Mogućnosti primjene IEEE 802.15.4 i ZigBee standarda u IoT okruženju s naglaskom na sigurnosne aspekte

Pejković, Ana

SVEUČILIŠTE JOSIPA JURJA STROSSMAYERA U OSIJEKU
FAKULTET ELEKTROTEHNIKE, RAČUNARSTVA I INFORMACIJSKIH TEHNOLOGIJA OSIJEK

Sveučilišni studij

MOGUĆNOSTI PRIMJENE IEEE 802.15.4 I ZIGBEE STANDARDA U IOT OKRUŽENJU S NAGLASKOM NA SIGURNOSNE ASPEKTE

Diplomski rad

Ana Pejković

Osijek, 2020.

SADRŽAJ:

1. UVOD

Internet stvari (engl. *Internt of Things*) je zbirka "stvari" građene od elektronike, softvera, senzora i pogona povezanih putem Interneta namijenjene za prikupljanje i razmjenu podataka jedno s drugim. Internet stvari je opremljen senzorima i procesnim snagama koji im omogućava upotrebu u mnogim sredinama. Razlika između Interneta stvari i tradicionalnog Interneta je odsustvo uloge čovjeka. *IoT* uređaj može stvarati informacije o ponašanju pojedinca, analizirati ih i poduzimati akcije na temelju prikupljenih informacija. Internet stvari se brzo razvija tijekom aktualnog desetljeća zbog širokog spektra primjene kao što su upravljanje prometom, pametne poljoprivrede i automatizacija kuća. Ulazak Interneta stvari u naš svakodnevni život osim velikog broja prednosti predstavlja i ogromne rizike gubitka privatnosti i sigurnosnih pitanja. Kako bi postigli osiguranje Interneta stvari provedena su mnogi istraživački radovi kako bi se ti problemi sigurnosti i privatnosti suzbili i pronašli bolji načini za uklanjanje tih rizika ili barem umanjili njihov utjecaj. Neka od glavnih sigurnosnih pitanja su: provjera autentičnosti, kontrola pristupa, povjerljivost, privatnost, povjerenje, sigurnost *middleware*, mobilna sigurnost i provođenje politike. Osim toga Internet stvari (engl. IoT) se koristi za nadgledanje, praćenje i kalibriranje industrijskih instrumenata kako bi se omogućile aplikacije za kritične zadatke. Ove kritične aplikacije zahtijevaju visoku propusnost, malu potrošnju energije i zajamčenu isporuku podataka s dopuštenim kašnjenjem. Većina ovih kritičnih aplikacija ne zahtjeva visoku brzinu prijenosa. IEEE standard je razvio standard za nisku brzinu i malu snagu WPAN-a poznat kao IEEE 802.15.4, standard djeluje na fizičkom i MAC (eng. *Medium Access Network*) sloj i preferira se za bežične mreže koje zahtijevaju nisku brzinu prijenosa podataka s manjom potrošnjom energije kao što su WSN (eng. *Wireless Sensor Networks*). [1] [2]

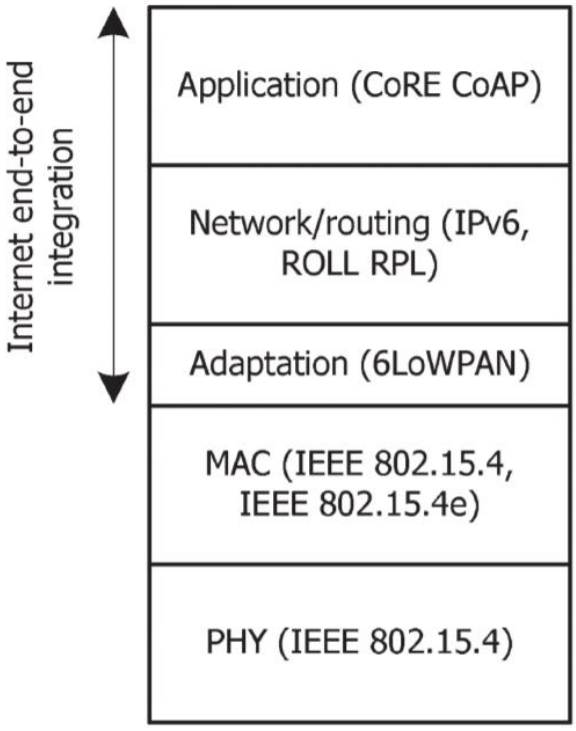
1.1. Zadatak diplomskog rada

IoT (Internet of Things) podrazumijeva modernu komunikacijsku platformu koja primjenom različitih komunikacijskih tehnologija omogućava povezivanje i međusobnu interakciju različitih heterogenih uređaja i sustava. IEEE 802.15.4 standard zajedno sa ZigBee specifikacijom predstavlja jednu od komunikacijskih tehnologija koja svoju primjenu pronalazi unutar IoT okruženja. Potrebno je sustavno analizirati mogućnosti i primjere primjene IEEE802.15.4/ZigBee tehnologije u IoT okruženju, s posebnim naglaskom na aspekte sigurnosti i privatnosti. ZigBee komunikaciju unutar IoT-a analizirati u testnom okruženju, te komentirati dobivene rezultate, te naglasiti smjernice za povećanje razine sigurnosti i privatnosti.

2. IEEE 802.15.4

Buduće Internet stvari koristit će IEEE 802.15.4 komunikaciju zasnovanu na niskoj brzini prijenosa podataka za razne primjene. IEEE 802.15.4 je tehnički standard koji definira rad bežičnih osobnih mreža niske brzine (LR-WPAN). Određuje fizički sloj i kontrolu pristupa mediju za LR-WPAN, a održava ga IEEE 802.15 radna skupina koja je definirala standard 2003.godine. IEEE 802.15 standard je u suprotnosti s drugim pristupima kao što je Wi-Fi, koji nude veću propusnost i zahtijevaju veću snagu. Naglasak je na vrlo jeftinoj komunikaciji obližnjih uređaja s malo ili bez osnovne infrastrukture, s namjerom da se to iskoristi kako bi još više smanjili potrošnju energije. IEEE proizvodi standarde koji omogućuju zajedničku platformu pravila za novi tehnološki razvoj. To je i cilj standarda 802.15.4 dizajniranog da podrži pogodan omjer između energetske učinkovitosti, raspona i brzine prijenosa podataka. Kako je prikazano na slici 2.1, komunikacijski protokol za IoT koristi IEEE 802.15.4 s ciljem podupiranja niskoenergetske komunikacija na fizičkom i MAC sloju. Osnovni okvir zamišlja komunikacijski raspon od 10 metara sa brzinom prijenosa od 250 kbit/s. Kao što je već spomenuto, glavna identifikacijska značajka IEEE 802.15.4 među WPAN-ovima je postizanje izuzetno niskih troškova proizvodnje i rada te tehnološke jednostavnosti, bez žrtvovanja fleksibilnosti i općenitosti. Važne značajke uključuju prikladnost u stvarnom vremenu rezerviranjem zajamčenih vremenskih termina (GTS), izbjegavanje kolizije putem CSMA / CA i integriranu podršku za sigurnu komunikaciju. Uređaji uključuju i funkcije upravljanja napajanjem poput kvalitete veze i detekcije energije. Standard ima odredbe za podršku aplikacijama osjetljivim na vrijeme i brzinu zbog njegove sposobnosti da rade u čistim CSMA / CA ili TDMA načinima pristupa. TDMA način rada podržan je putem GTS značajke standarda. Uređaji koji odgovaraju IEEE 802.15.4 mogu koristiti jedan od tri moguća frekvencijska opsega za rad (868 / 915 / 2450 MHz). Uređaji su zamišljeni da međusobno komuniciraju preko konceptualno jednostavne bežične mreže. Definicija mrežnih slojeva temelji se na OSI modelu, iako su u standardu definirani samo donji slojevi, predviđena je interakcija s gornjim slojevima je moguća koristeći IEEE 802.2 upravljački sloj logičke veze koji pristupa MAC-u preko konvergencijskog sloja. Implementacije se mogu pouzdati u vanjske uređaje ili biti čisto ugrađeni, samo-funkcionalni uređaji. Izvorni IEEE 802.15.4 standard iz 2006. ažuriran je 2011.godine, uglavnom radi uključivanja rasprave o tržišnoj primjenjivosti i praktičnoj primjeni standarda. Ostale izmjene i dopune izvedene su za standard IEEE 802.15.4a koji specificira dodatni fizičke slojeve, IEEE 802.15.4c za potporu pokrenutim frekvencijskim pojasevima u Kini i IEEE 802.15.4d sa sličnim ciljem za Japan. Dodatak IEEE 802.15.4e kojim se definiraju promjene na MAC sloju s ciljem pružanja podrške vremenu-sinkronizacija *multi-hop* komunikacije.

Mehanizmi koji čine ovaj stog (eng. *Stack*) na slici 2.1 moraju omogućiti internetsku komunikaciju na način da uključe ograničene senzorske uređaje, uz istodobno kopiranje zahtjeva iz okruženja s niskom potrošnjom energije. Okolina s niskoenergetskom komunikacijom koristi IEEE 802.15.4 rezerviran na najviše 102 bajta za prijenos podataka na višim razinama stoga (eng. *Stack*), vrijednost koja je znatno manja od maksimalne prijenosne jedinice (MTU) od 1280 bajtova potrebnih za IPv6. Prilagodni 6LoWPAN sloj omogućava prijenos IPv6 paketa preko IEEE.802.15.4. 6LoWPAN također provodi mehanizme fragmentacije i ponovnog sastavljanja paketa. Usmjeravanje preko 6LoWPAN okruženja podržano je protokolom usmjeravanja za mreže niske snage i gubicima (eng. *Routing Protocol for Low-power and Lossy Networks* - RPL). Umjesto da predstavlja protokol usmjeravanja, RPL pruža okvir koji je prilagodljiv potrebama određenih domena IoT aplikacije. Programi specifični za aplikaciju već su definirani za prepoznavanje odgovarajućih zahtjeva usmjeravanja i ciljeva optimizacije. Protokol ograničene aplikacije (CoAP) podržava komunikaciju na aplikacijskom sloju. [1]



Slika 2.1 *Komunikacijski protokoli u IoT-u [1]*

Zbog svoje prikladnosti za niskoenergetsko bežično komunikacijsko okruženje, IEEE 802.15.4 postavlja temelje za dizajn standardiziranih tehnologija poput 6LoWPAN ili CoAP na višim slojevima. IEEE 802.15.4 također je prihvaćen kao temelj industrijskih WSN standarda poput ZigBee, ISA 100.11a i WirelessHART. ZigBee definira profile koji ciljaju tržišna područja poput automatizacije kuća i pametne energije dok WirelessHART i ISA 100.11a ciljaju industrijsko tržište automatizacije i kontrole. IEEE 802.15.4 fizički sloj upravlja fizičkim primopredajnikom radiofrekvencija (RF) na senzornom uređaju te donosi odluku o odabiru kanala, upravlja signalom i energijom. Standard podržava 16 kanala u 2,4 GHz industrijskom , znanstvenom i medicinskom (ISM) radio pojasu, primjenom DSS, UWB i CSS modulacijskih tehnika. DSS je predstavljen u izvornoj verziji standarda iz 2006.godine, dok su UWB i CSS dodani kasnije 2007.godine u dodatku IEEE 802.15.4a. Glavni cilj ovih tehnika modulacije je postizanje pouzdanosti transformiranjem prenesene informacije, tako da ona zauzima veću širinu pojasa pri manjoj gustoći spektralne snage kako bi se postigla manja smetnja duž frekvencijskih pojaseva, zajedno s poboljšanim odnosom signal šum (SNR) na prijemniku. Okvir podataka fizičkog sloja zauzima najviše 128 bajtova, a takvi paketi su mali kako bi se na najmanju moguću mjeru svela vjerojatnost pogreška koje se događaju u niskoenergetskom bežičnom komunikacijskom okruženju. U IEEE 802.15.4 sigurnost je dostupna samo na razini MAC sloju. [4]

MAC sloj osim upravljanja podatkovnim uslugama, upravlja i drugim operacijama, a to su pristup fizičkom kanalu, umrežavanje signala (eng. *network beaconing*), potvrđivanje (validacija) okvira, zajamčeni vremenski interval (GTS), udruživanje čvorova i sigurnost. Standard razlikuje senzorske uređaje prema mogućnostima i ulogama u mreži. Uređaj s potpunom funkcijom (FFD) može koordinirati mrežu uređaja, dok uređaj sa smanjenom funkcijom (RFD) može komunicirati samo s drugim uređajima (tipa FFD ili RFD). Koristeći RFD i FFD uređaje, IEEE 802.15.4 može podržati mrežne topologije poput zvijezda, *peer-to-peer* i klaster mreže. IEEE 802.15.4 uređaji se mogu identificirati pomoću 16-bitnog kratkog identifikatora ili 64-bitnog IEEE EUI-64 identifikatora. Kratki identifikatori se obično koriste u ograničenim okruženjima, dok je 64-bitni identifikator identifikator uređaja. Što se tiče oblikovanja podataka za prijenos, IEEE 802.15.4 ima četiri vrste okvira: okvir podataka, okvir za potvrdu, okvir za signale (eng. *beacon frame*) i MAC naredbeni okvir. Kolizijom tijekom komunikacije podataka upravlja se putem CSMA/CA ili ,alternativno, koordinator može uspostaviti superokvir u okviru kojeg aplikacije s unaprijed definiranim zahtjevima za pojasnu širinu mogu rezervirati i koristit jedan ili više vremenskih slotova. U ovoj situaciji okviri za signale (eng. *beacon frame*) djeluju kao granice super okvira i pružaju sinkronizaciju drugim uređajima kao i informacije o konfiguraciji. [1]

2.2 Sigurnost IEEE 802.15.4

IoT uređaji su opremljeni senzorima i procesnim snagama koje im omogućuju uporabu u mnogim sredinama.

Slika 2.2 *IoT aplikacije [2]*

Slika 2.2 prikazuje mnoštvo uobičajenih IoT aplikacija, uključujući pametni dom, pametni grad, pametne mreže, medicinska i zdravstvena oprema, povezana vozila itd. Usluge koje pružaju IoT aplikacije nude veliku korist za čovjekov život, ali mogu doći s ogromnom cijenom s obzirom na privatnost i sigurnost osobe. Sigurnost i privatnost ostaju važni problemi za IoT uređaje, koji uvode posve novi stupanj brige o privatnosti na mreži za potrošače. To je zato što uređaji ne samo da prikupljaju osobne podatke poput korisničkog imena i telefonskog broja, već mogu nadzirati i korisničke aktivnosti (npr. kada se korisnici nalaze u svojim kućama i što su imali za ručak). [2]

2.2.1 Ograničenja IoT uređaja

Zašto je teško osigurati i primijeniti one sigurnosne značajke koje se koriste u tradicionalnom Internetu na IoT? Dva glavna ograničenja su kapacitet baterije i računalne snage. Kako su neki IoT uređaji raspoređeni u okruženjima gdje punjenje nije dostupno, oni imaju ograničenu energiju za izvršavanje dizajnirane funkcionalnosti, a zahtjevne sigurnosne upute mogu isprazniti resurse uređaja. Postoje tri moguća pristupa za ublažavanje ovoga problema. Prvi je korištenje minimalnih sigurnosnih zahtjeva na uređaju, što se ne preporučuje posebno kod posla s osjetljivim podacima. Drugi pristup je povećati kapacitet baterije. Međutim, većina IoT uređaja dizajnirana je kao lagana i u maloj veličini, što znači da nema dodatnog mjesta za veću bateriju. Zadnji pristup je prikupljanje energije iz prirodnih resursa (npr. svjetlost, vrućina, vibracija, vjetar), ali takav pristup zahtjeva nadogradnju hardvera i značajno povećava novčane troškove. Konvencionalna kriptografija ne može raditi na IoT sustavima jer uređaji imaju ograničeni memorijski prostor koji ne može podnijeti zahtjeve za računanje i pohranu naprednih kriptografskih algoritama. Za potporu sigurnosnim mehanizmima za ograničene uređaje [2]

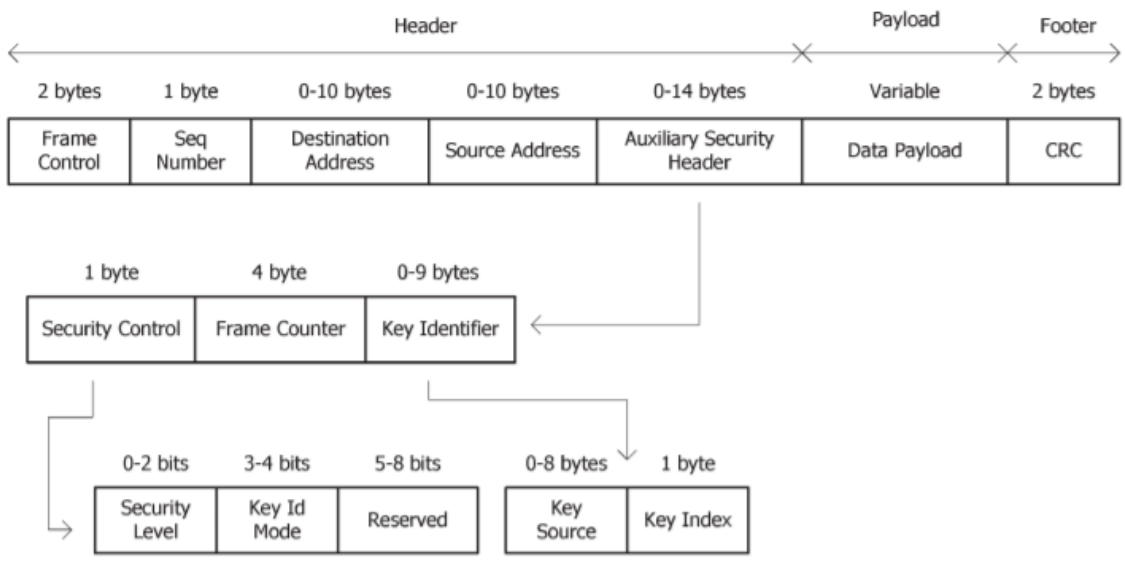
2.2.2 Načini sigurnosti

IEEE 802.15.4 podržava različite načine sigurnosti na razini MAC sloja koji su prikazani u tablici 2.3

Security mode	Security provided
No Security	Data is not encrypted Data authenticity is not validated
AES-CBC-MAC-32	Data is not encrypted Data authenticity using a 32-bit MIC
AES-CBC-MAC-64	Data is not encrypted Data authenticity using a 64-bit MIC
AES-CBC-MAC-128	Data is not encrypted Data authenticity using a 128-bit MIC
AES-CTR	Data is encrypted Data authenticity is not validated
AES-CCM-32	Data is encrypted Data authenticity using a 32-bit MIC
AES-CCM-64	Data is encrypted Data authenticity using a 64-bit MIC
AES-CCM-128	Data is encrypted Data authenticity using a 128-bit MIC

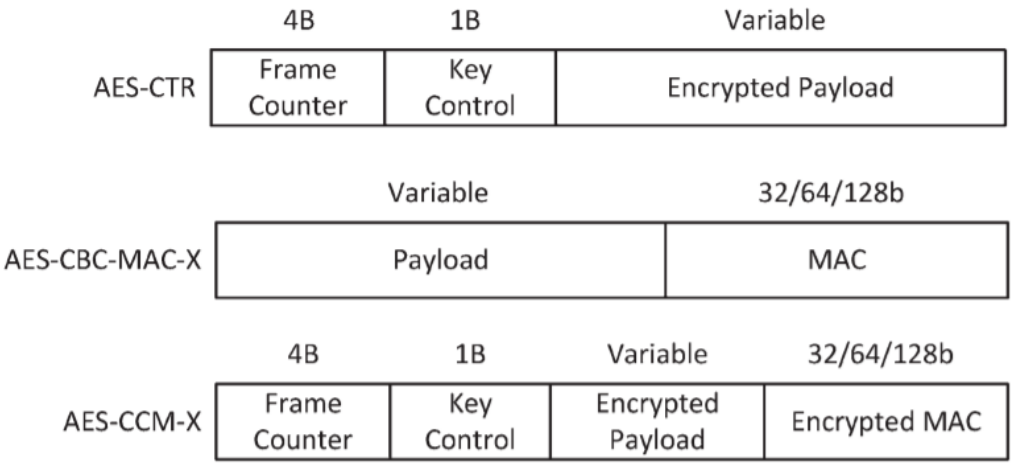
Tablica 2.1 *Načini sigurnosti u IEEE 802.15.4 standardu [1]*

Dostupni načini zaštite razlikuju se prema sigurnosnom jamstvu i veličini upotrijebljenih cjelokupnih podataka.



Slika 2.4 *Sigurnosni podaci i kontrolna polja u IEEE 802.15.4 [4]*

Slika 2.4 prikazuje primjenu sigurnosti na IEEE 802.15.4 sloju veze podatkovni okvir. Zaštićeni okvir prepoznaje se po Sigurnosnom omogućenom bitnom polju iz polja kontrole (eng. *Frame Control*) koji se postavlja na početku zaglavlja. Pomoćno sigurnosno zaglavlje (eng.*Auxiliary Securitiy Header*) upotrijebljeno je samo kada se koristi sigurnost i identificira primjenu sigurnosti na okvir. U pomoćnom sigurnosnom zaglavlju, polje sigurnosna kontrola (eng. *Security Control*) identificira način sigurnosne razine (eng. *Security Level*) iz načina identificiranja iz tablice 2.1, te kako će pošiljatelj i primatelj odrediti kriptografski ključ potreban za obradu sigurnosti za okvir sloja veze. Standard koristi 128-bitne ključeve koje dvije komunikacijske strane mogu prepoznati implicitno ili s druge strane određene od informacija koje se prenose u izvoru ključa (eng. *Key Source*) i indeksu ključa (eng. *Key Index*) potpoljima identifikator ključa (eng. *Key Identifier*). Potpolje izvornog ključa (eng. *Key Source*) određuje pokretača grupnih ključeva, a potpolje indeks ključa (eng. *Key Index*) identificira ključ iz određenog izvora.



Slika 2.5 *Formati podatka korisnog tereta s IEEE 802.15.4 [1]*

Različiti načini zaštite zahtijevaju prijenos informacija u različitim konfiguracijama kao na slici 2.5

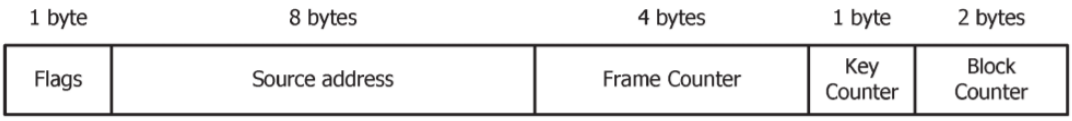
Povjerljivost: Sigurnost koja je definirana normom IEEE 802.15.4 je opcionalna, aplikacija se može odlučiti za ni jedan oblik sigurnosti ili za sigurnost na drugim slojevima protokolnog stoga (eng. *protocol stacka*). Za aplikacije koje zahtijevaju samo povjerljivost podataka preko komunikacije sloja veze, preneseni podaci mogu se kriptirati pomoću AES-a u načinu rada CTR, upotrebom AES-CTR sigurnosnog načina rada. Kao i kod svih sigurnosnih načina dostupnih na IEEE 802.15.4 MAC sloju, 128-bitni ključevi koriste se za podržavanje ovog zahtjeva. [1]

Autentičnost i integritet podataka: Aplikacije koje zahtijevaju autentičnost i integritet komunikacije na sloju veze mogu koristiti jednim od načina zaštite koji primjenjuje AES u načinu povezivanja blokova (eng. *Cypher Block Chaining*-CBC) koji proizvodi kod integriteta poruke (eng. *Message Integrity Code*-MIC) ili kod za provjeru autentičnosti poruke (eng. *Message Authentication Code-MAC*) dodan prenesenim podacima. Sigurnosni načini koji to podržavaju su AES-CBC-MAC-32, AES-CBC-MAC-64 i AES-CBC-MAC-128, koji se razlikuju u veličini proizvedenog koda integriteta. Ovaj kod se stvara s podacima iz 802.15.4 MAC zaglavlja uvećanih za korisne podatke (eng. *payload*), a u takvim se sigurnosnim načinima korisni podaci (eng. *payload*) prenose nešifrirano. [1]

Povjerljivost, zaštita podataka i integritet: CTR i CBC načini rada mogu se zajedno koristiti pomoću kombiniranog brojača (eng. *Counter*) s načinom šifriranja CBC-MAC AES/CCM, koji se u IEEE 802.15.4 koristi za podršku povjerljivosti kao i vjerodostojnosti podataka i integriteta za komunikaciju na sloju veze. Ovaj način rada podržan je na senzorskim platformama poput TelosB-a u varijanti CCM također nudi integritet i isključivo šifriranje. Taj način upotrebe AES-a osigurava povjerljivost, integritet poruka i autentičnost za podatkovnu komunikaciju. Načini zaštite su AES-CCM-32, AES-CCM-64 i AES-CCM-128, koji se ponovno razlikuju po veličini MIC koda nakon svake poruke. AES-CCM zahtijevaju transport svih polja koja se odnose na sigurnost nakon šifriranja korisnih podataka (eng. *payload*),, kao što je prikazano na slici 2.5.

Semantička sigurnost i zaštita od napada ponavljanja poruka:

Brojač okvira (eng. *Frame Counter*) i kontrola ključa (eng. *Key Control*) polja od IEEE 802.15.4 pomoćnog sigurnosnog zaglavlja (eng. *Auxiliary Security Header*) može biti postavljen od strane pošiljatelja i s time pružiti podršku za semantičku zaštitu i zaštitu od ponovne reprodukcije poruka u svim sigurnosnim načinima IEEE 802.15.4. Brojač okvira postavlja jedinstvenu ID poruku i kontrolu ključeva (eng. *Key Control*) je pod kontrolom aplikacije, što ga može povećati ako se dostigne maksimalna vrijednost brojača okvira. Pošiljatelj razbija izvorni paket u blokove od 16 bajta, pri čemu je svaki blok identificiran vlastitim brojačem blokova. Da bi se podržala semantička sigurnost i zaštita od ponovne reprodukcije, svaki se blok šifrira korištenjem različite *nonce* ili inicijalizacijskog vektora (IV).



Slika 2.6 *Format inicijalizacijskog vektora za AES-CRT i AES-CCM sigurnost u IEEE 802.15.4 [1]*

Kao što je prikazano na slici 2.6 brojač okvira i brojač ključeva, zajedno s statičkim 1-bajtnim poljem zastavice, adresom pošiljatelja i 2-bajtnim brojačem bloka (eng. *Block Conuter*) čine inicijalizacijski vektor (IV). Brojač blokova se ne prenosi s porukom, već je izveden od strane primatelja za svaki blok. Inicijalizacijski vektor (IV) se također koristi za šifriranje korištenjem sigurnosnih načina rada zasnovanih na prethodno opisanim AES/CCM. [1]

Mehanizmi kontrole pristupa:

IEEE 802.15.4 standard također nudi funkciju kontrole pristupa, omogućujući senzornom uređaju da koristi izvornu i odredišnu adresu okvira za traženje informacija u sigurnosnom načinu rada i informacija u vezi sa zaštitom koje su potrebne za obradu sigurnosti za poruke. Radijski čipovi 802.15.4 uređaja pohranjuju popise kontrola pristupa (ACL) s najviše 255 unosa, od kojih svaki sadrži podatke potrebne za obradu sigurnosti za komunikaciju s određenim odredišnim uređajem. [1]

Slika 2.7 *prikazuje format ACL unos kako je definirano u IEEE 802.15.4 standardu [1]*

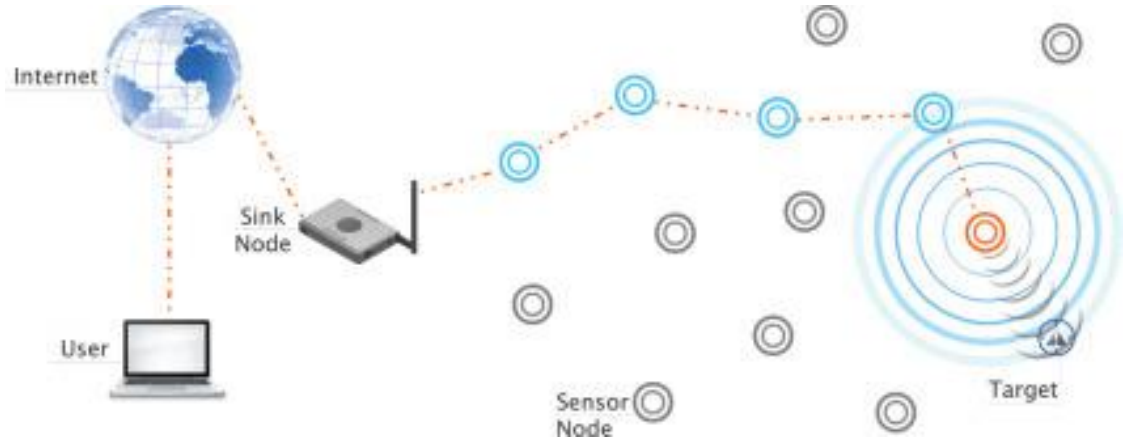
ACL unos sa slike 2.7 pohranjuje IEEE 802.15.4 adresu, polje identifikatora sigurnosni paket (eng. *Security Suite*) i sigurnosni materijal potreban za obradu sigurnosti za komunikaciju s uređajem koji je identificiran u polju adrese. Taj se sigurnosni materijal sastoji od kriptografskog ključa za pakete (eng. *suits*) koji podržavaju šifriranje , *Nonce* (IV) koji moraju sačuvati u različitim zahtjevima za šifriranje. Kada je aktivna zaštita od ponovne reprodukcije, ACL također pohranjuje *high water mark* najnovijeg primljenog identifikatora paketa u polje brojač ponavljanja (eng. *Replay Counter*). [1]

Sigurnost s vremenski sinkroniziranom komunikacijom:

Kao što je prethodno navedeno, IEEE 802.15.4e dodatak uvodi vremenski sinkroniziranu komunikaciju između kanala (eng. *channel-hopping*) te u skladu s tim prilagođava sigurnost. IEEE 802.15.4e, prilagođavajući zaštitu reprodukcije i semantičku sigurnost vremenski sinkroniziranim mrežnim komunikacijama, što je dopunjeno dodatkom. Dodatak definira mogućnost korištenja *null* ili 5-bajtne brojače okvira (eng. Frame Counter) vrijednosti, koja se kasnije treba postaviti na globalni apsolutni broj utora (eng. *Absolute Slot Number*) mreže. ASN pohranjuje ukupan broj vremenskih utora koji su prošli od početka mreže, a čine ga uređaji koji su već u mreži čime se omogućuje sinkronizacija novih uređaja. Upotreba ASN-a kao globalnog brojača okvira omogućava sigurnost koja ovisi o vremenu, zaštitu reprodukcije i semantičku sigurnost. Kako bi se omogućilo korištenje vrijednosti od 5 bajtnog brojača okvira (eng. Frame Counter), IEEE 802.15.4e uvodi izmjene u polje sigurnosna kontrola (eng. *Securtiy Control*) prikazano na slici 2.4, pored polja razine sigurnosti (eng. *Security Level*) i načina ključnog identifikatora (eng. *Key Identifier Mode*), koristi dva bita iz rezerviranog prostora, bit 5 za omogućavanje suzbijanja polja *Frame Counter* i bit 6 za razlikovanje između polja brojača okvira koji zauzima 4 ili 5 bajta. Posljedično, pomoćno zaglavlje sigurnosti prikazano na slici 2.4 sada može prenositi nulti, 4-bajtni ili 5-bajtni polje brojača okvira. CCM-IV za AES šifriranje sada može sadržavati 5-bajt *Frame Counter* umjesto 4-bajt *Frame Counter*, nakon čega slijedi 1-bajt *Key Control* kao što je prikazano na slici 2.6 [1]

2.2.3 Klasifikacija i analiza sigurnosnih napada u WSN i IEEE 802.15.4 standardu

IEEE 802.15.4 je dominantna tehnologija za WSN (Wireless sensor networks). WSN se sastoji od prostorno raspoređenih senzora i jednog ili više *sink* čvorova (koji se nazivaju i bazne stanice). Senzori u stvarnom vremenu nadgledaju fizičke uvjete, poput temperature, vibracije ili kretanja i proizvode senzorne podatke. Senzorski čvor mogao bi se ponašati i kao pokretač podataka i kao usmjerivač podataka. *Sink*, s druge strane prikuplja podatke od senzora. Na primjer, u aplikaciji za nadgledanje događaja senzori su dužni slati podatke *sink*-u kada otkriju pojavu događaja od interesa. *Sink* može komunicirati s krajnjim korisnikom putem izravnih veza, interneta, satelita ili bilo koje vrste bežičnih veza. Slika 2.8 prikazuje tipičnu WSN arhitekturu. U arhitekturi se može nalaziti više *snik*-ova i više korisnika. [3]



Slika 2.8 *WSN arhitektura [3]*

Nakon što su raspoređene te mreže su nezaštićene i bez nadzora tako da su sklone nekoliko sigurnosnih napada. Ovi senzorski čvorovi ne mogu koristiti konvencionalna rješenja za pružanje sigurnosti zbog ograničenog napajanja baterije i memorije. Također su WNS-ovi podložni napadima zbog emitirane prirode medija, ograničenih resursa SN-ova, dinamične topologije mreže i velike mrežne skale. U posljednjem desetljeću naglo je došlo do sve veće potražnje za bežičnim komunikacijskim uslugama i infrastrukturama. Ti su bežični uređaji osjetljivi na kiberkriminalitet, krivotvorenje podataka, hakiranje računala, zlonamjerne napade te krađu informacija. Stoga je poboljšanje sigurnosti u bežičnim komunikacijama od najveće važnosti. U selektivnom napadu prosljeđivanja, kompromitirani čvorovi neprestano prelaze na podskup paketa te pogoršavaju performans mreže. To ima ozbiljne negativne utjecaje na integritet podataka za aplikacije osjetljive na zaštitu podataka. Mnoge druge vrste napada poput *Sybil* napada, napad crvotočina, *man-in-the-middle* napad, napadi crnih rupa su pokrenute kako bi se umanjio učinak WSN-a u smislu omjera dostave podataka. Senzorski čvorovi (SN) u WSN-ima imaju ograničenu memoriju, opskrbu baterije, pojasnu širinu i mogućnost računanja. SN-ovi su gusto raspoređeni u tisućama brojeva te se topologija WSN-a često se mijenja zbog pokretljivosti čvorova. To omogućuje da SN-ovi lako kompromitiraju od strane protivnika. Zbog toga svega sigurnosni aspekti WSN-ova vrlo su kompliciranI. IEEE 802.15.4 standard jedan je od najvažnijih tehnologija koju koriste WSN-ovi. Upravljački slojevi medija (MAC sloj) i fizički slojevi WSN-ova su definirani u IEEE 802.15.4. Ovi slojevi su glavni cilj protivnika jer ti slojevi čine bazu WSN-a. [4]

2.2.4 IEEE 802.15.4 povezani napadi

Različite vrste napada na IEEE 802.15.4 standard mogu se svrstati u tri glavne kategorije:

- Radio ometanja
- Napadi poruka (Manipulacija napadima poruka)
- Steganografski napadi

Radio ometanje:

To je napad fizičkog sloja pokrenut za stvaranje napada uskraćivanje usluge ,tj. resursa u mreži. To se postiže namjernim emisijama radio signala radi smanjenja omjera signala i šuma te se na taj način narušava rad mreže. Postoje četiri različita pristupa za radio ometanja:

- Konstantno ometanje
  To uključuje kontinuirani prijenos radio signala preko ciljanog kanala.
- Zavodljivo ometanje (eng. Deceptive jamming)
  To uključuje neprestano ometanje kanala. Protivnik emitira redovne okvire umjesto radio signala preko ciljanog komunikacijskog kanala.
- Nasumično ometanje
  To uključuje ometanje ciljanih komunikacijskih kanala nasumice. Ovo koristi kombinaciju konstantnog ometanja i zavodljivog ometanja u nasumičnim trenucima koristeći kontinuirani radio signal za konstantno ometanje ili redovite okvire za zavodljivo ometanje
- Reaktivno ometanje
  To uključuje ometanje ciljanog komunikacijskog kanala kad god se na kanalu osjeti aktivnost mreže. Aktivnost mreže može se osjetiti na više načina. Na temelju toga, reaktivno ometanje može se razvrstati u četiri glavne kategorije: prekid ometanja, ometanje aktivnosti, ometanje prevare i ometanje prijenosa poruka.[4]

Manipulacija napadima poruka:

Napadači ih koriste za ubrizgavanje lažnih podataka u uređaje senzorskih mreža. To uključuje transformaciju valjanog (validnog) okvira podataka u izmijenjeni okvir podataka koji sadrži informacije napadača. To se može postići pomoću dvije osnovne tehnike:

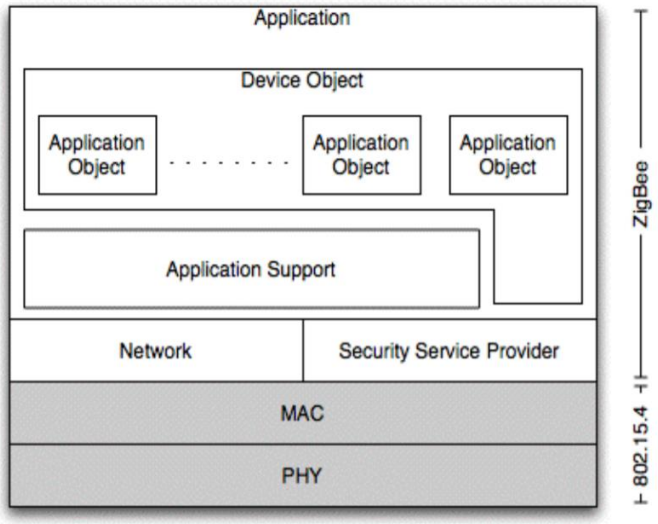
- Prevrtanje simbola (eng. *Symbol flipping*)
  Napadači emitiraju RF valove čije su faze i amplitude sinkronizirani s originalnim signalom. Ako se ti valovi kombiniraju s originalnim signalom, to dovodi do novih signala koji imaju lažno ubrizgane podatke.
- Sjenčanje signala (eng. *Signal shadowing*)
  To uključuje kutne modulacijske sheme u kojima se prima jači sudarajući signal.

Steganografski napadi:

Napad na fizičke i MAC slojeve od 802.15.4 protokola uz pomoć steganografije. Ova tehnika se može koristiti za skrivanje postojanja podataka. To se može postići pokrivanjem podataka koji rezultiraju *stego* porukom. Fizičko zaglavlje fizičkih okvira je jedan bajt i može se koristiti za skrivanje podataka u 802.15.4 mrežama. Ovi napadi u suradnji s protivnikom stvaraju skriveni kanal u mreži. Skriveni kanali mogu se koristit za pokretanje različitih napada u mreži. To se može pokrenuti i podacima koji se skrivaju unutar MAC polja od 802.15.4. [4]

3. ZigBee TEHNOLOGIJA

ZigBee tehnologija predstavljena je od strane ZigBee Saveza. ZigBee tehnologija se razvila na temelju standardiziranog niza rješenja nazvanih “Slojevi“. Ovi optimalno dizajnirani slojevi pružili su ZigBee-u jedinstvene značajke, uključujući niske troškove, jednostavnu implementaciju, pouzdanost, malu snagu i visoku sigurnost. ZigBee je izgrađen po IEEE 802.15.4 standardu. Uzimajući ovaj standard kao “postolje“, ZigBee Savez odredio je gornje slojeve ZigBee standarda. Uređaji su glavni sastavni dijelovi WPAN-a. ZigBee je jedan od najčešćih standarada primopredajnika u bežičnim senzornim mrežama. Uređaji su kategorički definirani kao fizički tip i logički tip. Uređaji fizičkog tipa dodatno se razvrstavaju u dvije vrste: uređaji s potpunom funkcijom (FFD) i uređaji s reduciranom funkcijom (RFD). Logički uređaji su dodatno klasificirani kao tri tipa, koordinator, usmjerivač i krajnji uređaj. Među tim logičkim uređajima koordinator je najsposobniji uređaj koji stvara korijen mrežnog stabla. U mreži treba postojati točno jedan ZigBee koordinator kako bi pokrenuo formiranje mrežnog stabla, također djeluje kao most prema drugim mrežama. Krajnji uređaji ZigBee imaju ograničenu funkcionalnost za komuniciranje samo s koordinatorom ili usmjerivačem mreže, ne može prenositi podatke za druge uređaje. Zbog te ograničene funkcionalnosti krajnji uređaji mogu „spavati“ značajni iznos vremena što im omogućuje dug radni vijek. [5] [6]



Slika 3.1 *ZigBee i IEEE 802.15.4 [5]*

Protokolni stog definiran od strane ZigBee Saveza s obzirom na standard protokolnog stoga IEEE 802.15.4 prikazan je na slici 3.1. Arhitektura protokola temelji se na OSI modelu. Savez ZigBee definira mrežni sloj i aplikacijski sloj. [5][6]

Mrežni sloj je odgovoran za formiranje mreže i usmjeravanje. Usmjeravanje je odabir puta za prenošenje poruka do odredišnog čvora. To čini mrežu koja uključuje priključivanje i napuštanje čvorova, održavanje tablica usmjeravanja (koordinator/usmjerivač), stvarno usmjeravanje i dodjelu adresa. ZigBee koordinator ili usmjerivač će izvesti otkriće rute. Ovaj sloj osigurava sigurnost na razini mreže i omogućuje uređajima male snage da maksimiziraju trajanje baterije. Od osnovnih topologija postoje tri mrežne topologije u IEEE 802.15.4 ,a to su zvijezda, klaster stabla i mreža. [6]

Aplikacijski sloj najviši je protokolarni sloj i u njemu se nalaze objekti aplikacije. ZigBee specifikacija razdvaja aplikacijski sloj u tri različita sloja: podsloj potpora aplikacije (eng. *Appllication Support*- APS), ZigBee objektne uređaje (ZDO) i korisnički definirane profile aplikacija. APS podsloj obrađuje odlazno/dolazne okvire radi sigurnosnog prijenosa/primanja okvira i uspostavlja/upravlja kriptografskim ključevima. Odgovornosti APS podsloja uključuje održavanje određenih tablica koje sadrže informacije koje se koriste za usklađivanje i uspostavljanje komunikacije među uređajima. Tijekom faze otkrivanja ove tablice koriste i uređaj za identifikaciju drugih uređaja koji rade u operativnom prostoru. ZDO provodi tri glave operacije: otkrivanje usluga, sigurnost i vezivanje. Uloga otkrića je pronaći čvorove i pitati o MAC adresi koordinatora/usmjerivača koristeći jednoznačne poruke. Otkriće ujedno olakšava postupak pronalaženja nekih usluga putem njihovih identifikatora profila. Sigurnosne usluge u ZDO imaju ulogu autentifikacije i izvođenje potrebnih ključeva za šifriranje podataka. Mrežni upravljač implementira se u koordinatora i njegova uloga je odabrati postojeću PAN za međusobno povezivanje. Također podržava stvaranje novih PAN-ova. ZDO određuje prirodu uređaja (koordinator, FFD ili RFD) u mreži. Također odgovara na obvezujuće zahtjeve za osiguranje zaštićenog odnosa između dva uređaja. Korisnički definirana aplikacija odnosi se na krajnji uređaj koji je u skladu s ZigBee standardom. ZigBee uređaji imaju 64-bitne adrese s opcijom da omoguće kraće adrese za smanjene veličine paketa, te da rade u bilo koje od dva načina adresiranja. Neke druge tehnološke značajke ZigBee-a navedene su u tablici 3.2. [5]

Parameter	Value
Data Rate	250 kb/s, 40 kb/s, and 20 kb/s
Topology	Star or Peer-to-Peer
Addressing	16-bit (short) or 64-bit (extend)
Multiple Access Technique	Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA)
Frequency	868 (Europe) 915 MHz (North America) 2.4 GHz (Worldwide)
Range	10-20 meter
Channels	11 channels (868/915 MHz0 16 channels (2.4 GHz)

Tablica 3.1 *Značajke ZigBee tehnologije [5]*

U mreži ZigBee koriste se dva načina komunikacije navigacijski (eng. *beacon*) način rada i bez navigacijski (eng. *nonbeacon)* način rada. Navigacijski način rada se koristi od strane koordinatora baterije (eng. *battery operated coordinator)* da bi se uštedjela energija. Uređaj čeka *beacons* koje koordinator periodično šalje i traži poruke upućene na njega. Ako je prijenos poruka završen, koordinator postavlja raspored za sljedeći *beacon* za taj uređaj. Nakon saznanja za sljedeći raspored uređaj može "zaspati". S druge strane, *non-beacon* način rada koristi koordinator napajanja mrežom (eng. *mains-powered coordinator*). Svi uređaji u umreženoj mreži znaju raspored za komunikaciju jedni s drugima i moraju se " probuditi" u predviđenom vremenu kako ne bi propustili *beacon*. Dakle, s uređajima treba povezati prilično precizan vremenski krug. To znači da će doći do povećanja potrošnje energije. *Non-beacon* komunikacija prikladna je za aplikacije poput uređaja za otkrivanje dima i protuprovalnih alarma gdje uređaji "spavaju" gotovo čitavo vrijeme. [5] Snaga potrebna za ZigBee je vrlo mala. U većini slučajeva koristi se 1mW ili manje snage, ali nudi raspon od 150 metara na otvorenom, što se postiže tehnikom DSSS. Radi u 868 MHz (Europa), 915 MHz (Sjeverna Amerika i Australija) i 2,4 GHz (dostupan diljem svijeta) ISM opsegu do 20kbps, 40kbps i 250kbps brzine podataka. Budući da se ovi valni pojasevi razlikuju od opsega trenutnih uobičajenih bežičnih mreža, WiFi-a, Bluetooth-a, bežičnog USB-a itd. Međusobne smetnje između njih neće se pojaviti, stoga ovo jamči da naš sustav neće ometati druge bežične mreže i da neće biti međusobnog utjecaja. Standard IEEE 802.15.4 koristi 64-bitne i 16-bitne kratke adrese za teoretsku podršku više od 65.000 čvorova po mreži. ZigBee mreža može imati do 653356 uređaja, udaljenost između ZigBee uređaja može biti do 50 metara, a svaki čvor može prenijeti podatke na druge čvore. To dovodi do mogućnosti stvaranja vrlo velike mreže koja pokriva značajne udaljenosti. [6]

Uređaj ZigBee kombinacija je aplikacije (kao što su senzor za svijetlo, kontrola rasvjete itd.), ZigBee logičke (koordinator, usmjerivač, krajnji uređaj) i ZigBee fizičke vrste uređaja (uređaj s potpunom funkcijom i uređaj sa smanjenom funkcijom).

- ZigBee fizičke vrste uređaja

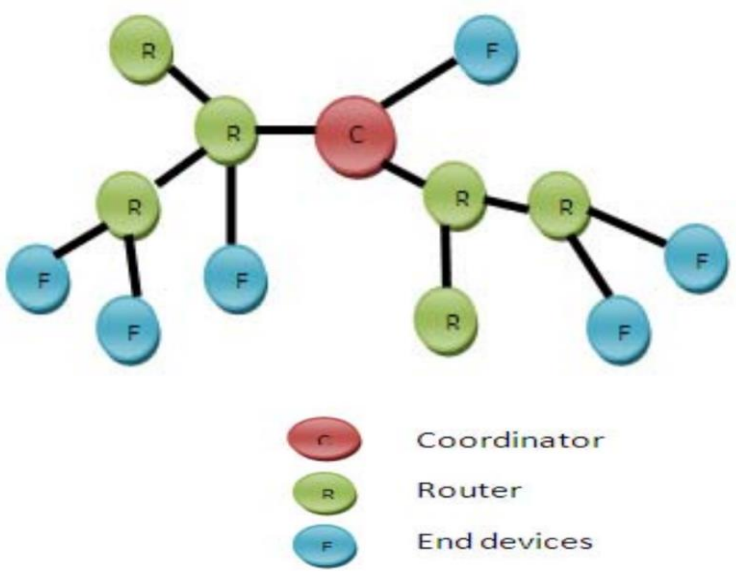
Na temelju mogućnosti obrade podataka, u IEEE 802.15.4 nalaze se dvije vrste fizičkih uređaja: uređaj s potpunom funkciji (eng. *Full Functional Devce*-FFD) i uređaj s reduciranom funkcijom (eng. *Reduced Functional Devce*-RFD). Tipičan FFD u ZigBee mreži napajat će se izmjeničnom strujom jer mora uvijek biti aktivan i osluškivati mrežu. RFD-ovi su krajnji uređaji kao što su senzori za aktivatore koji rade samo ograničene zadatke poput snimanja podataka o temperaturi, praćenje stanja rasvjete ili kontrola vanjskih uređaja. Postojeći ZigBee standard zahtjeva da FFD-ovi uvijek budu uključeni, što u praksi znači da se FFD-ovi moraju stalno napajati.

- ZigBee tipovi logičkih uređaja

U ZigBee sustavu postoje tri kategorije čvorova. Oni su koordinatori, usmjerivači i krajnji uređaji.

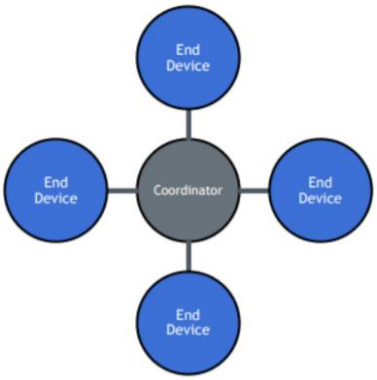
1) Koordinatori:
   Tvori korijen mrežnog stabla i može se prenositi na druge mreže. U svakoj je mreži točno jedan koordinator. Odgovoran je za pokretanje mreže i odabir mrežnih parametara kao što su radiofrekvencijiski kanal, jedinstveni identifikator mreže i postavljanje ostalih operativnih parametara. Također može pohraniti informacije o mreži, sigurnosnim ključevima.
2) Usmjerivač
   Djeluje kao posredni čvor, prenoseći podatke s drugih uređaja. Usmjerivač se može povezati s već postojećom mrežom, također može prihvatiti veze s drugih uređaja i biti neka vrsta predajnika na mrežu.
3) Krajnji uređaji:
   To mogu biti uređaji s malom snagom te uređaji koji rade na bateriju. Oni mogu prikupljati razne informacije od senzora i sklopki. Imaju dovoljno funkcionalnosti za razgovor s roditeljima (koordinator ili usmjerivač) i ne mogu prenositi podatke iz drugih uređaja. Ovom smanjenom funkcionalnosti omogućuje se smanjenje njihovih troškova. Podržavaju bolje modele male snage. Ovi uređaji ne moraju ostati “budni“ cijelo vrijeme , dok uređaji

koji pripadaju drugim dvjema kategorijama moraju. Svaki krajnji uređaj može imati do 240 krajnjih čvorova koji su zasebni zahtjevi koji dijele isti radio.[6]

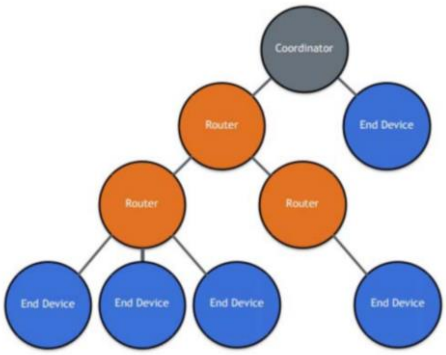


Slika 3.3 *ZigBee mreža [6]*

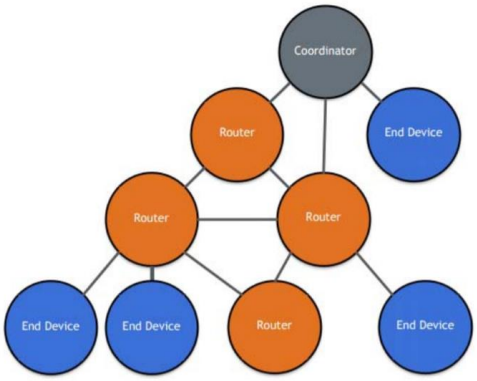
ZigBee mreža može imati zvijezda, stablo ili mrežastu topologiju kao što je prikazano na slikama 3.4, 3.5, 3.6



Slika 3.4 *ZigBee topologija zvijezde [7]*



Slika 3.5 *ZigBee topologija stabla [7]*



Slika 3.6 *ZigBee mrežasta topologija [7]*

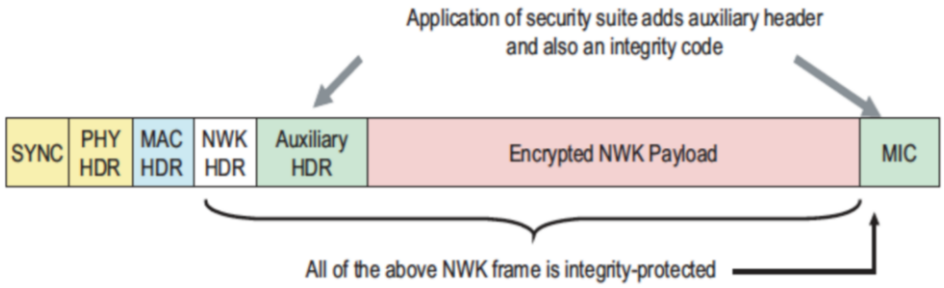
Topologija zvijezda sastoji se od jednog koordinatora i bilo kojeg broja krajnjih uređaja. U topologiji zvijezde usvojen je mrežni model *master – slave* gdje je *master* ZigBee koordinator koji je FFD, a *slave* će biti ili FFD ili RFD. Krajnji uređaji ZigBee fizički su i električno odvojeni jedno od drugih i prenose informacije putem koordinatora. Uređaji mogu komunicirati samo s koordinatorom. Topologija stabla slična je topologiji zvijezde. Razlika je u tome što drugi čvorovi mogu međusobno komunicirati kako bi se više RFD/FFD- ova moglo povezati s nekoordinatorskim FFD-ovima. Prednost ove topologije je mogućnost geografskog širenja mreže. U mrežastoj topologiji, svaki čvor može komunicirati s bilo kojim drugim čvorom u svome dometu. Mrežna topologija je kompleksnija za održavanje, ali je robusnija te ima veću toleranciju na greške. [6]

3.1 Sigurnost ZigBee-a

ZigBee kao i svaka bežična tehnologija, osjetljiva je na mnoge mrežne napade zbog niske složenosti u veličini memorije i brzini obrade. ZigBee je jedan od najčešće korištenih standarda za bežičnu komunikaciju između različitih IoT uređaja, a usvojile su ga mnoge velike tvrtke poput Samsunga i Philipsa. Iako je ZigBee dizajniran s obzirom na važnost sigurnosti, napravljeni su kompromisi kako bi uređaji ostali jeftiniji, niskoenergetski i visoko kompatibilni. ZigBee tvrdi da pruža najsuvremenije sigurnosne alate koji tvrtaka članicama omogućuje stvaranje nekih od najsigurnijih IoT bežičnih uređaja. Njegova sigurnost se temelji na simetričnoj kriptografiji, u kojoj dvije strane moraju dijeliti iste ključeve za komunikaciju. ZigBee koristi visoko siguran 128-bitni sustav šifriranja zasnovan na AES-u. ZigBee protokol izgrađen je na IEEE 802.15.4 bežičnom standardu, koji ima dva sloja, fizički sloj (PHY) i srednji sloj za kontrolu pristupa (MAC). ZigBee gradi mrežni (NWK) i aplikacijski (APL) sloj na vrhu PHY i MAC. Kao niskobudžetni protokol, ZigBee pretpostavlja model "otvorenog povjerenja" gdje slojevi protokola međusobno imaju povjerenja. Stoga kriptografska zaštita postoji samo između uređaja ,ali ne i između različitih slojeva u uređaju. To omogućava ponovnu upotrebu ključeva među slojevima istoga uređaja. Radi jednostavnosti interoperabilnosti uređaja, ZigBee koristi istu razinu sigurnosti za sve uređaje na određenoj mreži i sve slojeve uređaja. Nadalje, uspostavlja se princip „sloj koji stvara okvira odgovoran je za njegovo prvobitno osiguranje" . Osim toga ZigBee naredba uključuje brojač okvira za zaustavljanje ponovnih napad (u kojem bi napadač mogao snimiti i ponoviti poruku naredbe). Krajnja točka koja prima uvijek provjerava brojač okvira i zanemaruje dvostruke poruke. ZigBee također podržava frekvencijsku agilnost, u kojoj se njegova mreža premješta u slučaju napada ometanja. [8] ZigBee aplikacije mogu se razlikovati od jednostavnih kućnih uređaja za daljinsko upravljanje do kritičnijih operacija kao što su pametno mjerenje i pametna mreža. ZigBee mrežasta topologija smatra se "samoizlječivom" jer ima elemente otkrivanja koji će pronaći najbolji put za razmjenu poruka. To je zbog toga što u mrežnoj topologiji najfleksibilnije umrežavanje koje nude ZigBee usmjerivači mogu izravno komunicirati s drugim usmjerivačima ili koordinatorom unutar domene, dopuštajući različite rute u mreži. Postoji nekoliko ugrađenih sigurnosnih usluga koje ZigBee standard nudi za zaštitu okvirne komunikacije između čvorova:

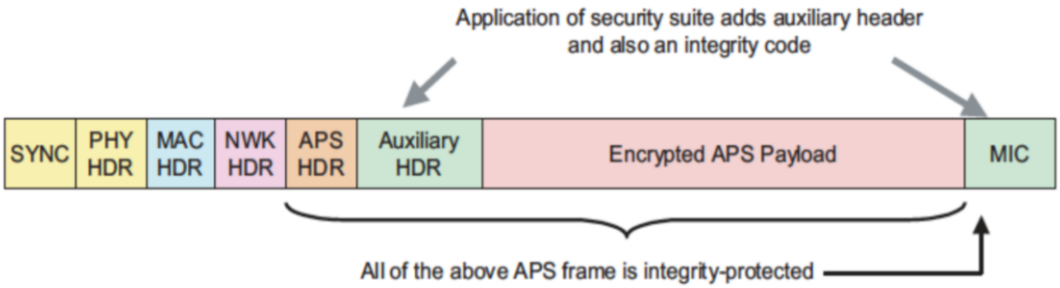
1. Koristi simetričnu šifru kako bi zaštito privatnost podataka od drugih strana bez posjedovanja kriptografskog ključa.
2. ZigBee koristi AES algoritam s *Cryptographic block Ciphers Mode* (Brojač s CBC-MAC). Nudi i autentifikaciju i povjerljivost tijekom prijenosa podataka. Međutim ZigBee pojednostavljuje postupak šifriranja omogućujući ponovnu uporabu istog ključa na svakoj razini ZigBee stoga.
3. Kako bi se sačuvao integritet podataka od izmjene drugih strana, ZigBee raspoređuje provjeru integriteta poruka (eng. *message integrity check- MIC*). Ova usluga također može osigurati da podaci dolaze s čvora koji ima kriptografski ključ.
4. ZigBee može spriječiti napad prosljeđivanja osiguranjem sekvencijalnog brojača za svježinu (eng. *freshness counter*) redoslijeda okvira (ulazni ili izlazni okvir). Svaki put kada se novi okvir pošalje/primi, ovaj brojač će se resetirati. Zbog toga, ako bilo koji zlonamjerni čvor prekine komunikaciju kako bi se neki od prethodnih primljenih ili poslanih okvira mogao proslijediti, to će se lako otkriti iz brojača svježine. Dakle to nam omogućuje sprječavanje napadača da prisili mrežu na traženje drugog puta.
5. Autentifikacija se može održavati na mrežnom sloju i aplikacijskom sloju upotrebnom aktivnog mrežnog ključa i ključa veze. Slijedom toga, informacije se mogu sinkronizirati između uređaja, istodobno pružajući autentičnost putem zajedničkih ključeva.
6. Jedna od sigurnosnih ugrađenih usluga koje ZigBee koristi je centar povjerenja (eng. *trust centar*). On upravlja novim uređajima koji su integrirani u mrežu i redovito ažurira mrežni zajednički ključ. Obično je čvor koji je koordinator centar povjerenja i bit će prepoznat od strane svih ostalih čvorova unutar mreže. Funkcije centra za povjerenje su: upravljanje (distribucija) zajedničkim ključevima za provjeru autentičnosti novih uređaja i omogućuje sigurnost s kraja na kraj između uređaja ili čvorova. [7]

Mrežni sloj odgovoran je za korake obrade potrebne za prijenos odlaznih okvira i sigurno primanje dolaznih okvira. Slično MAC sloju, gornji slojevi postavljaju odgovarajuće ključeve i brojače okvira te utvrđuju koju razinu sigurnosti koristiti. Mrežni sloj ponekad emitira poruke zahtjeva za rutu i obrađuje primljene poruke odgovora na rutu. Pritom mrežni sloj koristi ključeve veze ako su dostupni, u suprotnom koristi svoj aktivni mrežni ključ. Ovdje format okvira izričito označava ključ koji će se koristiti za zaštitu okvira, slika 3.7 prikazuje enkriptiranog mrežnog sloja.



Slika 3.7 *ZigBee okvir sa zaštitom na mrežnom sloju [8]*

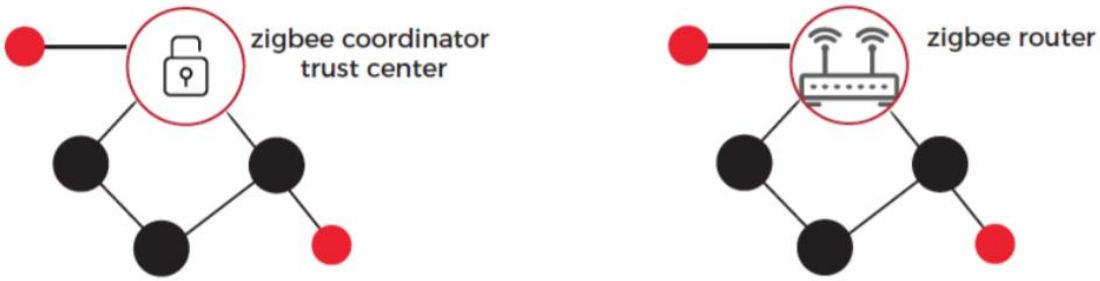
Svom sigurnošću povezanom s aplikacijskim slojevima upravlja APS (podrška za aplikacije) podsloj. Aplikacijski sloj odgovoran je za korake obrade potrebne za siguran prijenos odlaznih okvira i sigurno uspostavljanje i upravljanje kriptografskim ključevima. Gornji slojevi kontroliraju razinu sigurnosti ili upravljaju kriptografskim ključevima izdavanjem primitiva aplikacijskog sloja. Slika 3.8 prikazuje primjer šifriranog aplikacijskog sloja. U ZigBee 3.0, ZigBee protokol također može stvoriti sigurnu vezu na razini aplikacije između para uređaja u mreži uspostavljanjem jedinstvenog skupa AES-128 ključeva za enkripciju između para uređaja. Ovo podržava virtualne privatne veze između para uređaja koji trebaju veću sigurnost.



Slika 3.8 *ZigBee okvir sa zaštitom na aplikacijskom sloju [8]*

3.1.1 Modeli sigurnosti

Kako bi zadovoljio širok raspon primjene uz istodobno održavanje niske troškova i snage, ZigBee tvrdi da nudi dvije mrežne arhitekture i odgovarajuće sigurnosne modele: distribuirani i centralizirani. Razlikuju se po načinu na koji primaju nove uređaje u mrežu i po tome kako štite poruke u mreži. Distribuirani sigurnosni model pruža manju sigurnost i jednostavniji sustav. Ima dvije vrste uređaja usmjerivače i krajnje uređaje. Ovdje usmjerivač može formirati distribuiranu sigurnosnu mrežu kada ne može pronaći ni jednu postojeću mrežu. Svaki usmjerivač može izdati mrežne ključeve. Kako se više usmjerivača i uređaja pridružuje mreži, prethodni usmjerivači na mreži šalju ključ. Da bi sudjelovali u distribuiranim sigurnosnim mrežama, svi usmjerivači i krajnji uređaji moraju biti unaprijed konfigurirani ključem veze koji se koristi za šifriranje mrežnog ključa prilikom prenošenja s roditelja usmjerivača na novo pridruženi čvor. Svi uređaji u mreži šifriraju poruke s istim mrežnim ključem. Centralizirani sigurnosni model pruža veću sigurnost. Također je i kompliciraniji jer uključuje i treći tip uređaja, centar povjerenja (eng. *Trust Center- TC*), koji je obično i mrežni koordinator. Centar povjerenja formira centraliziranu mrežu, konfigurira i vrši autentifikaciju usmjerivača i uređaja za pridruživanje mreži. TC uspostavlja jedinstveni TC ključ veze za svaki uređaj na mreži dok se pridružuju i povezuje ključeve za svaki par uređaja prema potrebi. TC također određuje mrežni ključ. Za sudjelovanje u centraliziranom modelu sigurnosne mreže, svi entiteti moraju biti unaprijed konfigurirani s ključem veze koji se koristi za šifriranje mrežnog ključa prilikom prelaska iz TC-a u novo pridruženi entitet. Oba sustava prikazana su na slici 3.9 [8]



Slika 3.9 *Centralizirana vs. Distribuirana ZigBee mreža [8]*

3.1.2 Sigurnosne pretpostavke

Osim modela otvorenog povjerenja između slojeva, sigurnost ZigBee-a u konačnici ovisi o sljedećim pretpostavkama:

1. Čuvanje simetričnih ključeva. ZigBee pretpostavlja da tajni ključevi nisu dostupni izvan uređaja na nezaštićeni način, što znači da sav prijenos ključeva mora biti šifriran. Iznimka od toga je za vrijeme predkonfiguracije novog uređaja, u kojem se jedan ključ može poslati nezaštićen, stvarajući kratku ranjivost. Ako su ključevi ukradeni u tome vremenu protivnik ima fizički pristup uređajima te tada postaju dostupne mnoge informacije. Sigurnosna politika ZigBee-a ne štiti od napada na hardver zbog svoje niske cijene.
2. Zaštita korištenog mehanizma. Svi čvorovi usmjerivača i krajnjih uređaja trebali bi podržavati centralizirani i distribuirani sigurnosni model prilagođavajući se sigurnosnom sustavu koji koristi mreža kojoj se oni pridružuju.
3. Uključena pravilna implementacija kriptografskog mehanizma i povezanih sigurnosnih politika. Ovdje se pretpostavlja da programeri ZigBee-a u praksi slijede kompletan protokol. ZigBee također pretpostavlja dostupnost gotovo savršenih generatora slučajnih brojeva. [8]

3.1.3 Sigurnosni ključevi

ZigBee mreža i uređaji koriste ključ mreže i ključeve veze za komunikaciju. Primatelj uvijek zna koji se ključevi koriste u zaštiti poruka. Mrežni ključ je 128-bitni ključ koji dijele svi uređaji u mreži, a koristi se za *broadcasting* komunikaciju. Postoje dva tipa mrežnih ključeva: standardni i visoko sigurnosni. Tip obično kontrolira način na koji se mrežni ključ distribuira jer mrežni ključ sam mora biti zaštićen enkripcijom kada se proslijedi čvoru koji se pridružuje. Za ovu enkripciju koristi se unaprijed konfigurirani ključ veze; ovaj ključ znaju i TC i uređaj koji se pridružuje za centraliziranu sigurnost , a u distribuiranoj sigurnosti ovaj ključ je poznat svim čvorovima. Ključ veze je 128-bitni ključ koji dijele dva uređaja. Postoje dva tipa ključeva veze: globalni i jedinstveni. Tip određuje način na koji uređaj obrađuj razne TC poruke (APS naredbe). U centraliziranoj sigurnosnoj mreži postoje tri vrste ključa veze 1) globalni ključ veze koji koriste TC-ovi i svi čvorovi u mreži 2) jedinstveni ključ veze koji se koristi za jedan-na-jedan relaciju između TC-a i čvora, kasnije zamijenjen TC ključem veze i 3) *application link key* koji se koristi između para uređaja. [8]

U centraliziranoj sigurnosnoj mreži ključevi mrežnog sloja su sljedeći:

- Mrežni ključ
- Unaprijed konfigurirani globalni ključ veze (eng. *Global link key*), koji se koristi za enkripciju mrežnog ključa kada se prenosi s TC-a na uređaje. Ovaj ključ veze isti je za sve čvorove mreže. To može biti ZigBee definiran ili od strane proizvođača definiran
  - ZigBee definirani ključ 5A 69 67 42 65 65 41 6C 6C 69 61 6E 63 65 30 39 (ZigbeeAlliance09), koji omogućuje čvorovima od različitih proizvođača da se pridruže mreži
  - Proizvođački definiran ključ koji omogućuje samo čvorovima određenog proizvođača da se pridruže mreži
- Unaprijed konfigurirani jedinstveni ključ veze (eng. *Pre-configured unique link key*), koji se također koristi za šifriranje mrežnog ključa kada se šalje s TC-a na čvor. Ovaj ključ veze isključiv je za svaki par (TC, čvor) tako da je različit za svaki čvor. Ovaj ključ veze obično je unaprijed konfiguriran ili programiran u odgovarajuće čvorove bilo u tvornici ili tijekom puštanja u pogon. U novoj verziji, ZigBee 3.0, unaprijed konfigurirani jedinstveni ključ veze obično je u obliku instalacijskog koda, slučajnog 128-bitnog broja zaštićenog 16-bitnim CRC-om (ciklička provjera redundancije) unaprijed instaliranim u uređajima. [8]

Jednom kada se uspostavi sigurnost na razini mreže, može se postaviti zaštita na razini aplikacije za sigurniju komunikaciju. Ključevi za aplikacijski sloj su sljedeći:

- Unaprijed konfigurirani globalni ključ veze (eng. *Pre-configured global link key),* koristi se za komunikaciju između TC-a i svih ostalih čvorova
- Unaprijed konfigurirani jedinstveni ključ veze (eng. *Pre-configured unique link key*), koristi se za komunikaciju između TC-a i jednog drugog čvora
- *Trust Centar Link Key* (TCLK), koji se koristi između TC-a i jednog drugog čvora. Ovaj 128-bitni ključ izveden je iz unaprijed konfiguriranog jedinstvenog ključa veze koristeći *Matyas-Meyer-Oseas* (MMO) *hash* funkciju ili nasumično generiran od strane TC-a. Ovaj se ključ prenosi s TC-a na odgovarajući čvor s enkripcijom koristeći mrežni ključ i ,ako postoji, prethodno konfigurirani jedinstveni ključ veze za čvor. Ovaj TCLK tada se koristi za enkripciju sve sljedeće komunikacije između TC-a i relevantnog čvora, zamjenjujući unaprijed konfigurirani jedinstveni ključ veze. Međutim, čvor i dalje zadržava unaprijed konfigurirani ključ veze u slučaju da se bude trebao ponovno pridružiti u budućnosti.

- Ključ aplikacijske veze (eng. *Application Link Key*) koji se koristi između para čvorova (bez TC-a) za komunikaciju. Ovaj ključ se zahtjeva od TC-a od strane jednog od dva krajnja uređaja, a zatim ga generira TC u suradnji s IEEE/MAC adresama dva čvora. TC enkriptira ovaj ključ mrežnim ključem i ,ako postoji, unaprijed konfigurirani jedinstveni ključ veze za svaki čvor za prijenos toga ključa do svakog čvora.

Ključevi koji se koriste na mrežnom i aplikacijskom sloju u distribuiranom modelu su sljedeći:

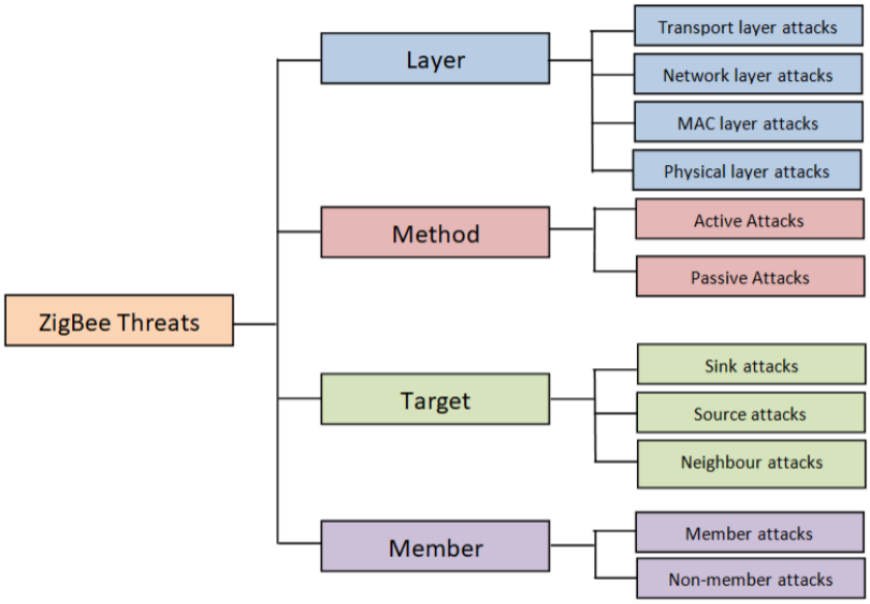
- Mrežni ključ
- Ključ veze distribuirane globalne sigurnosti (eng. *Distributed Security Global Link Key*), koji se koristi za enkripciju komunikacije između usmjerivača roditelja i pridruženog čvora. Ovaj je ključ tvornički programiran u svim čvorovima.
- Unaprijed konfigurirani ključ veze (eng. *Pre-configured Link Key*) koji se također koristi za enkripciju komunikacije između usmjerivača roditelja i pridruženog čvora. Ovaj je ključ također tvornički programiran u svim čvorovima pomoću alata za puštanje u pogon. Postoje tri vrste ovoga ključa: 1) Razvojni ključ koji se koristi tijekom razvoja prije certificiranja ZigBee-a. 2) Glavni ključ (eng. *Master Key*), koji se koristi nakon uspješne ZigBee certifikacije. 3) Certifikacijski ključ, koji se koristi tijekom ZigBee certifikacijskog testiranja

  Na kraju, korišteni ključ veze trebao bi biti glavni ključ koji pokazuje uspješnost ZigBee certifikacije.

3.1.4 ZigBee sigurnosna pitanja i ranjivosti

U ovom potpoglavlju identificirane su neke od mogućih prijetnji u ZigBee tehnologiji. Na primjer, napadi bi mogli biti usmjereni na probijanje mreže kako bi se ukrali legitimni akreditivi te s time prouzrokovali gubitak povjerljivosti i autentičnosti. Ova vrsta napada mogla bi biti u obliku pasivnog: gdje protivnik želi oštetiti vašu mrežu bez obzira na sredinu u kojoj je napad izvršen ili aktivni napad: gdje protivnik cilja određene privatne podatke. Kako bi prevladali ovaj napad, predloženo je poboljšanje algoritma šifriranja primjenom XOR-a dva puta, kao i ažuriranjem ključa za šifriranje na temelju vremenske sinkronizacije. Još jedna vrsta napada koja utječe na protokole kontrole pristupa u ZigBee-u je *Man-in-the-middle* napad dok je mreža još uvijek u formiranju ili uvodi lažne podatke o usmjeravanju tijekom otkrivanja čvora ili rute. Slijedom toga integritet okvira može biti pogođen kao i njegova autentičnost. Da bi pobijedili takve napade predložena je upotreba novog sustava raspodjele ključeva za algoritam *DiffieHellman* kombinirajući ga s protokolom ručnog potresanja (eng. *hand-shake protocol*) koji se koristi za nove čvorove tijekom pridruživanja mreži. U nekim okolnostima napadači bi mogli pokušati poslati krivotvoreni paket podatkovnih okvira kako bi zavarali primatelja i stvorili još jednu vrstu napada kao u DoS-u. Stoga bi to moglo utjecati na dostupnost, integritet i autentičnost ZigBee mreže. Kao rješenje predloženo je korištenje *Recived Signal Strenght* (RSS) za sprječavanje krađe identiteta ili prevare podataka. Otkrili su da bi različite vrijednosti RSS-a svaki put pomogle u razlikovanju legitimnog okvira podataka od maskiranog. Slijedom toga njihova predložena rješenja pomogla bi u otkrivanju napada i zaustavljanju ili filtriranju zlonamjernog okvira prije nego što se proširi mrežom. Još jedan oblik napada usmjeren je na profile javnih aplikacija ZigBee-a. [7]

Od prve verzije 2004 ZigBee je postigao mnoga učinkovita i sigurnosna poboljšanja, njegova mala računalna snaga učinila bi ga osjetljivim na mrežne napade. Od ključne je važnosti vrjednovati mrežne i sigurnosne prijetnje na ZigBee standardu, procijeniti njihov utjecaj te kasnije predložiti odgovarajuće sigurnosne kontrole i protumjere. Kao i kod bilo koje bežične senzorske mreže (WSN), prijetnje se mogu prepoznati prema tome kako se napadi provode, u kojem su sloju komunikacijskog stoga ti napadi prepoznati, je li namjeravani zlonamjerni čvor dio mreže ili ne, te na kraju koji dio mreže napada.



Slika 3.10 *ZigBee model prijetnji [7]*

Slika 3.10 prikazuje ZigBee moguće prijetnje i napade usvajanjem WSN modela prijetnji. Napadi mogu varirati od prisluškivanja radijskog kanala ZigBee mreže kako bi se dodao zlonamjerni sadržaj ili ponovno poslao stari paket, do ozbiljnijih napada kao što je dodavanje zlonamjernog čvora u mrežu kako bi se prepisala memorija od normalnog razmještaja čvorova. Kao što je prikazano na Slici 3.10 napadi na ZigBee mogu se kategorizirati u sljedeće:

A. Napadi slojeva

1. Napadi transportnog sloja:

   Ovaj se sloj koristi za potporu komunikacijskim vezama za senzore koji se tek pridružuju mreži. Napadi mogu uključivati poplave (eng. *flooding*) i desinkronizaciju, gdje je ciljano čvorište poplavljeno brojnim nevažećim zahtjevima za uspostavu veze (poplavni napad) i krivotvorenje paketa na jednom ili oba kraja veze tako da domaćin zatraži retransmisiju nedostajućih okvira paketa (napad desinkronizacije).

2. Napadi mrežnog sloja:

   Ovaj sloj je odgovoran za proces usmjeravanja i mrežni promet. Napadi mogu uključivati crvotočine i selektivne napade prosljeđivanja. U napadu crvotočina trebala bi postojati dva zlonamjerna čvora koja se nalaze na različitim *hops* mreže. Kada čvor pošiljatelja prenosi podatkovni okvir, jedan zlonamjerni čvor tunelira te podatke drugom zlonamjernom čvoru koji će ga zatim poslati susjednim

čvorovima. Posljedično tome maliciozni čvor je prevaren da se maliciozni čvorovi nalaze jedan ili dva skoka dalje, no isti mogu biti izvan dosega

3. Napadi MAC sloja

   Uključuje MAC zaglavlje koje pomaže prijemniku da zna duljinu paketa, vrši retransmisiju okvira u slučaju greške i raspoređuje resurse za nove spojene čvorove. Blokiranje (eng. *jamming)* sloja veze jedan je primjer napada MAC sloja koji se pokreće za stvaranje DoS prekidajući razmjenu poruka između odašiljačkih i prijemnih čvorova. Time bi se degradirao i smanjio učinak mreže.

4. Napadi fizičkog sloja

   Napadi uglavnom iskorištavaju zajednički radio signal kako bi prisluškivali ili dodavali informacije okvirima podatkovnih paketa.

B. Metode napada

C.

1. Aktivni napadi

   Ovaj napad zahtjeva stvarno odsijecanje (presretanje) mreže gdje protivnik može modificirati podatke, ubacivati pogrešne podatkovne okvire te sa svime time na rad mreže utjecati negativno. Štoviše integritet i povjerljivost podatka su ugroženi

2. Pasivni napadi

   Za razliku od aktivnih napada, nema presretanja stvarnog komunikacijskog toka, već napadač nadzire promet podataka bez utjecaja na njihov integritet. Međutim povjerljivost podataka je izložena jer se osjetljive informacije mogu prikupiti za neke druge zlonamjerne namjere.

D. Ciljani napadi

1. *Sink* napadi

   Sinkhole ili jednostavno *sink* napad može se dogoditi kada zlonamjerni čvor najavi rutu koja je najkraći put. A budući da svi algoritmi usmjeravanja odaberu najkraći put, privući će više mrežnog prometa koji će biti tuneliran prema njemu. Obično se ovaj napad kombinira s napadom crvotočine.

2. Izvorni napadi

   U tim napadima, protivnik kompromitira jedan legitiman čvor koji će djelovati kao čvor crne rupe. Tada taj čvor selektivno ispusti primljene pakete ili sve primljene pakete kako bi zavarao druge susjedne čvorove da potraže drugu rutu jer prethodna ruta nije bila uspješna.

3. Susjedski napadi

   Ova vrsta napada iskorištava postupak otkrivanja drugih susjednih čvorova emitiranjem HELLO poruke. Zlonamjerni čvor šalje HELLO poruke s velikom prijenosnom snagom, te stoga prijemni čvorovi smatraju ovaj čvor svojim susjedom i u zamjenu će poslati osjetljive paketne podatke. Zbog toga će se potrošiti ogromna količina energije, a uslijed toga može doći do zagušenja.

4. Napadi članova

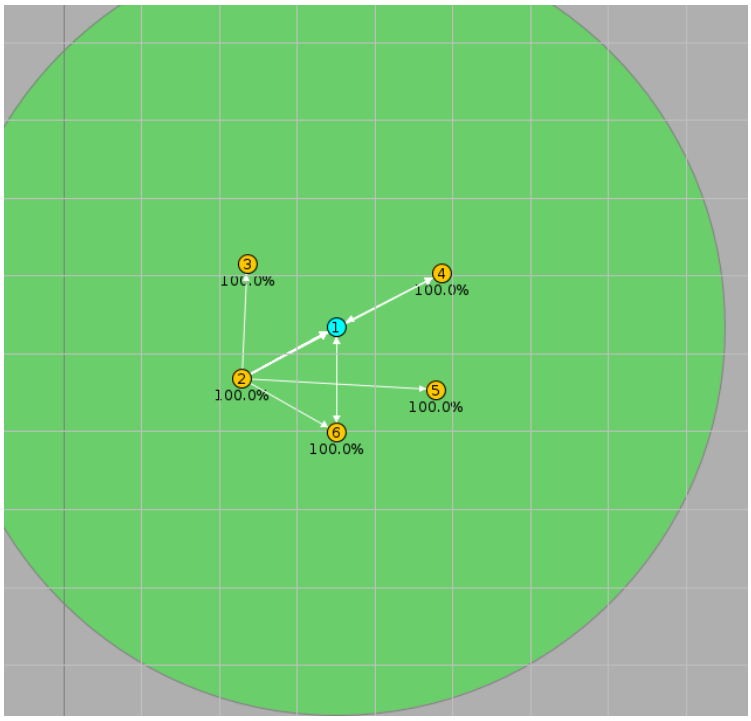
   Ponekad se nazivaju izopćenim i insajderskim napadima. U slučaju vanjskih napada, napadački član nije dio mreže, ali je ovlašten prijetiti mreži. S druge strane napadi iznutra, napad insajdera (člana) događa se kada je zlonamjerni čvor dio mreže bilo kompromitiranjem ili je napadač učitao lažni profil i zatražio pridruživanje mreži.

5. Napad potrošnje energije (eng. *Ghost Attack*)

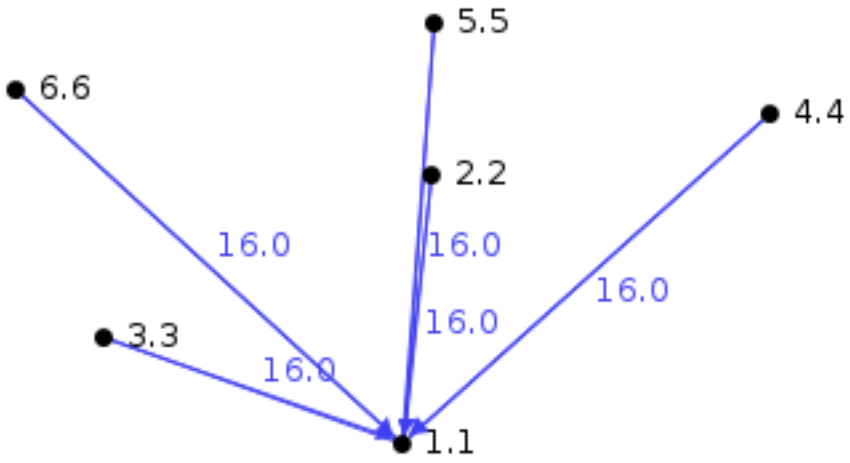
   Napadač šalje lažne poruke kako bi namamio čvor da troši energiju zbog suvišnih proračuna povezanih sa sigurnošću. Time će skratiti životni vijek čvora i omogućiti napadaču da pokrene nekoliko napada nakon iscrpljivanja kao što je slučaj s DoS napadom. [7]

4. EKSPERIMENTALNI DIO

Razvojem sljedeće generacije IoT-a, bežično umrežavanje kratkog dometa prihvaća internetske tehnologije. Kao rezultat toga komunikacija između Interneta i bežičnih senzorskih mreža (WSN-a) postaje žarišno područje istraživanja. Međutim dobro je poznato da je internetska struktura neprikladna za WSN mreže zbog njihovih strogih ograničenja na resurse, potrošnju energije i kvalitetu komunikacijskih kanala. Kako bi se zadovoljile potrebe i riješili problemi, IETF je razvio IP protokole za mreže male snage i gubitke putem radnih grupa 6LoWPAN i RoLL, koje nam pružaju mogućnost korištenja IPv6 u WSN-ovima. Za analizu podataka koristi se operativni sustav *Contiki* i simulator COOJA pomoću kojeg se prate parametre kao što su latencija, potrošnja energije i tako dalje. Navedeni parametri su ključni za ukupnu učinkovitost bežične senzorske mreže. RPL se temelji na protokolu usmjeravanja IPv6 koji se koriste mreže s niskom potrošnjom i niskim gubicima (LLN). [9]

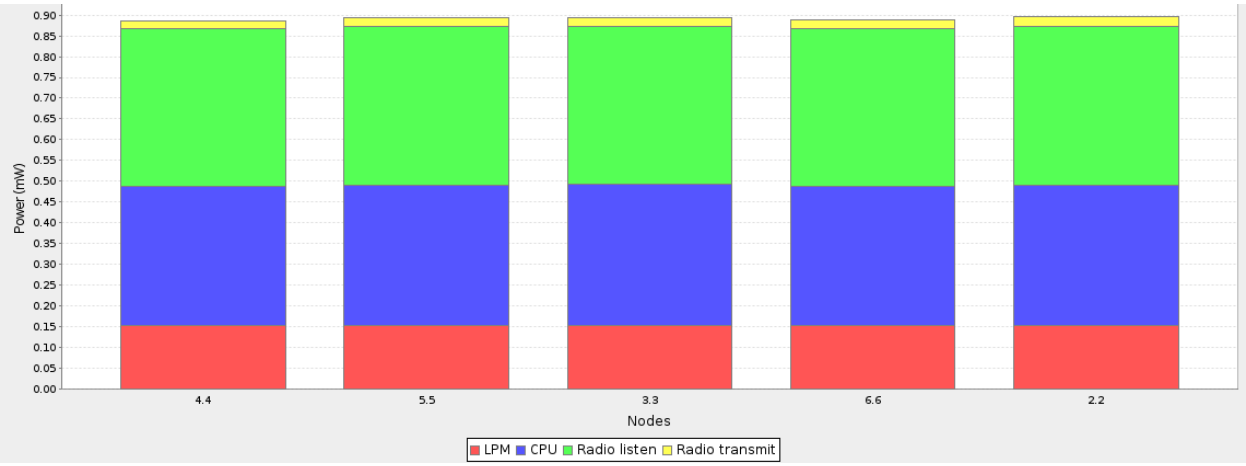


Slika 4.1 *Topologija WSN-a s pet čvorova*



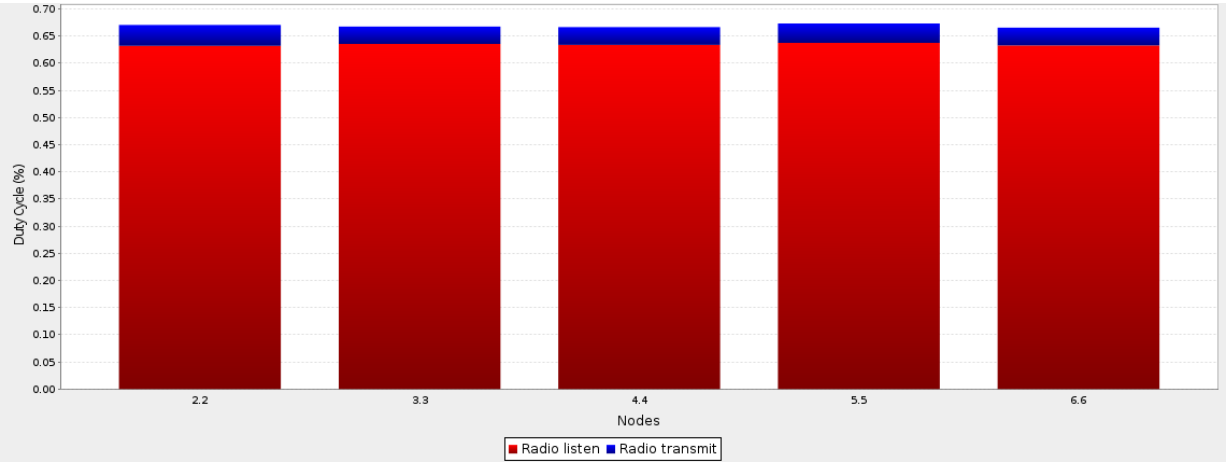
Slika 4.2 *Mrežna topologija čvorova*

Na slici 4.1 prikazana je topologija WSN-a (1 *sink* čvor i 5 klijent čvorova) koju je konstruirao COOJA, a strijelce na slici 4.2 prikazuju smjer prijenosa paketa. Svih pet čvorova se nalaze u dometu *snik*-a te s njim izravno komuniciraju.



Slika 4.3 *Prosječna potrošnja energije*

Na slici 4.3 je prikazana prosječna potrošnja energije po čvorovima, svi čvorovi imaju približno jednaku potrošnju i ona iznosi oko 0,90 mW. Čvorovi veći dio energije troše na osluškivanje i rad centralne procesorske jedinice te vrlo mali dio na prijenos.



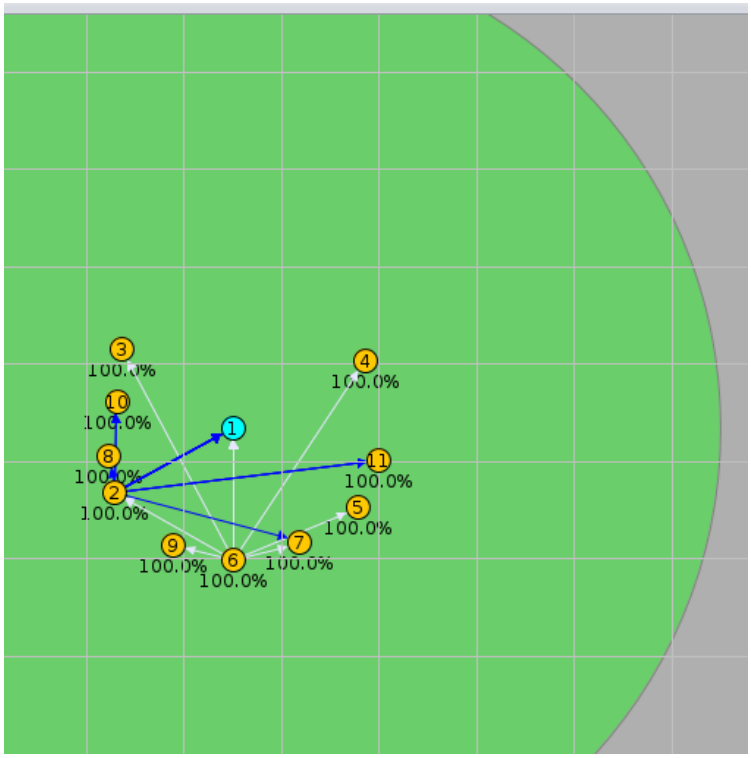
Slika 4.4 *Prosječna radni ciklus (eng. Radio Duty Cycle)*

Na slici 4.4 je prikazan postotak osluškivanja i prijenosa za pojedine čvorove. Svih pet čvorova većinu vremena osluškuju ,a tek mali dio vremena prenose.

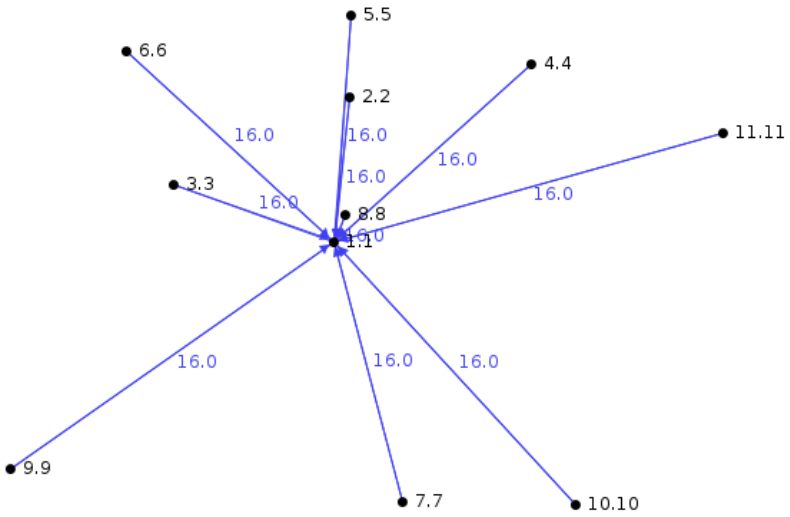
Node	Received	Lost	Hops	Rtmetric	ETX	CPU Power	LPM Power	Listen Power	Transmit Power	Power	Listen Duty Cycle	Transmit Duty Cycle
1.1	0	0	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000
2.2	68	0	1.000	416.574	16....	0.337	0.153	0.378	0.018	0.887	0.630	0.035
3.3	67	0	1.000	417.388	16....	0.338	0.153	0.381	0.016	0.889	0.635	0.030
4.4	68	0	1.000	416.794	16....	0.334	0.153	0.380	0.016	0.884	0.634	0.030
5.5	68	0	1.000	416.574	16....	0.336	0.153	0.382	0.017	0.889	0.637	0.032
6.6	67	0	1.000	417.448	16....	0.336	0.153	0.380	0.016	0.886	0.634	0.030
7.7	0	0	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000
Avg	**67.600**	**0.000**	**1.000**	**416.955**	**16....**	**0.336**	**0.153**	**0.380**	**0.017**	**0.887**	**0.634**	**0.031**

Tablica 4.1 *Informacije o čvorovima*

U tablici 4.1 prikazane su informacije o pojedinim čvorovima te prosječne informacije na osnovu tih pet čvorova. Iz tablice vidimo da svi čvorovi sa *sink*-om komuniciraju iz jednog skoka ,tj.izravno te da nema gubitka paketa.

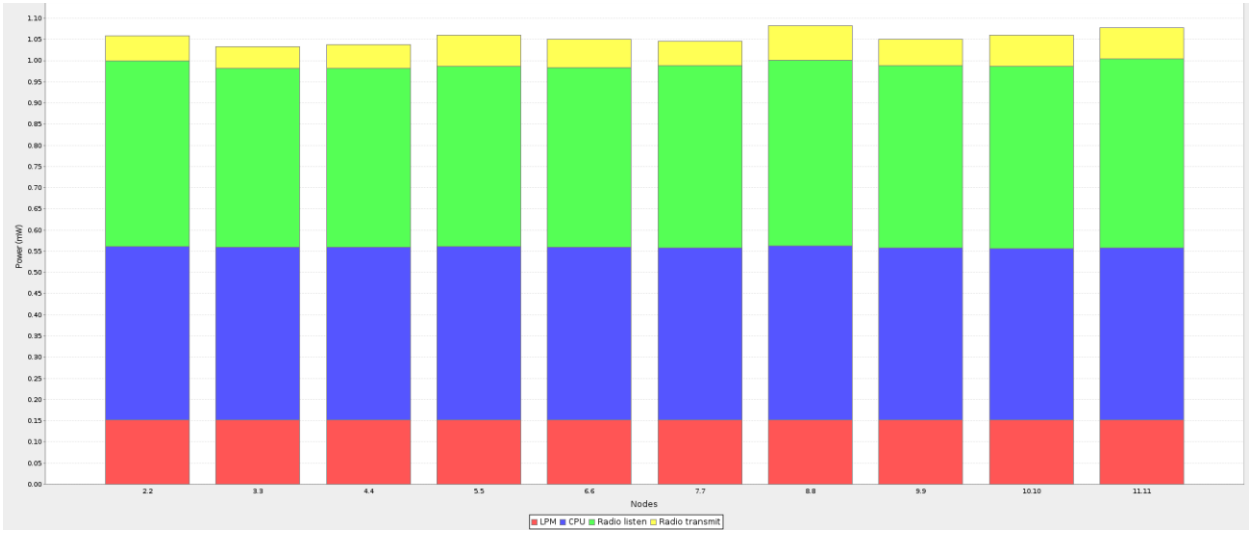


Slika 4.5 *Topologija WSN-a s deset čvorova*



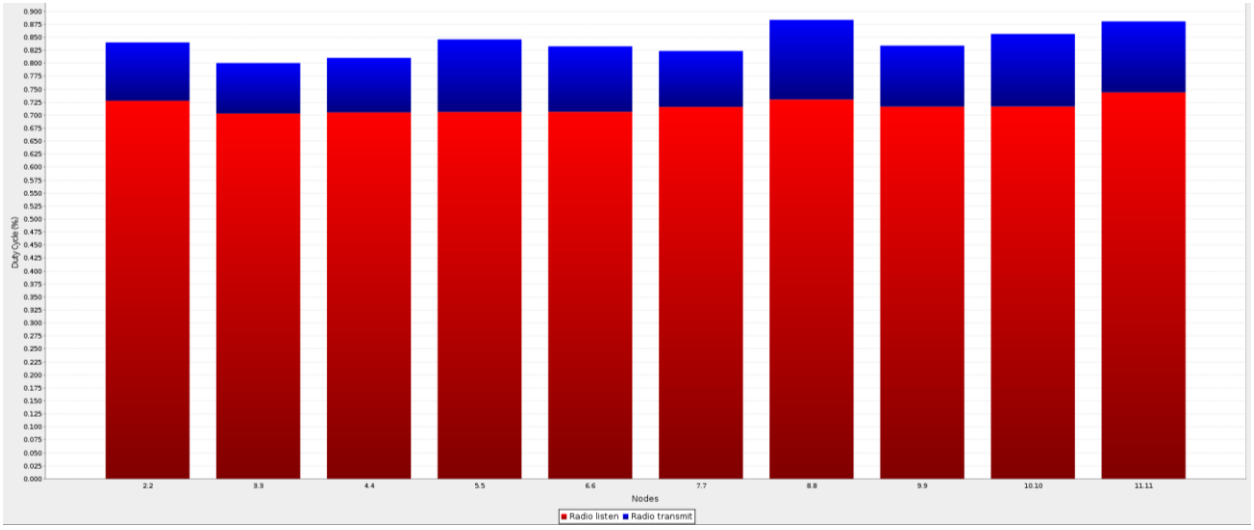
Slika 4.6 *Mrežna topologija čvorova*

Broj čvorova je povećan s pet na deset, ali i dalje svi čvorovi komuniciraju izravno sa baznom stanicom ,tj. *sink*-om.



Slika 4.7 *Prosječna potrošnja energije*

U odnosu na mrežu s pet čvorova potrošnja centralne procesorske jedinice, radio prijenosa i radio osluškivanja je povećana što je vidljivo na slici 4.7 pa se s time i cjelokupna potrošnja veća od mreže s pet čvorova.



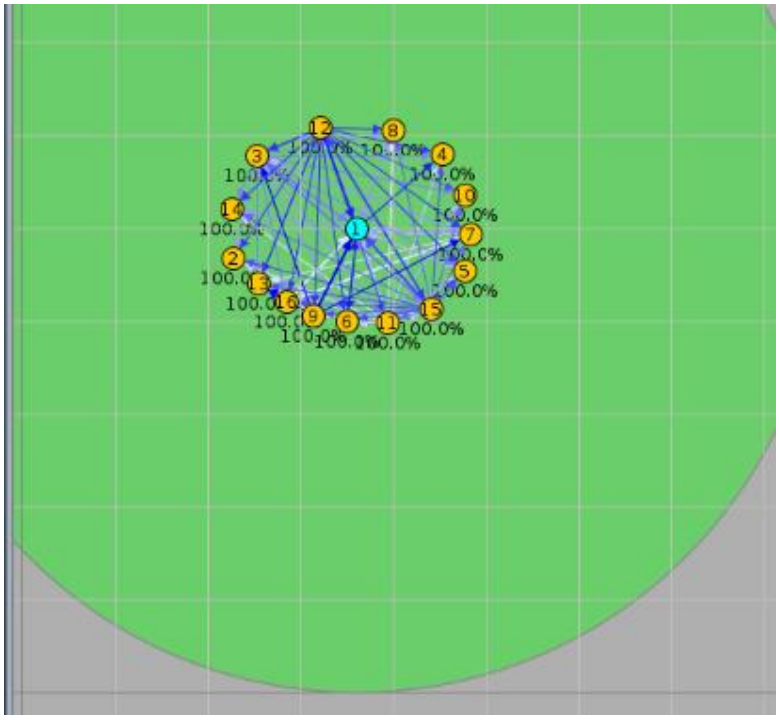
Slika 4.8 *Prosječna radni ciklus (eng. Radio Duty Cycle)*

Na slici 4.8 vidimo povećanje postotaka osluškivanja i prijenosa u odnosu na mrežu s pet čvorova.

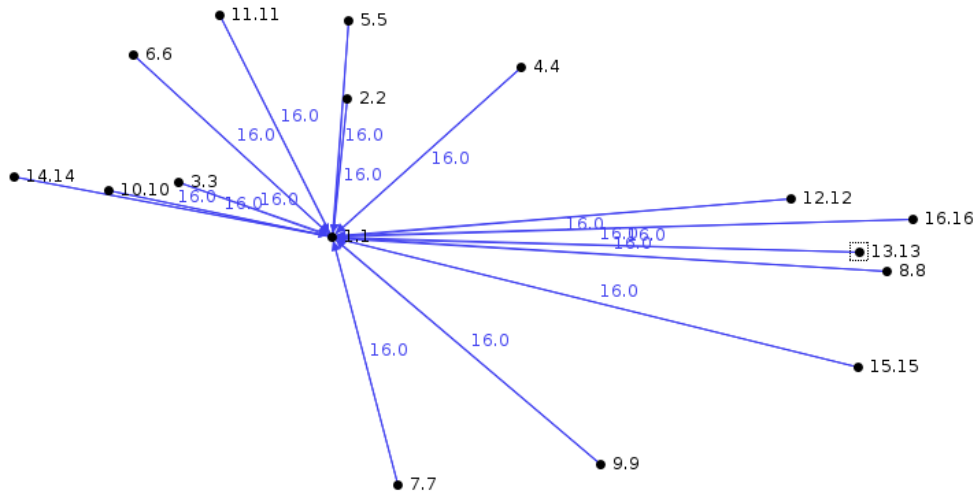
Node	Received	Lost	Hops	Rtmetric	ETX	CPU Power	LPM Power	Listen Power	Transmit Power	Power	Listen Duty Cycle	Transmit Duty Cycle
1.1	0	0	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000
2.2	6	0	1.000	713.833	16....	0.411	0.151	0.437	0.060	1.058	0.728	0.112
3.3	6	0	1.000	713.833	16....	0.408	0.151	0.422	0.051	1.033	0.703	0.097
4.4	7	0	1.000	700.714	16....	0.408	0.151	0.423	0.056	1.038	0.705	0.105
5.5	6	0	1.000	713.833	16....	0.411	0.151	0.424	0.074	1.060	0.706	0.140
6.6	7	0	1.000	694.714	16....	0.408	0.151	0.424	0.067	1.050	0.707	0.126
7.7	7	0	1.000	700.714	16....	0.407	0.151	0.430	0.057	1.045	0.716	0.107
8.8	7	0	1.000	694.714	16....	0.411	0.151	0.438	0.081	1.082	0.730	0.153
9.9	7	0	1.000	694.714	16....	0.407	0.151	0.430	0.062	1.050	0.717	0.117
10.10	6	0	1.000	713.833	16....	0.405	0.151	0.430	0.074	1.060	0.717	0.140
11.11	7	0	1.000	694.714	16....	0.407	0.151	0.446	0.073	1.077	0.744	0.137
Avg	**6.600**	**0.000**	**1.000**	**703.562**	**16....**	**0.408**	**0.151**	**0.430**	**0.066**	**1.055**	**0.717**	**0.123**

Tablica 4.2 *Informacije o čvorovima*

Iz tablice 4.2 vidimo da svi čvorovi sa *sink*-om komuniciraju iz jednog skoka ,tj. izravno te da nema gubitka paketa.

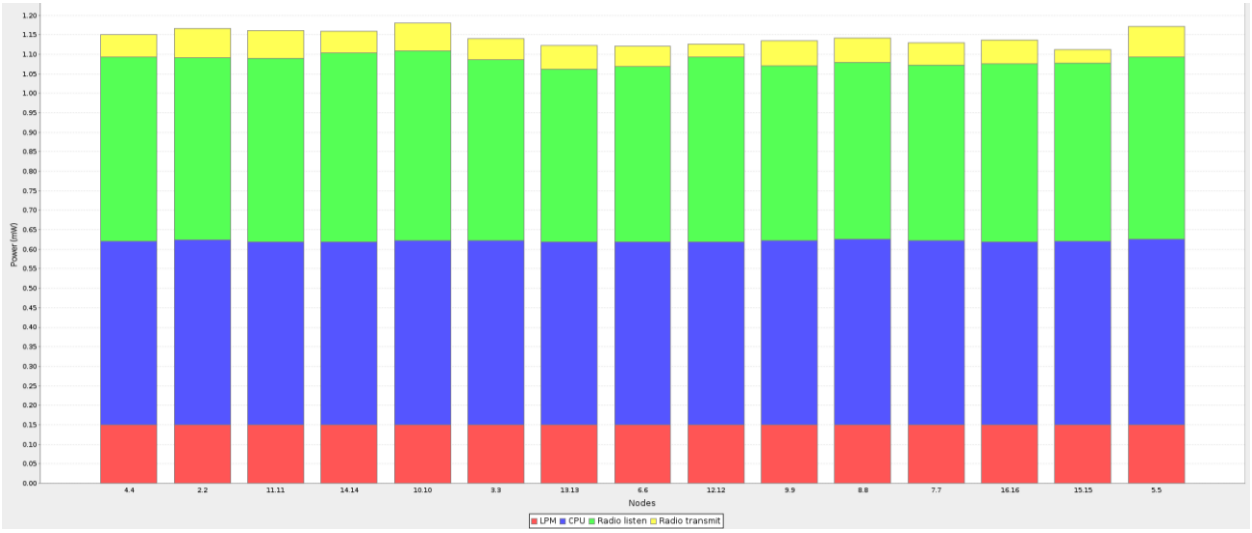


Slika 4.9 *Topologija WSN-a s petnaest čvorova*



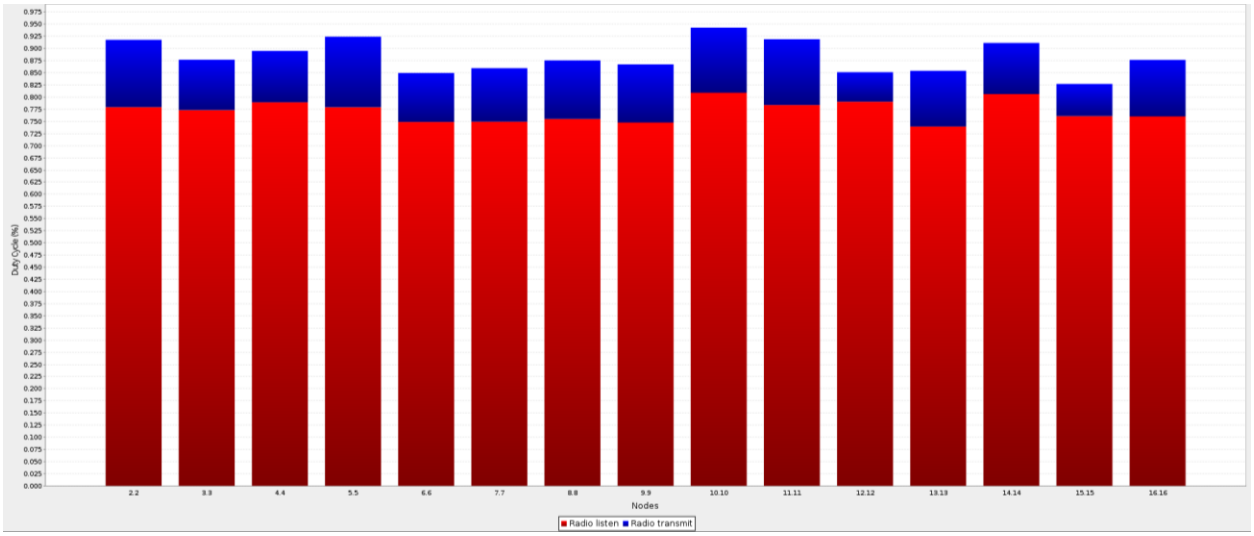
Slika 4.10 *Mrežna topologija čvorova*

Na slici 4.9 vidimo povećanje broja čvorova WSN-a s deset na petnaest čvorova, ali i dalje u izravnoj komunikaciji s baznom stanicom



Slika 4.11 *Prosječna potrošnja energije*

Na slici 4.11 je svi čvorovi imaju približno jednaku potrošnju i ona iznosi oko 1,15 mW. Za razliku od mreže s deset čvorova potrošnja centralne procesorske jedinice, radio prijenosa i radio osluškivanja je povećana pa se s time i cjelokupna potrošnja veća od mreže s deset čvorova.



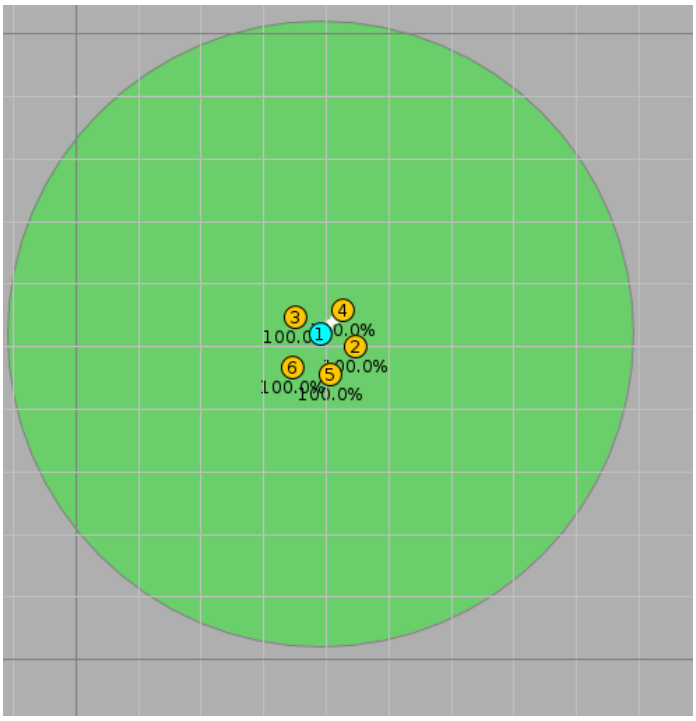
Slika 4.12 *Prosječna radni ciklus (eng. Radio Duty Cycle)*

Na slici 4.12 za razliku od mreže s deset čvorova veći je postotak osluškivanja i prijenosa.

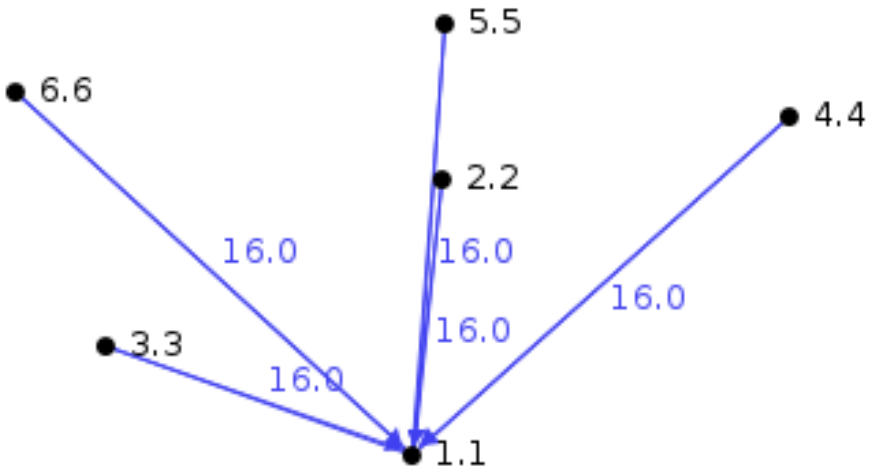
Node	Received	Lost	Hops	Rtmetric	ETX	CPU Power	LPM Power	Listen Power	Transmit Power	Power	Listen Duty Cycle	Transmit Duty Cycle
1.1	0	0	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000
2.2	8	0	1.000	677.875	16....	0.475	0.149	0.468	0.074	1.166	0.780	0.138
3.3	8	0	1.000	677.875	16....	0.472	0.149	0.464	0.055	1.141	0.773	0.104
4.4	8	0	1.000	677.875	16....	0.471	0.149	0.474	0.056	1.150	0.789	0.106
5.5	8	0	1.000	680.625	16....	0.477	0.149	0.468	0.077	1.171	0.779	0.145
6.6	8	0	1.000	677.875	16....	0.469	0.149	0.449	0.053	1.121	0.749	0.101
7.7	8	0	1.000	677.875	16....	0.473	0.149	0.450	0.058	1.130	0.749	0.110
8.8	8	0	1.000	677.875	16....	0.476	0.149	0.453	0.064	1.142	0.755	0.121
9.9	8	0	1.000	677.875	16....	0.473	0.149	0.449	0.064	1.134	0.748	0.120
10.10	8	0	1.000	677.875	16....	0.474	0.149	0.485	0.071	1.180	0.809	0.134
11.11	8	0	1.000	677.875	16....	0.470	0.149	0.470	0.072	1.162	0.784	0.135
12.12	8	0	1.000	683.125	16....	0.470	0.149	0.474	0.032	1.126	0.791	0.061
13.13	8	0	1.000	677.875	16....	0.469	0.149	0.444	0.061	1.123	0.740	0.115
14.14	8	0	1.000	677.875	16....	0.470	0.149	0.484	0.056	1.159	0.806	0.105
15.15	8	0	1.000	680.625	16....	0.471	0.149	0.457	0.035	1.112	0.761	0.066
16.16	8	0	1.000	680.625	16....	0.470	0.149	0.456	0.062	1.137	0.760	0.116
Avg	**8.000**	**0.000**	**1.000**	**678.775**	**16....**	**0.472**	**0.149**	**0.463**	**0.059**	**1.144**	**0.772**	**0.112**

Tablica 4.3 *Informacije o čvorovima*

U tablici 4.3 naznačena je komunikacija sa baznom stanicom iz jednog skoka ,tj. izravna komunikacija.

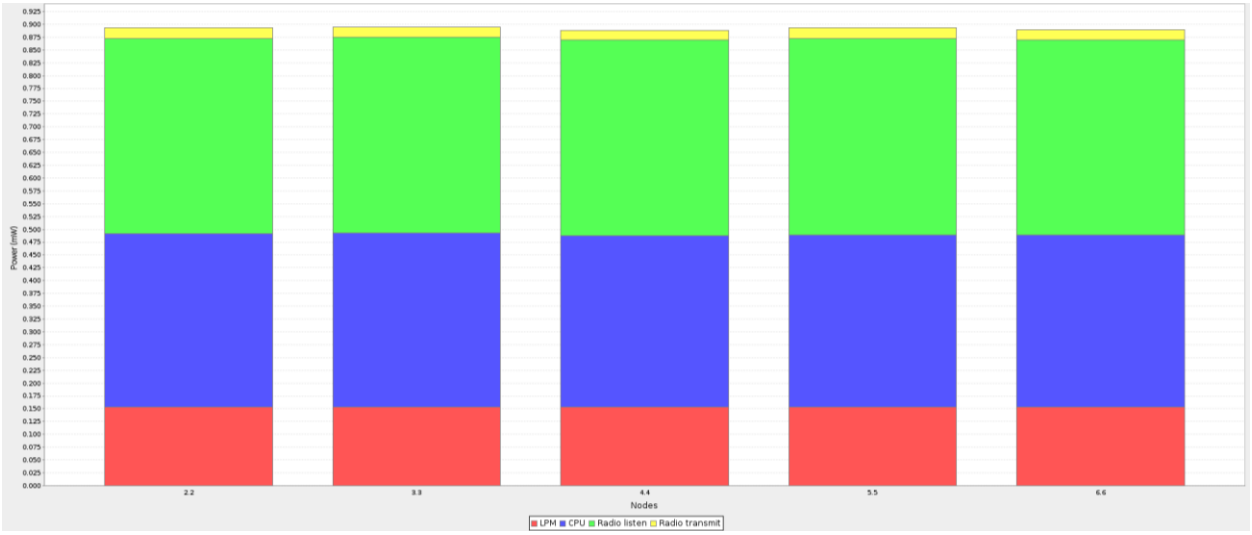


Slika 4.13 *Topologija WSN-a s udaljenim čvorova*



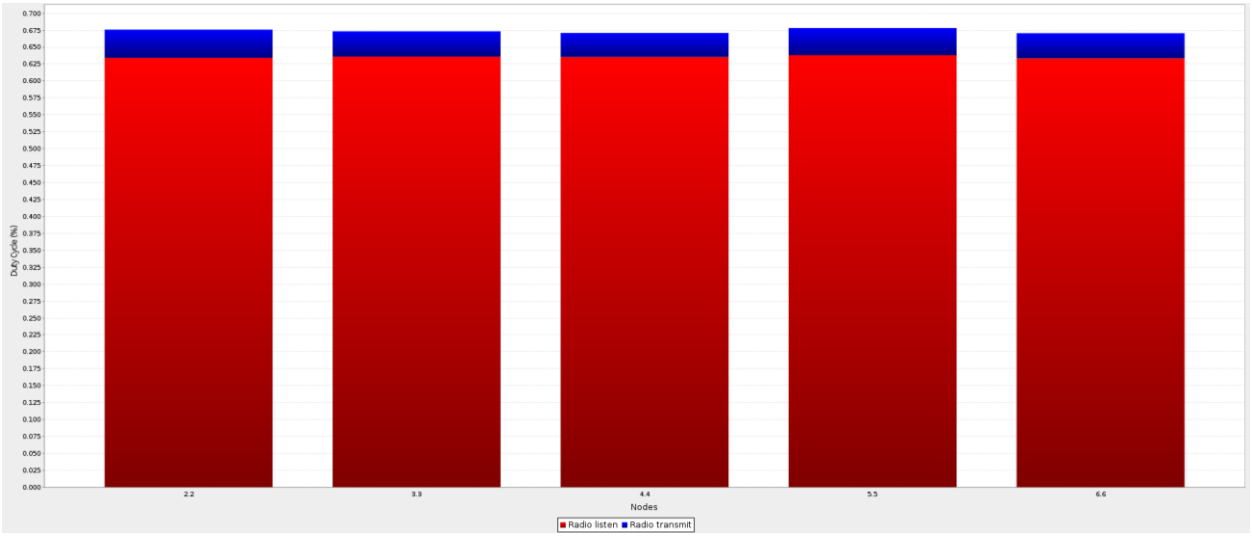
Slika 4.14 *Mrežna topologija čvorova*

Na slici 4.13 svih pet čvorova nalaze se u neposrednoj blizini *sink*-a te zbog toga s njim imaju izravnu komunikaciju.



Slika 4.15 *Prosječna potrošnja energije*

Slika 4.15 prikazuje potrošnju čvorova koja iznosi oko 0,90 mW te je približno jednaka za sve čvorove te da veći dio energije troše na osluškivanje i rad centralne procesorske jedinice te vrlo mali dio na prijenos.

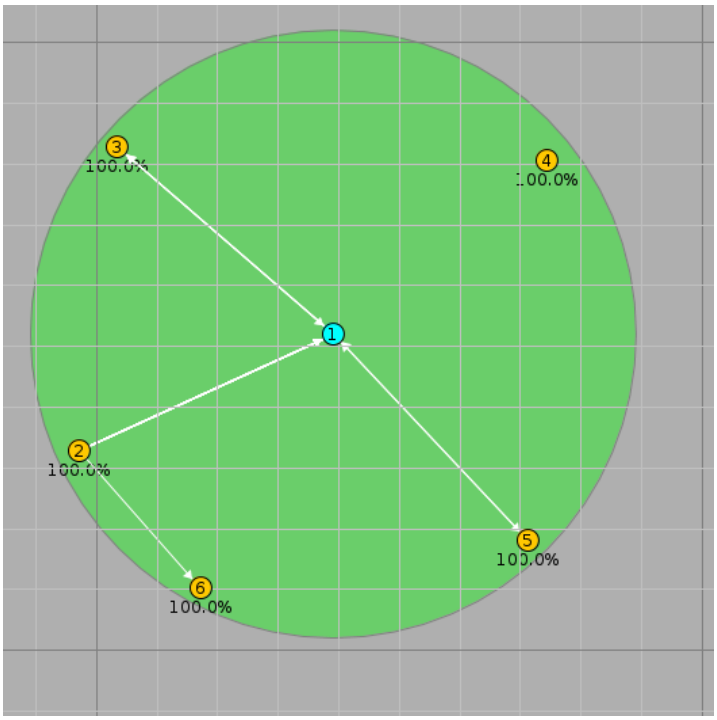


Slika 4.16 *Prosječna radni ciklus (eng. Radio Duty Cycle)*

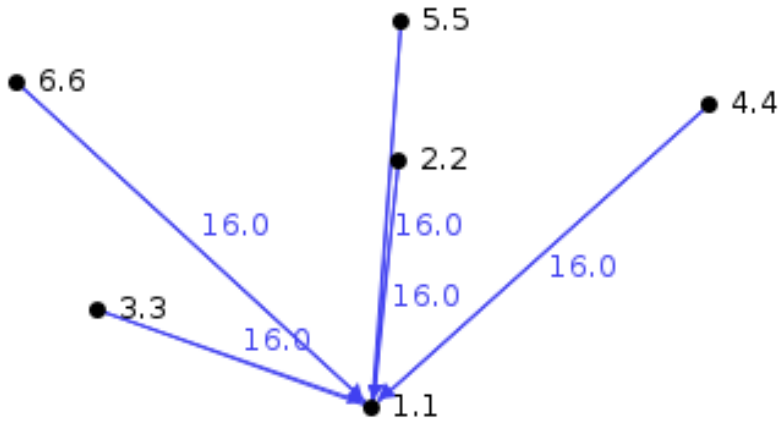
Node	Received	Lost	Hops	Rtmetric	ETX	CPU Power	LPM Power	Listen Power	Transmit Power	Power	Listen Duty Cycle	Transmit Duty Cycle
1.1	0	0	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000
2.2	45	0	1.000	433.222	16....	0.338	0.153	0.381	0.022	0.894	0.634	0.042
3.3	45	0	1.000	433.711	16....	0.340	0.153	0.382	0.020	0.894	0.636	0.037
4.4	45	0	1.000	433.556	16....	0.335	0.153	0.381	0.019	0.888	0.635	0.036
5.5	45	0	1.000	433.222	16....	0.336	0.153	0.383	0.021	0.893	0.638	0.040
6.6	45	0	1.000	433.800	16....	0.336	0.153	0.380	0.020	0.889	0.633	0.037
7.7	0	0	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000
Avg	**45.000**	**0.000**	**1.000**	**433.502**	**16....**	**0.337**	**0.153**	**0.381**	**0.020**	**0.892**	**0.635**	**0.038**

Tablica 4.4 *Informacije o čvorovima*

Svih pet čvorova većinu vremena osluškuju, a tek mali dio vremena prenose što je vidljivo na slici 4.16 te u tablici 4.4

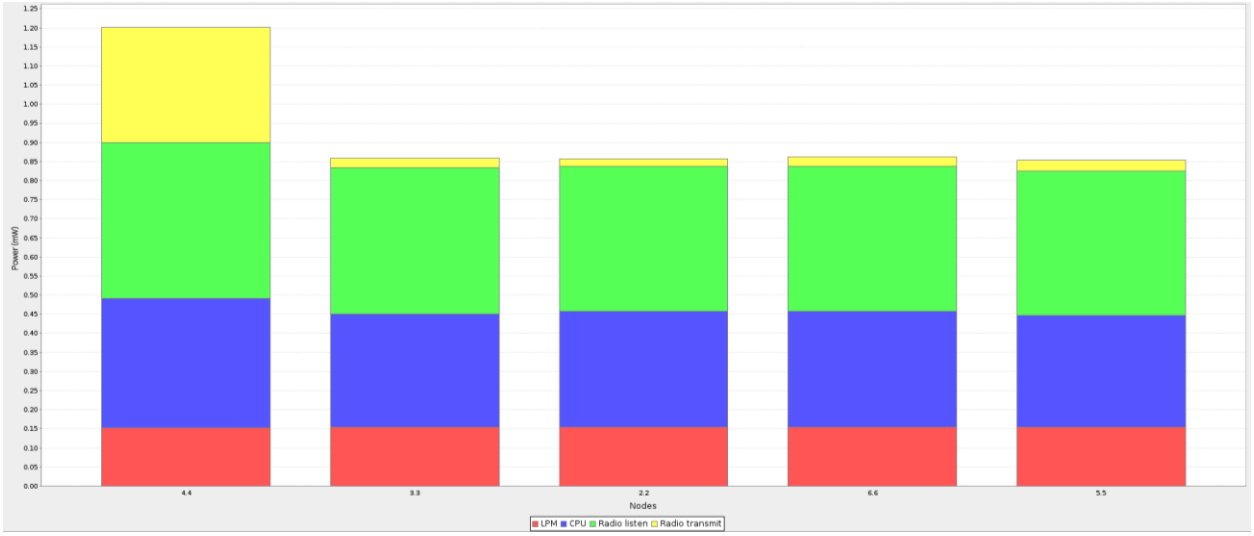


Slika 4.17 *Topologija WSN-a s udaljenim čvorova*



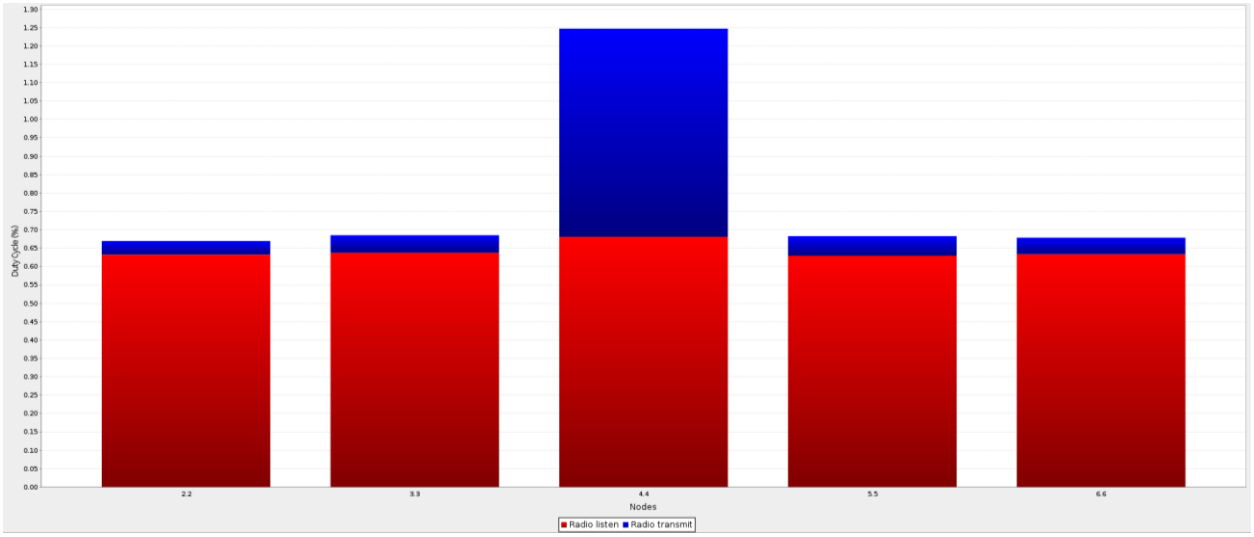
Slika 4.18 *Mrežna topologija čvorova*

Svi čvorovi su udaljeni od *sink*-a te se nalaze u njegovom dometu i imaju izravnu komunikaciju ,ali na samoj granici dometa što je vidljivo na slikama 4.17 i 4.18.



Slika 4.19 *Prosječna potrošnja energije*

Čvorovi 2, 3, 5 i 6 imaju približno jednaku potrošnju oko 0,85 mW dok čvor 4 ima veću potrošnju koja iznosi 1,201 mW. Čvorovi 2, 3, 5, 6 veći dio energije troše na osluškivanje i rad centralne procesorske jedinice te vrlo mali dio na prijenos. U odnosu na ostale čvorove, čvor 4 troši veći iznos energije na osluškivanje što je vidljivo iz slike 4.19.

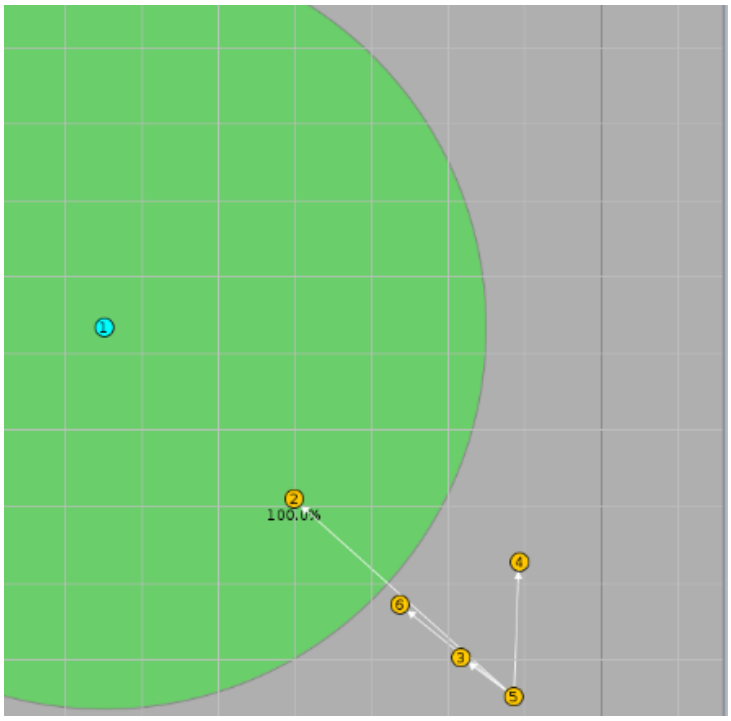


Slika 4.20 *Prosječna radni ciklus (eng. Radio Duty Cycle*

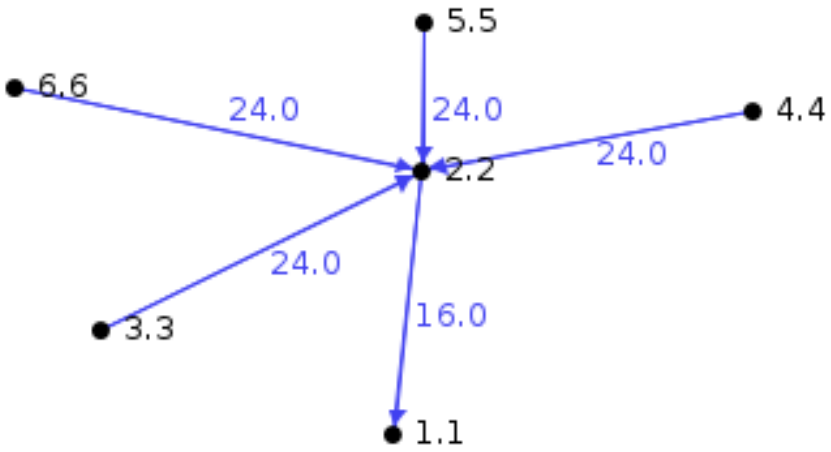
Node	Received	Lost	Hops	Rtmetric	ETX	CPU Power	LPM Power	Listen Power	Transmit Power	Power	Listen Duty Cycle	Transmit Duty Cycle
1.1	0	0	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000
2.2	29	0	1.000	469.379	16....	0.303	0.154	0.379	0.020	0.857	0.632	0.037
3.3	29	0	1.000	461.138	16....	0.296	0.155	0.382	0.025	0.859	0.637	0.048
4.4	1	0	1.000	718.000	16....	0.338	0.153	0.409	0.301	1.201	0.681	0.566
5.5	29	0	1.000	462.138	16....	0.292	0.155	0.378	0.028	0.853	0.629	0.053
6.6	29	0	1.000	469.793	16....	0.304	0.154	0.380	0.024	0.862	0.634	0.045
7.7	0	0	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000
Avg	**23.400**	**0.000**	**1.000**	**516.090**	**16....**	**0.307**	**0.154**	**0.386**	**0.080**	**0.926**	**0.643**	**0.150**

Tablica 4.5 *Informacije o čvorovima*

Na slici 4.20 i tablici 4.5 prikazani su čvorovi 2, 3, 5 i 6 koji mali postotak vremena prenose dok većinu vremena osluškuju. Čvor 4 ima skoro pa jedak postotak osluškivanja i prijenosa u korist osluškivanja.

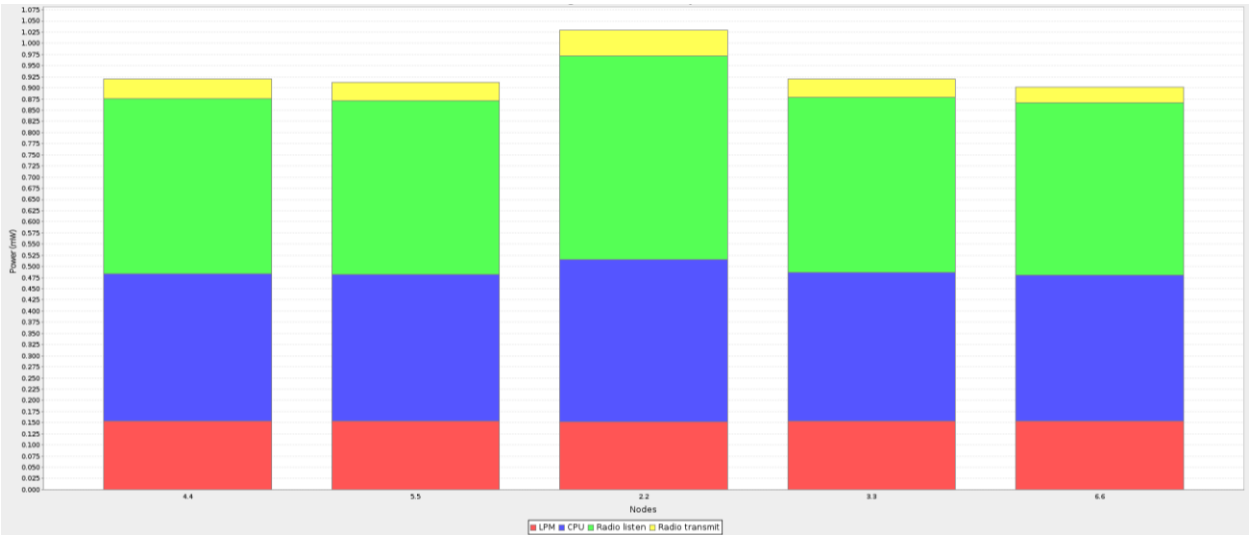


Slika 4.21 Topologija WSN-a s udaljenim *čvorova*



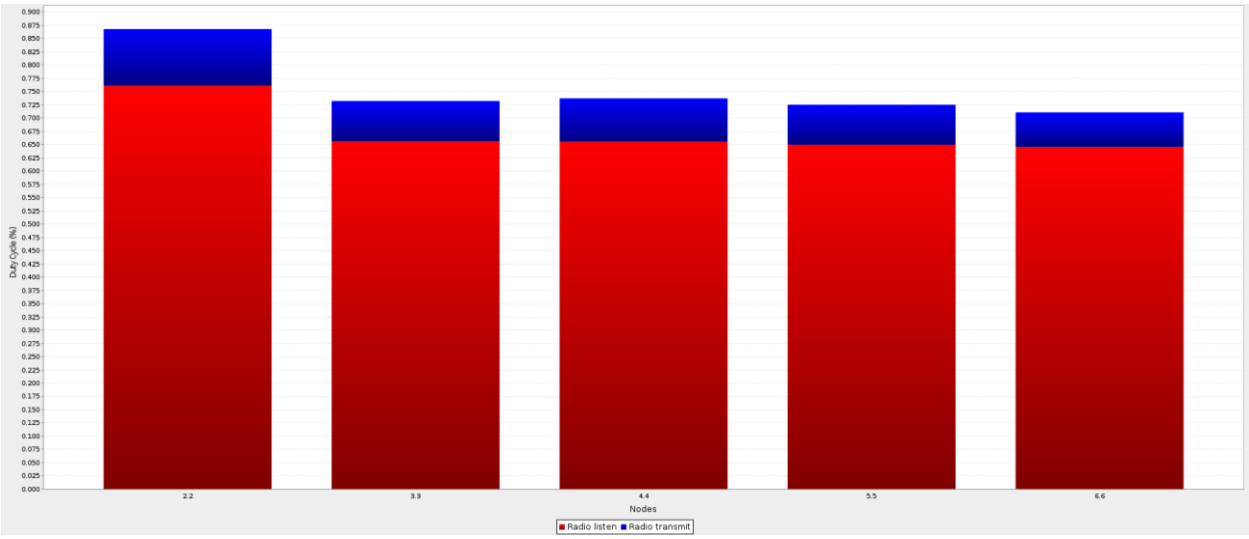
Slika 4.22 *Mrežna topologija čvorova*

Na slici 4.21 vidljivo je da se čvor 2 jedino nalazi unutar dometa *sink*-a i komunikacija se odvija izravno, dok ostali čvorovi 3, 4, 5 i 6 nisu u dometu *snik*-a te ne mogu izravno komunicirati sa s*ink*-om. Na slici 4.22 vidimo da se komunikacija čvorova 3, 4, 5, 6 odvija preko čvora 2.



Slika 4.23 *Prosječna potrošnja energije*

Na slici 4.23 čvorovi 3, 4, 5 i 6 imaju približno jednaku potrošnju oko 0,920 mW dok čvor 2 ima veću potrošnju koja iznosi 1,029 mW. Čvor 2 ima povećanu potrošnju energije jer preko njega ostali čvorovi u dva skoka dolaze do *sink*-a. Čvorovi veći dio energije troše na osluškivanje i rad centralne procesorske jedinice, a vrlo mali dio na prijenos.



Slika 4.24 *Prosječna radni ciklus (eng. Radio Duty Cycle)*

Na slici 4.24 je prikazan postotak osluškivanja i prijenosa za pojedine čvorove. Čvorovi veći postotak osluškuju dok manji dio odlazi na prijenos. Čvor dva ima nešto veći postotak i prijenosa i osluškivanja zbog njegove uloge posrednika ostalim čvorovima do *sink*-a.

Node	Received	Lost	Hops	Rtmetric	ETX	CPU Power	LPM Power	Listen Power	Transmit Power	Power	Listen Duty Cycle	Transmit Duty Cycle
1.1	0	0	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000
2.2	28	0	1.000	385.536	16....	0.363	0.153	0.457	0.057	1.029	0.761	0.107
3.3	28	0	2.000	597.143	24....	0.333	0.153	0.394	0.041	0.920	0.656	0.077
4.4	28	0	2.000	601.179	24....	0.330	0.154	0.393	0.044	0.920	0.655	0.082
5.5	28	0	2.000	599.393	24....	0.329	0.154	0.390	0.040	0.912	0.650	0.076
6.6	28	0	2.000	601.107	24....	0.326	0.154	0.387	0.035	0.902	0.645	0.066
7.7	0	0	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000
Avg	**28.000**	**0.000**	**1.800**	**556.871**	**22....**	**0.336**	**0.153**	**0.404**	**0.043**	**0.937**	**0.673**	**0.081**

Tablica 4.6 *Informacije o čvorovima*

Iz tablice 4.6 vidimo da samo jedan čvor (2) može komunicirati sa *sink*-om ,a ostali čvorovi do njega dolaze u dva skoka pomoću posrednika, čvora 2.

4.1. Analiza podataka

Rađene simulacije pokazuju razlike u potrošnji energije prilikom različitog broja klijent čvorova (pet, deset ili petnaest) te udaljenosti klijent čvorova od bazne stanice ,tj. *sink*-a. Potrošnja energije najvažniji je čimbenik niske razine mreže napajanja i gubitaka te je to također glavni ograničavajući čimbenik senzorskih mreža. Povećanjem broja klijent čvorova koje poslužuje jedna bazna stanica u mreži povećava se i potrošnja energije zbog povećanog zahtjeva rada centralne procesorske jedinice, povećane potrebe za osluškivanjem i prijenosom. Povećanjem udaljenosti klijent čvorova od bazne stanice raste i potrošnja energije, a scenarij u kojem klijent čvorovi nisu u dometu bazne stanice te oni ne mogu izravno komunicirati ,već vrše komunikaciju preko čvora posrednika u više skokova dodatno povećava potrošnju istoga.

5. ZAKLJUČAK

U ovom radu predstavljeni su sigurnosni problemi i privatnost u IoT sustavima. Svi IoT uređaji mogu biti ranjivi na određenu vrstu napada. To ukazuje na potrebe razvoja opće sigurnosne politike i standarda za IoT potrebe. IoT proizvodna industrija mora usko surađivati s nadzornim agencijama kao što su, FSA i DHS, i organizacijom za standardizaciju kako bi se borila protiv novonastalih prijetnji, kao i razvijati snažne i robusne sigurnosne standarde za IoT uređaje i sustave Analizirana su ograničenja IoT uređaja u pogledu baterije i računalnih resursa. Sigurnosni zahtjevi WSN mreža imaju veliku važnost budući da su iste podložne raznim napadima. Senzorni čvorovi u WSN imaju ograničenu memoriju, bateriju, propusnost i mogućnost računanja. Senzorni čvorovi su raspoređeni gusto u tisućama brojevima. Topologija WSN-ova se često mijenja zbog pokretljivosti čvorova, spajanja ili neuspjeha. Zbog toga se čvorovi mogu lako kompromitirati od strane protivnika. Sigurnosni aspekt WSN-ova vrlo je složen i ovaj rad predstavlja detaljni pregled različitih prijetnji i protumjera u WSN-ovima. Standard IEEE 802.15.4 jedna je od najdominantnijih tehnologija koju koriste WSN-ovi. Sloj kontrole pristupa medijima (MAC sloj) i fizički slojevi WSN-a definirani su IEEE 802.15.4 standardom. Ti su slojevi glavna meta protivnika jer ti slojevi čine bazu WSN-a. U ovom radu predstavljen je tehnički pregled IEEE 802.15.4 i ZigBee tehnologije, gdje je naglasak je na vrlo jeftinoj komunikaciji obližnjih uređaja s malo ili bez osnovne infrastrukture, s namjerom da se to iskoristi kako bi još više smanjili potrošnju energije. ZigBee je osjetljiva na mnoge mrežne napade zbog niske složenosti u veličini memorije i brzini obrade podataka. U ovom radu istraživana je sigurnost ZigBee-a iz različitih perspektiva, istaknute su njegove sigurnosne usluge i ugrađene značajke koje će eliminirati neke od mogućih sigurnosnih prijetnji. Osim toga obrađeni su i napadi koji bi se mogli dogoditi i utjecati na izvedbu ZigBee protokola, a istaknute su i odgovarajuće sigurnosne kontrole i protumjere. Budući da za sada ne postoje globalni standardi u bežičnim senzorskim mrežama, ZigBee ima ključnu ulogu u većini bežičnih aplikacija. Bilo da su senzori vrlo male veličine raspršeni preko tla u šumi ili na Marsu ili senzorske/upravljačke mreže koje omogućuju mikorkontrolu poljoprivrednog okruženja ili komercijalne zgrade, 802.15.4 nudi osnovne alate koji osiguravaju robusnu i pouzdanu komunikaciju u većini uvjeta. Već dostupne tehnike umrežavanja, poput ZigBee saveza, i 802.15.4, pružaju viziju budućeg svijeta u kojem najjednostavniji strojevi mogu međusobno komunicirati.

LITERATURA

[1] C. Mahmoud and S. Aouag, “Security for internet of things: A state of the art on existing protocols and open research issues,” *ACM Int. Conf. Proceeding Ser.*, vol. 17, no. 3, pp. 1294–1312, 2019, doi: 10.1145/3361570.3361622.

[2] T. Garg, N. Kagalwalla, P. Churi, A. Pawar, and S. Deshmukh, “A survey on security and privacy issues in IoV,” *Int. J. Electr. Comput. Eng.*, vol. 10, no. 5, pp. 5409–5419, 2020, doi: 10.11591/IJECE.V10I5.PP5409-5419.

[3] “Wireless Sensor Network - an overview | ScienceDirect Topics.” https://www.sciencedirect.com/topics/engineering/wireless-sensor-network (accessed Aug. 16, 2020).

[4] M. Sharma, A. Tandon, S. Narayan, and B. Bhushan, “Classification and analysis of security attacks in WSNs and IEEE 802.15.4 standards : A survey,” *Proc. - 2017 3rd Int. Conf. Adv. Comput. Commun. Autom. (Fall), ICACCA 2017*, vol. 2018-Janua, pp. 1–5, 2018, doi: 10.1109/ICACCAF.2017.8344727.

[5] T. Obaid, H. Rashed, A. A. -Elnour, M. Rehan, M. Muhammad Saleh, and M. Tarique, “Zigbee Technology and its Application in Wireless Home Automation Systems: A Survey,” *Int. J. Comput. Networks Commun.*, vol. 6, no. 4, pp. 115–131, 2014, doi: 10.5121/ijcnc.2014.6411.

[6] C. M. Ramya, M. Shanmugaraj, and R. Prabakaran, “Study on ZigBee technology,” *ICECT 2011 - 2011 3rd Int. Conf. Electron. Comput. Technol.*, vol. 6, no. February 2019, pp. 297–301, 2011, doi: 10.1109/ICECTECH.2011.5942102.

[7] S. Khanji, F. Iqbal, and P. Hung, “ZigBee Security Vulnerabilities: Exploration and Evaluating,” *2019 10th Int. Conf. Inf. Commun. Syst. ICICS 2019*, no. July, pp. 52–57, 2019, doi: 10.1109/IACS.2019.8809115.

[8] X. Fan *et al.*, “Security Analysis of Zigbee,” *MWR InfoSecurity*, no. May, pp. 1–18, 2017, doi: 10.1109/ISADS.2017.23.

[9] T. Zhang and X. Li, “Evaluating and analyzing the performance of RPL in Contiki,” *Proc.*

Int. Symp. Mob. Ad Hoc Netw. Comput., vol. 2014-Augus, no. August, pp. 19–24, 2014, doi: 10.1145/2633675.2633678.

SAŽETAK

Internet stvari se brzo razvija tijekom aktualnog desetljeća zbog širokog spektra primjene kao što su upravljanje prometom, pametne poljoprivrede i automatizacija kuća. Ulazak internet stvari u naš svakodnevni život osim velikog broja prednosti predstavlja i ogromne rizike gubitka privatnosti i sigurnosnih pitanja. Dva glavna ograničenja IoT uređaja su kapacitet baterije i računalne snage. Buduće Internet stvari koristit će IEEE 802.15.4 komunikaciju zasnovanu na niskoj brzini prijenosa podataka za razne primjene. IEEE 802.15.4 je tehnički standard koji definira rad bežičnih osobnih mreža niske brzine (LR-WPAN). Određuje fizički sloj i kontrolu pristupa mediju za LR-WPAN. ZigBee tehnologija predstavljena je od strane ZigBee Saveza. ZigBee tehnologija se razvila na temelju standardiziranog niza rješenja nazvanih "Slojevi". Ovi optimalno dizajnirani slojevi pružili su ZigBee-u jedinstvene značajke, uključujući niske troškove, jednostavnu implementaciju, pouzdanost, malu snagu i visoku sigurnost. ZigBee je izgrađen po IEEE 802.15.4 standardu. Uzimajući ovaj standard kao "postolje", ZigBee Savez odredio je gornje slojeve ZigBee standarda.

Cilj ovog rada je utvrditi potrošnju energije u slučaju korištenja IEEE 802.15.4 standarda.

Ključne riječi: IEEE 802.15.4, ZigBee, sigurnost, Internet stvari

ABSTRACT

The Internet of Things describes a network of physical objects whose purpose is to connect and exchange data over the Internet. IoT technology can impact the world we live in by improving industry, connecting vehicles and creating smart cities. However, it is a great challenge to discover a large area using IoT. To achieve reliable communication, low-power broadband networks are a good solution. One such technology is precisely LoRa.

LoRaWAN offers the ability to develop private networks and easy integration with numerous network platforms spread around the world. With a communication range of over ten kilometers and a long battery life, LoRa technology enables male power applications for long ranges and low consumption. Some of the applications of LoRa technology are smart city, smart healthcare, environmental monitoring, smart farming. Precisely because of the great range of communication, LoRa technology has found numerous applications in agriculture.

The aim of this paper is to determine the energy consumption in the case of using LoRa technology. Experiments were conducted to determine that LoRa has optimized consumption compared to other systems tested in the work.

Key words: IEEE 802.15.4, ZigBee, Security, IT

ŽIVOTOPIS

Ana Pejković je rođena 26.11.1996. u Osijeku, Republika Hrvatska. Pohađala je Osnovnu školu Višnjevac te nakon završene osnovne škole upisuje Opću gimnaziju u Osijeku. Poslije srednje škole upisuje preddiplomski studij elektrotehnike na Fakultetu elektrotehnike, računarstva i informacijskih tehnologija u Osijeku, te na drugoj godini upisuje smjer Komunikacije i informatika. Godine 2017. završava preddiplomski studij Elektrotehnike te upisuje diplomski studij smjer Mrežne tehnologije.