

Usporedba LoRaWAN, Sigfox i NB-IoT bežičnih senzorskih mreža

Cvitković, Marko

Undergraduate thesis / Završni rad

2022

Degree Grantor / Ustanova koja je dodijelila akademski / stručni stupanj: **Josip Juraj Strossmayer University of Osijek, Faculty of Electrical Engineering, Computer Science and Information Technology Osijek / Sveučilište Josipa Jurja Strossmayera u Osijeku, Fakultet elektrotehnike, računarstva i informacijskih tehnologija Osijek**

Permanent link / Trajna poveznica: <https://um.nsk.hr/um:nbn:hr:200:575995>

Rights / Prava: [In copyright](#)/[Zaštićeno autorskim pravom.](#)

Download date / Datum preuzimanja: **2024-08-03**

Repository / Repozitorij:

[Faculty of Electrical Engineering, Computer Science and Information Technology Osijek](#)



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

Sveučilišni studij

**Usporedba LoRaWAN, Sigfox i NB-LoT bežičnih senzorskih
mreža**

Završni rad

Marko Cvitković

Osijek, 2022.

**FERIT**FAKULTET ELEKTROTEHNIKE, RAČUNARSTVA
I INFORMACIJSKIH TEHNOLOGIJA OSIJEK

Obrazac Z1P - Obrazac za ocjenu završnog rada na preddiplomskom sveučilišnom studiju

Osijek, 06.09.2022.

Odboru za završne i diplomske ispite

Prijedlog ocjene završnog rada na preddiplomskom sveučilišnom studiju

Ime i prezime Pristupnika:	Marko Cvitković
Studij, smjer:	Preddiplomski sveučilišni studij Računarstvo
Mat. br. Pristupnika, godina upisa:	R 4328, 22.07.2019.
OIB Pristupnika:	06177244864
Mentor:	Prof.dr.sc. Drago Žagar
Sumentor:	Matko Zrnić, mag. ing. comp.
Sumentor iz tvrtke:	
Naslov završnog rada:	Usporedba LoRaWAN, Sigfox i NB-IoT bežičnih senzorskih mreža
Znanstvena grana rada:	Telekomunikacije i informatika (zn. polje elektrotehnika)
Zadatak završnog rad:	Posljednjih godina nekoliko LPWA mrežnih tehnologija razvilo se i pronašlo svoje mjesto na tržištu IoT-a. Navedene mrežne tehnologije se razlikuju po usvajanju i dostupnosti, standardizaciji, sigurnosti, kao i po učinkovitosti. Pristupačnost raličitih tehnologija može otežati krajnjim korisnicima pronalaženje optimalnog rješenja za njihov IoT projekt. Zadatak ovog rada je napraviti usporedbu LoraWAN, Sigfox i NB-IoT tehnologije, s pregledom dosadašnjih rješenja, trenutnog razvoja i budućih trendova razvoja, te analizirati prednosti i nedostatke svake pojedine tehnologije. Sumentor: Matko Zrnić, mag.ing.
Prijedlog ocjene završnog rada:	Vrlo dobar (4)
Kratko obrazloženje ocjene prema Kriterijima za ocjenjivanje završnih i diplomskih radova:	Primjena znanja stečenih na fakultetu: 2 bod/boda Postignuti rezultati u odnosu na složenost zadatka: 2 bod/boda Jasnoća pismenog izražavanja: 2 bod/boda Razina samostalnosti: 2 razina
Datum prijedloga ocjene od strane mentora:	06.09.2022.
Datum potvrde ocjene od strane Odbora:	21.09.2022.
Potvrda mentora o predaji konačne verzije rada:	<i>Mentor elektronički potpisao predaju konačne verzije.</i>
	Datum:

**FERIT**FAKULTET ELEKTROTEHNIKE, RAČUNARSTVA
I INFORMACIJSKIH TEHNOLOGIJA OSIJEK**IZJAVA O ORIGINALNOSTI RADA**

Osijek, 21.09.2022.

Ime i prezime studenta:

Marko Cvitković

Studij:

Preddiplomski sveučilišni studij Računarstvo

Mat. br. studenta, godina upisa:

R 4328, 22.07.2019.

Turnitin podudaranje [%]:

13

Ovom izjavom izjavljujem da je rad pod nazivom: **Usporedba LoRaWAN, Sigfox i NB-IoT bežičnih senzorskih mreža**

izrađen pod vodstvom mentora Prof.dr.sc. Drago Žagar

i sumentora Matko Zrnić, mag. ing. comp.

moj vlastiti rad i prema mom najboljem znanju ne sadrži prethodno objavljene ili neobjavljene pisane materijale drugih osoba, osim onih koji su izričito priznati navođenjem literature i drugih izvora informacija. Izjavljujem da je intelektualni sadržaj navedenog rada proizvod mog vlastitog rada, osim u onom dijelu za koji mi je bila potrebna pomoć mentora, sumentora i drugih osoba, a što je izričito navedeno u radu.

Potpis studenta:

Sadržaj

1. Uvod.....	1
1.1. Zadatak završnog rada	1
2. IoT.....	2
2.1. Arhitektura IoT-a.....	2
2.2. Lpwan.....	4
3. LoRaWan	6
3.1. Arhitektura LoRaWan-a	7
3.2. Prednosti i nedostaci LoRaWAN-a:	8
3.3 Vrsta komunikacija.....	9
3.3.1. Klasa A	9
3.3.2. Klasa B.....	10
3.2.3. Klasa C	11
3.4. Struktura paketa u LoRa.....	11
4. SigFox	13
4.1. Arhitektura Sigfox-a	13
4.2. Prednosti i nedostaci SigFox-a	14
4.3. Način rada SigFox-a.....	14
5. NB-IoT.....	16
5.1. Arhitektura NB-IoT-a.....	16
5.2. Načini rada NB-Iot-a.....	18
5.3. Prednosti i nedostaci NB-IoT-a:	18
6. Usporedba LoRaWAN, Sigfox i NB-IoT bežičnih senzorskih mreža.....	20
6.1. Tehnološki podaci.....	20
6.2. Kvaliteta prijenosa	20
6.3. Pokrivenost i domet.....	21
6.4. Energetska učinkovitost i latencija	22
6.5. Sigurnost	23
6.6. Troškovi.....	24
7. Zaključak	25
Literatura	26
Sažetak.....	28
Abstract.....	29

1. Uvod

U današnje vrijeme tehnologije interneta stvari IoT (*eng. Internet of Things*) je neizostavan dio svakodnevnog života. Primjenjuje se u raznim područjima poput poljoprivrede, sigurnosti, pametnog doma i pametnog grada. IoT aplikacije imaju specifične zahtjeve kao što su dug komunikacijski domet, vrlo niska potrošnja energije i isplativost. Široko korištene tehnologije kratkog dometa komunikacije (npr. BLE i ZigBee) nisu prilagođene zahtjevima dugog dometa prijenosa. Nadalje, rješenja temeljena na mobilnoj staničnoj komunikaciji (npr. 2G, 3G i 4G) mogu osigurati veći domet prijenosa, ali troše mnogo energije. Stoga zahtjevi IoT aplikacija dovode do pojave širokopojasne mreže male snage LPWAN (*eng. Low Power Wide Area Network*). LPWAN tehnologije osiguravaju veliki domet prijenosa, nisku potrošnju energije i isplativo rješenje za implementaciju. Omogućuje domet komunikacije do 40 km u ruralnim zonama i 10 km u urbanim zonama, do 10 godina trajanja baterije, manje od 5 \$ troška uređaja i manje od 1 \$ po uređaju godišnje troškova pretplate operatera [20]. Posebno je dizajniran za IoT aplikacije koje zahtijevaju prijenos nekoliko poruka dnevno u dugom radijskom dometu. Ove su prednosti potaknule različite studije performansi LPWAN-a u vanjskom i unutarnjem okruženju. Još početkom 2013. pojam "LPWAN" nije niti postojao. Mnoge LPWAN tehnologije nastale su u licenciranom i nelicenciranom frekvencijskom spektru. Među njima, Sigfox, LoRaWAN i NB-IoT danas su vodeće nove tehnologije. Završni rad je podijeljen u 7 dijelova:

- 1.) Uvod
- 2.) Iot
- 3.) LoRaWAN
- 4.) Sigfox
- 5.) NB-IoT
- 6.) Usporedba LoRaWAN-a, Sigfox-a i NB-IoT-a
- 7.) Zaključak

U uvodu je opisan cilj i svrha završnog rada. Dok je u drugom dijelu opisana IoT tehnologija kroz poglavlja arhitekture i LPWAN. U iduća tri dijela se nalazi detaljan opis LoRaWAN-a, Sigfox-a i NB-IoT-a kroz arhitekture, njihove prednosti i mane te načini rada. Šesto poglavlje je usporedba svih tih mreža po kvaliteti prijenosa, dometa, sigurnosti, troškova i u zaključku donosim rezime svih tih rezultata.

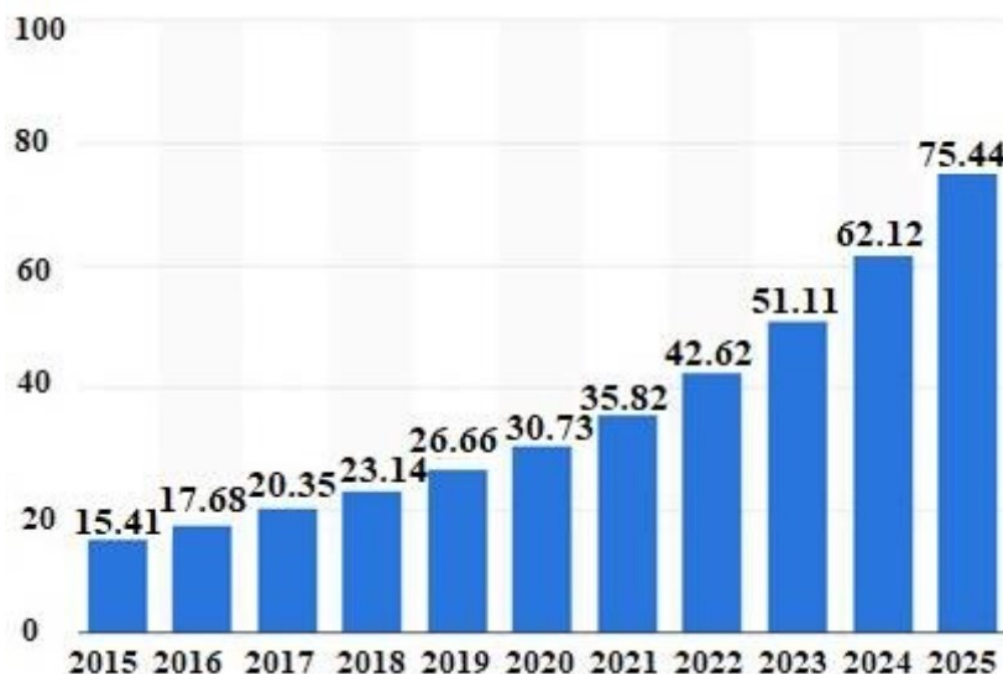
1.1. Zadatak završnog rada

Posljednjih godina nekoliko LPWA mrežnih tehnologija razvilo se i pronašlo svoje mjesto na tržištu IoT-a. Navedene mrežne tehnologije se razlikuju po usvajanju i dostupnosti, standardizaciji, sigurnosti, kao i po učinkovitosti. Pristupačnost različitih tehnologija može otežati krajnjim korisnicima pronalaženje optimalnog rješenja za njihov IoT projekt. Zadatak ovog rada je napraviti usporedbu LoRaWAN, Sigfox i NB-IoT tehnologija, s pregledom dosadašnjih rješenja, trenutnog razvoja i budućih trendova razvoja, te analizirati prednosti i nedostatke svake pojedine tehnologije.

2. IoT

IoT je sustav koji međusobno povezuje različite uređaje, mehaničke i digitalne strojeve, objekte i ljude koji imaju jedinstvene identifikatore (UID) i omogućava im komunikaciju i prijenos različitih podataka preko interneta u realnom vremenu bez ljudske uključenosti.

Sve više i više različitih industrija koristi IoT tehnologiju zbog lakšeg i učinkovitijeg poslovanja, boljeg komuniciranja s kupcima i donošenje boljih odluka što dovodi do velike uštede vremena i novca. Kako postoji puno dobrih stvari u vezi sve većeg rasta IoT tehnologija tako i postoje veliki problemi u području privatnosti i sigurnosti korisnika te njihova zloupotreba. IoT se u početku najviše koristio za poslovanje i proizvodnju, ali kako je započela široka primjena pametnih uređaja u svakodnevici, s vremenom je naglasak stavljen i na korištenje IoT-a i u kućanstvima i uredima.



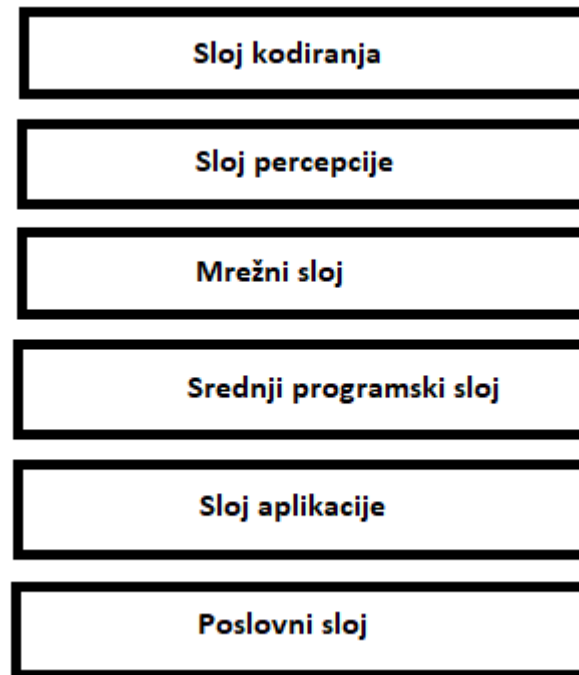
Slika 1.1. Zastupljenost IoT uređaja tijekom godina u milijardama

Slika 1.1. prikazuje porast povezanih uređaja gdje je 2015. godine bilo oko 15 milijardi uređaja, 2022. skoro 3 puta više i pretpostavlja se da će ih 2025. biti oko 75 milijardi [1].

2.1. Arhitektura IoT-a

Za arhitekturu IoT mreža najvažnije je osigurati pouzdanu komunikaciju, što brže dobivanje podataka te određenu razinu sigurnosti i privatnosti. Trenutno ne postoji jedinstveni dogovor o arhitekturi za IoT. Stoga imamo više različite arhitekture predložene od strane različitih stručnjaka [3]. U navedenom radu opisane su tri ključne razine arhitekture IoT-a koje se sastoje od sloja aplikacije, mrežnog sloja i sloja percepcije dok je u radu [4] opisana arhitektura s četiri

ključne razine gdje je još dodan poslovni sloj. Za razliku od prethodna dva rada, arhitektura je opisana u pet slojeva koristeći najbolje značajke arhitekture mreža za upravljanje internetom i telekomunikacijama na temelju IP(*eng. Internet Protocol*) odnosno TMN (*eng. Telecommunication Management Network*) modela [5]. U predloženom modelu arhitektura bi se sastojala od poslovnog sloja, sloja primjene, sloja obrade, sloja transporta i posljednjeg sloja percepcije.



Slika 2.1. Arhitektura IoT-a

Slično je predložena i šestoslojna arhitektura na temelju hijerarhijske strukture mreže [6]. Dakle, najopćenitije je podijeljena u šest slojeva kao što je prikazano na slici 2.1. Sastoji se od sloja kodiranja, sloja percepcije, mrežnog sloja, srednjeg programskog sloja, sloja aplikacije i poslovnog sloja.

1) Sloj kodiranja je temelj IoT-a koji pruža identifikaciju objekata od interesa. U ovom sloju svakom objektu se dodjeljuje jedinstveni ID koji olakšava razaznavanje objekata [6].

2) Sloj percepcije je sloj uređaja IoT-a koji svakom objektu daje fizičko značenje. Sastoji se od senzora podataka u različitim oblicima poput RFID (*engl. Radio-Frequency Identification*) oznaka, IR senzora ili drugih senzorskih mreža. Ovisno o vrsti senzora, informacije mogu biti o lokaciji, temperaturi, orijentaciji, kretanju, vibracijama, ubrzanju, vlažnosti, kemikalijama promjene u zraku itd. Ovaj sloj prikuplja korisne informacije o objektima sa senzorskih uređaja povezanih s njima i pretvara informacije u digitalne signale koji se zatim prosljeđuju na mrežni sloj za daljnje djelovanje [6].

3) Svrha mrežnog sloja je primanje korisnih informacija iz sloja percepcije i prijenosa na sustave za obradu u srednjem sloju putem medija za prijenos kao što su WiFi, Bluetooth, WiMaX, Zigbee i GSM (*eng. Global System for Mobile Communications*). Dakle, mrežni sloj prenosi informacije od sloja percepcije do srednjeg sloja [6].

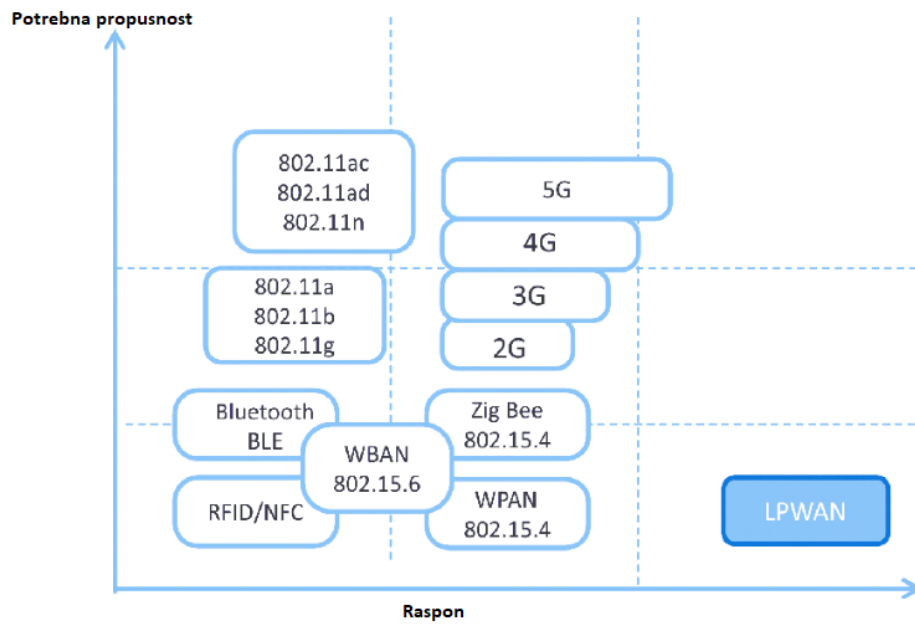
4) Srednji programski sloj služi da obrađuje informacije primljene od senzorskih uređaja. Uključuje tehnologije kao što su računarstvo u oblaku i UBICOMP (*eng. Ubiquitous computing*) koje osigurava izravan pristup bazi podataka za pohranjivanje svih potrebnih informacija u njoj. Korištenjem neke inteligentne opreme za obradu, informacije se obrađuju i poduzimaju se potpuno automatizirane radnje na temelju obrađenih rezultata informacija [6].

5) Sloj aplikacije pruža globalno upravljanje aplikacijom na temelju informacija o objektima obrađen u srednjem sloju. Ovaj sloj ostvaruje primjene IoT-a za sve vrste industrije, na temelju obrađenih podataka. Budući da aplikacije promiču razvoj IoT-a, ovaj sloj je vrlo koristan u razvoju IoT mreže. Aplikacije povezane s internetom stvari mogu biti pametno zdravlje, pametna poljoprivreda, pametna kuća, pametni grad, inteligentni prijevoz itd [6].

6) Poslovni sloj je odgovoran za upravljanje cjelokupnim IoT sustavom uključujući aplikacije i usluge. Gradi poslovne modele, grafikone, dijagrame toka itd. na temelju podataka primljenih iz sloja aplikacije. Pravi uspjeh IoT tehnologije također ovisi o dobrim poslovnim modelima. Bazirano na analiza rezultata, ovaj sloj će pomoći u određivanju buduće akcije i poslovne strategije [6].

2.2. Lpwan

IoT ima specifične potrebe kao što su veliki komunikacijski doseg, jako malu energetske potrošnje i isplativost. Široka primjena tehnologija poput BLE i ZigBee nisu prilagođene za veliki domet prijenosa. Nadalje solucije osnovane na mobilnoj komunikaciji (2G,3G,4G,5G) bi mogle osigurati veći domet, ali troše previše energiju. Stoga je došlo do pojave LPWAN-a. LPWAN tehnologija osigurava veliki domet, nisku potrošnju i nisku cijenu. To dopušta do 40 km dometa u ruralnim područjima i do 10 km u urbanim. Mnoge LPWAN tehnologije nastale su u licenciranom i nelicenciranom frekvencijskom spektru. Među njima, Sigfox, LoRaWAN i NB-IoT su danas među vodeće nove tehnologije koje uključuju mnoge tehničke razlike. Na slici 2.2. se vidi da LPWAN ima puno veći domet i manju propusnost u odnosu na Zig Bee, 5G, 4G [15]...



Slika 2.2. Raspon LPWAN-a u odnosu na propusnost u usporedbi s drugi tehnologijama.

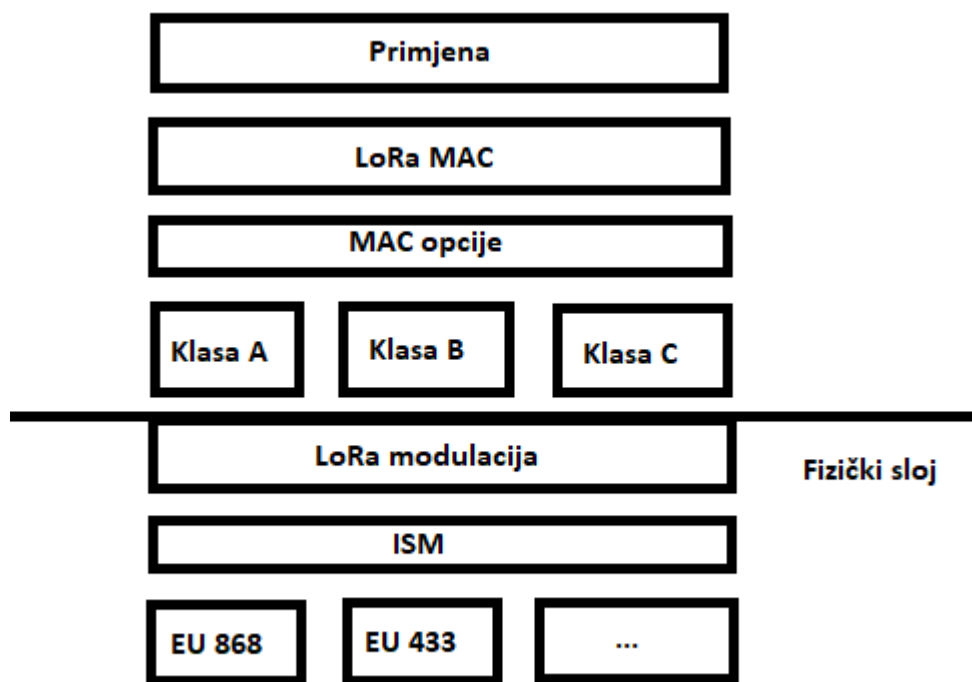
3. LoRaWan

LoRa koji je dobio ime po 'Long Range', je patentirana tehnologija bežične komunikacije podataka. Tehnologiju je razvio Cycleo iz Grenoblea, Francuska, a kupio ju je Semtech 2012. Ključna značajka koja razlikuje LoRa od ostalih dostupnih bežičnih WAN-ova tehnologije je prijenos na velike udaljenosti s malom potrošnjom energije. Međutim, podržava aplikacije niske brzine prijenosa s manje zahtjevne mobilnosti i pouzdanosti. Ova je tehnologija razvijena da podrži vrstu bežične telekomunikacijske mreže na cijelom području. Uobičajeno poznate kao LPWAN. Ovisno o regiji u kojoj je smještena, mreža koristi različite frekvencijske pojaseve. Na primjer u Južnoj Americi koristi 915 MHz pojas, u Europi 867-869 MHz itd., kao što je prikazano na slici 3.1. [7].



Slika 3.1. Frekvencijski pojasevi za LoRa tehnologiju [7]

Budući da LoRa definira donji fizički sloj, potrebno je bilo definirati ostale slojeve. LoRaWAN je jedan od nekoliko protokola koji su razvijeni za definiranje gornjih slojeva mreže. LoRaWAN je protokol sloja za kontrolu pristupa medijima, ali djeluje uglavnom kao protokol mrežnog sloja za upravljanje komunikacijom između LPWAN pristupnika i uređaja krajnjih čvorova kao protokol za usmjeravanje, koji održava LoRa Alliance. LoRaWAN definira komunikacijski protokol i arhitekturu sustava za mrežu, dok LoRa fizički sloj omogućuje komunikacijsku vezu dugog dometa. LoRaWAN je također odgovoran za upravljanje komunikacijskim frekvencijama, brzinom podataka i snagom za sve uređaje. Uređaji u mreži su asinkroni i prenose kada imaju dostupne podatke za slanje. Podaci koje prenosi uređaj krajnjeg čvora prima višestruki pristupnik, koji prosljeđuje pakete podataka centraliziranom mrežnom poslužitelju. Podaci se zatim prosljeđuju poslužiteljima aplikacija. Tehnologija pokazuje visoku pouzdanost za umjereno opterećenje, no ima nekih problema s performansama u vezi sa slanjem potvrda. LoRa radi na frekvencijama koje su otvorene i ne trebaju državnu dozvolu. To znači da su moguće smetnje na toj frekvenciji i brzina prijenosa podataka može biti smanjena [8].



Slika 3.2. Slojevita organizacija LoRa i LoRaWAN

Razlika između Lora i LoRaWAN prikazana je slikom 3.2. LoRaWAN predstavlja komunikacijski protokol, a LoRa fizički sloj [8].

3.1. Arhitektura LoRaWan-a

Na slici 3.3 prikazana je arhitektura LoRaWAN koja se dijeli na krajnje uređaje, pristupnike, mrežne poslužitelje i aplikacijske poslužitelje. Krajnji uređaji su senzori ili aktuatori koji šalju LoRa modularane bežične poruke na pristupnike ili bežično primaju poruke natrag od pristupnika. Često rade na baterije i uređaji su bežično povezani na LoRaWAN mrežu putem pristupnika koristeći LoRa RF modulaciju. Pristupnici onda primaju poruke s krajnjih uređaja i prosljeđuju ih na mrežni poslužitelj. Svaki pristupnik je registriran (koristeći konfiguracijske postavke) na LoRaWAN mrežnom poslužitelju. Pristupnici su povezani s mrežnim poslužiteljem koristeći eng. *backhaul* kao što je WiFi, Ethernet, optička ili 2,4 GHz radio veza. Mrežni poslužitelji su dio softvera koji radi na poslužitelju koji upravlja cijelom mrežom, a aplikacijski poslužitelji su dio softvera koji radi na poslužitelju koji je odgovoran za sigurnu obradu podataka aplikacije. Poslužitelj pridruživanja je također dio softvera koji radi na poslužitelju koji obrađuje poruke zahtjeva za pridruživanjem koje šalju krajnji uređaji [9].



Slika 3.3. Arhitektura LoRaWAN-a

Krajnji uređaji komuniciraju s obližnjim pristupnicima i svaki pristupnik je povezan s mrežnim poslužiteljem. LoRaWAN mreže koriste protokol koji se temelji na ALOHA. Poruke poslone s krajnjih uređaja putuju kroz sve pristupnike unutar dometa. Ove poruke prima mrežni poslužitelj. Ako je mrežni poslužitelj primio više kopija iste poruke, zadržava jednu kopiju poruke i odbacuje druge [9].

3.2. Prednosti i nedostaci LoRaWAN-a:

Prednosti LoRaWAN-a:

- 1.) Senzori male snage koji mogu pokriti široko područje mjereno u miljama.
- 2.) Mala snaga znači dugo trajanje baterije za uređaje. Baterije senzora mogu trajati dvije do pet godina (Klasa A i Klasa B)
- 3.) Savršeno za praćenje imovine raspoređene na terenu.
- 4.) Široko se koristi za IoT aplikacije.
- 5.) Funkcionalnost dugog dometa omogućuje pametna rješenja, kao što su aplikacije za pametne gradove.
- 6.) Bežični, jednostavan za postavljanje i brza implementacija.
- 7.) Sigurnost: sloj sigurnosti za mrežu i jedan za aplikaciju s AES (*eng. Advanced Encryption Standard*) enkripcijom.
- 8.) Potpuno dvosmjerna komunikacija.

Nedostaci LoRaWAN-a:

- 1.) Nije za velike količine podataka, opterećenje ograničeno na 0,3 ~ 5,5 kBps.

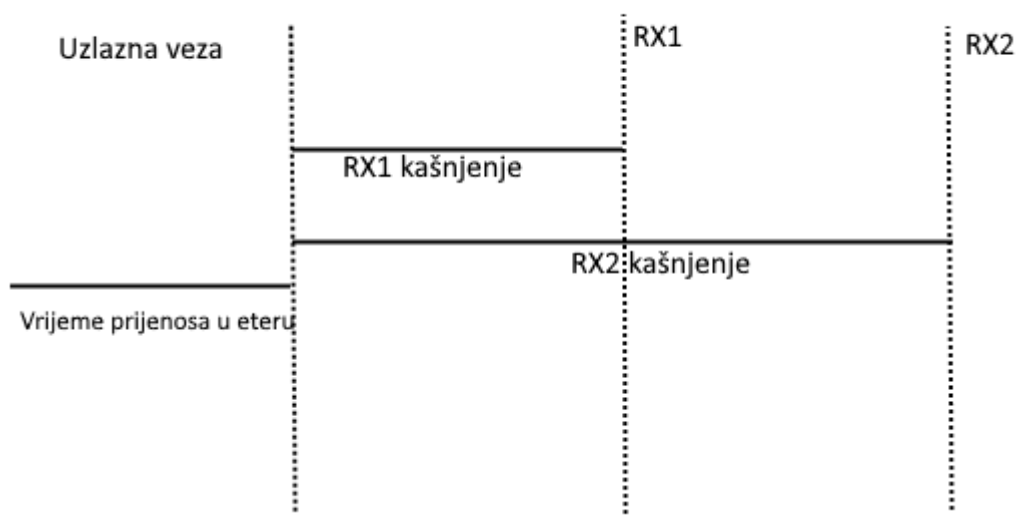
- 2.) Nema podršku za audio ili video.
- 3.) Ograničeno na komunikaciju u liniji vidljivosti (LOS).
- 4.) Nije za kontinuirano praćenje (osim uređaja klase C).
- 5.) Nije idealan kandidat za aplikacije u stvarnom vremenu koje zahtijevaju niže kašnjenje i ograničeno podrhtavanje zahtjevima.

3.3 Vrsta komunikacija

Specifikacija LoRaWAN definira tri vrste komunikacije: klasu A, klasu B i klasu C. Svi LoRaWAN uređaji moraju implementirati klasu A, dok su klasa B i klasa C proširenja specifikacije uređaja klase A. Sve klase uređaja podržavaju dvosmjernu komunikaciju (uzlazna i silazna veza). Većina uređaja može koristiti sve 3 klase.

3.3.1. Klasa A

Svi LoRaWAN krajnji uređaji moraju podržavati implementaciju klase A. Komunikaciju klase A uvijek pokreće krajnji uređaj. Uređaj može poslati poruku na ulaznoj vezi u bilo kojem trenutku. Kada je prijenos uzlazne veze dovršen, uređaj otvara dva kratka prozora za primanje (silazna veza). Postoji kašnjenje između kraja prijenosa uzlazne veze i početka prozora za primanje (RX1 i RX2) respektivno kao što je prikazano na slici 3.4. Ako mrežni poslužitelj ne odgovori tijekom ova dva prozora za primanje, sljedeća silazna veza biti će nakon sljedećeg prijenosa uzlazne veze [9].



Slika 3.4. Prozori za primanje klase A

Poslužitelj može odgovoriti tijekom prvog prozora primanja (RX1) ili tijekom drugog prozora primanja (RX2), ali ne koristi oba prozora. Postoje 3 slučaja primanja:

1.) Krajnji uređaj otvara oba prozora za primanje, ali ne prima poruku za silaznu vezu tijekom oba prozora za primanje.

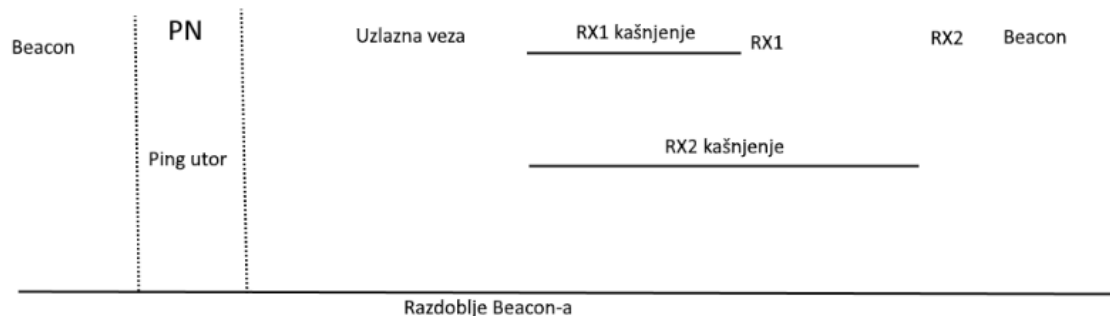
2.) Krajnji uređaj prima silaznu vezu tijekom prvog prozora za primanje i stoga ne otvara drugi prozor za primanje.

3.) Krajnji uređaj otvara prvi prozor za primanje, ali ne prima silaznu vezu. Stoga otvara drugi prozor za primanje i prima silaznu vezu tijekom drugog prozora za primanje.

Krajnji uređaji klase A: često se napajaju baterijama, imaju najmanju potrošnju energije, većinu vremena provodite u stanju mirovanja, obično drže duge intervale između uzlaznih veza, imaju visoku latenciju silazne veze (da bi primio silaznu vezu, krajnji uređaj mora poslati uzlaznu). Neki uobičajeni slučajevi upotrebe krajnjih uređaja klase A: praćenje okoliša, praćenje životinja, detekcija požara, detekcija curenja vode, rano otkrivanje potresa, praćenje lokacije [9].

3.3.2. Klasa B

Uz prozore za primanje pokrenute klasom A, uređaji klase B otvaraju zakazane prozore za primanje poruka na silaznoj vezi (*eng. downlink*) od mrežnog poslužitelja. Koristeći vremenski sinkronizirane *eng. beacons* koje prenosi pristupnik, uređaji povremeno otvaraju prozore za primanje. Uređaj otvara 'ping utore' za silaznu vezu u zakazano vrijeme za primanje poruka od mrežnog poslužitelja. Uređaji klase B također otvaraju prozore za primanje nakon slanja uzlazne veze kao što je prikazano na slici 3.5. [9].

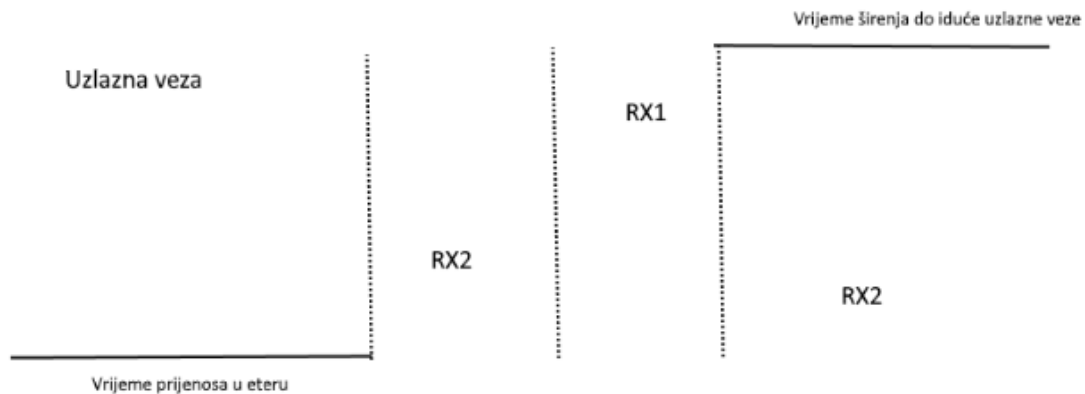


Slika 3.5. Prozori za primanje klase A

Krajnji uređaji klase B imaju manje kašnjenje od krajnjih uređaja klase A, jer su dostupni u unaprijed konfigurirano vrijeme i ne moraju slati uzlaznu vezu da bi primili silaznu. Trajanje baterije je kraće u klasi B nego u klasi A, jer uređaj provodi više vremena u aktivnom načinu rada, tijekom *eng. beacons* i *eng. ping* utora. Neki uobičajeni slučajevi upotrebe krajnjih uređaja klase B: brojila komunalnih usluga, izvještavanje o temperaturi [9].

3.2.3. Klasa C

Uređaji klase C proširuju klasu A držeći prozore za prijem otvorenim osim ako ne odašilju, kao što je prikazano na slici 3.6. To omogućuje komunikaciju niske latencije, ali znatno više troši energiju od uređaja klase A. Krajnji uređaji klase C se često napajaju iz mreže, nemaju kontinuirani prozor primanja. Neki uobičajeni slučajevi upotrebe krajnjih uređaja klase C: brojila komunalnih usluga sa prekidačima, ulična rasvjeta [9].



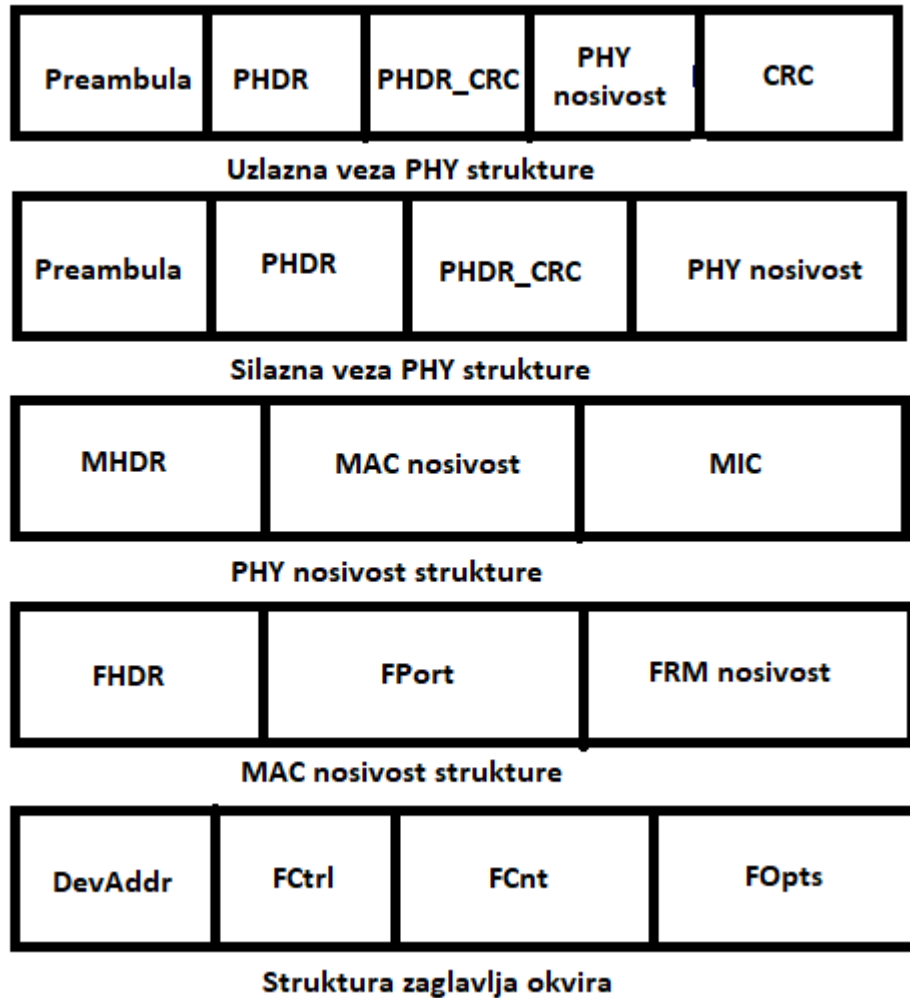
Slika 3.6. Prozori za primanje klase A

3.4. Struktura paketa u LoRa

Struktura paketa LoRa se sastoji od tri elementa: preambule, opcionalnog zaglavlja i tereta podataka kao što je prikazano na slici 3.7. Preambula se koristi u svrhu sinkronizacije između prijarnika i dolaznog toka podataka. To je programabilna varijabla što znači da se duljina preambule može produžiti prema zahtjevima aplikacija, dok je zadana konfiguracija niz od 12 simbola za paket. Proces otkrivanja preambule poduzima prijernik koji se povremeno ponovno pokreće i stoga bi duljina preambule trebala biti konfigurirana identično duljini preambule odašiljača. Maksimalna duljina preambule treba biti programirana na strani prijernika ako duljina preambule nije poznata ili može varirati [10].

Dostupne su dvije vrste zaglavlja na temelju odabranog načina rada, a to su: eksplicitni način zaglavlja i način implicitnog zaglavlja. Eksplicitni način rada zaglavlja je zadani način rada u kojem zaglavlje pruža informacije o duljini korisnog opterećenja u bajtovima, proslijeđenom kodnom omjeru ispravljanja pogrešaka i prisutnosti opcionalnog 16-bitnog CRC-a (*eng. Cyclic Redundancy Check*) za korisno opterećenje. U slučajevima kada su korisni teret, brzina kodiranja i prisutnost CRC-a fiksni ili poznati unaprijed, implicitni način zaglavlja može se odabrati umjesto eksplicitnog načina zaglavlja kako bi se smanjilo vrijeme prijena. Korisno opterećenje paketa je

polje varijabilne duljine koje sadrži stvarne podatke kodirane stopom pogreške. Stopa pogreške je navedena u zaglavlju u eksplicitnom načinu rada ili u postavkama registra u implicitnom načinu [10].



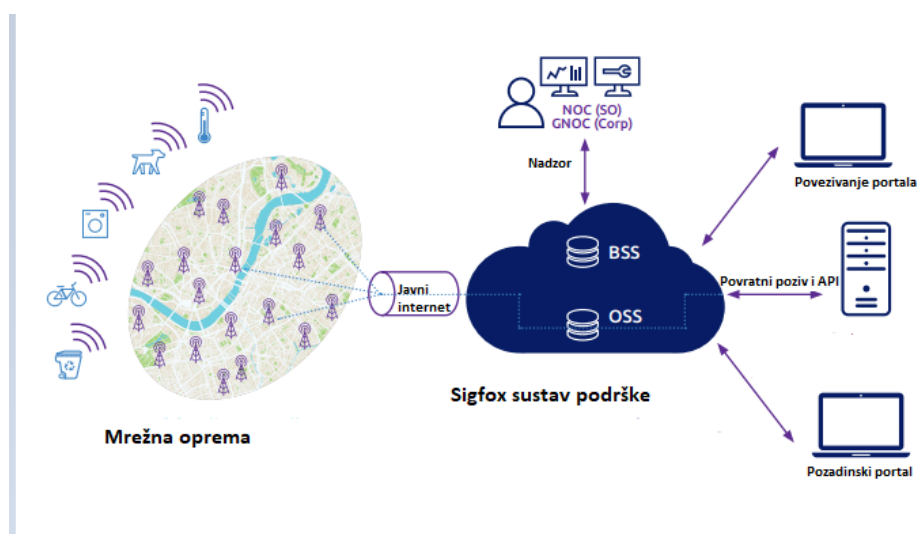
Slika 3.7. Struktura paketa u LoRaWAN-u

4. SigFox

SigFox je oblik bežične komunikacije dugog dometa, male snage i niske brzine prijenosa koji je razvijen za pružanje bežičnog povezivanja za uređaje poput daljinskih senzora, aktuatora i drugih M2M (eng. *Machine to Machine*) i IoT uređaja. Bežično sučelje SigFox razvijeno je kako bi omogućilo da svaka komunikacija koja se odvija troši minimalnu količinu energije. Na taj način udaljeni uređaji mogu raditi na baterijsko napajanje kroz vrlo duga razdoblja bez potrebe za bilo kakvom izmjenom baterije ili održavanjem. Osim toga, M2M i IoT komunikacije će komunicirati na velikim udaljenostima, a sustav SigFox je dizajniran da omogući prijenosima da pokriju velike udaljenosti. Udaljeni SigFox čvorovi mogu komunicirati s baznim stanicama koje imaju internetsku povezanost, čime se omogućuje daljinsko upravljanje i prikupljanje podataka s bilo kojeg mjesta s internetskom vezom. Na ovaj način, SigFox je u mogućnosti osigurati vezu niske brzine prijenosa podataka na bilo koje mjesto koje je pokriveno mrežom uz vrlo nisku cijenu za mnoge M2M i IoT aplikacije [12].

4.1. Arhitektura Sigfox-a

Arhitektura Sigfox mreže je horizontalna i tanka, te ima 2 sloja. Prvi sloj sastoji se od mrežne opreme uglavnom baznih stanica i ostalih elemenata. Svrha ovog sloja je primanje poruka od oglasa IoT uređaja i njihovo prijenos na sustave podrške. Ova mreža ima topologiju zvijezde jednog skoka koja omogućuje povezivanje IoT uređaja s bilo kojom baznom stanicom u blizini. Drugi sloj je Sigfox Support System gdje se poruke s baznih stanica obrađuju i šalju putem povratnih poziva korisničkom sustavu. Ovaj sloj također pruža ulaznu točku za različite aktere kao što su Sigfox, krajnji kupci, Sigfox operateri i kanali u ekosustav koristeći web sučelja ili API-je. Sloj ima spremište i druge alate za analizu podataka koje prikuplja mreža. Sloj također sadrži module i značajke koje podržavaju implementaciju, rad i nadzor mreže. Značajke uključuju BSS (eng. *Business Support System*) za naplatu i naručivanje te Radio Planning za podršku postavljanja mreže i nadzora. Javni internet povezuje dva sloja preko sigurnih VPN veza kao što je prikazano na slici 4.1. [12].



Slika 4.1. Arhitektura SigFox-a

4.2. Prednosti i nedostatci SigFox-a

Sljedeće su prednosti Sigfoxa:

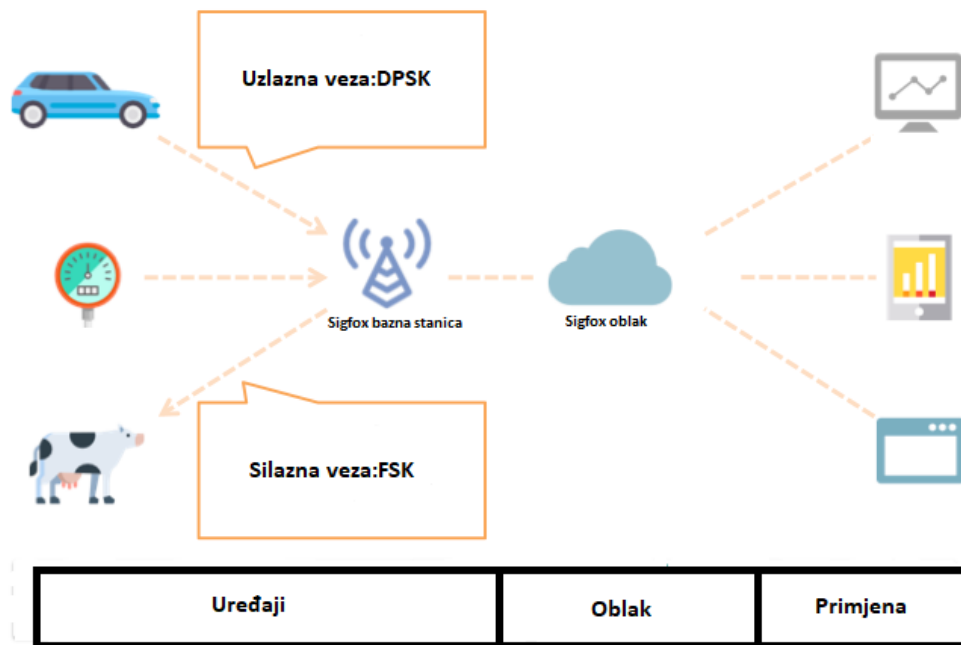
- 1.) Kako ima manje podataka za prijenos, potrebno je manje energije i time će se produžiti vijek trajanja baterije.
- 2.) Zbog manjeg opterećenja biti će dostupno više prostora za prijenos korisničkih podataka i time će se u većoj mjeri povećati kapacitet mreže.
- 3.) Sigfox je uskopojasna tehnologija i stoga će prihvatiti veći broj kanala u istom prostoru u usporedbi sa širokopojasnim bežičnim sustavima. Zbog toga će Sigfox učinkovitije koristiti fizički kanal. Stoga se može postići veći kapacitet mreže.
- 4.) Sigfox podržava široko područje pokrivenosti i koristi se za aplikacije niske brzine prijenosa podataka.
- 5.) Manji trošak mrežnih operacija i vlasništva.
- 6.) Koristi se u mnogim aplikacijama, tj. pametni grad, mjerenje, automobilska, mobilna povezanost za rasterećenje prometa itd.

Nedostatci SigFox-a:

- 1.) CSMA (*eng. Carrier Sense Multiple Access*) ili druge takve tehnike za otkrivanje/izbjegavanje sudara ne koriste se u Sigfoxu.
- 2.) Uskopojasni spektar koji emitira pojedinačni Sigfox krajnji uređaj uzrokuje jake smetnje obližnjem postojećem širokopojasnom sustavu. Više takvih sigfox uređaja dodatno će pojačati smetnje.
- 3.) Sigfox podržava jednosmjernu komunikaciju bez potvrde. To zahtijeva višestruke prijenose ako poslužitelj ne prima podatke bez grešaka. Zbog toga će se povećati potrošnja energije što ovisi o broju ponovnih prijenosa.
- 4.) Zbog podrške niske brzine prijenosa podataka, ne može se koristiti za aplikacije visoke brzine prijenosa podataka.

4.3. Način rada SigFox-a

SigFox koristi D-BPSK (*eng. Differential Binary Phase-Shift Keying*) modulacija za koju poruka ima fiksnu širinu pojasa od 100Hz i šalje se velikom brzinom od 100bps (za Europu) ili 600bps (za SAD), unutar nelicencirani frekvencijski spektar koji je ispod 1 GHz, za Europu 868MHz i 915MHz za Ameriku. Mreža SigFox sastoji se od ovih elemenata: objekti (uređaji), bazne stanice i oblak (internet). Slika 4.2. ilustrira ključne elemente prijenosa podataka putem SigFoga.



Slika 4.2. Prijenos podataka putem SigFoxa

Prijenos podataka SigFoxa može se bolje razumjeti na sljedeći način: objekti (uređaji) su povezani na internet korištenjem SigFox mreže. Objekt može biti senzor temperature, vlažnosti i/ili zasićenja koji se nalazi unutar 1000 metara od bazne stanice. Sigfox koristi DPSK (eng. *Phase Shift Keying*) za komunikaciju između uređaja i oblaka ili uzlaznu vezu i FSK (eng. *Frequency Shift Keying*) za komunikaciju između oblaka i uređaja ili silazne veze. Uzlazna veza može do 140 poruka po danu i maksimalna veličina po poruci je 12 bajtova za razliku od silazne veze koji može samo 4 poruke i veličina može biti samo 8 bajtova [12].

DPSK je metoda koju koriste bazne stanice za pretvaranje signala, njegovo otklanjanje pogrešaka, pretvaranje natrag za slanje u oblak. Kada signal putuje od uređaja do bazne stanice, neizbježno nailazi na smetnje iz okoline (npr. kiša ili guste šume). Interferencija je univerzalna, bilo koji signal s bilo koje internetske mreže postat će oslabljen i izgledat će malo drugačije kada stigne na odredište. SigFox ublažava ovaj problem korištenjem DPSK-a. Uloga DPSK-a je osigurati da signal koji napušta baznu stanicu bude isti točan signal koji je napustio uređaj. Frekvencijski pomak sličan DPSK u smislu da oba procesa pretvaraju ulazni signal, analiziraju/otkrivaju oštećenja, eliminiraju ih i pretvaraju podatke natrag u izvorni signal. Međutim, umjesto da pomiče i analizira fazu, FSK pomiče i analizira frekvenciju. Baš kao i fazni pomaci u DPSK-u, pomaci frekvencije u FSK-u otkrivaju oštećenja signala gdje ih sofisticirani sklopovi mogu otkloniti [12].

5. NB-IoT

NB-IoT je tehnologija koja omogućuje velikom broju uređaja slanje podataka tamo gdje nema standardne pokrivenosti mobilnom mrežom. Koristi licencirani frekvencijski spektar gdje nema smetnji s drugim uređajima što jamči pouzdaniji prijenos podataka. NB-IoT je LPWAN mreža koja može pokriti velika područja uz korištenje manjih količina energije. Podržan od strane svih glavnih proizvođača mobilne opreme i modula, NB-IoT može koegzistirati s 2G, 3G i 4G mobilnim mrežama. Također ima koristi od svih značajki sigurnosti i privatnosti mobilnih mreža, kao što je podrška za povjerljivost identiteta korisnika, autentifikacija entiteta, povjerljivost, integritet podataka i identifikacija mobilne opreme. Prva komercijalna lansiranja NB-IoT-a su završena, a globalno uvođenje se dogodilo u 2017./18. godini [13].

NB-IoT je primjenjiv u različitim scenarijima i industrijama i mogao bi biti puno bolje rješenje od većine drugih tehnologija i protokola kada je u pitanju npr. automatsko očitavanje brojala. Kao što je već spomenuto, NB-IoT se može koristiti za prijenos većih količina podataka, posebno u nepristupačnim područjima udaljenim ili ruralnim lokacijama. Dobar primjer bi također bio scenarij u kojem su moduli postavljeni ispod zemlje budući da NB-IoT ima bolju duboku pokrivenost u zatvorenom prostoru nego GSM ili LTE (eng. Long-Term Evolution). 3GPP (eng. *The 3rd Generation Partnership Project*) je definirao skup frekvencijskih pojaseva za koje se može koristiti NB-IoT. Na tablici 5.1 je pregled frekvencijskih pojaseva podržanih u različitim regijama [13]:

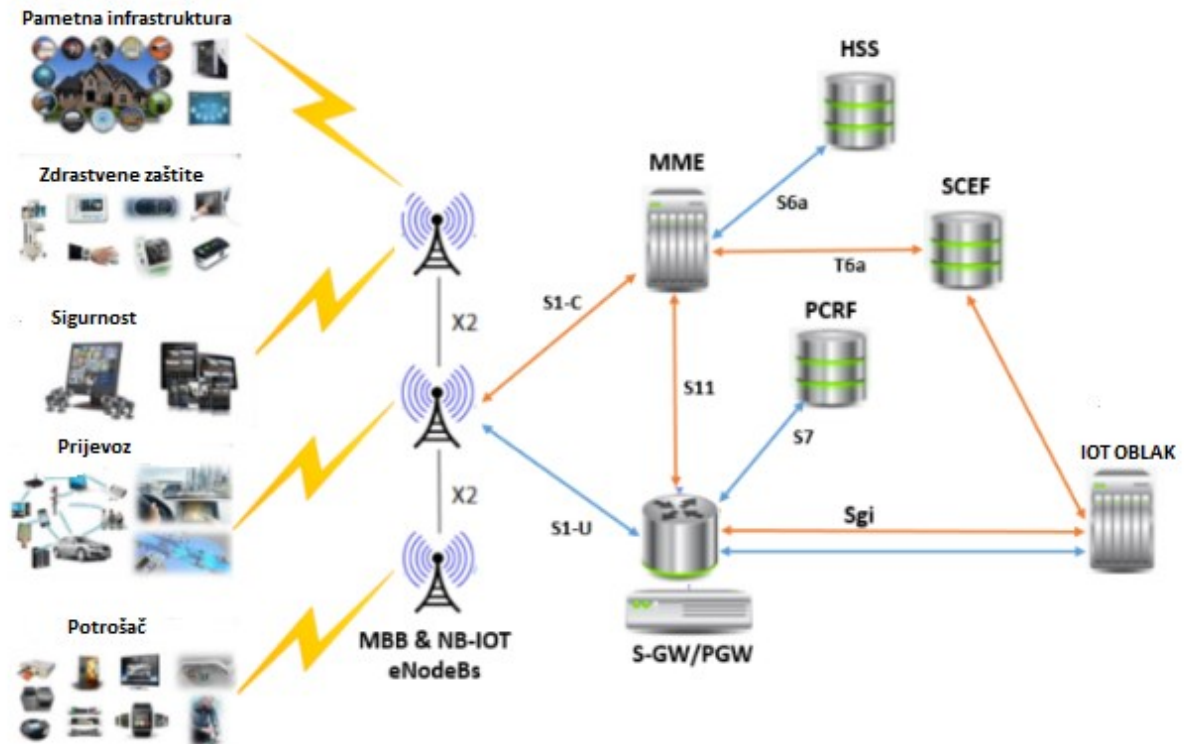
Regije	Pojas
Europa	3,8,20
Sjeverna Amerika	2,4,5,12,66,71,26
Azija i Pacifik	1,3,5,8,18,20,26,28
Afrika	3,8
Južna Amerika	2,3,5,28

Tablica 5.1. Frekvencijski pojasevi za NB-IoT

5.1. Arhitektura NB-IoT-a

NB-LTE također koristi istu mrežnu arhitekturu kao i konvencionalna LTE mreža uz određenu optimizaciju koja je potrebna za podršku zahtjevima korisnika IoT Massive. Osnovna arhitektura za NB-LTE prikazana je u nastavku i slična LTE mreži sastoji se od dva dijela, odnosno

pristupne mreže i jezgrene mreže razvijenog paketnog sustava (EPS). U arhitekturi pristupne mreže nema promjena, ali u jezgri mreže te korisničkoj i kontrolnoj ravni učinjene su neke druge optimizacije za podršku IoT aplikaciji. Uveden je novi čvor kao SCEF (*eng. Service Capability Exposure Function*). SCEF je dizajniran posebno za podatke o tipu stroja. Koristi se za isporuku ne internetski protokol podataka preko kontrolne ravnine i pruža sučelje za mrežne usluge (provjera autentičnosti i autorizacija, otkrivanje i mrežne mogućnosti pristupa).



Slika 5.2 Arhitektura NB-IoTa

Na upravljačkoj ravni, UL podaci se mogu prenijeti iz eNB-a u MME (*eng. Mobility Management Entity*). Od toga se može ili prenijeti preko poslužiteljskog pristupnika (SGW) na mrežni pristupnik paketnih podataka (PGW) ili u funkciju izlaganja mogućnosti usluge (SCEF) što je međutim moguće samo za pakete podataka koji nisu internetski protokol. Iz tih čvorova konačno se prosljeđuju na poslužitelj aplikacija ili IoT usluge. Isto je prikazano narančastom linijom na slici 5.2. DL podaci se prenose istim putovima u obrnutom smjeru. Ovaj pristup ne zahtijeva radijske nositelje, umjesto toga se paketi podataka mogu slati na signalizacijski radio-nosač. Posljedično, ovo rješenje je najprikladnije za prijenos rijetkih i malih paketa podataka [15].

Uz optimizaciju EPS (*eng. Evolved Packet System*) korisničkog plana, podaci se prenose na isti način kao i konvencionalni podatkovni promet, tj. preko radio-nosača preko SGW-a (*eng. Serving Gateway*) i PGW-a (*eng. PDN Gateway*) do aplikacijskog poslužitelja. Stoga stvara određene troškove za izgradnju veze radio nositelja, ali olakšava slijed paketa podataka koji se šalju. Ovaj pristup zahtijeva podršku isporuke i IP i ne-IP paketa podataka s EPS-om. Druga moguća optimizacija može se napraviti za smanjenje signalizacije usmjeravanjem IoT uređaja da rjeđe izvode povremena ažuriranja lokacije i optimizacijom stranica. Smanjenje signalizacije može

pomoći u izbjegavanju situacija preopterećenja u masivnoj mreži uređaja. Rukovanje pohranom podataka o pretplatnicima u HSS-u također treba biti optimizirano za podršku velikom broju IoT-a [15].

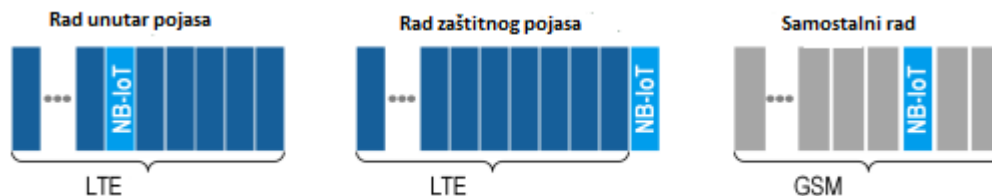
5.2. Načini rada NB-IoT-a

NB-IoT je standard za prijenos podataka dizajniran da omogući uređajima rad u mrežama mobilnih operatera. NB-IoT tehnologija koristi signale niske propusnosti za komunikaciju unutar postojećih GSM i LTE tehnologija. Posebno dizajnirani uređaji i senzori osnovne su komponente u NB-IoT sustavima. Ovi uređaji prikupljaju informacije iz svoje okoline i prenose ih do NB-IoT baznih stanica ili prijenosnih čvorova. Pojedinačne bazne stanice spojene su na IoT pristupnik i IoT aplikacijske poslužitelje u oblaku za centralizirano praćenje i analizu podataka. NB-IoT koristi novi fizički sloj sa signalima i kanalima kako bi zadovoljio zahtjeve proširene pokrivenosti u ruralnim područjima i duboko u zatvorenom prostoru, istovremeno omogućavajući vrlo nisku složenost uređaja. Osnovna tehnologija je mnogo manje složena od one kod GSM/GPRS modula. NB-IoT tehnologija zauzima frekvencijski pojas širine pojasa od 180 kHz, što odgovara jednom bloku resursa u LTE prijenosu [14]. Na slici 5.3. prikazani su sljedeći mogući načini rada:

1.) Samostalni rad (*eng. Stand alone operation*)- najvjerojatniji scenarij je upotreba trenutno korištenih GSM frekvencijskih opsega. Uz njihovu širinu pojasa od 200 kHz i dalje postoji zaštitni interval od 10 kHz, koji ostaju na obje strane spektra [14].

2.) Rad zaštitnog pojasa (*eng. Guard band operation*)- koristeći neiskorištene blokove resursa unutar LTE operatera gard-band [14].

3.) Rad unutar pojasa (*eng. In-band operation*)- koristeći blokove resursa unutar LTE nositelja [14].



Slika 5.3. Načini rada NB – IoT tehnologije

5.3. Prednosti i nedostaci NB-IoT-a:

Prednost NB-IoT-a su:

1.) Sveprisutna pokrivenost i povezanost NB-IoT može pomoći u podršci velikom broju uređaja uspostavljanjem NB-IoT mreža koje se mogu povezati s milijardama čvorova. Dizajnirani za proširenu pokrivenost u zatvorenom prostoru, niža složenost uređaja omogućuje povezivanje i komunikaciju velikog dometa.

2.) Energetski zahtjevi su smanjeni jer ne treba pokretati težak operativni, kao što je Linux, niti puno obrađivati signale, što ga čini energetski učinkovitijim u usporedbi s drugim staničnim tehnologijama.

3.) Niska cijena uređaja budući da je lakše stvoriti uređaje manje složenosti, cijena uređaja je vrlo niska, oko 5 USD po modulu.

4.) Višegodišnji vijek trajanja baterije donosi mogućnost poboljšane potrošnje energije, omogućuje NB-IoT-u da podrži višegodišnje trajanje baterije za uređaje.

5.) Sigurnost NB-IoT je osiguran slično kao 4G, uključujući sve značajke enkripcije i provjere autentičnosti temeljene na SIM kartici.

Nedostatci NB-IoT-a:

1.) Ograničena mobilnost uređaja koji ostaju povezani samo unutar ograničenog okruženja i samo na jednog mrežnog operatera. To bi moglo značiti ograničenja za takve namjene kao što su nosivi uređaji koji napuštaju određene perimetre. Ako osoba s nosivim uređajem, na primjer uđe u drugu zemlju, uređaj bi mogao postati neupotrebljiv ako operater nije prisutan na lokalnoj razini.

2.) Ograničen prijenos podataka, prijenos glasa ili videa nije opcija jer NB-IoT može prenijeti samo manje od kilobajta podataka dnevno, otprilike jednako tekstualnoj poruci. Brzina prijena podataka NB-IoT je oko 20 Kbps, i niska je u usporedbi s konkurentskim tehnologijama. Njegova širina pojasa je oko 200 kHz.

3.) Nedostaje dokaz koncepta budući da je komercijalno uvođenje relativno ograničeno, teško je odrediti je li tehnologija bila uspješna.

6. Usporedba LoRaWAN, Sigfox i NB-IoT bežičnih senzorskih mreža

Cilj je pružiti što bolja rješenja uz nižu potrošnju energije, nižu cijenu i veću pokrivenost. Međutim, tehnologije se razlikuju i svaka od njih su dobre ili loše za pojedine zahtjeve IoT aplikacija. U nastavku će se usporediti LoRaWAN, Sigfox i NB-IoT mreže na temelju sljedećih čimbenika:

- 1.) Tehnološki podaci
- 2.) Kvaliteta prijenosa
- 3.) Pokrivenost i domet
- 4.) Energetska učinkovitost i latencija
- 5.) Sigurnost
- 6.) Troškovi

6.1. Tehnološki podaci

U tablici 6.1 prikazani su tehnološki podaci za svaku mrežu poput maksimalne brzine prijenosa podataka, brzine prijenosa podatka u najgorem slučaju i mnoge druge. Iz tablice se vidi da najveću brzinu prijenosa podataka ima NB-IoT kao i maksimalnu nosivost podataka po poruci, a najmanju brzinu ima Sigfox, dok LoRaWAN ima najmanji maksimalni gubitak podataka i za uzlaznu i za silaznu vezu [18].

	NB-IoT	LoRaWAN	Sigfox(EU)
Tehnologija	Otvoreni standard	vlasnički	vlasnički
Licencirani spektar	da	ne	ne
Maksimalna brzina prijenosa podataka	27 kbit/s	5,47 kbit/s	0,1 kbit/s
Minimalna brzina prijenosa podataka	5-6 kbit/s	0,297 kbit/s	0,1 kbit/s
Maksimalna nosivost	>1000 B	51 B(EU)/11 B(US)	12 B
Kapacitet silazne veze	neograničeno	jako mala	Jako mala
Maksimalni gubitak podataka(Uzlazna veza)	164 dB	141-146 dB	163 dB
Maksimalni gubitak podataka(silazna veza)	164 dB	151-156 dB	158 dB

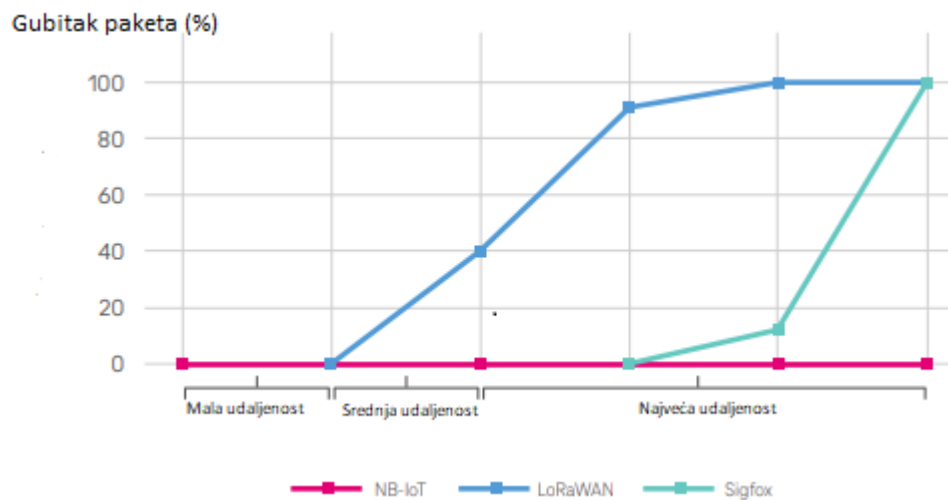
Tablica 6.1. Tehnološki podaci za NB-IoT, Sigfox i LoRaWAN

6.2. Kvaliteta prijenosa

LoRaWAN i SigFox ne koriste licencirani LTE frekvencijski raspon pa zbog toga moraju odašiljati preko slobodne i općenito dostupne ISM frekvencije. Dakle opada im kvaliteta prijenosa čim ima previše prometa na SigFox-u baznoj stanici ili LoRaWAN-u tako da im se povećava vjerojatnost gubitka poruke. Osim toga, broj ponavljanja poruka je ograničen zakonom čime se smanjuje prodor u nepovoljnim uvjetima. Zakonom EU-a snaga je ograničena na 14 dBm. Zbog

toga što su pod utjecajem smetnji povećava se postotak gubitka paketa, a to dovodi do veće potrošnje energije i višestrukih prijenosa podataka. LoRaWAN gubi veliki broj paketa čak i na kratkim udaljenostima i pri njegovoj upotrebi treba prihvatiti gubitak paketa od oko 40% na udaljenosti od četiri kilometara. SigFox-om je pouzdan na kraćim relacijama dok na većim se i kod njega javljaju veliki gubitci paketa kao što je prikazano na slici 6.2. [17].

Za razliku od navedene dvije senzorske mreže, NB-IoT koristi LTE čime sprječava smetnje i osigurava definiranu kvalitetu usluge također poruke se mogu ponavljati vrlo često i zajedno sa prijenosnom snagom od 23 dBm povećava se prodor u nepovoljnim uvjetima kao što su podrumi kuća ili zgrada. NB-IoT za razliku od SigFox-a i LoRaWAN-a nema veliki postotak gubitka paketa ni na kraćim udaljenostima ni na većim. LoRaWAN i Sigfox imaju manje pouzdan prijenos zbog toga što imaju nisku otpornost na smetnje. NB-IoT pruža najučinkovitiji prijenos podataka zahvaljujući svojim rezerviranim kanalima [17].



Slika 6.2 Postotak gubitak paketa u odnosu na udaljenost

6.3. Pokrivenost i domet

Postoje velike razlike u pokrivenosti između ove 3 tehnologije, tu su SigFox i LoRaWAN u velikom nedostatku u odnosu na NB-IoT. Glavnu razliku donosi činjenica da NB-IoT koristi 3GPP LTE industrijski standard koji radi na istoj bazi staničnu opremu i stoga može koristiti LTE infrastrukturu. Na primjer, u Njemačkoj postoji oko 60 000 LTE baznih postaja i oko 20 000 baznih postaja po pružatelju mrežnih usluga te je uslijed toga moguće osigurati dostupnost u cijeloj zemlji. Postavljanje i rad dovoljnog broja baznih postaja za LoRaWAN i SigFox ne bi bio održiv. Iako LoRaWAN pruža javnu mrežu u urbanim mjestima, ona ne osigurava jamstvo kvalitete. Preko 100 mobilnih operatera u 60 zemalja već koristi NB-IoT [17].

Osim toga, kako bi se još više osigurala globalna dostupnost, mnogi NB-IoT moduli mogu se vratiti na 2G/3G ili LTE-M bežične mreže. LoRaWAN mreže postoje u savezu LoRa 160 zemalja, uglavnom kao lokalne instalacije. Pouzdani ugovorni okvir postoji u samo nekoliko slučajeva zbog čega je roaming težak. Druga opcija je decentralizirani roaming između otvorenih,

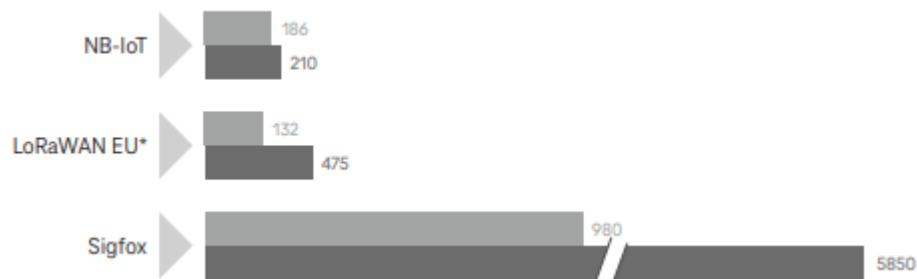
privatnih i javnih mreža, ali predstavlja rizik za sigurnost i pouzdanost. Razlike u frekvencijskim pojasevima i nacionalnim propisima LoRaWAN pravila također su jedan od razloga zašto nisu univerzalno kompatibilna između Europe, Amerike i Azije. Sigfox navodi da se koristi u oko 75 zemalja. Globalno centralizirana infrastruktura mreže olakšava korištenje stranih mreža, ali zbog malog broja baznih stanica po zemlji nema pouzdanih međunarodnih (unutarnjih) pokrivenost mrežom. Svatko tko koristi IoT aplikacije otkrit će da samo mobilni standardi kao što je NB-IoT mogu ponuditi potrebno pokriće [17].

Glavna mana NB-IoT-a je ta što ima najnižu mogućnost pokrivanja i domet koji je manji od 10 km. Također implementacija NB-IoT-a u ruralnim i prigradskim područjima je problem zbog toga što je ograničen na LTE bazne stanice, a u većini slučajeva ta područja nisu pokrivena. Za razliku od LoRaWAN-a koji je prikladan u tim područjima, ima domet oko 20 km i grad veličine Barcelone bi se mogao pokriti za 3 bazne postaje. Sigfox ima duplo veći domet od LoRaWAN-a što mu je jedna od najvećih prednosti i najprikladniji je za ruralna i prigradska područja [17].

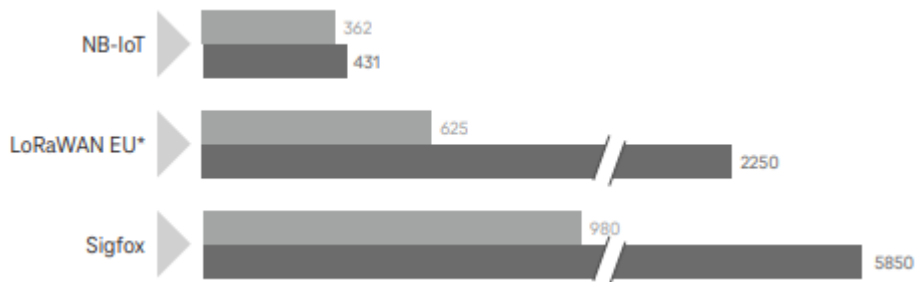
6.4. Energetska učinkovitost i latencija

U IoT je najvažnije koristiti što je moguće manje energije jer je to jedini način pri kojoj modul može raditi dugo bez održavanja baterije. To čini uređaje neovisne o fiksnom izvoru napajanja i održava troškove rada niskim. Energetska učinkovitost je stoga jako važna za masovnu upotrebu LPWAN. Veća količina podataka znači i veću potrošnju energije.

NB-IoT uređaji mogu slati velike pakete podataka u jednom komadu. Za razliku od toga, Sigfox bi trebao podijeliti u 6 zasebnih paketa poruku od 64 bajta što zahtjeva 6 puta više energije za prijenos. S gotovo 1000 mWs za svaki paket, potrošnja energije bi bila iznimno visoka jer Sigfox tehnologija ne dopušta prilagodbu snage prijema prema uvjetima prijema. Stoga česta izvješća o statusu ili položaju nisu kompatibilna s dugim trajanjem baterije. LoRaWAN je relativno ekonomičan u dobrim uvjetima pokrivenosti i s vrlo malim količinama podataka kao što se vidi na slikama 6.3 i 6.4, ali ne radi u teškim uvjetima prijema kao što se vidi na slici 6.5. Automatski veće udaljenosti dovode do povećanog postotka gubitka paketa što rezultira ponovno slanje paketa s time se i povećava potrošnja energije [18].



Slika 6.3. Optimalni vanjski uvjeti prijema [18]



Slika 6.4. Mješoviti uvjeti prijema [18]



Slika 6.5. Teški uvjeti prijema [18]

NB-IoT nudi prednost niske latencije. Za razliku od Sigfox-a i LoRa koji pruža klasu C za rukovanje niskom dvosmjernom latencijom na račun povećane potrošnje energije. Stoga, za aplikacije koje su neosjetljive na kašnjenje i nemaju veliku količinu podataka za slanje, Sigfox i klasa-A LoRa su najbolje opcije. Za aplikacije koje zahtijevaju malo kašnjenje, NB-IoT i klasa C LoRa su bolji izbor.

6.5. Sigurnost

LoRaWAN je u početku imao velike problema u sigurnosti sa svojom v1.0 verzijom. Izlaženje nove v1.1 verzije riješena su većina problema i eliminirane su ranjivosti poput end-to-end enkripcije nosivosti okvira kod koje mrežni poslužitelj dobiva pristup ključu tijekom procesa spajanja terminalnog uređaja. Sigfox je bez obzira na svoj integrirani sigurnosni mehanizam, jako ranjiv na napade zbog jako male veličine. Na temelju troškova u pravilu nemaju sigurnosni element – čip sigurno koji pohranjuje kriptografske podatke, kao što su tajni ključevi. Hacker stoga može uspjeti izvući tajne ključeve ili umetnuti uređaj s kompromitiranim firmware-om. Korištenje uređaja bez sigurnosnog elementa može čak i end-to-end enkripciju učiniti beskorisnom [18].

Nasuprot tome, NB-IoT koristi LTE sigurnosne značajke koje su se pokazale kao najsigurnije rješenje. Oni uključuju uzajamnu provjeru autentičnosti terminalnog uređaja i mreže, AES i sigurno generiranje i razmjena ključeva. S mrežne strane zračno sučelje NB-IoT-a uvijek je šifrirano. Još jedna prednost NB-IoT su SIM kartice zaštićene od neovlaštenog otvaranja jer sadrže sigurnosne elemente. End-to-end enkripcija nije standardna, ali mrežni operateri mogu uvesti višu

razinu sigurnosti korištenjem, na primjer, sigurnosnog tunela između jezgrene mreže i aplikacijskog poslužitelja. Za roaming u NB-IoT mrežama dodatne sigurnosne mjere kao što je end-to-end enkripcija trebale bi biti implementirane. Najsigurnija opcija je NB-IoT zbog toga što koristi LTE sigurnosne značajke i ima razne sigurnosne elemente koje štite SIM kartice od neovlaštenog otvaranja. Međutim, s vremenom sve tri mreže polako poboljšavaju sigurnost kao što je vidljivo u novijim verzijama LoRaWAN-a [18].

6.6. Troškovi

Troškovi LPWAN tehnologija u najvećoj mjeri ovise o načinu rada, to jest o implementaciji i upravljanju vlastitom mrežom ili pretplati na mrežnog operatera. Cijena NB-IoT hardvera brzo opadaju zbog stalne povećane prodaje i zbog visoke proizvodnje, što je rezultiralo da je cijena od 4 eura po modulu premašena u samo nekoliko godina nakon prvog postavljanja NB-IoT mreže. SigFox moduli i uređaji trenutno su najjeftiniji [19].

Za pravu usporedbu treba uzeti različite aspekte troškova kao što su trošak spektra, trošak krajnjeg uređaja i trošak postavljanja. U tablici 6.6 prikazuju se troškovi Sigfoxa, LoRa i NB-IoT za ta tri navedena aspekta. Što se tiče troška spektra za Sigfox i LoRa on je besplatan za razliku od NB-IoT-a. Troškovi postavljanja najviši su za NB-IoT, a najniži za LoRa. Sigfox ima najjeftiniji uređaj koji je 10 puta jeftiniji od uređaja za NB-IoT. Očito je iz tablice da su Sigfox i LoRa isplativiji u usporedbi s NB-IoT. Za većinu slučajeva korištenja IoT-a ukupni trošak vlasništva je niži za NB-IoT nego za LoRaWAN i Sigfox. Dakle, što je dulje predviđeno da IoT aplikacija radi, veća je isplativost NB-IoT-a. Međutim, mogu postojati slučajevi kada bi LoRaWAN mreža mogla biti bolji izbor [19].

	Cijena spektra	Troškovi postavljanja	Cijena uređaja
Sigfox	Besplatno	>4000/bazna stanica	<2€
LoRa	Besplatno	>1000/bazna stanica	3-5€
NB-IoT	>500 M€/MHz	>15000€/bazna stanica	>20€

Tablica 6.6. Troškovi Sigfox-a, LoRa i NB-IoT

7. Zaključak

LoRaWAN, Sigfox i NB-IoT su vodeće LPWAN mreže koje imaju istu namjenu, ali razlikuju se u mnogo tehničkih značajki, poput arhitekture, načina rada uređaja, prijenosa podataka, modulacije itd. Svaka tehnologija ima određenu primjenu za IoT. Sigfox i LoRa služe kao uređaji s nižom cijenom, s vrlo velikim dometom (visoka pokrivenost) i vrlo dugim vijekom trajanja baterije kao što je prikazano na slici 7.1. Obje mreže su prikladne za primjenu u poljoprivedi i srodnim djelatnostima zbog dugotrajnog vijeka baterije krajnjih uređaja. Za razliku od Sigfoxa, LoRa također služi za postavljanje lokalne mreže i pouzdanu komunikaciju. Nasuprot tome, NB-IoT pruža prijenos podataka uz nisko kašnjenje i visoku kvalitetu usluge, ali ukupna cijena mreže je dosta veća, zbog toga što za rad koristi licencirane frekvencijske pojaseve. Unatoč testovima mobilnih kompanija, nedostatak NB-IoT komercijalnih implementacija trenutno ostavlja otvorena pitanja o stvarnom vijeku trajanja baterije i učinak koji se može postići ovom tehnologijom u stvarnim uvjetima. NB-IoT tehnologija pogodna je za primjenu u rješenjima namijenjenima poslovnim i privatnim korisnicima npr. kod sustava za pametno parkiranje, za upravljanje otpadom, za praćenje kvalitete zraka, za praćenje stvari i pošiljaka, za pametna brojila, kod sustava pametnog doma, sustava za praćenje zdravstvenog stanja i slično. IoT čimbenici i tehničke razlike Sigfoxa, LoRaWAN-a i NB-IoT-a određuju koja je tehnologija prikladna za svaku pojedinu aplikaciju. Kao što je već spomenuto u ovome radu, pojedina IoT tehnologija ne može biti jednako prikladna za primjenu u različitim IoT aplikacijama.



Slika 7.1 Usporedba Sigfox, LoRaWAN i NB-IoT

Literatura

- [1] T. Alam. ResearchGate: https://www.researchgate.net/figure/Internet-of-Things-IoT-connected-devices-from-2015-to-2025-in-billions_fig1_325645304[Pristupljeno: svibanj 2022.].
- [2] F. Muhammad Waseem Sadia, M. Anjum, K. KhairiTalha. A Review on Internet of Things. IoTM.U. March 2015 ,2-3.
- [3] W. Chen. AN IBE BASED SECURITY SCHEME OF INTERNET OF THINGS, in Cloud Computing and Intel-ligent Systems (CCIS), 2012, str. 1046, 1049.
- [4] H. Suo, J. Wan, C. Zou, J. Liu. Security in the Internet of Things: A Review in Computer Science and Electronics Engineering (ICCSEE), 2012, str. 648-651.
- [5] M. Wu, Ting-lie Lu, Fei-Yang Ling, Ling Sun, Hui-Ying Du. Research on the architecture of Internet of things, in Advanced Computer Theory and Engineering (ICACTE), 2010,str. 484-487.
- [6] X. Cheng, M. Zhang, F. Sun. Architecture of internet of things and its key technology integration based-on RFID, in Fifth International Symposium on Computational Intelligence and Design, 2012, str. 294-297.
- [7] TechDesign, 2021 May 17: <https://blog.techdesign.com/quick-guide-to-understand-lora-and-lora-modules/>[Pristupljeno: svibanj 2022.].
- [8] D. Meaney. Vice President of Global Technical Sales and Marketing. LoRaWAN .str 1-2.
- [9] The Things network: <https://www.thethingsnetwork.org/docs/lorawan/architecture/>[Pristupljeno: svibanj 2022.]
- [10] B. Paul. An Overview of LoRaWAN. Department of Electrical and Electronic Engineering Shahjalal University of Science and Technology Kumargaon, Bangladesh, 2020. str 234.
- [11] Ubidots: <https://ubidots.com/blog/explaining-sigfox/>[Pristupljeno: svibanj 2022.]
- [12] Circuit Digests: <https://circuitdigest.com/article/what-is-sigfox-basics-architecture-and-security-features>[Pristupljeno: svibanj 2022.]
- [13] NB-IoT Deployment Guide to Basic Feature set Requirements, June 2019.
- [14] J. Schlien, D. Raddino. Narrowband Internet of Things ,str 9.
- [15] M. Luthra, R. Atri, M. Sadeghian, S. Malik, P. Rekhi. Long Term Evolution for IOT, str 9.
- [16] ResearchGate: https://www.researchgate.net/figure/LPWAN-range-vs-bandwidth-in-comparison-with-other-technologies_fig9_311530837[Pristupljeno: svibanj 2022.]
- [17] Sebastian E. J, Sikora A. Test and Measurement of LPWAN and Cellular IoT Networks in a Unified Testbed, 2019.

[18] Naumann H. & Oelers W. NB-IoT, LoRaWAN, Sigfox: An up-to-date comparison, 2020.

[19] K. Mekki, E. Bajić, F. Chaxel, F. Meyer. A comparative study of LPWAN technologies for large-scale IoT deployment, 2019.

[20] M. Won. Experimental Study on Low Power Wide Area Networks (LPWAN) for Mobile Internet of Things, 2019.

Sažetak

Internet stvari ili IoT sustav je međusobno povezanih računalnih uređaja, mehaničkih i digitalnih strojeva, objekata, životinja ili ljudi koji imaju jedinstvene identifikatore (UID) i mogućnost prijenosa podataka preko mreže bez potrebe za komunikacijom od čovjeka do interakcija čovjeka ili čovjeka s računalom. Nagli razvoj IoT-a i problemi s pokrivenosti i potrošnjom energije koji postojeći protokoli nisu zadovoljavali doveli su do pojave mreža velikog dometa i male potrošnje. Vodeće LPWAN mreže su LoRaWAN, Sigfox i NB-IoT bežične senzorske mreže. Oni zadovoljavaju potrebe cijene, učinkovitosti, dometa, kvalitete... Prenose male količine podataka na velike udaljenosti uz nisku potrošnju energije. U radu su opisane te tri bežične senzorske mreže i navede su njihove glavne karakteristike te nakraju njihova međusobna usporedba po cijeni, pokrivenosti, dometu, sigurnosti... i doneseni su zaključci koja mreža je najbolja i najučinkovitija za pojedine zahtjeve IoT aplikacija.

KLJUČNE RIJEČI: IoT, Lpwan, LoRaWAN, Sigfox, NB-IoT

Abstract

The Internet of Things or IoT is a system of interconnected computer devices, mechanical and digital machines, objects, animals or people that have unique identifiers (UID) and the ability to transfer data over a network without the need for human-to-human communication or human-computer interactions. The rapid development of IoT and problems with coverage and energy consumption that existing protocols did not satisfy led to the emergence of LPWAN, that is, low-power wide area networks. The leading LPWAN networks are LoRaWAN, Sigfox and NB-IoT wireless sensor networks. They meet the needs of price, efficiency, range, quality... They transmit small amounts of data over long distances with small energy consumption. The paper describes these three wireless sensor networks and lists their main characteristics, and finally their mutual comparison in terms of price, coverage, range, security... and conclusions are drawn as to which network is the best and most efficient for certain requirements of IoT applications.

KEYWORDS: IoT, Lpwan, LoRaWAN, Sigfox, NB-IoT