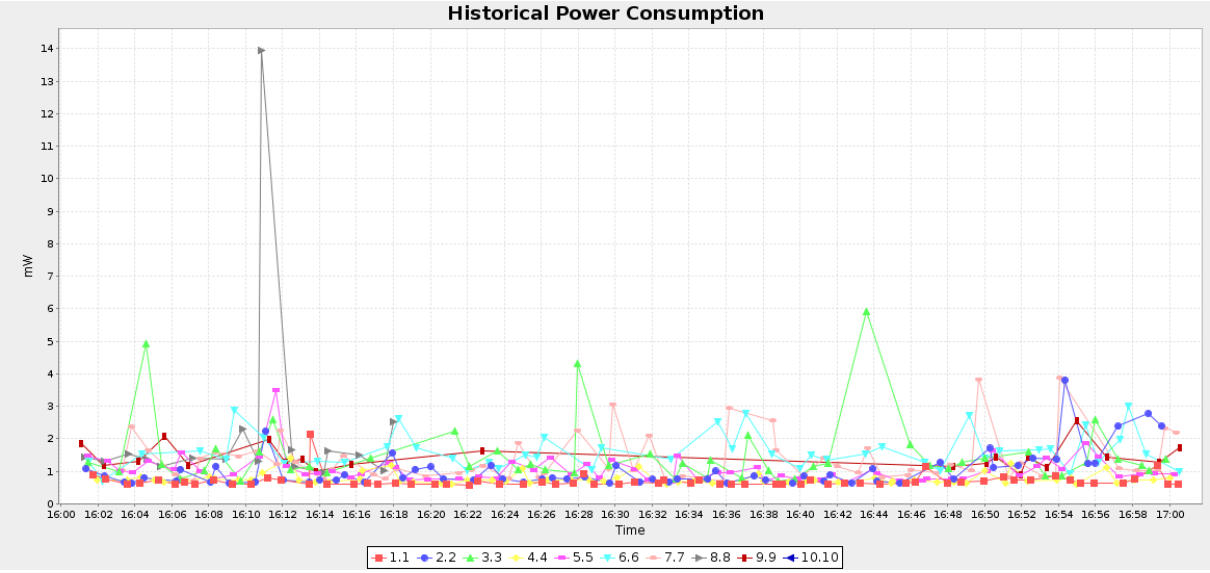
Slika 6.119 prikazuje radne cikluse primopredajnika senzorskih čvorova u trećem scenariju mreže s 10 čvorova u koju je implementiran IDS sustav.



Slika 6.119 Prosječni radni ciklus primopredajnika (10 čvorova, scenarij 3, sa IDS-om)

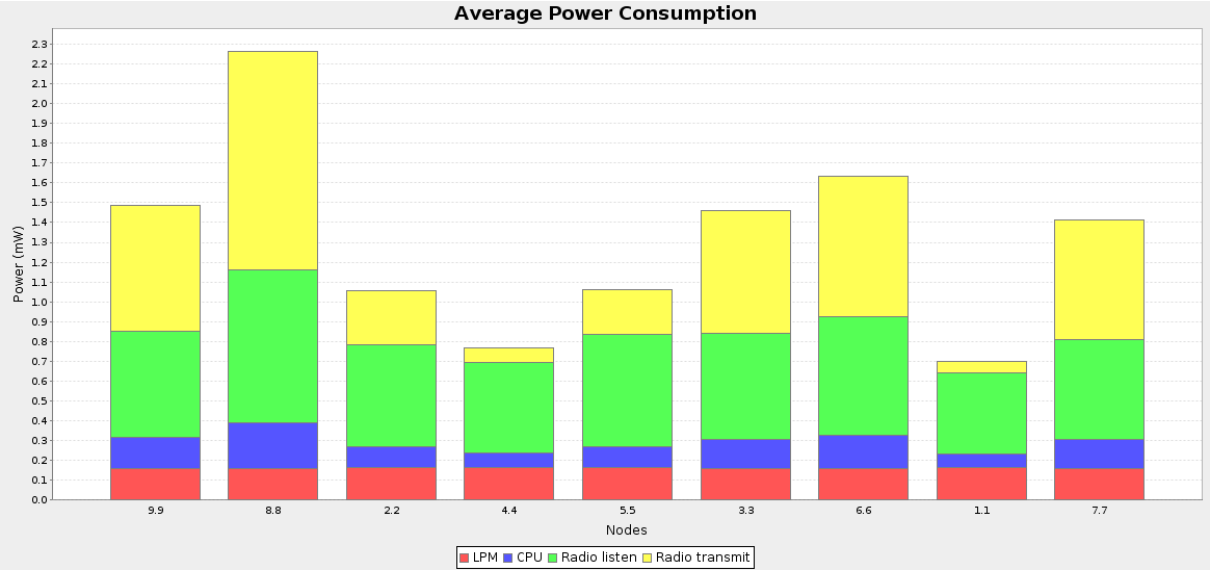
Sa slike je vidljivo značajnije povećanje razdoblja aktivne predaje kod čvorova udaljenijih od bazne stanice uslijed čestih potreba za retransmisijom paketa.

Na slici 6.120 prikazana je potrošnja energije u trećem simuliranom scenariju mreže sa 10 čvorova.



Slika 6.120 Potrošnja energije (10 čvorova, scenarij 3, sa IDS-om)

Slika 6.121 prikazuje prosječnu potrošnju energije za svaki pojedini čvor u trećem scenariju mreže sa 10 čvorova.



Slika 6.121 Prosječna potrošnja energije (10 čvorova, scenarij 3, sa IDS-om)

Vidljivo je da je potrošnja energije veća u odnosu na prethodne scenarije (zbog većeg broja retransmisija), no usporedi li se s odgovarajućim scenarijem bez implementiranog IDSa (slike 6.59 i 6.60) ne bilježi se značajno povećanje potrošnje.

U tablici 6.15 su pregledno prikazane dobivene vrijednosti u trećem simuliranom scenariju mreže s 10 čvorova u koju je implementiran IDS sustav.

TABLICA 6.15 Mreža sa 10 čvorova, scenarij 3, sa IDS-om

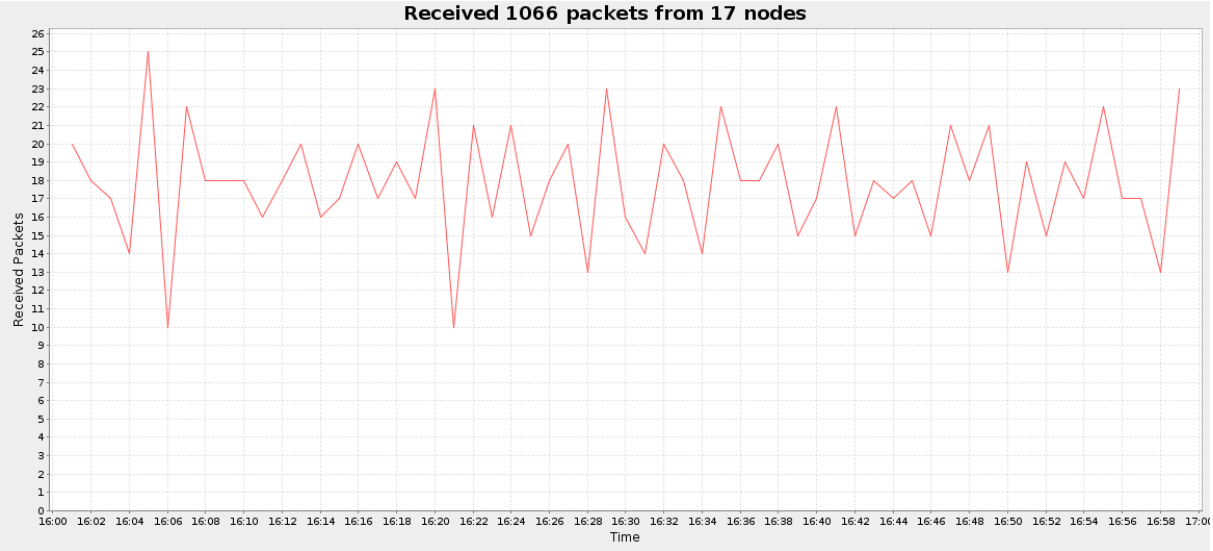
Čvor	Primljeni paketi	Izgubljeni paketi	Skokovi do baze	ETX	Potrošnja energije (mW)					Radni ciklus (%)	
					CPU	LPM	Slušanje	Predaja	Ukupno	Slušanje	Predaja
1	67	0	1.000	1.138	0.068	0.161	0.411	0.055	0.696	0.686	0.104
2	63	3	1.206	2.065	0.108	0.160	0.516	0.270	1.055	0.860	0.509
3	50	16	2.260	7.582	0.147	0.159	0.533	0.618	1.458	0.889	1.164
4	66	0	1.000	1.127	0.076	0.161	0.459	0.070	0.766	0.764	0.132
5	66	0	1.000	1.782	0.105	0.160	0.569	0.228	1.062	0.948	0.429
6	46	21	2.000	7.674	0.168	0.158	0.596	0.711	1.634	0.994	1.339
7	59	6	2.000	7.424	0.147	0.159	0.502	0.606	1.414	0.837	1.141
8	17	3	2.000	6.022	0.232	0.156	0.771	1.105	2.264	1.285	2.081
9	21	46	3.000	6.173	0.154	0.159	0.540	0.634	1.487	0.901	1.195
Prosjek	**50.556**	**10.556**	**1.718**	**4.554**	**0.134**	**0.159**	**0.544**	**0.478**	**1.315**	**0.907**	**0.899**

6.6.3. IDS sustav implementiran u mrežu sa 17 čvorova

Osim mreža sa 6 i 10 čvorova predloženi IDS sustav implementiran je još i u mrežu sa 17 čvorova. I u mreži sa 17 čvorova njegovo ponašanje također je analizirano kroz tri karakteristična scenarija. Topologija mreže i simulirani scenariji detaljnije su opisani u poglavlju 6.5. Topologija mreže i svi preostali parametri nepromijenjeni su u odnosu na mrežu sa 17 čvorova bez implementiranog IDS-a (slika 6.61), pa tako nema nikakve razlike glede broja susjednih čvorova i broja potrebnih skokova do bazne stanice.

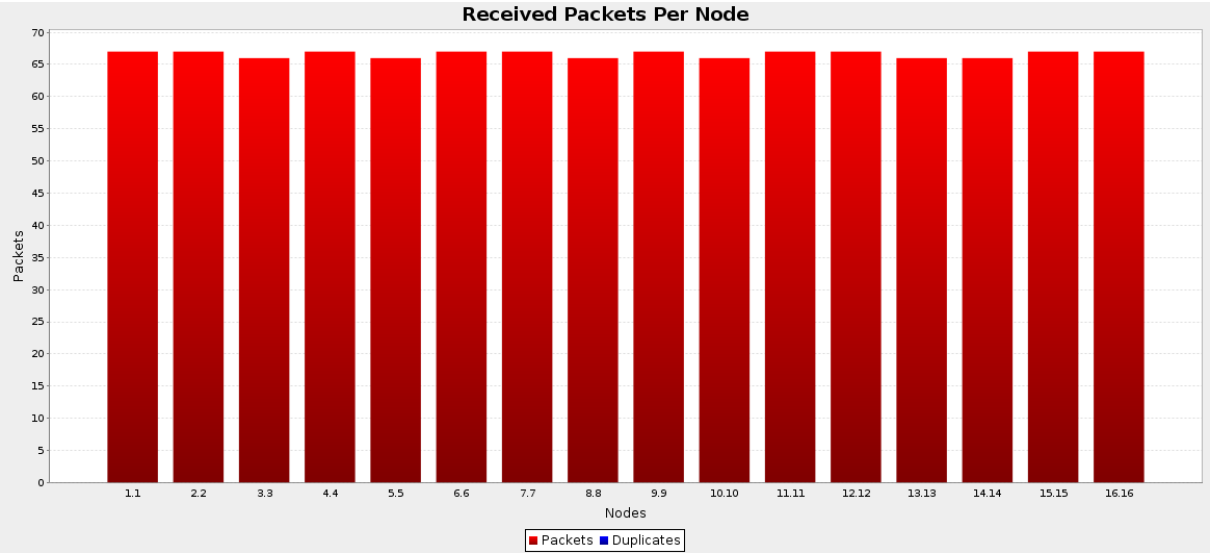
Scenarij 1 (Rx/Tx=100%)

Na slici 6.122 prikazano je kretanje broja primljenih paketa tijekom jednog sata u prvom simuliranom scenariju u mreži sa implementiranim IDS sustavom.



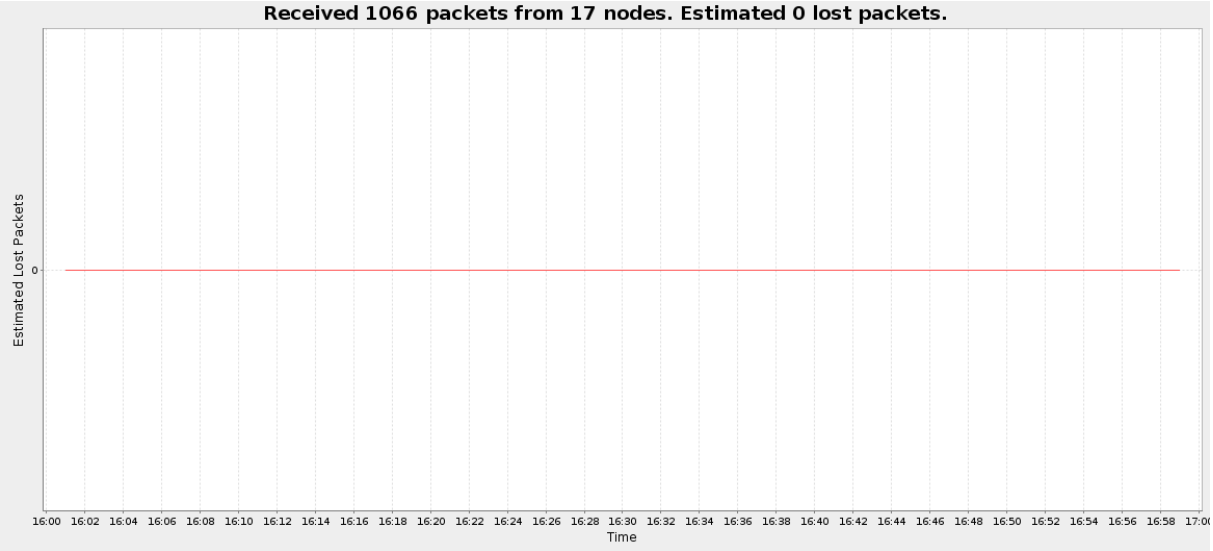
Slika 6.122 Broj primljenih paketa (17 čvorova, scenarij 1, sa IDS-om)

Slika 6.123 prikazuje broj primljenih paketa za svaki mrežni čvor pojedinačno.



Slika 6.123 Broj primljenih paketa za svaki čvor (17 čvorova, scenarij 1, sa IDS-om)

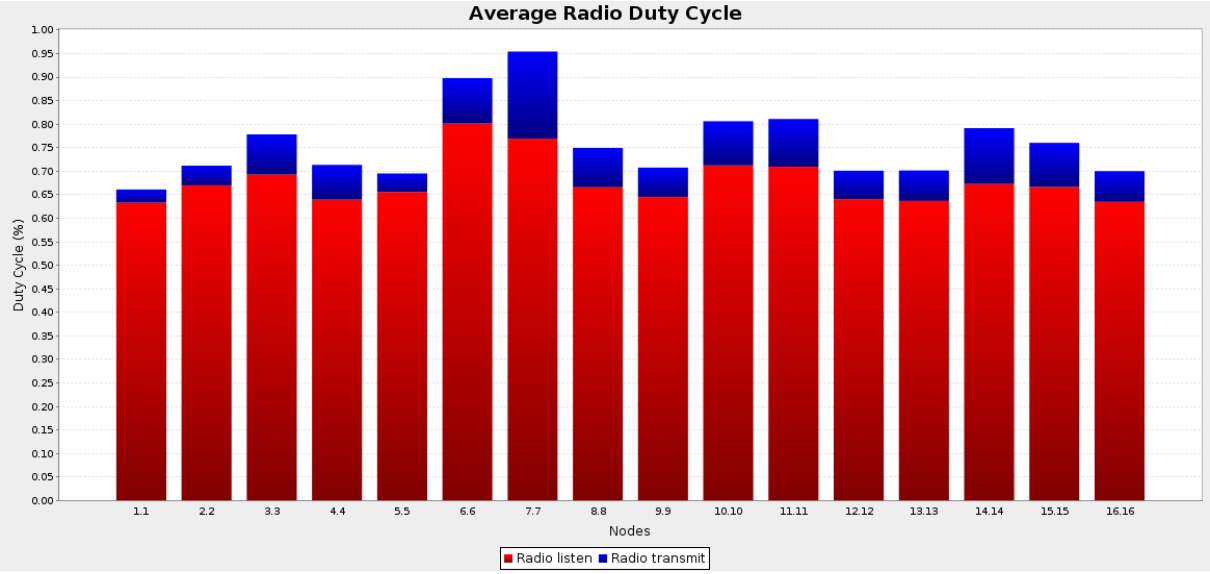
Promatrani scenarij predstavlja „idealan slučaj“, pa u njemu nema izgubljenih paketa, što je vidljivo na slici 6.124.



Slika 6.124 Izgubljeni paketi (17 čvorova, scenarij 1, sa IDS-om)

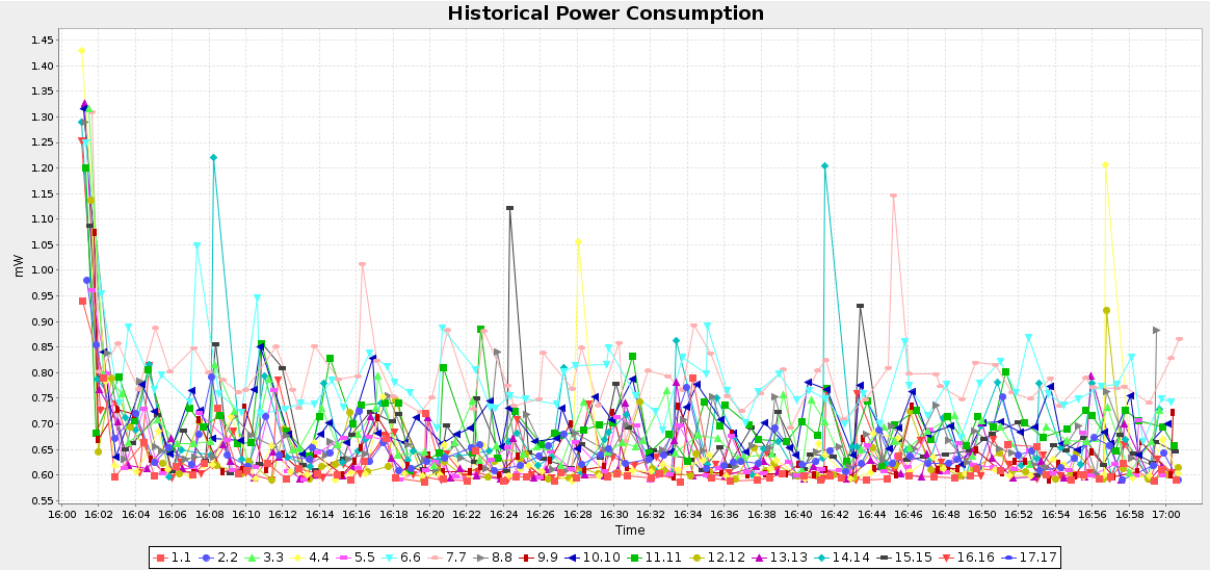
Ako se broj primljenih paketa usporedi sa ekvivalentnim scenarijem bez implementiranog IDS-a (slike 6.65 i 6.66) vidljivo je njegovo povećanje. Do povećanja prometa u mreži dolazi zbog komunikacije IDS agenata, pa je dobiveni rezultat u skladu s očekivanjima.

Na slici 6.125 prikazani su prosječni radni ciklusi radio-primopredajnika za svaki pojedini mrežni čvor u prvom scenariju.



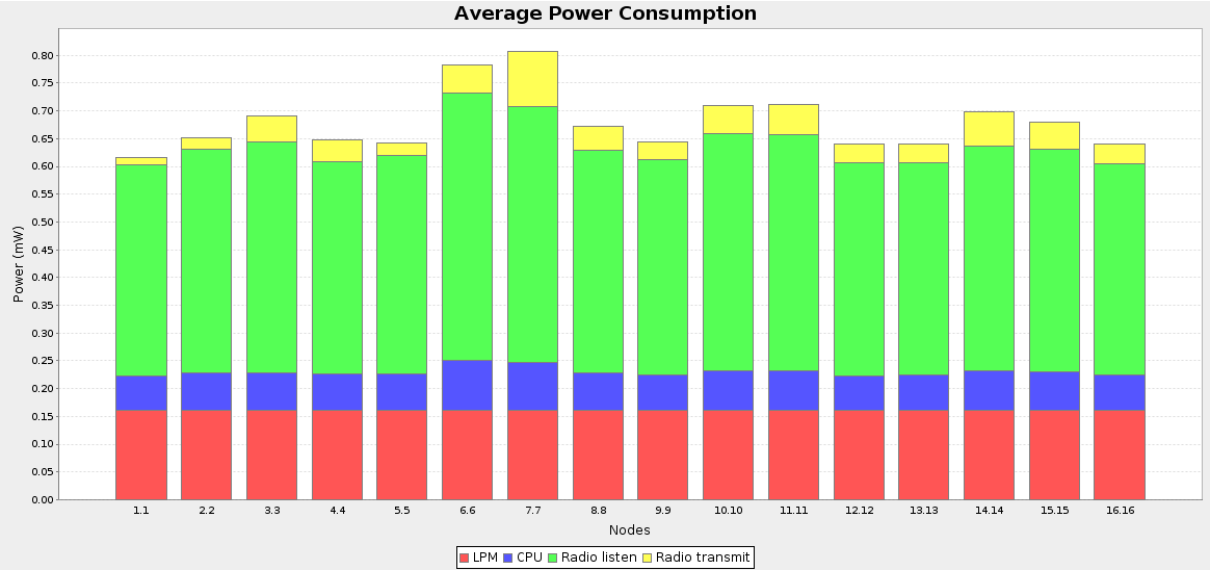
Slika 6.125 Prosječni radni ciklus primopredajnika (17 čvorova, scenarij 1, sa IDS-om)

Slika 6.126 prikazuje potrošnju energije za prvi scenarij mreže sa 17 čvorova uz implementiran IDS.



Slika 6.126 Potrošnja energije (17 čvorova, scenarij 1, sa IDS-om)

Na slici 6.127 prikazana je prosječna potrošnja energije za svaki pojedini čvor u mreži sa 17 čvorova u prvom simuliranom scenariju.



Slika 6.127 Prosječna potrošnja energije (17 čvorova, scenarij 1, sa IDS-om)

Kao i u mreži bez implementiranog IDS-a, nešto veća potrošnja energije zabilježena je na središnjim čvorovima, zbog veće aktivnosti njihovog radio primopredajnika. Međutim, važno je primijetiti da implementacija IDS sustava ne dovodi do značajnog povećanja potrošnje energije u mreži.

Rezultati dobiveni simulacijom prvog scenarija u mreži sa 17 čvorova, uz implementiran IDS sustav pregledno su prikazani u tablici 6.16.

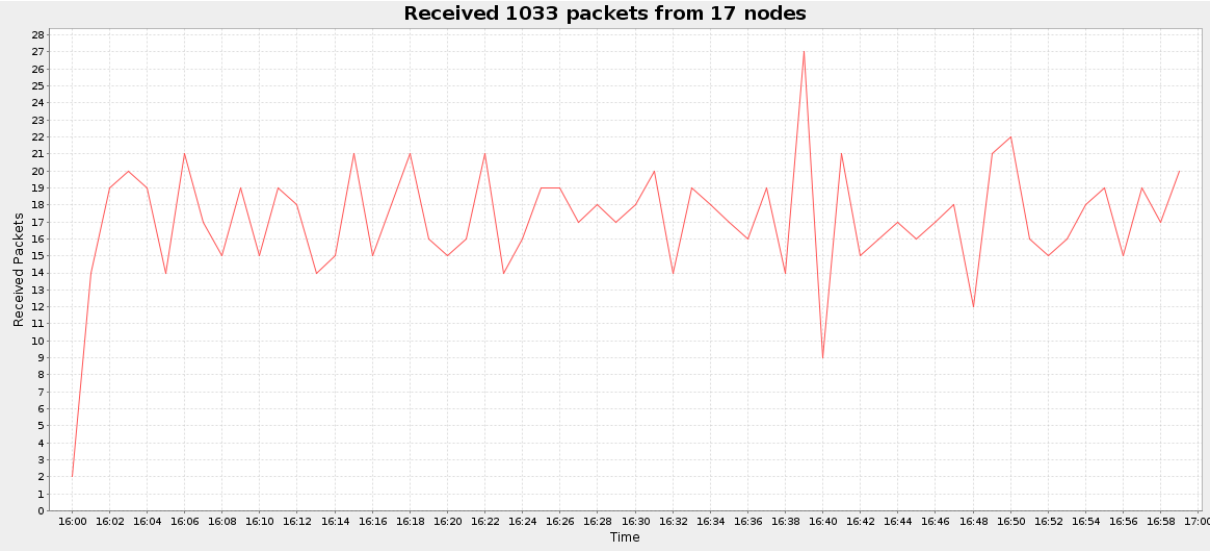
TABLICA 6.16 Mreža sa 17 čvorova, scenarij 1, sa IDS-om

Čvor	Primljeni paketi	Izgubljeni paketi	Skokovi do baze	ETX	Potrošnja energije (mW)					Radni ciklus (%)	
					CPU	LPM	Slušanje	Predaja	Ukupno	Slušanje	Predaja
1	67	0	1.000	1.000	0.060	0.162	0.380	0.015	0.617	0.633	0.028
2	67	0	1.000	1.000	0.067	0.161	0.402	0.022	0.652	0.670	0.042
3	66	0	2.000	1.000	0.068	0.161	0.416	0.045	0.690	0.693	0.085
4	67	0	3.000	1.000	0.064	0.162	0.384	0.039	0.649	0.639	0.074
5	66	0	1.000	1.000	0.065	0.162	0.393	0.021	0.641	0.656	0.040
6	67	0	1.000	1.000	0.091	0.161	0.481	0.051	0.783	0.801	0.097
7	67	0	2.000	1.000	0.086	0.161	0.461	0.098	0.807	0.769	0.185
8	66	0	3.000	1.000	0.067	0.161	0.400	0.044	0.673	0.666	0.084
9	67	0	2.000	1.000	0.063	0.162	0.387	0.033	0.645	0.645	0.063
10	66	0	2.000	1.000	0.070	0.161	0.427	0.050	0.709	0.712	0.094
11	67	0	3.000	1.000	0.070	0.161	0.426	0.054	0.711	0.709	0.102
12	67	0	4.000	1.000	0.061	0.162	0.384	0.032	0.640	0.641	0.061
13	66	0	4.000	1.000	0.062	0.162	0.382	0.034	0.640	0.637	0.065
14	66	0	3.000	1.000	0.071	0.161	0.404	0.063	0.699	0.673	0.119
15	67	0	4.000	1.000	0.069	0.161	0.400	0.050	0.680	0.666	0.094
16	67	0	5.000	1.000	0.062	0.162	0.381	0.035	0.639	0.635	0.065
Prosjek	**66.625**	**0.000**	**2.563**	**1.000**	**0.069**	**0.161**	**0.407**	**0.043**	**0.680**	**0.678**	**0.081**

Scenarij 2 (Rx/Tx=80%)

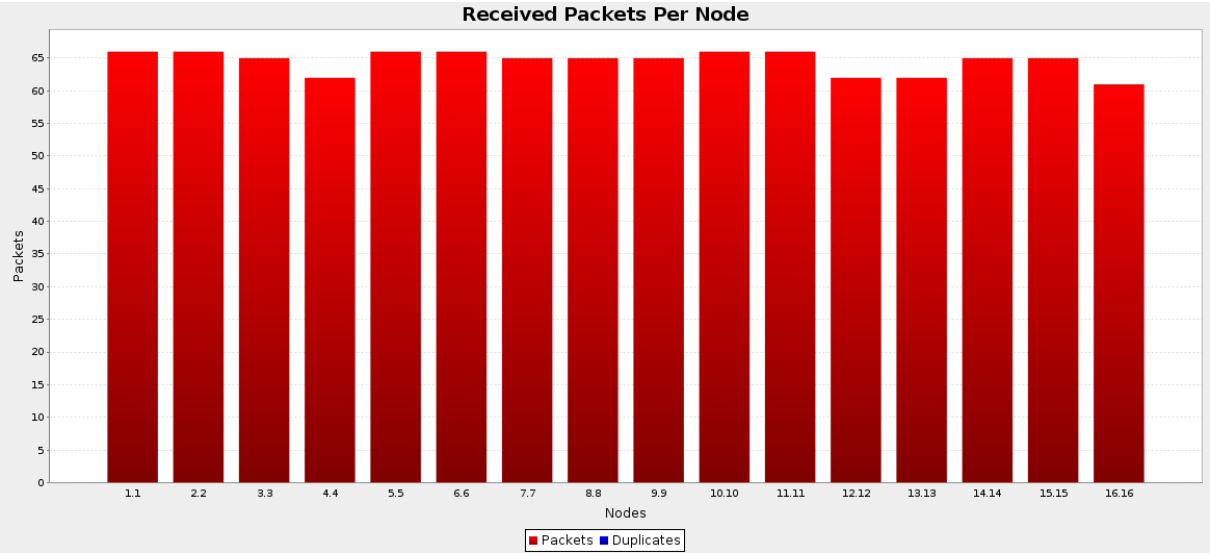
U drugom simuliranom scenariju u istoj mreži (mreža sa 17 čvorova uz implementiranog IDS agenta na svakom od njih) vjerojatnost uspješnog slanja i prijema paketa postavljena je na 80% (analogno drugom simuliranom scenariju u mreži bez IDS sustava).

Slika 6.128 prikazuje primljeni promet u mreži sa 17 čvorova u drugom simuliranom scenariju.



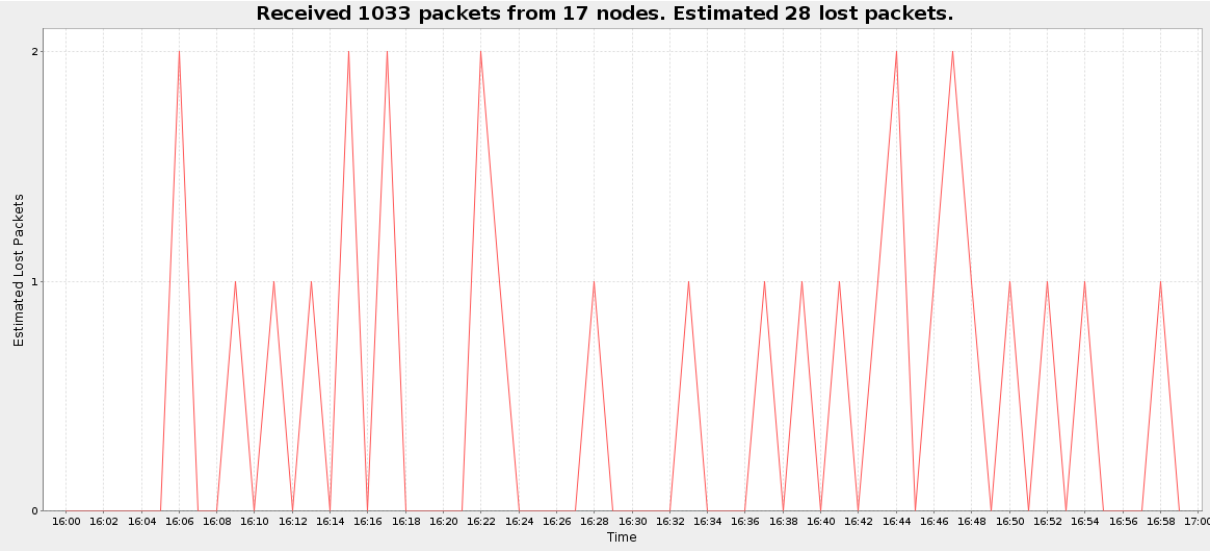
Slika 6.128 Broj primljenih paketa (17 čvorova, scenarij 2, sa IDS-om)

Broj primljenih paketa za svaki pojedinačni čvor dan je na slici 6.129.



Slika 6.129 Broj primljenih paketa za svaki čvor (17 čvorova, scenarij 2, sa IDS-om)

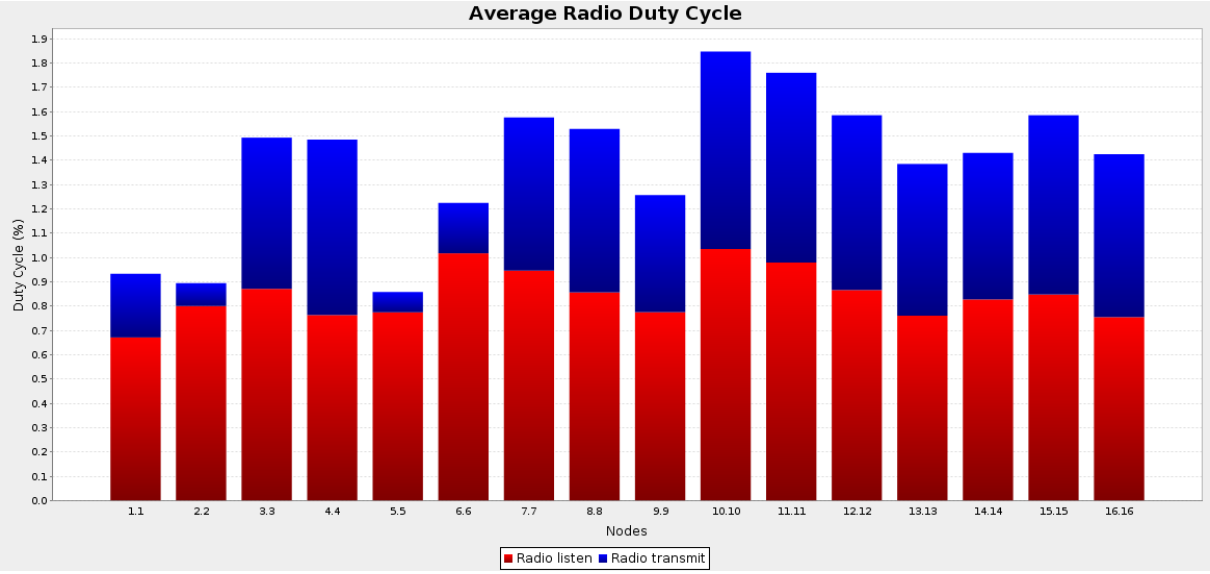
U ovom scenariju jedan dio paketa biva izgubljen, što prikazuje slika 6.130.



Slika 6.130 Izgubljeni paketi (17 čvorova, scenarij 2, sa IDS-om)

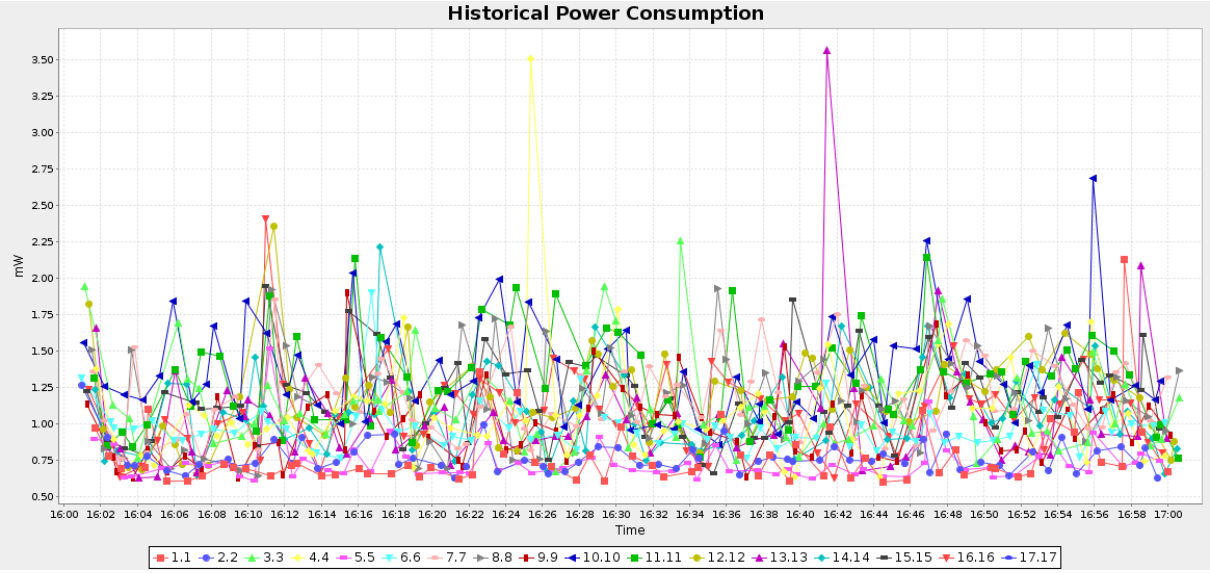
U drugom scenariju dolazi do gubitka određenog dijela paketa, ali i do povećanog broja primljenih paketa u usporedbi sa istim scenarijem u mreži bez IDS sustava (slike 6.72 i 6.73). Ovakav rezultat očekivan je, budući da agenti IDS sustava međusobno razmjenjuju poruke.

Slika 6.131 prikazuje prosječni radni ciklus primopredajnika u mreži sa 17 čvorova u drugom scenariju.



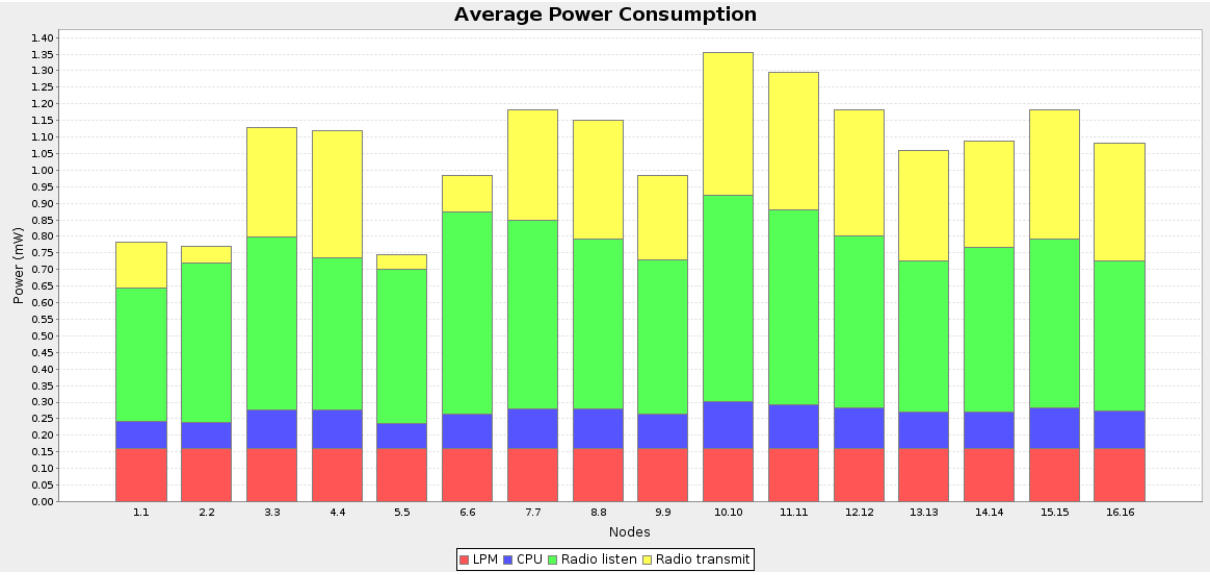
Slika 6.131 Prosječni radni ciklus primopredajnika (17 čvorova, scenarij 2, sa IDS-om)

Slika 6.132 prikazuje potrošnju energije tijekom jednog sata u drugom simuliranom scenariju mreže sa 17 čvorova.



Slika 6.132 Potrošnja energije (17 čvorova, scenarij 2, sa IDS-om)

Slika 6.133 prikazuje prosječnu potrošnju energije za svaki pojedini mrežni čvor.



Slika 6.133 Prosječna potrošnja energije (17 čvorova, scenarij 2, sa IDS-om)

U usporedbi sa prethodnim scenarijima primjećuje se povećanje potrošnje energije zbog povećane aktivnosti primopredajnika, što je posebno izraženo na udaljenijim čvorovima. Međutim, značajno je da u usporedbi sa identičnim scenarijem u mreži bez implementiranog IDS-a (slike 6.77 i 6.78) nema značajnog povećanja potrošnje koja bi bila prouzrokovana radom samog IDS sustava.

U tablici 6.17 pregledno su prikazane vrijednosti dobivene za drugi simulirani scenarij u mreži sa 17 čvorova, uz implementiran IDS sustav.

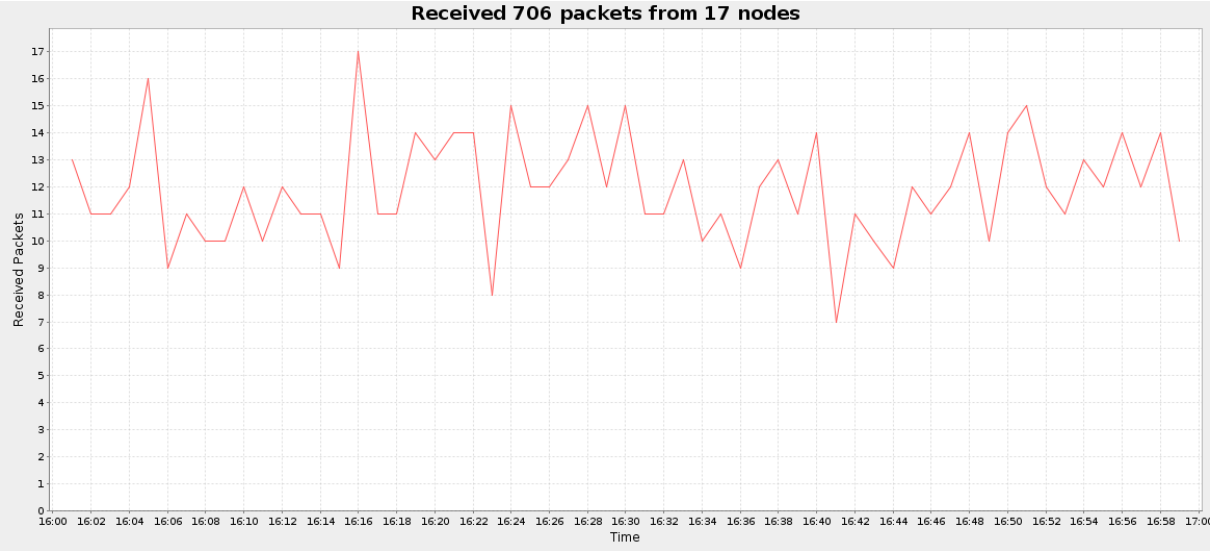
TABLICA 6.17 Mreža sa 17 čvorova, scenarij 2, sa IDS-om

Čvor	Primljeni paketi	Izgubljeni paketi	Skokovi do baze	ETX	Potrošnja energije (mW)					Radni ciklus (%)	
					CPU	LPM	Slušanje	Predaja	Ukupno	Slušanje	Predaja
1	66	0	2.000	1.778	0.080	0.403	0.671	0.139	0.783	0.671	0.262
2	66	0	1.000	1.000	0.079	0.480	0.800	0.050	0.770	0.800	0.095
3	65	2	2.000	2.625	0.116	0.522	0.871	0.330	1.129	0.871	0.622
4	62	4	3.000	2.944	0.117	0.458	0.763	0.383	1.118	0.763	0.722
5	66	0	1.000	1.002	0.073	0.465	0.775	0.044	0.744	0.775	0.083
6	66	0	1.000	1.004	0.102	0.610	1.017	0.110	0.983	1.017	0.207
7	65	1	2.000	2.819	0.120	0.568	0.946	0.334	1.182	0.946	0.630
8	65	2	3.169	1.985	0.119	0.514	0.856	0.357	1.150	0.856	0.672
9	65	1	2.000	2.338	0.103	0.465	0.775	0.256	0.984	0.775	0.482
10	66	0	2.000	2.313	0.143	0.621	1.035	0.431	1.355	1.035	0.812
11	66	1	3.182	2.148	0.134	0.588	0.979	0.414	1.295	0.979	0.780
12	62	5	4.452	1.833	0.122	0.520	0.866	0.382	1.183	0.866	0.719
13	62	4	3.242	2.452	0.110	0.456	0.760	0.332	1.058	0.760	0.624
14	65	2	3.031	2.394	0.110	0.496	0.827	0.320	1.087	0.827	0.603
15	65	1	4.215	2.054	0.122	0.509	0.848	0.392	1.183	0.848	0.738
16	61	5	5.082	1.775	0.112	0.453	0.755	0.356	1.081	0.755	0.670
Prosjek	**64.563**	**1.750**	**2.648**	**2.029**	**0.110**	**0.508**	**0.847**	**0.289**	**1.068**	**0.847**	**0.545**

Scenarij 3 (Rx/Tx=60%)

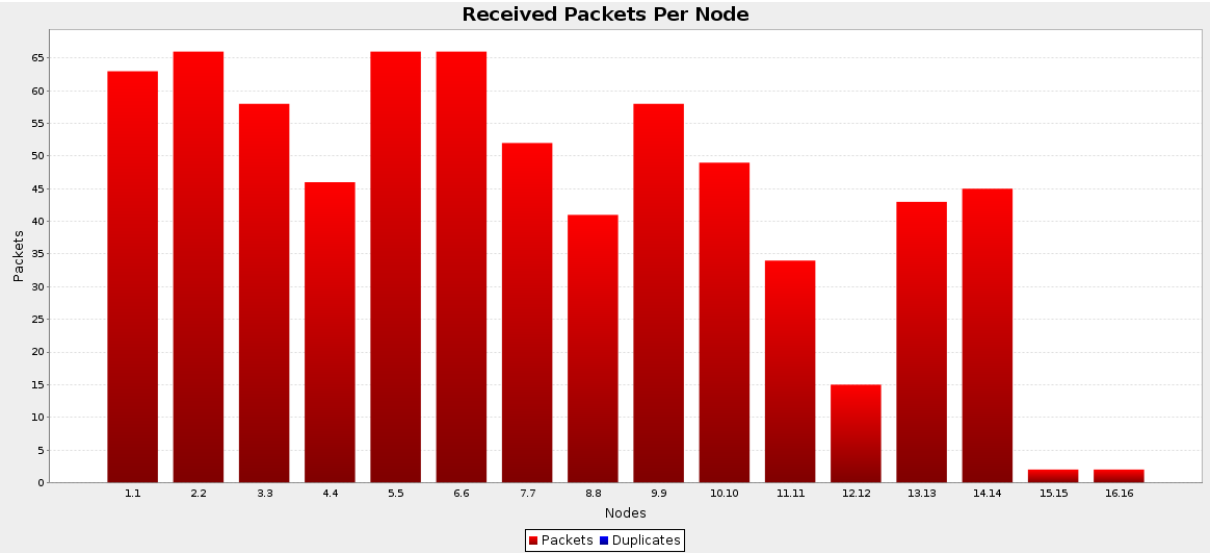
Treći simulirani scenarij u mreži sa 17 čvorova podrazumijeva vjerojatnost uspješnog slanja i prijema paketa od 60% uz implementiran IDS sustav. Po ostalim parametrima ne razlikuje se od prethodna dva scenarija.

Slika 6.134 prikazuje primljene pakete u mreži sa 17 čvorova za simulirani treći scenarij u trajanju od jednog sata.



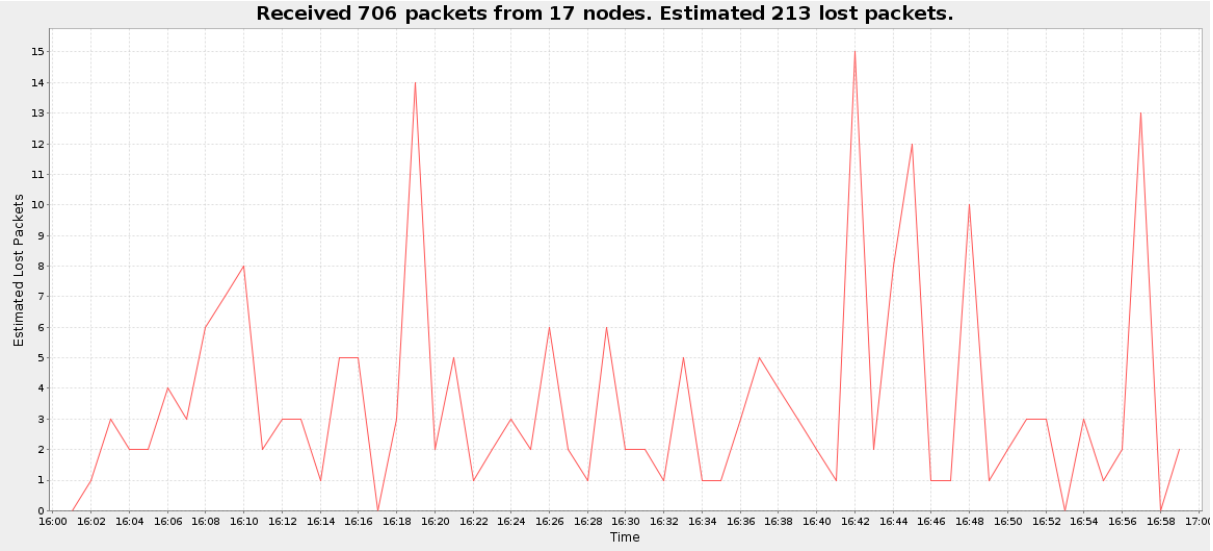
Slika 6.134 Broj primljenih paketa (17 čvorova, scenarij 3, sa IDS-om)

Na slici 6.135 prikazan je broj primljenih paketa za svaki pojedinačni čvor.



Slika 6.135 Broj primljenih paketa za svaki čvor (17 čvorova, scenarij 3, sa IDS-om)

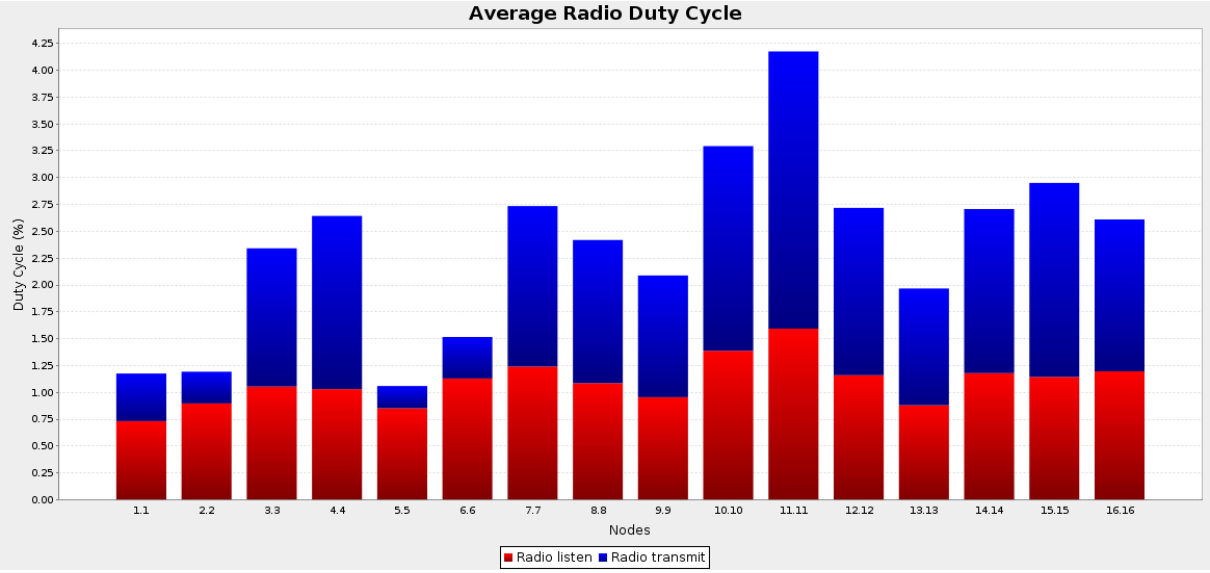
Na slici 6.136 prikazana je procjena gubitaka paketa u trećem scenariju mreže sa 17 čvorova.



Slika 6.136 Izgubljeni paketi (17 čvorova, scenarij 3, sa IDS-om)

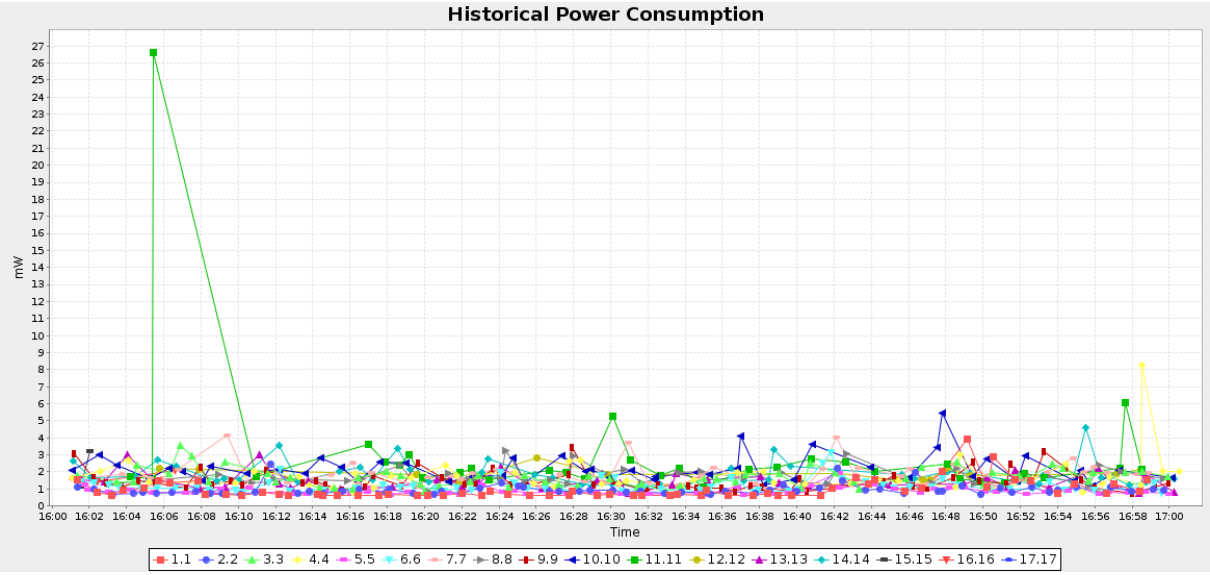
U odnosu na prethodne scenarije zamjetan je porast broja izgubljenih paketa, što je i očekivano s obzirom na smanjenu vjerojatnost uspješnog slanja i prijema paketa. Međutim u usporedbi sa istim scenarijem u mreži bez implementiranog IDS-a (slike 6.79 i 6.80), primjećuje se porast broja primljenih paketa. Najviše gubitaka zabilježeno je za čvorove koji su više skokova udaljeni od bazne stanice (tako je primjerice sa čvorova 15 i 16 primljeno samo po dva paketa).

Slika 6.137 prikazuje radne cikluse primopredajnika svih čvorova u trećem scenariju mreže sa 17 čvorova.



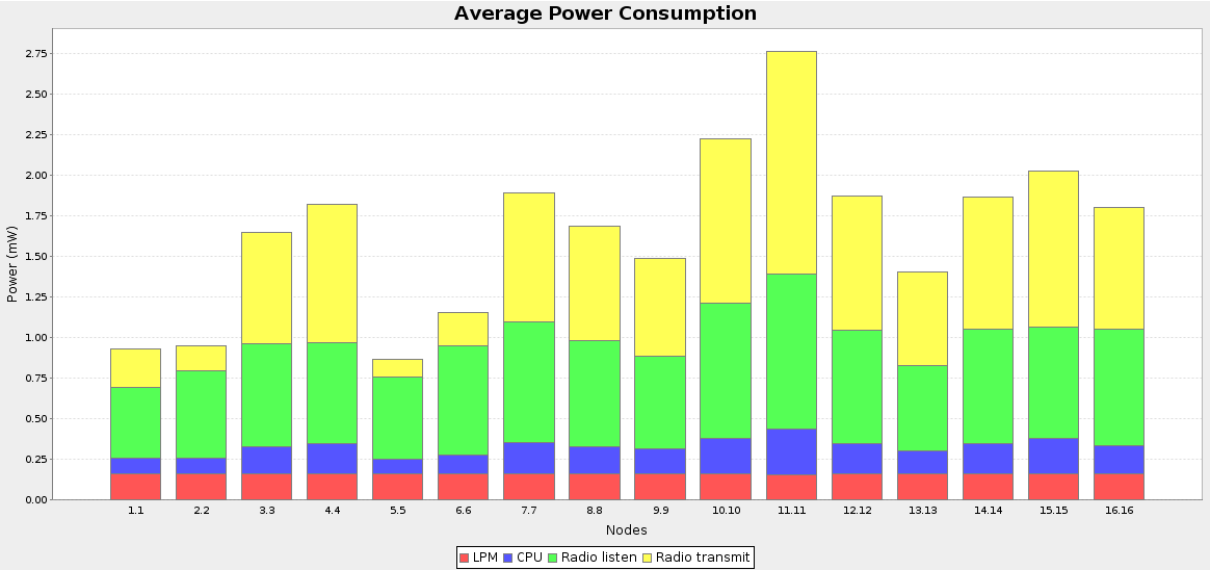
Slika 6.137 Prosječni radni ciklus primopredajnika (17 čvorova, scenarij 3, sa IDS-om)

Slika 6.138 prikazuje potrošnju energije u mreži kroz razdoblje od jednog sata.



Slika 6.138 Potrošnja energije (17 čvorova, scenarij 3, sa IDS-om)

Na slici 6.139 prikazana je prosječna potrošnja energije za svaki pojedini čvor.



Slika 6.139 Prosječna potrošnja energije (17 čvorova, scenarij 3, sa IDS-om)

Moguće je primijetiti značajan porast potrošnje energije u odnosu na prethodne scenarije, ponajviše na račun značajnog povećanja udjela potrošnje predajnika u stanju aktivne predaje. Međutim, usporedba sa istim scenarijem u mreži bez IDS sustava (slike 6.84 i 6.85) pokazuje da potrošnja nije u većoj mjeri porasla zbog implementacije IDS agenata.

Tablica 6.18 pregledno prikazuje dobivene vrijednosti za treći simulirani scenarij u mreži sa 17 čvorova uz implementiran IDS sustav.

TABLICA 6.18 Mreža sa 17 čvorova, scenarij 3, sa IDS-om

Čvor	Primljeni paketi	Izgubljeni paketi	Skokovi do baze	ETX	Potrošnja energije (mW)					Radni ciklus (%)	
					CPU	LPM	Slušanje	Predaja	Ukupno	Slušanje	Predaja
1	63	2	1.397	2.917	0.094	0.161	0.439	0.236	0.929	0.732	0.444
2	66	0	1.000	1.163	0.094	0.161	0.538	0.157	0.950	0.896	0.296
3	58	8	2.034	7.892	0.170	0.158	0.632	0.684	1.645	1.054	1.288
4	46	21	3.065	8.505	0.190	0.158	0.618	0.857	1.822	1.030	1.614
5	66	0	1.000	1.142	0.086	0.161	0.511	0.109	0.868	0.852	0.206
6	66	0	1.000	1.108	0.113	0.160	0.678	0.205	1.155	1.129	0.386
7	52	13	2.019	7.870	0.193	0.158	0.744	0.794	1.889	1.240	1.495
8	41	23	3.049	7.436	0.170	0.158	0.651	0.708	1.688	1.086	1.334
9	58	8	2.017	8.302	0.154	0.159	0.573	0.602	1.487	0.955	1.134
10	49	17	2.000	8.518	0.223	0.157	0.833	1.012	2.224	1.388	1.906
11	34	28	3.000	7.353	0.280	0.155	0.956	1.371	2.763	1.593	2.582
12	15	45	4.000	7.600	0.190	0.158	0.696	0.828	1.871	1.160	1.559
13	43	23	3.023	8.023	0.142	0.159	0.528	0.577	1.406	0.880	1.087
14	45	21	3.000	6.967	0.187	0.158	0.707	0.812	1.864	1.179	1.529
15	2	0	4.000	1.813	0.223	0.157	0.686	0.960	2.025	1.144	1.808
16	2	4	5.000	4.813	0.173	0.158	0.718	0.751	1.800	1.196	1.414
Prosjek	**44.125**	**13.313**	**2.538**	**5.714**	**0.168**	**0.158**	**0.657**	**0.666**	**1.649**	**1.095**	**1.255**

6.6.4. Testiranje performansi sustava – pregled

Potpoglavlje 6.6.4 daje sumarni pregled rezultata testiranja performansi IDS sustava i njegovog utjecaja na normalan rad mreže (dobiven usporedbom istih scenarija, sa i bez implementiranog IDS sustava) koji su detaljno prikazani i analizirani u poglavljima 6.5 i 6.6 kroz 9 različitih simuliranih scenarija (po 3 karakteristična scenarija u svakoj od 3 različite mreže). Važno je napomenuti da dobivene vrijednosti nisu rezultat preciznih laboratorijskih mjerenja, nego tek procjena na temelju određenih softverskih modela implementiranih u sam simulator. Također, sam postupak simulacije temeljen je na stohastičkim algoritmima, te je gotovo nemoguće uzastopnim ponavljanjem simulacijskog postupka, čak i uz iste početne parametre, dobiti identične rezultate. Zbog toga prikazane vrijednosti ne treba smatrati apsolutno točnim i preciznim, nego treba prihvatiti mogućnost određenih odstupanja. Međutim, unatoč tome ove vrijednosti predstavljaju dobar pokazatelj ponašanja cjelokupne mreže, te omogućavaju praćenje promjena u mreži do kojih dolazi uslijed promjena nekih njezinih parametara.

U tablici 6.19 prikazane su prosječne vrijednosti promatranih parametara dobivene simulacijama u mreži sa 6 čvorova. Tablica prikazuje vrijednosti dobivene simulacijom za tri karakteristična scenarija, i to usporedno prije i nakon implementacije IDS-a.

TABLICA 6.19 Pregled rezultata za mrežu sa 6 čvorova - prosječne vrijednosti

6 čvorova	Primljeni paketi	Izgubljeni paketi	Skokovi do baze	ETX	Potrošnja energije (mW)					Radni ciklus (%)	
					CPU	LPM	Slušanje	Predaja	Ukupno	Slušanje	Predaja
Scenarij 1 (Rx/Tx=100%)											
Bez IDS-a	59.200	0.000	1.600	1.008	0.065	0.162	0.391	0.033	0.650	0.651	0.062
Sa IDS-om	65.800	0.000	1.600	1.002	0.064	0.162	0.389	0.029	0.649	0.649	0.054
Scenarij 2 (Rx/Tx=80%)											
Bez IDS-a	58.400	0.600	1.600	2.256	0.083	0.161	0.419	0.146	0.808	0.699	0.274
Sa IDS-om	65.800	0.600	1.600	2.057	0.083	0.161	0.423	0.138	0.806	0.706	0.260
Scenarij 3 (Rx/Tx=60%)											
Bez IDS-a	50.600	7.000	1.629	5.991	0.135	0.159	0.514	0.484	1.292	0.857	0.912
Sa IDS-om	57.800	8.800	1.600	5.793	0.134	0.159	0.521	0.498	1.312	0.868	0.938

U prvom simuliranom scenariju, koji predstavlja idealan slučaj u kojem nema gubitaka paketa, primjećuje se porast broja primljenih paketa nakon implementacije IDS-a, što je i očekivano, budući da dodatni promet generiraju IDS agenti. Međutim, važno je primijetiti da nema značajne promjene u ukupnoj potrošnji energije (koja je najstrožije ograničeni resurs u BSM) nakon implementacije IDS sustava u mrežu (minimalna odstupanja u zabilježenim vrijednostima mogu se protumačiti primjenom stohastičkih algoritama i nemogućnošću precizne procjene realne potrošnje).

U drugom scenariju (u kojem je vjerojatnost uspješnog slanja i prijema paketa postavljena na 80%) unatoč mehanizmima potvrde i retransmisije dolazi do manjih gubitaka paketa. Povećanje prosječne ETX vrijednosti u odnosu na prvi scenarij pokazatelj je da u mreži dolazi do retransmisije određenog broja paketa. Potreba za retransmisijom paketa dovodi do povećane aktivnosti primopredajnika, što je vidljivo iz njihovog radnog ciklusa. Budući da je primopredajnik energetski najzahtjevnija komponenta senzorskog čvora, njegova povećana aktivnost dovodi i do povećanja potrošnje energije u odnosu na prvi scenarij. Međutim, i u ovom slučaju sama implementacija IDS sustava ne unosi značajnu razliku u potrošnji energije.

Treći scenarij zbog dodatno smanjene vjerojatnosti uspješnog prijenosa paketa (na 60%) dodatno povećava potrebu za retransmisijom (pokazatelj je ETX metrika), što također dovodi i do dodatnog povećanja potrošnje. Unatoč retransmisiji, bilježi se i povećan broj izgubljenih

paketa. U trećem scenariju sa implementiranim IDS sustavom bilježi se i blago povećanje ukupne prosječne potrošnje u odnosu na slučaj bez IDS-a.

U tablici 6.20 prikazane su prosječne vrijednosti promatranih parametara za analizirane scenarije u mreži sa 10 čvorova (slučajevi bez IDS sustava i s njim, usporedno).

TABLICA 6.20 Pregled rezultata za mrežu sa 10 čvorova - prosječne vrijednosti

10 čvorova	Primljeni paketi	Izgubljeni paketi	Skokovi do baze	ETX	Potrošnja energije (mW)					Radni ciklus (%)	
					CPU	LPM	Slušanje	Predaja	Ukupno	Slušanje	Predaja
Scenarij 1 (Rx/Tx=100%)											
Bez IDS-a	62.222	0.000	1.667	1.000	0.064	0.162	0.392	0.029	0.647	0.654	0.055
Sa IDS-om	67.444	0.000	1.667	1.000	0.065	0.162	0.394	0.032	0.652	0.657	0.060
Scenarij 2 (Rx/Tx=80%)											
Bez IDS-a	58.667	1.222	1.690	1.766	0.081	0.161	0.431	0.133	0.806	0.718	0.250
Sa IDS-om	65.889	0.667	2.079	1.914	0.098	0.161	0.473	0.219	0.951	0.789	0.412
Scenarij 3 (Rx/Tx=60%)											
Bez IDS-a	51.889	7.333	1.692	5.148	0.122	0.160	0.527	0.409	1.218	0.878	0.770
Sa IDS-om	50.556	10.556	1.718	4.554	0.134	0.159	0.544	0.478	1.315	0.907	0.899

I u mreži sa 10 čvorova, analogno prethodnoj mreži, prvi scenarij predstavlja „idealni“ slučaj, bez gubitaka. U tom slučaju nema potrebe za retransmisijama paketa i nema izgubljenih paketa. Implementacija IDS sustava uvodi u mrežu malu količinu dodatnog prometa, no to u ovom slučaju ne povećava značajno ukupnu potrošnju. Ukupna prosječna potrošnja u prvom scenariju mreže sa 10 čvorova usporediva je s potrošnjom u ekvivalentnom scenariju mreže sa 6 čvorova.

Smanjenjem vjerojatnosti uspješnog prijenosa paketa u drugom scenariju javlja se potreba za retransmisijom određenog broja paketa, a počinju se javljati i gubici. Povećana aktivnost primopredajnika dovodi i do povećanja potrošnje energije (koja je usporediva sa potrošnjom u drugom scenariju u mreži sa 6 čvorova). Nakon implementacije IDS-a zabilježeno je blago povećanje prosječne potrošnje, no ne u tolikoj mjeri da implementacija IDS-a ne bi bila opravdana.

Dodatnim smanjenjem vjerojatnosti uspješnog prijenosa paketa u trećem scenariju povećava se i broj nužnih retransmisija (pokazatelj je ETX metrika), što se odražava i na povećanje prosječne potrošnje energije zbog povećane aktivnosti primopredajnika. Sa implementiranim IDS-om u mreži zabilježena je nešto veća prosječna potrošnja nego bez njega, no povećanje je manje od 10% i ne dovodi u pitanje opravdanost implementacije IDS sustava.

Tablica 6.21 prikazuje rezultate dobivene analizom triju karakterističnih scenarija u mreži sa 17 čvorova (usporedno su prikazane vrijednosti za slučajeve sa i bez implementiranog IDS sustava).

TABLICA 6.21 Pregled rezultata za mrežu sa 17 čvorova - prosječne vrijednosti

17 čvorova	Primljeni paketi	Izgubljeni paketi	Skokovi do baze	ETX	Potrošnja energije (mW)					Radni ciklus (%)	
					CPU	LPM	Slušanje	Predaja	Ukupno	Slušanje	Predaja
Scenarij 1 (Rx/Tx=100%)											
Bez IDS-a	59.500	0.000	2.563	1.001	0.068	0.161	0.405	0.042	0.676	0.675	0.079
Sa IDS-om	66.625	0.000	2.563	1.000	0.069	0.161	0.407	0.043	0.680	0.678	0.081
Scenarij 2 (Rx/Tx=80%)											
Bez IDS-a	58.375	1.250	2.582	2.001	0.108	0.160	0.502	0.276	1.047	0.837	0.520
Sa IDS-om	64.563	1.750	2.648	2.029	0.110	0.508	0.847	0.289	1.068	0.847	0.545
Scenarij 3 (Rx/Tx=60%)											
Bez IDS-a	44.267	13.867	2.366	5.574	0.160	0.159	0.644	0.605	1.568	1.073	1.140
Sa IDS-om	44.125	13.313	2.538	5.714	0.168	0.158	0.657	0.666	1.649	1.095	1.255

Kao i u slučaju mreža sa 6 i 10 čvorova, i u prvom simuliranom scenariju mreže sa 17 čvorova nema gubitaka paketa niti potreba za retransmisijama („idealan“ slučaj). Također, nema niti značajne razlike u potrošnji energije u slučaju kada je u mrežu implementiran IDS sustav u odnosu na isti scenarij bez njega.

U drugom scenariju smanjenjem vjerojatnosti uspješnog prijenosa paketa pojavljuju se gubici, a retransmisija paketa povećava prosječnu potrošnju energije. Prosječna potrošnja energije nešto je veća nego u ekvivalentnom scenariju u mrežama s manjim brojem čvorova (6 i 10), no niti u ovom scenariju implementacija IDS sustava ne dovodi do značajnijeg povećanja prosječne potrošnje energije.

Treći scenarij u mreži sa 17 čvorova bilježi najveće gubitke i najveći broj retransmisija, a time i najmanji broj uspješno primljenih paketa. Štoviše, u jednom simuliranom scenariju zbog prevelikih gubitaka paketa najudaljeniji čvor čak nije niti uspio uspostaviti komunikaciju sa baznom stanicom (od bazne stanice bio je udaljen pet skokova). Očekivano, u trećem scenariju mreže sa 17 čvorova zabilježena je i najveća potrošnja energije. Međutim, čak niti u ovom scenariju prosječna potrošnja energije nije značajno porasla nakon implementacije IDS sustava.

Provedeni simulacijski postupci i analize pokazale su da implementacija predloženog rješenja sustava za otkrivanje zlonamjernog ponašanja senzorskih čvorova u IPv6-temeljenu BSM ne dovodi do primjetne degradacije njezinih performansi. Također, od velike je važnosti

činjenica da implementacija ovog sustava ne dovodi do značajnog povećanja potrošnje energije, kao najstrože ograničenog resursa BSM. Štoviše, u nekim simuliranim scenarijima razlika u potrošnji je gotovo neprimjetna (jer je po iznosu manja od mogućih pogrešaka koje se mogu očekivati prilikom procjene potrošnje višestrukim izvođenjem simulacije), dok u drugim scenarijima ne prelazi nekoliko postotaka.

Energetska učinkovitost, odnosno vrlo mali dodatni zahtjevi za energijom, predstavljaju jedan od dva najvažnija preduvjeta koja sustav za otkrivanje zlonamjernih čvorova u mreži mora zadovoljavati da bi se uopće mogla razmatrati mogućnost njegove praktične primjene i implementacije u stvarnu BSM. Drugi važan preduvjet jest njegova sposobnost uspješne detekcije zlonamjernih čvorova. Zbog toga u poglavlju 6.7 slijedi analiza uspješnosti detekcije zlonamjernih čvorova za predloženi IDS sustav.

6.7. Testiranje uspješnosti otkrivanja zlonamjernog ponašanja u mreži

Analiza uspješnosti otkrivanja zlonamjernog ponašanja senzorskih čvorova u IPv6-temeljenoj BSM za predloženi IDS sustav provedena je (slično kao i analiza njegovih performansi) u tri prethodno opisane mreže, sa 6, 10 i 17 čvorova. U svakoj od ovih mreža uspješnost detekcije testirana je u sva tri karakteristična scenarija (kao i prilikom testiranja performansi sustava). U prvom scenariju vjerojatnost uspješnog slanja i prijema paketa iznosi 100% („idealan“ slučaj, bez gubitaka), u drugom ta vjerojatnost iznosi 80%, a u trećem 60%. Važno je sustav testirati u ovakvim scenarijima u kojima uzrok odbacivanja paketa nije isključivo zlonamjerna aktivnost, nego do gubitka paketa dolazi i prilikom uobičajenog rada mreže, primjerice zbog smetnji i kolizija, budući da je u tom slučaju otežano razlučivanje zlonamjernog ponašanja.

Za potrebe testiranja uspješnosti detekcije IDS sustava u svakom analiziranom scenariju u mrežu je namjerno postavljen jedan zlonamjerni čvor (radi pojednostavljenja maksimalni broj zlonamjernih čvorova u mreži ograničen je na jedan). Taj zlonamjerni čvor selektivno prosljeđuje pakete na način da za 20% paketa koje treba proslijediti to doista i učini, dok 80% paketa odbacuje. U svakom scenariju razmatrana su dva slučaja. U prvom slučaju zlonamjerni čvor na opisani način selektivno prosljeđuje pakete (80% odbacuje, 20% prosljeđuje), dok u drugom slučaju osim što selektivno prosljeđuje pakete on za isti postupak lažno optužuje svoje susjede, i time IDS sustavu namjerno otežava ispravnu detekciju.

Karakteristično za predloženi IDS sustav jest da on osim što pojedini čvor može okarakterizirati kao zlonamjerni ili dobronamjerni, on procjenjuje i vjerojatnost njegove malicioznosti (na način podrobnije opisan u poglavlju 6.4). Za potrebe testiranja granična vjerojatnost iznad koje se čvor smatra zlonamjernim iznosi 50%, iako se ovaj prag može prilikom implementacije sustava u stvarnu mrežu prilagoditi konkretnoj aplikaciji. U tablicama koje slijede po recima su dane odgovarajuće procjene zlonamjernosti koje svaki čvor daje za svoje susjede, a u posljednjem retku su konačne procjene zlonamjernosti za svaki stupac. Zasivljene ćelije znače da čvorovi nisu susjedi, pa prema tome nema niti procijenjenih vjerojatnosti zlonamjernog ponašanja. Cilj analize jest utvrditi utjecaj različitih faktora poput broja čvorova, količine odbačenih paketa i ponašanja samog zlonamjernog čvora na uspješnost detekcije zlonamjernog ponašanja.

6.7.1. Otkrivanje zlonamjernog ponašanja u mreži sa 6 čvorova

U mreži sa 6 čvorova (topologija je ista kao i prilikom testiranja performansi sustava, slika 6.11) zlonamjeran je čvor 3. U tablici 6.22 prikazane su procijenjene vjerojatnosti zlonamjernog ponašanja za prvi scenarij (Rx/Tx=100%) u mreži sa 6 čvorova.

TABLICA 6.22 Detekcija u mreži sa 6 čvorova, scenarij 1

	2	**3**	**4**	**5**	**6**
2			0.0	0.0	
3				0.0	0.0
4	0.0				
5	0.0	80.3			
6		80.3			
$p_M(\%)$	0.0	**80.3**	0.0	0.0	0.0

U ovom slučaju IDS sustav bez poteškoća ispravno zaključuje da je zlonamjeran čvor 3, uz procijenjenu vjerojatnost od 80.3%. U tablici 6.23 prikazane su procijenjene vjerojatnosti u istoj mreži (scenarij 1) u slučaju kada zlonamjerni čvor (čvor 3) dodatno lažno optužuje svoje susjede za zlonamjerno ponašanje.

TABLICA 6.23 Detekcija u mreži sa 6 čvorova, scenarij 1 (uz lažno optuživanje susjeda)

	2	**3**	**4**	**5**	**6**
2			0.0	0.0	
3				80.3	80.3
4	0.0				
5	0.0	80.3			
6		80.3			
$p_M(\%)$	0.0	**80.3**	0.0	**80.3**	**80.3**

U ovoj situaciji postoje čak tri čvora sa jednakom procijenjenom vjerojatnosti da su zlonamjerni (čvorovi 3, 5 i 6), odnosno za koje procijenjena vjerojatnost prelazi postavljeni

prag od 50% (i iznosi 80.3%). Unatoč tome, i u ovoj situaciji IDS sustav ipak može ispravno zaključiti da je zlonamjeran čvor 3, budući da jedino za njega postoje dvije procjene koje prelaze prag (od strane čvorova 5 i 6), dok za čvorove 5 i 6 postoji samo po jedna takva procjena. Međutim, vidljivo je da lažne procjene od strane zlonamjernog čvora mogu značajno zakomplicirati postupak detekcije pa čak u konačnici dovesti i do krivih zaključaka.

U tablici 6.24 prikazane su procijenjene vjerojatnosti za drugi scenarij u mreži sa 6 čvorova (Rx/Tx=80%).

TABLICA 6.24 Detekcija u mreži sa 6 čvorova, scenarij 2

	2	**3**	**4**	**5**	**6**
2			0.0	1.5	
3				1.5	3.0
4	0.0				
5	0.0	79.1			
6		77.9			
$p_M(\%)$	0.0	**78.5**	0.0	1.5	3.0

Iz tablice se vidi da je detekcija u ovom scenariju uspješna (procijenjena vjerojatnost da je čvor 3 zlonamjeran iznosi 78.5%). Međutim, vidljivo je da dodatni gubici paketa koji postoje u ovom scenariju uzrokuju da je procijenjena vjerojatnost za zlonamjerni čvor nešto manja nego u prvom scenariju (idealni slučaj), a pojavljuju se i određene vjerojatnosti da su i neki od preostalih čvorova zlonamjerni.

Tablica 6.25 prikazuje detekciju u drugom scenariju mreže sa 6 čvorova, u slučaju kada čvor 3 dodatno lažno optužuje svoje susjede.

TABLICA 6.25 Detekcija u mreži sa 6 čvorova, scenarij 2 (uz lažno optuživanje susjeda)

	2	**3**	**4**	**5**	**6**
2			0.0	1.5	
3				82.1	83.3
4	0.0				
5	0.0	79.1			
6		77.9			
$p_M(\%)$	0.0	**78.5**	0.0	41.8	**83.3**

Iz tablice 6.25 vidljivo je da postoje dvije procjene koje prelaze prag (za čvor 3 i čvor 6), te se ispravna odluka donosi tek na osnovu činjenice da za čvor 3 postoje dvije procjene koje prelaze prag, dok za čvor 6 postoji samo jedna.

Tablica 6.26 prikazuje postupak otkrivanja zlonamjernog čvora u trećem scenariju mreže sa 6 čvorova (Rx/Tx=60%).

TABLICA 6.26 Detekcija u mreži sa 6 čvorova, scenarij 3

	2	**3**	**4**	**5**	**6**
2			22.4	21.5	
3				21.5	22.4
4	0.0				
5	0.0	63.2			
6		62.6			
$p_M(\%)$	0.0	**62.9**	22.4	21.5	22.4

Iz tablice 6.26 vidljivo je da sustav donosi ispravnu odluku, te čvor 3 proglašava zlonamjernim. Međutim, također je vidljivo da se zbog dodatno povećanih gubitaka paketa u mreži (vjerojatnost ispravnog prijenosa smanjena na 60%) kvaliteta procjene (vjerojatnost) smanjuje (na 62.9%), dok se istovremeno povećavaju krivo procijenjene vjerojatnosti (za čvorove koji nisu zlonamjerni), koje u ovom slučaju još uvijek ne prelaze prag.

U tablici 6.27 prikazani su rezultati za isti scenarij, ali u slučaju da zlonamjerni čvor namjerno unosi lažne informacije i krivo optužuje svoje susjede.

TABLICA 6.27 Detekcija u mreži sa 6 čvorova, scenarij 3 (uz lažno optuživanje susjeda)

	2	**3**	**4**	**5**	**6**
2			22.4	21.5	
3				85.1	85.1
4	0.0				
5	0.0	63.2			
6		62.6			
p_M(%)	0.0	**62.9**	22.4	**53.3**	**85.1**

Iz tablice 6.27 vidljivo je da procijenjene vjerojatnosti za čak tri čvora prelaze prag od 50% (čvorovi 3, 5 i 6), te da se ispravna odluka i u ovom slučaju može donijeti tek na temelju činjenice da za čvor 3 postoje dva „glasa“ (od čvorova 5 i 6) koji prelaze prag.

6.7.2. Otkrivanje zlonamjernog ponašanja u mreži sa 10 čvorova

U mreži sa 10 čvorova za potrebe testiranja sposobnosti detekcije zlonamjerno ponašanje pokazuje čvor 8. Testiranje je također provedeno za sva tri karakteristična scenarija. Tablica 6.28 prikazuje postupak procjene zlonamjernosti u prvom scenariju (Rx/Tx=100%).

TABLICA 6.28 Detekcija u mreži sa 10 čvorova, scenarij 1

	1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**
1		0.0		0.0					
2	0.0		0.0		0.0				
3		0.0				0.0			
4	0.0				0.0		0.0		
5		0.0		0.0		0.0		80.1	
6			0.0		0.0				0.0
7				0.0				80.1	
8					0.0		0.0		0.0
9						0.0		80.1	
p_M(%)	0.0	0.0	0.0	0.0	0.0	0.0	0.0	**80.1**	0.0

U ovom slučaju IDS sustav ispravno prepoznaje zlonamjerni čvor (čvor 8) uz procijenjenu vjerojatnost od 80.1%.

U tablici 6.28 prikazan je postupak detekcije u istom scenariju, ali u slučaju kada zlonamjerni čvor namjerno umeće lažne informacije u mrežu optužujući svoje susjede za zlonamjerno ponašanje.

TABLICA 6.29 Detekcija u mreži sa 10 čvorova, scenarij 1 (uz lažno optuživanje susjeda)

	1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**
1		0.0		0.0					
2	0.0		0.0		0.0				
3		0.0				0.0			
4	0.0				0.0		0.0		
5		0.0		0.0		0.0		80.1	
6			0.0		0.0				0.0
7				0.0				80.1	
8					80.6		80.6		80.1
9						0.0		80.1	
$p_M(\%)$	0.0	0.0	0.0	0.0	20.2	0.0	40.1	**80.1**	40.1

Iz tablice 6.29 se vidi da je zaključivanje IDS sustava i u ovom slučaju ispravno, međutim pojavljuju se i procjenjene vjerojatnosti zlonamjernog ponašanja za neke druge čvorove (zbog lažnih optužbi zlonamjernog čvora) koje u ovom slučaju još ne prelaze postavljeni prag.

Tablica 6.30 prikazuje postupak otkrivanja zlonamjernog ponašanja u drugom scenariju mreže sa 10 čvorova (Rx/Tx=80%).

TABLICA 6.30 Detekcija u mreži sa 10 čvorova, scenarij 2

	1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**
1		0.0		0.0					
2	0.0		1.5		0.0				
3		1.5				1.5			
4	0.0				0.0		0.0		
5		0.0		0.0		0.0		80.6	
6			1.5		0.0				4.5
7				0.0				80.6	
8					0.0		0.0		4.5
9						4.5		79.8	
$p_M(\%)$	0.0	0.5	1.5	0.0	0.0	2.0	0.0	**80.3**	4.5

Iz tablice je vidljivo da će IDS sustav ispravno prepoznati zlonamjerno ponašanje čvora 8, iako će se u ovom slučaju (zbog gubitaka određenog broja paketa) pojaviti i vjerojatnosti da su i neki drugi čvorovi zlonamjerni. Međutim, ove vjerojatnosti su po svojim iznosima daleko ispod postavljenog praga od 50%, a po svojem iznosu manje su i od procjenjenih vjerojatnosti u drugom scenariju mreže sa 6 čvorova, budući da u mreži sa većim brojem čvorova svaki čvor u prosjeku ima više susjeda, pa su i konačne procjene točnije.

Tablica 6.31 prikazuje isti scenarij, ali slučaj u kojem zlonamjerni čvor lažno optužuje svoje susjede.

TABLICA 6.31 Detekcija u mreži sa 10 čvorova, scenarij 2 (uz lažno optuživanje susjeda)

	1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**
1		0.0		0.0					
2	0.0		1.5		0.0				
3		1.5				1.5			
4	0.0				0.0		0.0		
5		0.0		0.0		0.0		80.6	
6			1.5		0.0				4.5
7				0.0				80.6	
8					83.6		83.6		81.5
9						4.5		79.8	
p_M(%)	0.0	0.5	1.5	0.0	20.9	2.0	41.8	**80.3**	43.0

Tablica 6.31 pokazuje da je i u ovom slučaju detekcija zlonamjernog ponašanja uspješna. Međutim, vidljivo je da lažne optužbe od strane zlonamjernog čvora povećavaju vjerojatnosti krive procjene zlonamjernog ponašanja legitimnih čvorova.

Tablica 6.32 prikazuje postupak otkrivanja zlonamjernog ponašanja u trećem scenariju mreže sa 10 čvorova (Rx/Tx=60%).

TABLICA 6.32 Detekcija u mreži sa 10 čvorova, scenarij 3

	1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**
1		4.5		0.0					
2	4.5		23.1		0.0				
3		3.4				23.7			
4	0.0				0.0		9.2		
5		4.5		0.0		31.3		82.3	
6			16.6		0.0				47.1
7				0.0				74.7	
8					0.0		7.8		58.4
9						9.8		25.8	
p_M(%)	2.3	4.1	19.9	0.0	0.0	21.6	8.5	**60.9**	**52.75**

Iz tablice 6.32 vidljivo je da će sustav uspješno detektirati zlonamjerno ponašanje, ali da se s povećanjem broja izgubljenih paketa u trećem scenariju kvaliteta procjene pogoršava. Procijenjena vjerojatnost zlonamjernog ponašanja manja je nego u prethodnim scenarijima (iznosi 60.9%), ali još uvijek je iznad postavljenog praga. Istovremeno povećavaju se i vjerojatnosti pogrešnih procjena, pa se tako dogodilo da procijenjena vjerojatnost za čvor 9 također prelazi prag od 50%, iako se radi o legitimnom čvoru.

U tablici 6.33 prikazan je postupak detekcije u istom scenariju, ali uz činjenicu da zlonamjerni čvor lažno optužuje svoje susjede.

TABLICA 6.33 Detekcija u mreži sa 10 čvorova, scenarij 3 (uz lažno optuživanje susjeda)

	1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**
1		4.5		0.0					
2	4.5		23.1		0.0				
3		3.4				23.7			
4	0.0				0.0		9.2		
5		4.5		0.0		31.3		82.3	
6			16.6		0.0				47.1
7				0.0				74.7	
8					82.3		89.2		94.0
9						9.8		25.8	
$p_M(\%)$	2.3	4.1	19.9	0.0	20.6	21.6	49.2	**60.9**	**70.6**

Iz tablice 6.33 vidljivo je da lažne informacije koje zlonamjerni čvor ubacuje u mrežu značajno otežavaju postupak ispravnog zaključivanja. U situaciji prikazanoj u tablici 6.33, zahvaljujući lažnoj procjeni čvora 8, najveća procijenjena vjerojatnost p_M je za čvor 9, koji je zapravo legitimni čvor (prag prelazi i procijenjena vjerojatnost za čvor 8). U tom slučaju IDS sustav ispravan zaključak donosi tek na temelju činjenice da za čvor 8 postoje dvije procjene koje prelaze prag (od čvorova 5 i 7), a za čvor 9 samo jedna (od čvora 8). Međutim, treba istaknuti da je procjena čvora 6 za čvor 9 bila vrlo bliska vrijednosti praga (47.1%). Iako se radi o pogrešnoj procjeni (prouzrokovanoj gubicima paketa u mreži) lako se moglo dogoditi da ta procjena prijeđe vrijednost praga, i u tom slučaju bi IDS sustav pogrešno zaključio da je zlonamjeran čvor 9, iako se zapravo radi o legitimnom čvoru. Također, u tablici se vidi da je

čvor 9, opet zbog velikih gubitaka paketa u mreži, loše procijenio zlonamjerni karakter čvora 8 (procijenjena vjerojatnost 25.8%), što također bitno otežava ispravno odlučivanje.

6.7.3. Otkrivanje zlonamjernog ponašanja u mreži sa 17 čvorova

Za potrebe testiranja u mreži sa 17 čvorova čvor 10 se ponaša zlonamjerno. Postupak otkrivanja zlonamjernog čvora u prvom scenariju (Rx/Tx=100%) u mreži sa 17 čvorova prikazan je u tablici 6.34.

TABLICA 6.34 Detekcija u mreži sa 17 čvorova, scenarij 1

	1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**	**16**
1		0.0			0.0											
2	0.0		0.0			0.0										
3		0.0		0.0			0.0									
4			0.0					0.0								
5	0.0					0.0			0.0							
6		0.0			0.0		0.0			80.3						
7			0.0			0.0		0.0			0.0					
8				0.0			0.0					0.0				
9					0.0					80.3			0.0			
10						0.0			0.0		0.0			0.0		
11							0.0			80.3		0.0			0.0	
12								0.0			0.0					0.0
13									0.0					0.0		
14										80.3			0.0		0.0	
15											0.0			0.0		0.0
16												0.0			0.0	
p_M(%)	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	**80.3**	0.0	0.0	0.0	0.0	0.0	0.0

Tablica 6.34 pokazuje da u prvom scenariju („idealan“ slučaj, bez gubitaka paketa) IDS sustav bez poteškoća detektira zlonamjerno ponašanje čvora 10.

Tablica 6.35 prikazuje postupak detekcije u istom scenariju, ali u slučaju kada čvor 10 lažno optužuje svoje susjede.

TABLICA 6.35 Detekcija u mreži sa 17 čvorova, scenarij 1 (uz lažno optuživanje susjeda)

	1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**	**16**
1		0.0			0.0											
2	0.0		0.0			0.0										
3		0.0		0.0			0.0									
4			0.0					0.0								
5	0.0					0.0			0.0							
6		0.0			0.0		0.0			80.3						
7			0.0			0.0		0.0			0.0					
8				0.0			0.0					0.0				
9					0.0					80.3			0.0			
10						80.6			80.6		80.6			80.3		
11							0.0			80.3		0.0			0.0	
12								0.0			0.0					0.0
13									0.0					0.0		
14										80.3			0.0		0.0	
15											0.0			0.0		0.0
16												0.0			0.0	
p_M**(%)**	0.0	0.0	0.0	0.0	0.0	20.2	0.0	0.0	26.9	**80.3**	20.2	0.0	0.0	26.8	0.0	0.0

U tablici 6.35 se vidi da i u ovom slučaju sustav ispravno detektira zlonamjerni karakter čvora 10. Također, može se primijetiti da se pojavljuju procjene vjerojatnosti zlonamjernog ponašanja drugih (legitimnih) čvorova uslijed lažnih optužbi od strane zlonamjernog čvora, ali ove vjerojatnosti ne prelaze postavljeni prag.

Tablica 6.36 prikazuje postupak otkrivanja zlonamjernog čvora u drugom scenariju (Rx/Tx=80%) mreže sa 17 čvorova.

TABLICA 6.36 Detekcija u mreži sa 17 čvorova, scenarij 2

	1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**	**16**
1		0.0			0.0											
2	0.0		3.0			0.0										
3		0.0		5.9			1.5									
4			2.8					2.8								
5	0.0					0.0			1.5							
6		0.0			0.0		1.5			80.3						
7			2.9			0.0		2.9			1.5					
8				5.9			1.5					7.2				
9					0.0					79.1			6.0			
10						0.0			1.5		1.5			3.0		
11							1.5			79.1		7.4			1.5	
12								2.8			1.4					7.0
13									1.4					2.8		
14										75.4			5.7		1.4	
15											1.5			2.9		7.5
16												6.9			1.4	
p_M**(%)**	0.0	0.0	2.9	5.9	0.0	0.0	1.5	2.8	1.5	**78.5**	1.5	7.2	5.9	2.9	1.4	7.3

Iz tablice 6.36 vidljivo je da je i u drugom scenariju detekcija zlonamjernog čvora uspješna, ali i da se zbog određenih gubitaka paketa pojavljuju i vjerojatnosti zlonamjernog ponašanja legitimnih čvorova (sve su ispod vrijednosti praga).

Tablica 6.37 prikazuje isti scenarij, ali slučaj u kojem zlonamjerni čvor 10 lažno optužuje svoje susjede.

TABLICA 6.37 Detekcija u mreži sa 17 čvorova, scenarij 2 (uz lažno optuživanje susjeda)

	1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**	**16**
1		0.0			0.0											
2	0.0		3.0			0.0										
3		0.0		5.9			1.5									
4			2.8					2.8								
5	0.0					0.0			1.5							
6		0.0			0.0		1.5			80.3						
7			2.9			0.0		2.9			1.5					
8				5.9			1.5					7.2				
9					0.0					79.1			6.0			
10						80.3			83.1		83.1			83.6		
11							1.5			79.1		7.4			1.5	
12								2.8			1.4					7.0
13									1.4					2.8		
14										75.4			5.7		1.4	
15											1.5			2.9		7.5
16												6.9			1.4	
p_M**(%)**	0.0	0.0	2.9	5.9	0.0	20.1	1.5	2.8	28.7	**78.5**	21.9	21.5	5.9	29.8	1.4	7.3

I u slučaju prikazanom u tablici 6.37 detekcija je uspješna, ali se može primijetiti i povećanje procijenjenih vjerojatnosti zlonamjernosti legitimnih čvorova uslijed lažnih optužbi od strane zlonamjernog čvora.

U tablici 6.38 prikazan je postupak detekcije u trećem scenariju (Rx/Tx=60%) u mreži sa 17 čvorova.

TABLICA 6.38 Detekcija u mreži sa 17 čvorova, scenarij 3

	1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**	**16**
1		0.0			0.0											
2	3.1		12.1			0.0										
3		0.0		27.5			17.6									
4			8.3					24.7								
5	3.1					0.0			12.1							
6		0.0			0.0		20.0			80.3						
7			9.7			0.0		28.8			36.1					
8				20.1			12.0					48.0				
9					0.0					70.6			30.6			
10						0.0			9.0		33.5			23.6		
11							11.0			44.0		41.1			53.2	
12								9.0			11.3					24.2
13									7.9					20.7		
14										54.8			23.8		66.1	
15											1.4			1.0		0.0
16												2.3			0.0	
p_M**(%)**	3.1	0.0	10.0	23.8	0.0	0.0	15.2	20.8	9.7	**62.4**	20.6	30.5	27.2	15.1	39.8	12.1

Tablica 6.38 pokazuje da je detekcija uspješna, ali da se s povećanjem gubitaka paketa povećavaju i pogrešne procjene o malicioznosti legitimnih čvorova. Povećani gubici paketa također negativno utječu na procjene legitimnih čvorova o zlonamjernom čvoru (tako primjerice čvorovi 11 i 14 za zlonamjerni čvor 10 daju procjene vjerojatnosti malicioznosti od svega 44.0% i 54.8%, dok legitimni čvor 15 pogrešno ocjenjuju zlonamjernim s procijenjenim vjerojatnostima od 53.2% i 66.1%).

Tablica 6.39 prikazuje situaciju u kojoj zlonamjerni čvor 10 dodatno unosi lažne informacije u mrežu optužujući za zlonamjerne aktivnosti svoje susjede.

TABLICA 6.39 Detekcija u mreži sa 17 čvorova, scenarij 3 (uz lažno optuživanje susjeda)

	1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**	**16**
1		0.0			0.0											
2	3.1		12.1			0.0										
3		0.0		27.5			17.6									
4			8.3					24.7								
5	3.1					0.0			12.1							
6		0.0			0.0		20.0			80.3						
7			9.7			0.0		28.8			36.1					
8				20.1			12.0					48.0				
9					0.0					70.6			30.6			
10						80.3			83.3		90.3			86.4		
11							11.0			44.0		41.1			53.2	
12								9.0			11.3					24.2
13									7.9					20.7		
14										54.8			23.8		66.1	
15											1.4			1.0		0.0
16												2.3			0.0	
p_M**(%)**	3.1	0.0	10.0	23.8	0.0	20.1	15.2	20.8	34.4	**62.4**	34.8	30.5	27.2	36.0	39.8	12.1

Iz tablice 6.39 vidi se da se unošenjem lažnih informacija od strane zlonamjernog čvora dodatno povećavaju krive procjene o zlonamjernosti legitimnih mrežnih čvorova. Ove vrijednosti ipak ne prelaze zadani prag, zahvaljujući procjenama većeg broja preostalih legitimnih susjeda koje umanjuju negativan učinak lažnih optužbi zlonamjernog čvora.

6.7.4. Zaključci testiranja uspješnosti detekcije IDS sustava

Testiranja i analize provedene kroz više karakterističnih scenarija pokazali su da predloženi sustav za otkrivanje zlonamjernog ponašanja senzorskih čvorova (IDS sustav) uspješno detektira pojavu zlonamjernog čvora u mreži, te time zadovoljava i drugi važan preduvjet (osim nužne energetske učinkovitosti i minimalnog utjecaja na normalan rad mreže i njezine performanse) za moguću implementaciju u realnu IPv6-temeljenu senzorsku mrežu.

Za razliku od drugih IDS sustava koji su poznati u klasičnim BSM, predloženi sustav osim što pojedini čvor može okarakterizirati kao legitimnog ili zlonamjernog, on daje i

procjenu njegove malicioznosti (ostali poznati sustavi samo utvrde je li čvor zlonamjeran ili legitiman). Provedena testiranja pokazala su koji parametri i na koji način utječu na kvalitetu ove procjene, pa čak i na samu sposobnost uspješne detekcije zlonamjernog ponašanja.

Na kvalitetu procjene zlonamjernosti čvora (visinu vjerojatnosti s kojom se on karakterizira zlonamjernim) negativno utječe gubitak podatkovnih paketa u mreži nastao uslijed smetnji, kolizija ili kvarova. Postojanje ovakvih gubitaka čvorovima znatno otežava razlučivanje nastaju li gubici iz navedenih razloga ili su prouzročeni eventualnom aktivnošću zlonamjernih čvorova koji namjerno odbacuju ili selektivno prosljeđuju pakete. Nadalje, gubici paketa dovode i do toga da se legitimni čvorovi također s određenom vjerojatnošću mogu smatrati zlonamjernim, pa u ekstremnim situacijama te vjerojatnosti mogu prijeći postavljenu vrijednost praga i dovesti do pogrešaka u postupku detekcije (situacija u kojoj se ne detektira prisustvo zlonamjernog čvora ili se legitimni čvor pogrešno proglasi zlonamjernim). Ovu činjenicu treba imati u vidu prilikom implementacije ovakvih sustava u realno okruženje, budući da stvarna senzorska mreža u komunikacijskom smislu predstavlja nestabilno okruženje u kojem su smetnje i gubici vrlo česta pojava. Zato nije dovoljno provesti testiranje sustava samo u idealnom scenariju (bez gubitaka), već prije eventualne implementacije treba provjeriti njegovo ponašanje u okruženju u kojem su gubici prisutni, kao i prilagoditi vrijednost praga vjerojatnosti (iznad kojeg se čvor smatra zlonamjernim) konkretnoj aplikaciji.

Pokazalo se da je broj susjednih čvorova također bitan čimbenik koji izravno utječe na kvalitetu procjene zlonamjernosti čvorova. U okruženju u kojem postoji više susjednih čvorova procjene će biti kvalitetnije, budući da će u tom slučaju biti više legitimnih čvorova u okruženju, pa će njihove procjene umanjiti negativan učinak lažnih procjena koje u mrežu ubacuje zlonamjerni čvor.

Uspješnost detekcije zlonamjernog ponašanja u mreži u kojoj se iz različitih razloga javljaju gubici paketa (tj. u kojoj je vjerojatnost uspješnog slanja i prijema paketa manja od 100%, $Rx/Tx<100\%$) ovisi i o izabranoj graničnoj vrijednosti procijenjene vjerojatnosti iznad koje se čvor smatra zlonamjernim. S povećanjem ove granične vjerojatnosti (u razmatranim primjerima ona iznosi 50%) smanjila bi se uspješnost detekcije, budući da povećani gubici paketa otežavaju postupak ispravne detekcije tako što utječu na smanjenje procijenjene vjerojatnosti za zlonamjerni čvor, a istovremeno povećavaju krivo procijenjene vjerojatnosti za legitimne čvorove. Primjerice, kada bi u razmatranim primjerima scenarija 3 ($Rx/Tx=60\%$)

mreže sa 17 čvorova ovaj prag bio postavljen na 65% detekcija bi bila neuspješna (budući da je zlonamjerno ponašanje čvora 10 bilo otkriveno uz procijenjenu vjerojatnost od 62.4%). Međutim, važno je voditi računa o tome da ova granična vrijednost ne bude postavljena prenisko, jer se u tom slučaju lako mogu dogoditi pogrešne procjene i krivo sumnjičenje legitimnih čvorova za zlonamjerno ponašanje (budući da u slučaju većih gubitaka u mreži rastu vrijednosti krivo procijenjenih vjerojatnosti za legitimne čvorove, pa se može dogoditi da neke od njih premaše graničnu vrijednost).

Provedeni testovi pokazali su da na kvalitetu procjene vjerojatnosti zlonamjernog ponašanja (a time i na uspješnost detekcije zlonamjernog čvora) utječe čitav niz različitih čimbenika, kao što su: topologija mreže (broj i raspored čvorova u mreži), broj susjednih čvorova za svaki pojedini čvor (posljedica rasporeda čvorova i njihovih međusobnih udaljenosti), gubici paketa u mreži (koji nisu izravna posljedica zlonamjernog ponašanja nekog od čvorova), te uzorak ponašanja zlonamjernog čvora. Zbog toga nije moguće definirati univerzalnu vrijednost granične vjerojatnosti koja bi bila adekvatna za sve mreže, već ju je u slučaju implementacije u realnu mrežu potrebno prilagoditi uvjetima koji u njoj vladaju (imajući u vidu topologiju, postotak gubitaka, kao i uzorke zlonamjernog ponašanja kakvi bi se mogli očekivati u mreži). Potrebno je i utvrditi ili predvidjeti maksimalni postotak očekivanih gubitaka paketa, odnosno minimalnu vjerojatnost uspješnog prijenosa paketa (Rx/Tx) u mreži, te ispitati sposobnost detekcije u tom slučaju (u analiziranim primjerima minimalna vjerojatnost Rx/Tx iznosi 60%).

7. Zaključak

U posljednjih nekoliko godina bežične senzorske mreže (BSM) ubrzano se razvijaju i neprestano proširuju područje svoje praktične primjene. Unatoč brojnim sličnostima sa drugim vrstama bežičnih mreža, stroga ograničenost njihovih resursa čini ih specifičnim. Zbog toga se za njih razvijaju i u njih implementiraju specifični mrežni mehanizmi (npr. sigurnosni ili usmjerivački) koji se razlikuju od ekvivalentnih mehanizama u drugim vrstama mreža. Također, u posljednje vrijeme sve je naglašeniji trend međusobnog povezivanja različitih vrsta mreža i različitih tipova uređaja, pa tako i integracija bežičnih senzorskih mreža sa drugim vrstama mreža. Protokolna arhitektura većine današnjih mreža temeljena je na IP protokolu, i u njima je u tijeku tranzicija na novu inačicu IP protokola (IPv6 protokol). Ovi paralelni procesi prirodno su doveli do implementacije IPv6 protokola u BSM.

BSM temeljene na IPv6 protokolu predstavljaju jedan od najnovijih trendova u području BSM, te kao takve za sada ostavljaju čitav niz problema i otvorenih pitanja koja zahtijevaju kvalitetno rješavanje. Problematika sigurnosti u ovakvim mrežama predstavlja jedno od najvažnijih područja unutar kojeg je potrebno pronaći kvalitetna rješenja koja bi jamčila širu primjenu ovih mreža u praksi. Upravo zbog toga je i područje ove disertacije sigurnost u bežičnim senzorskim mrežama temeljenim na IPv6 protokolu.

U disertaciji je dan kraći pregled samog koncepta BSM, te je nešto detaljnije razrađen postupak implementacije IPv6 protokola u BSM. Potom slijedi sustavna i detaljna analiza sigurnosnih aspekata bežičnih senzorskih mreža temeljenih na IPv6 protokolu. Pri tome se analiziraju postojeće sigurnosne prijetnje i različite vrste napada koji u većoj ili manjoj mjeri mogu narušiti sigurnost IPv6-temeljenih BSM kroz narušavanje njihovog integriteta, dostupnosti, povjerljivosti ili autentičnosti. Predlažu se i moguće protumjere za neke od ovih napada. Također, analiziraju se i neki postojeći sustavi za otkrivanje upada koji bi se uz odgovarajuće prilagodbe mogli u budućnosti implementirati u IPv6-temeljene BSM.

Nadalje, disertacija daje prijedlog cjelovitog sigurnosnog okvira namijenjenog IPv6-temeljenim BSM. Predloženi sigurnosni okvir je modularan (čine ga kriptografski modul, modul za sigurno usmjeravanje, modul za sigurnu agregaciju podataka, te modul za otkrivanje upada i zlonamjernog ponašanja senzorskih čvorova) i prožima sve slojeve protokolnog stoga koji se primjenjuje u IPv6-temeljenim BSM. Detaljno su objašnjeni struktura i funkcija pojedinih modula, te su dane najvažnije preporuke za njihovu implementaciju. Također,

analiziraju se i postojeća sigurnosna rješenja namijenjena klasičnim BSM i razmatraju potrebne prilagodbe kako bi ih se moglo uklopiti u cjeloviti sigurnosni okvir za IPv6-temeljene BSM.

U disertaciji se daje i rješenje distribuiranog adaptivnog sustava za otkrivanje zlonamjernog ponašanja senzorskih čvorova u IPv6-temeljenim BSM, što je prvo takvo rješenje implementirano u ovoj vrsti mreža. Sustav je distribuirane prirode, što znači da se izvršava na svakom senzorskom čvoru u mreži. Temelji se na kooperativnim algoritmima i postupku kolektivnog odlučivanja na temelju informacija prikupljenih kroz međusobnu komunikaciju IDS agenata na svim čvorovima. Svaki čvor u mreži prati („osluškuje“) ponašanje svojih susjeda, te za svoje susjede procjenjuje vjerojatnost zlonamjernog ponašanja. Nakon razmjene ovih vjerojatnosti za svaki čvor se utvrđuje konačna vjerojatnost malicioznosti. Ovakav koncept koji uključuje procjenu vjerojatnosti zlonamjernog ponašanja inovativan je, budući da takav koncept nije prisutan niti u klasičnim BSM (postojeći IDS sustavi namijenjeni klasičnim BSM u stanju su određeni senzorski čvor okarakterizirati kao zlonamjernog ili legitimnog, bez procjene stupnja njegove malicioznosti).

Predloženo rješenje implementirano je u nekoliko mreža različitih topologija, te su provedene njegove detaljne analize i testiranja kroz nekoliko karakterističnih scenarija u svakoj mreži. Ciljevi analize bili su ispitati performanse i energetsku učinkovitost predloženog rješenja, njegov utjecaj na normalan rad mreže, kao i sposobnost ispravne detekcije u različitim situacijama. Pri tome se pod uspješnom detekcijom podrazumijeva da je sustav ispravno ukazao na zlonamjerni čvor i izdvojio ga iz skupa legitimnih čvorova, dajući pri tome procjenu vjerojatnosti njegovog zlonamjernog ponašanja koja je iznad zadanog praga. Prilikom testiranja uspješnosti detekcije u mrežu je namjerno postavljan po jedan zlonamjerni čvor. Prema tome, unaprijed je poznato koji je čvor zlonamjeran, tako da je sa sigurnošću moguće utvrditi je li sustav prilikom testiranja donio ispravan zaključak, te izdvojio zlonamjerni čvor od preostalih legitimnih čvorova. Testiranja su pokazala da je predloženo rješenje energetski vrlo učinkovito, da ima minimalan utjecaj na normalan rad mreže, dok istovremeno pokazuje vrlo dobru sposobnost ispravnog zaključivanja o zlonamjernosti pojedinih mrežnih čvorova (u testiranim scenarijima uspješno je otkrio koji od mrežnih čvorova pokazuje zlonamjerno ponašanje, čak i unatoč njegovim pokušajima da lažno optužuje svoje susjede, i time onemogući ili značajno otežа postupak detekcije).

Ova disertacija rezultirala je određenim znanstvenim doprinosima, koji se u konačnici mogu sumirati kao:

- Cjelovita analiza sigurnosnih aspekata bežičnih senzorskih mreža temeljenih na IPv6 protokolu (uključuje analizu sigurnosnih prijetnji i napada uz prijedloge mogućih protumjera, te analizu postojećih sigurnosnih mehanizama koji bi se mogli prilagoditi za primjenu u IPv6-temeljenim BSM).
- Prijedlog novog cjelovitog sigurnosnog okvira namijenjenog IPv6-temeljenim BSM (okvir je modularan i prožima sve slojeve protokolnog stoga, i prvi je sigurnosni okvir posebno namijenjen ovakvim mrežama)
- Rješenje distribuiranog adaptivnog sustava za otkrivanje zlonamjernog ponašanja senzorskih čvorova u BSM temeljenim na IPv6 protokolu (prvo ovakvo rješenje za IPv6-temeljene BSM, uključuje mogućnost procjene vjerojatnosti zlonamjernog ponašanja)
- Implementacija, analiza i testiranje predloženog distribuiranog adaptivnog sustava (ispitivanje performansi, energetske učinkovitosti i mogućnosti uspješne detekcije zlonamjernog ponašanja)

Literatura

[1] Abeille J., Durvy M., Hui J., Dawson-Haggerty S.: **„Lightweight IPv6 Stacks for Smart Objects: the Experience of Three Independent and Interoperable Implementations“**, *IPSO Alliance (Internet Protocol for Smart Objects)*, White paper 2, studeni 2008.

[2] Agah A., Das S. K., Basu K., Asadi M.: **„Intrusion Detection in Sensor Networks: A Non-cooperative Game Approach“**, *NCA 2004 (Third IEEE International Symposium on Network Computing and Applications)*, 2004.

[3] Agah A., Das S. K.: **„Preventing DoS Attacks in Wireless Sensor Networks: A Repeated Game Theory Approach“**, *International Journal of Network Security*, Vol. 5, No. 2, 2007. (145-153)

[4] Ahmed K. R., Shihavuddin A. S. M., Ahmed K., Munir S., Asad A.: **„Abnormal Node Detection in Wireless Sensor Network by Pair Based Approach using IDS Secure Routing Methodology“**, *IJCSNS International Journal of Computer Science and Network Security*, Vol. 8, No. 12, 2008. (339-342)

[5] Akyildiz I. F., Su W., Sankarasubramaniam Y., Cayirci E.: **„A Survey on Sensor Networks“**, *IEEE Communications Magazine*, kolovoz 2002. (102-114)

[6] Alzaid H., Foo E., Nieto J. G.: **„Secure Data Aggregation in Wireless Sensor Network: a survey“**, *ACSC 2008 (Australasian Information Security Conference) proceedings*

[7] Amini F., Mišić V. B., Mišić J.: **„Intrusion Detection in Wireless Sensor Networks“**, Security in Distributed, Grid, Mobile and Pervasive Computing, Auerbach, 2007. (111-128)

[8] Anjum F., Subhadrabandhu D., Sarkar S., Shetty R.: **„On Optimal Placement of Intrusion Detection Modules in Sensor Networks“**, *BROADNETS 2004 (International Conference on Broadband Networks) proceedings*

[9] Axelsson S.: **„Intrusion Detection Systems: A Survey and Taxonomy“**, 2000.

[10] Baronti P., Pillai P., Chook V. W. C., Chessa S., Gotta A., Hu Y. F.: **„Wireless sensor networks: A survey on the state of the art and the 802.15.4 and ZigBee standards“**, *Computer Communications 30*, Elsevier, 2007. (1655-1695)

[11] Bellare M., Kilian J., Rogaway P.: **„The Security of the Cipher Block Chaining Message Authentication Code“**, *Journal of Computer and System Sciences*, Vol. 61, No. 3, 2000. (362-399)

[12] Bhuse V., Gupta A.: **„Anomaly Intrusion Detection in Wireless Sensor Networks“**, *Journal of High Speed Networks*, Vol. 15, No. 1, 2006.

[13] Blanchet M.: **„Migrating to IPv6“**, Wiley, 2006.

[14] Casado L., Tsigas P.: **„ContikiSec: A Secure Network Layer for Wireless Sensor Networks under the Contiki Operating System“**, *NordSec 2009 proceedings (14th Nordic Conference on Secure IT Systems)*

[15] Casado L., Tsigas P.: **„Secure Communication in Wireless Sensor Networks: An Overview of ContikiSec“**, *NordSec 2009 proceedings (14th Nordic Conference on Secure IT Systems)*

[16] Chakrabarti S., Shelby Z.: **„6LoWPAN Neighbor Discovery: A High-level Overview“**, *IPSO Alliance (Internet Protocol for Smart Objects)*, White paper 4, kolovoz 2009.

[17] Chan H., Perrig A., Song D.: **„Random Key Predistribution Schemes for Sensor Networks“**, *SECPRI 2003 (Symposium on Security and Privacy) proceedings*

[18] Chatzigiannakis I., Strikos A.: **„A Decentralized Intrusion Detection System for Increasing Security of Wireless Sensor Networks“**, *ETFA 2007 (IEEE Conference on Emerging Technologies and Factory Automation)*, 2007.

[19] Da Silva A. P. R., Martins M. H. T., Rocha B. P. S., Loureiro A. A. F., Ruiz L. B., Wong H. C.: **„Decentralized Intrusion Detection in Wireless Sensor Networks“**, *1st ACM International Workshop on Quality of Service & Security in Wireless and Mobile Networks*, 2005.

[20] Dini G., Tiloca M.: **„Considerations on Security in ZigBee Networks“**, *IEEE International Conference on Sensor Networks, Ubiquitous, and Trustworthy Computing 2010 proceedings*

[21] Loo C. E., Ng M. Y., Leckie C., Palaniswami M.: **„Intrusion detection for sensor networks“**, *International Journal of Distributed Sensor Networks*, 2005.

[22] Doumit S. S., Agrawal D. P.: **„Self-organized criticality and stohastic learning based intrusion detection system for wireless sensor networks“**, *MILCOM 2003 (IEEE Military Communications Conference)*, 2003.

[23] draft-ietf-6lowpan-hc-08: **„Compression Format for IPv6 Datagrams in 6LoWPAN Networks“**, srpanj 2010.

[24] draft-ietf-roll-of0-19: **„RPL Objective Function Zero“**, kolovoz 2011.

[25] draft-ietf-roll-routing-metrics-19: **„Routing Metrics used for Path Calculation in Low Power and Lossy Networks“**, ožujak 2011.

[26] draft-ietf-roll-rpl-19: **„RPL: IPv6 Routing Protocol for Low power and Lossy Networks“**, ožujak 2011.

[27] draft-ietf-roll-security-framework-06: **„A Security Framework for Routing over Low Power and Lossy Networks“**, lipanj 2011.

[28] draft-ietf-roll-security-framework-06: **„A Security Framework for Routing over Low Power and Lossy Networks“**, lipanj 2011.

[29] Du W., Deng J., Han Y. S., Chen S., Varshney P. K.: **„A Key Management Scheme for Wireless Sensor Networks Using Deployment Knowledge“**, *IEEE INFOCOM 2004 proceedings*

[30] Dunkels A., Alonso J., Voigt T., Ritter H., Schiller J.: **„Connecting Wireless Sensor Networks with TCP/IP Networks“**, *WWIC 2004 (International Conference on Wired/Wireless Internet Communications) proceedings*

[31] Dunkels A., Alonso J., Voigt T.: **„Making TCP/IP Viable for Wireless Sensor Networks“**, *EWSN 2004 (European Workshop on Wireless Sensor Networks) proceedings*

[32] Dunkels A., Gronvall B., Voigt T.: **„Contiki – a Lightweight and Flexible Operating System for Tiny Networked Sensors“**, *IEEE Workshop on Embedded Networked Sensors 2004 proceedings*

[33] Dunkels A., Vasseur J. P.: **„IP for Smart Objects“**, *IPSO Alliance (Internet Protocol for Smart Objects)*, White paper 1, rujan 2008.

[34] Durvy M., Abeille J., Wetterwald P., O'Flynn C., Leverett B., Gnoske E., Vidales M., Mulligan G., Tsiftes N., Finne N., Dunkels A.: **„Poster Abstract: Making Sensor Networks IPv6 Ready“**, *SenSys 2008 (ACM Conference on Networked Embedded Sensor Systems) proceedings*

[35] Eschenauer L., Gligor V. D.: **„A Key-Management Scheme for Distributed Sensor Networks“**, *CCS 2002 proceedings*

[36] Ganesan P., Venugopalan R., Peddabachagari P., Dean A., Mueller F., Sichitiu M.: **„Analyzing and Modeling Encryption Overhead for Sensor Network Nodes“**, *WSNA 2003 proceedings*

[37] Grgić K., Žagar D.: **„Wireless Sensor Networks – Applications and Development“**, *AgriControl (2nd IFAC International Conference on Modeling and Design of Control Systems in Agriculture)*, Osijek, 2007.

[38] Hać A.: **„Wireless Sensor Network Designs“**, Wiley, 2003.

[39] Hai T. H., Huh E. N.: **„Minimizing the Intrusion Detection Modules in Wireless Sensor Networks“**, *ICCSA 2008 (International Conference on Computational Sciences and Its Applications)*, 2008.

[40] Hamid A., Rashid M., Hong C. S.: **„Defense Against Laptop Class Attacker in Wireless Sensor Network“**, *ICACT proceedings*

[41] Hamid A., Rashid M., Hong C.S.: **„Routing Security in Sensor Network: HELLO Flood Attack and Defense“**, *ICNEWS 2006 proceedings*

[42] Hsin C. F., Liu M.: **„A Distributed Monitoring Mechanism for Wireless Sensor Networks“**, *International Conference on Mobile Computing and Networking*, 2006.

[43] Hu Y. C., Perrig A., Johnson D. B.: **„Packet Leashes: A Defense Against Wormhole Attacks in Wireless Networks“**, *IEEE INFOCOM 2003*

[44] Hui J. W., Culler D. E.: **„IP is Dead, Long Live IP for Wireless Sensor Networks“**, *SenSys 2008 proceedings*

[45] Hui J., Culler D., Chakrabarti S.: **„6LoWPAN: Incorporating IEEE 802.15.4 into the IP architecture“**, *IPSO Alliance (Internet Protocol for Smart Objects)*, White paper 3, siječanj 2009.

[46] Ioannis K., Dimitriou T., Freiling F. C.: **„Towards Intrusion Detection in Wireless Sensor Networks“**, *13th European Wireless Conference*, 2007.

[47] J. W. Hui, D. E. Culler: **„Extending IP to Low-Power, Wireless Personal Area Networks“**, *IEEE Computer* , srpanj/kolovoz 2008. (37-45)

[48] Jolly G., Kuscu M. C., Kokate P., Younis M.: **„A Low-Energy Key Management Protocol for Wireless Sensor Networks“**, *IEEE ISCC 2003 (International Symposium on Computers and Communication) proceedings*

[49] Karlof C., Sastry N., Wagner D.: **„TinySec: A Link Layer Security Architecture for Wireless Sensor Networks“**, *SenSys 2004 proceedings*

[50] Karlof C., Wagner D.: **„Secure routing in wireless sensor networks: attacks and countermeasures“**, *Ad Hoc Networks 1*, Elsevier, 2003. (293-315)

[51] Kavitha T., Sridharan D.: **„Security Vulnerabilities In Wireless Sensor Networks: A Survey“**, *Journal of Information Assurance and Security 5*, 2010. (31-44)

[52] Kersey C., Yu Z., Tsai J. J. P.: **„Intrusion Detection for Wireless Network“**, Wireless Ad Hoc Networking, Auerbach Publications, 2007.

[53] Kifayat K., Merabti M., Shi Q., Llewellyn-Jones D.: **„Group-Based Secure Communication for Large-Scale Wireless Sensor Networks“**, *Journal of Information Assurance and Security (JIAS)*, Vol. 2, No. 2, 2007.

[54] Krauss C., Schneider M., Eckert C.: **„On handling insider attacks in wireless sensor networks“**, *Information Security Technical Report 13*, Elsevier, 2008. (165-172)

[55] Krontiris I., Benenson Z., Giannetsos T., Freiling F. C., Dimitriou T.: **„Cooperative Intrusion Detection in Wireless Sensor Networks“**, *EWSN 2009 (6th European Conference on Wireless Sensor Networks)*, 2009.

[56] Krontiris I., Dimitriou T., Giannetsos T., Mpasoukos M.: **„Intrusion Detection of Sinkhole Attacks in Wireless Sensor Networks“**, *ICC 2006 (IEEE International Conference on Communications)*, 2006.

[57] Kuorilehto M., Kohvakka M., Suhonen J., Hamalainen P., Hannikainen M., Hamalainen T. D.: **„Ultra-Low Energy Wireless Sensor Networks in Practice – Theory, Realization and Deployment“**, John Wiley & Sons, 2007.

[58] Lauf A. P., Peters R. A., Robinson W. H.: **„A distributed intrusion detection system for resource-constrained devices in ad-hoc networks“**, *Ad Hoc Networks 8*, Elsevier, 2010. (253-266)

[59] Liu A., Ning P.: **„TinyECC: A Configurable Library for Elliptic Curve Cryptography in Wireless Sensor Networks“**, *IPSN 2008 (7th International Conference on Information Processing in Sensor Networks) proceedings*

[60] Lopez J., Zhou J.: **„Wireless Sensor Network Security“**, IOS Press, 2008.

[61] Luk M., Mezzour G., Perrig A., Gligor V.: **„MiniSec: A Secure Sensor Network Communication Architecture“**, *IPSN 2007 proceedings*

[62] Marchang N., Datta R.: **„Collaborative techniques for intrusion detection in mobile ad-hoc networks“**, *Ad Hoc Networks 6*, Elsevier, 2008. (508-523)

[63] Marti S., Giuli T. J., Lai K., Baker M.: **„Mitigating Routing Misbehavior in Mobile Ad Hoc Networks“**, *MobiCom 2000 (6th annual international conference on Mobile Computing and networking)*, 2000.

[64] Mishra A., Nadkarni K., Patcha A.: **„Intrusion Detection in Wireless Ad Hoc Networks“**, *IEEE Wireless Communications*, veljača 2004. (48-60)

[65] Mishra A.: **„Intrusion Detection“**, Security and Quality of Service in Ad Hoc Wireless Networks, Cambridge, 2008.

[66] Mitrokotsa A., Karygiannis A.: **„Intrusion Detection Techniques in Sensor Networks“**, Wireless Sensor Network Security, IOS Press, 2008. (251-272)

[67] Newsome J., Shi E., Song D., Perrig A.: **„The Sybil Attack in Sensor Networks: Analysis and Defenses“**, *IPSN 2004 proceedings*

[68] Ngai E. C. H., Liu J., Lyu M. R.: **„An efficient intruder detection algorithm against sinkhole attacks in wireless sensor networks“**, *Computer Communications 30*, Elsevier, 2007. (2353-2364)

[69] Ngai E. C. H., Liu J., Lyu M. R.: **„On the Intruder Detection for Sinkhole Attack in Wireless Sensor Networks“**, *IEEE ICC 2006 proceedings*

[70] Onat I., Miri A.: **„An intrusion detection system for wireless sensor networks“**, *IEEE International Conference on Wireless and Mobile Computing, Networking and Communications*, 2005.

[71] Osterlind F., Dunkels A., Eriksson J., Finne N., Voigt T.: **„Cross-Level Sensor Network Simulation with COOJA“**, *SenseApp 2006 (IEEE International Workshop on Practical Issues in Building Sensor Network Applications) proceedings*

[72] Perrig A., Szewczyk R., Wen V., Culler D., Tygar J. D.: **„SPINS: Security Protocols for Sensor Networks“**, *Mobile Computing and Networking 2001 proceedings*, Rome, Italy

[73] Prasad N. R., Alam M.: **„Security Framework for Wireless Sensor Networks“**, *Wireless Personal Communications 37*, Springer, 2006. (455-469)

[74] Rafsanjani M. K., Movaghar A., Koroupi F.: **„Investigating Intrusion Detection Systems in MANET and Comparing IDSs for Detecting Misbehaving Nodes“**, *Proceedings of World Academy of Science, Engineering and Technology*, Vol. 34, 2008. (351-355)

[75] Raymond D. R., Midkiff S. F.: **„Denial-of-Service in Wireless Sensor Networks: Attacks and Defenses“**, *IEEE Pervasive Computing*, Vol. 7, No. 1, 2008. (74-81)

[76] RFC 2460: **„Internet Protocol, Version 6 (IPv6) Specification“**, prosinac 1998.

[77] RFC 2464: **„Transmission of IPv6 Packets over Ethernet Networks“**, prosinac 1998.

[78] RFC 2474: **„Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers“**, prosinac 1998.

[79] RFC 3168: **„The Addition of Explicit Congestion Notification (ECN) to IP“**, rujan 2001.

[80] RFC 3306: **„Unicast-Prefix-based IPv6 Multicast Addresses“**, kolovoz 2002.

[81] RFC 3956: **„Embedding the Rendezvous Point (RP) Address in an IPv6 Multicast Address“**, studeni 2004.

[82] RFC 4291: **„IP Version 6 Addressing Architecture“**, veljača 2006.

[83] RFC 4861: **„Neighbor Discovery for IP version 6 (IPv6)“**, rujan 2007.

[84] RFC 4862: **„IPv6 Stateless Address Autoconfiguration“**, rujan 2007.

[85] RFC 4919: **„IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs): Overview, Assumptions, Problem Statement, and Goals“**, kolovoz 2007.

[86] RFC 4944: **„Transmission of IPv6 Packets over IEEE 802.15.4 Networks“**, rujan 2007.

[87] RFC 5548: **„Routing Requirements for Urban Low-Power and Lossy Networks“**, svibanj 2009.

[88] RFC 5673: **„Industrial Routing Requirements in Low-Power and Lossy Networks“**, listopad 2009.

[89] RFC 5826: **„Home Automation Routing Requirements in Low-Power and Lossy Networks“**, travanj 2010.

[90] RFC 5867: **„Building Automation Routing Requirements in Low-Power and Lossy Networks“**, lipanj 2010.

[91] RFC 768: **„User Datagram Protocol“**, kolovoz 1980.

[92] Rivest R. L.: **„The RC5 Encryption Algorithm“**, *FSE 1994 proceedings*

[93] Rogaway P., Bellare M., Black J., Krovetz T.: **„OCB: A Block-Cipher Mode of Operation for Efficient Authenticated Encryption“**, *ACM Transactions on Information and System Security(TISSEC)*, Vol. 6, No. 3, 2001. (365-403)

[94] Roman R., Zhou J., Lopez J.: **„Applying Intrusion Detection Systems to Wireless Sensor Networks“**, *CCNC 2006 (3rd IEEE Consumer Communications and Networking Conference)*, 2006.

[95] Sabahi F., Movaghar A.: **„Intrusion Detection: A Survey“**, *3rd IEEE International Conference on Systems and Networks Communications*, 2008.

[96] Saxena H., Ai C., Valero M., Li Y., Beyah R.: **„DSF – A Distributed Security Framework for Heterogeneous Wireless Sensor Networks“**, *MILCOM 2010 proceedings*

[97] Saxena M.: **„Security in Wireless Sensor Networks – A Layer-based Classification“**, Cerias Tech Report, 2007.

[98] Shaikh R. A., Jameel H., D'Auriol B. J., Lee H., Lee S., Song Y. J.: **„Intrusion-Aware Alert Validation Algorithm for Cooperative Distributed Intrusion Detection Schemes of Wireless Sensor Networks“**, *Sensors*, Vol. 9, 2009. (5989-6007)

[99] Sharma K., Ghose M. K.: **„Complete Security Framework for Wireless Sensor Networks“**, *IJCSIS (International Journal of Computer Science and Information Security)*, Vol. 3, No. 1, 2009.

[100] Sharma K., Ghose M. K.: **„Cross Layer Security Framework for Wireless Sensor Networks“**, *International Journal of Security and Its Applications*, Vol. 5, No. 1, 2011. (39-52)

[101] Shelby Z., Bormann C.: **„6LoWPAN: The Wireless Embedded Internet“**, Wiley, 2009.

[102] Shi E., Perrig A.: **„Designing Secure Sensor Networks“**, *Wireless Communications Magazine*, Vol. 11, No. 6, 2004. (38-43)

[103] Simplicio M. A., Barreto P. S. L. M., Margi C. B., Carvalho T. C. M. B.: **„A survey on key management mechanisms for distributed Wireless Sensor Networks“**, *Computer Networks 54*, Elsevier, 2010. (2591-2612)

[104] Singh V. P., Jain S., Singhai J.: **„Hello Flood Attack and its Countermeasures in Wireless Sensor Networks“**, *IJCSI International Journal of Computer Science Issues*, Vol. 7, Issue 3, No. 11, 2010. (23-27)

[105] Sobh T. S.: **„Wired and wireless intrusion detection system: Classifications, good characteristics and state-of-the-art“**, *Computer Standards & Interfaces 28*, Elsevier, 2006. (670-694)

[106] Sohraby K., Minoli D., Znati T. F.: **„Wireless Sensor Networks – Technology, Protocols and Applications“**, Wiley, 2007.

[107] Ssu K-F., Wang W-T., Chang W-C.: **„Detecting Sybil attacks in wireless sensor networks using neighboring information“**, *Computer Networks 53*, Elsevier, 2009. (3042-3056)

[108] Stammberger K., Semp M., Anand M. B., Culler D.: **„Introduction to Security for Smart Object Networks“**, *IPSO Alliance (Internet Protocol for Smart Objects)*, White paper 5, veljača 2010.

[109] Stavrou E., Pitsillides A.: **„A survey on secure multipath routing protocols in WSNs“**, *Computer Networks 54*, Elsevier, 2010. (2215-2238)

[110] Stavroulakis P., Stamp M.: **„Handbook of Information and Communication Security“**, Springer, 2010.

[111] Su C. C., Chang K. M., Kuo Y. H.: **„The New Intrusion Prevention and Detection Approaches for Clustering-based Sensor Networks“**, *WCNC 2005 (IEEE Wireless Communications and Networking Conference)*, 2005.

[112] Sun B., Osborne L., Xiao Y., Guizani S.: **„Intrusion Detection Techniques in Mobile Ad Hoc and Wireless Sensor Networks“**, *IEEE Wireless Communications*, listopad 2007. (56-63)

[113] Techateerawat T., Jennings A.: **„Energy Efficiency of Intrusion Detection Systems in Wireless Sensor Networks“**, *WI-IATW 2006 (International Conference on Web Intelligence and Intelligent Agent Technology) proceedings*

[114] Tsiftes N., Eriksson J., Dunkels A.: **„Poster Abstract: Low-Power Wireless IPv6 Routing with ContikiRPL“**, *IPSN 2010 (ACM/IEEE International Conference on Information Processing in Sensor Networks) proceedings*

[115] Vasseur J. P., Bertrand P., Aboussouan B., Gnoske E., Pister K., Culler D., Acra R., Huotari A.: **„A survey of several low power Link layers for IP Smart Objects“**, *IPSO Alliance (Internet Protocol for Smart bjects)*, White paper 6, lipanj 2010.

[116] Vasseur J. P., Dunkels A.: **„Interconnecting Smart Objects with IP – The Next Internet“**, Morgan Kaufmann, 2010.

[117] Wagner D.: **„Resilient Aggregation in Sensor Networks“**, *SASN 2004 proceedings*

[118] Wang Y., Attebury G., Ramamurthy B.: **„A Survey of Security Issues in Wireless Sensor Networks“**, *IEEE Communications Surveys & Tutorials*, Vol. 8, No. 2, 2006. (2-23)

[119] Wang Y., Ramamurthy B., Xue Y., Zou X.: **„A Security Framework for Wireless Sensor Networks Utilizing a Unique Session Key“**, *BROADNETS 2008 (International Conference on Broadband Communications, Networks and Systems) proceedings*

[120] Wang Y., Wang X., Xie B., Wang D., Agrawal D. P.: **„Intrusion Detection in Homogeneous and Heterogeneous Wireless Sensor Networks“**, *IEEE Transactions on Mobile Computing*, Vol. 7, No. 6, 2008. (698-711)

[121] Wood A. D., Stankovic J. A., Son S. H.: **„JAM: A Jammed-Area Mapping Service for Sensor Networks“**, *RTSS 2003 (IEEE Real-Time Systems Symposium) proceedings*

[122] Wood A. D., Stankovic J. A.: **„A Taxonomy for Denial-of-Service Attacks in Wireless Sensor Networks“**

[123] Wood A. D., Stankovic J. A.: **„Denial of Service in Sensor Networks“**, *IEEE Computer*, Vol. 35, No. 10, 2002. (54-62)

[124] Yang B.: **„Study on Security of Wireless Sensor Network Based on ZigBee Standard“**, *International Conference on Computational Intelligence and Security 2009 proceedings*

[125] Yang S., Park S., Lee E. J., Ryu J. H., Kim B-S., Kim H. S.: **„Dual Addressing Scheme in IPv6 over IEEE 802.15.4 Wireless Sensor Networks“**, *ETRI Journal*, Vol. 7, No. 5, 2008. (674-684)

[126] Yick J., Mukherjee B., Ghosal D.: **„Wireless sensor network survey“**, *Computer Networks 52*, Elsevier, 2008. (2292-2330)

[127] Zhou B., Shi Q., Merabti M.: **„Balancing intrusion detection resources in ubiquitous computing networks“**, *Computer Communications 31*, Elsevier, 2008. (3643-3653)

[128] Zhou Y., Fang Y., Zhang Y.: **„Securing Wireless Sensor Networks: A Survey“**, *IEEE Communications Surveys & Tutorials*, Vol. 10, No. 3, 2008. (6-28)

[129] Zhu S., Setia S., Jajodia S.: **„LEAP: Efficient Security Mechanisms for Large-Scale Distributed Sensor Networks“**, *CCS 2003 proceedings*

[130] Zia T., Zomaya A.: **„A Security Framework for Wireless Sensor Networks“**, *IEEE SAS 2006 (Sensors Applications Symposium) proceedings*

[131] Žagar D., Grgić K., Rimac-Drlje S.: **„Security aspects in IPv6 networks – implementation and testing“**, *Computers and Electrical Engineering 33*, Elsevier, 2007. (425-437)

[132] Žagar D., Grgić K.: **„IPv6 security threats and possible solutions“,** *WAC 2006 (World Automation Congress) proceedings*

Sažetak

U posljednje vrijeme javlja se trend implementacije IPv6 protokola u bežične senzorske mreže (BSM) kao posljedica težnje ka njihovoj integraciji sa drugim vrstama mreža temeljenih na IP protokolu. Ova disertacija bavi se sigurnosnim aspektima ovih IPv6-temeljenih BSM. Nakon kraćeg pregleda koncepta BSM detaljnije se razrađuje postupak implementacije IPv6 protokola u BSM. Potom slijedi detaljna analiza sigurnosnih prijetnji i napada prisutnih u IPv6-temeljenim BSM. Za neke od njih dane su i moguće protumjere. Nadalje, dan je prijedlog novog modularnog sigurnosnog okvira za IPv6 temeljene BSM. Objašnjeni su struktura i funkcije njegovih modula, te su dane preporuke za njihovu implementaciju. Također, dano je i rješenje distribuiranog adaptivnog sustava za otkrivanje zlonamjernih čvorova u IPv6-temeljenim BSM. Sustav se temelji na distribuiranim algoritmima i postupku kolektivnog odlučivanja. Predloženi sustav uvodi inovativni koncept procjene vjerojatnosti zlonamjernog ponašanja senzorskih čvorova. Sustav je implementiran i testiran kroz više različitih scenarija u tri različite mrežne topologije. U konačnici, provedena analiza pokazala je da je predloženi sustav energetski učinkovit i da pokazuje dobru sposobnost detekcije zlonamjernih čvorova.

Ključne riječi

bežične senzorske mreže, IPv6 protokol, sigurnost, sigurnosni okvir, otkrivanje upada

Abstract

Recently occures the trend of implementation of the IPv6 protocol into wireless sensor networks (WSN) as a consequence of tendency of their integration with other types of IP-based networks. This thesis deals with the security aspects of these IPv6-based WSN. After short review of the WSN concept, the implementation process of the IPv6 protocol into WSN is elaborated in more details. Afterwards, there is a detailed analysis of security threats and attacks which are present in IPv6-based WSN. For some of them possible countermeasures are given. Furthermore, the proposal of the novel and modular security framework for IPv6-based WSN is given. The structure and the functions of its modules are explained, and recommendations for their implementation are given. Also, the solution of adaptive distributed system for malicious node detection in IPv6-based WSN is given. The system is based on distributed algorithms and collective decision-making process. Proposed system introduces innovative concept of probability estimation for malicious behavior of sensor nodes. The system is implemented and tested through several different scenarios in three different network topologies. Finally, performed analysis showed that proposed system is energy efficient and has good capability for detection of malicious nodes.

Keywords

wireless sensor networks, IPv6 protocol, security, security framework, intrusion detection

Životopis

Rođen sam 12. svibnja 1981. godine u Vukovaru. Nakon završetka osnovne škole i opće gimnazije, 1999. godine upisujem Elektrotehnički fakultet u Osijeku. Tijekom studiranja bio sam stipendist MZOŠ RH. Zvanje diplomiranog inženjera elektrotehnike, smjer elektronika i automatizacija, stječem u veljači 2005. godine obranivši diplomski rad pod nazivom „Testiranje sigurnosnih ranjivosti i otkrivanje upada u IPv6 mrežama“. U ožujku iste godine zapošljavam se na Elektrotehničkom fakultetu u Osijeku kao laborant na Zavodu za komunikacije. U srpnju 2005. na istom zavodu dolazim na radno mjesto asistenta, kada upisujem i poslijediplomski znanstveni studij elektrotehnike, smjer telekomunikacije i informatika. Tijekom poslijediplomskog studija položio sam 11 ispita, te objavio 15 znanstvenih radova, od čega 3 u časopisima i 12 na međunarodnim konferencijama. Objavljeni radovi uglavnom su iz područja sigurnosti, bežičnih senzorskih mreža i širokopojasnih komunikacija. Aktivno sudjelujem u izvođenju nastave (auditorne i laboratorijske vježbe) iz više kolegija iz područja komunikacija na preddiplomskom, diplomskom i stručnom studiju ETF-a u Osijeku. Kao sumentor vodio sam veći broj studenata kroz izradu završnih i diplomskih radova. Kao suradnik sudjelovao sam i sudjelujem u nekolicini znanstvenih i stručnih projekata: „Širokopojasni pristup i internetske usluge u ruralnim područjima“, „Postupci raspoređivanja u samoodrživim raspodijeljenim računalnim sustavima“ (projekti MZOŠ), ITEA-ESNA *(European Sensor Network Architecture)*, CAR6Net. Član sam strukovne udruge IEEE.