Sigurnost LoRaWAN bežičnih mreža

Leon Baždar

Sadržaj

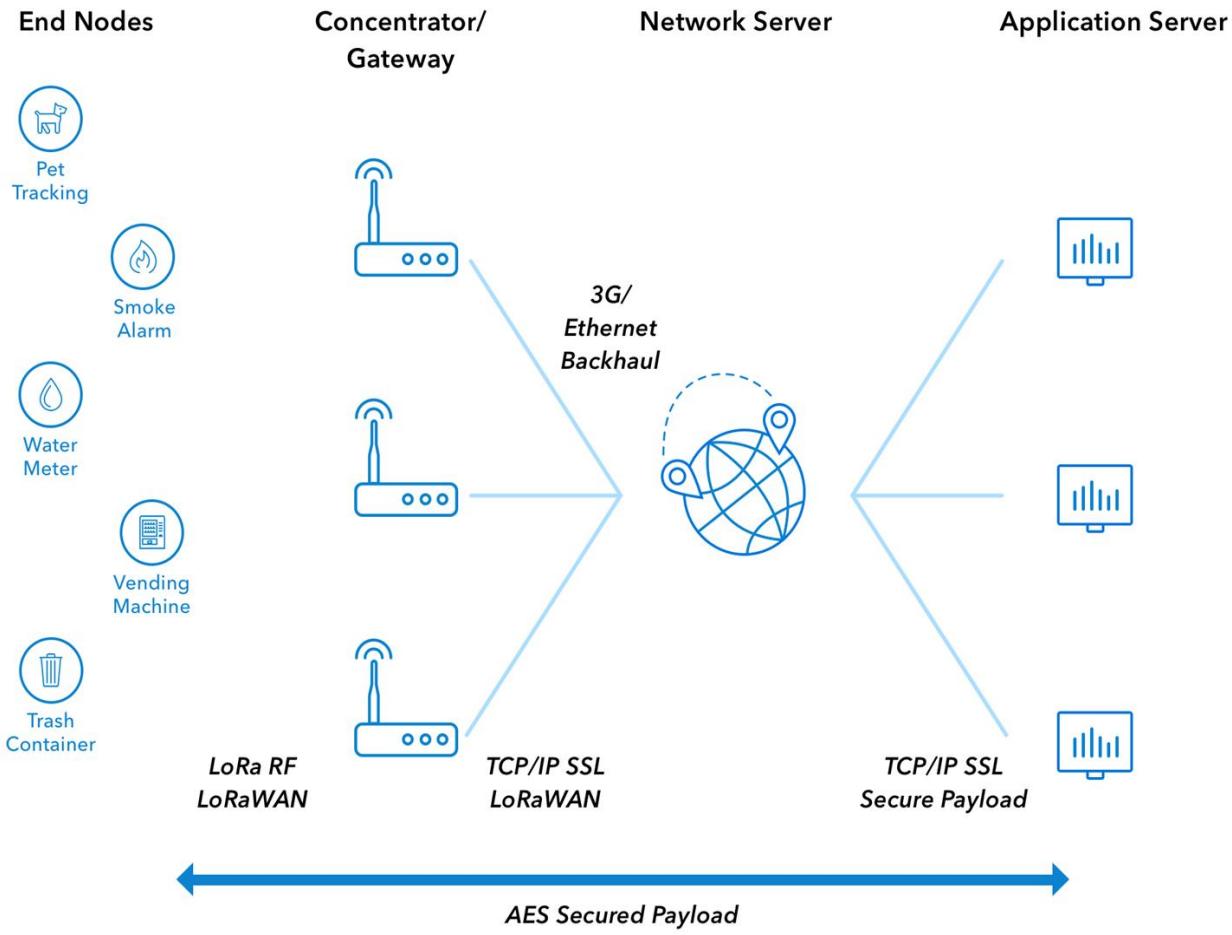
1. Uvod u LoRaWAN Tehnologiju

LoRaWAN (Long Range Wide Area Network) je bežična komunikacijska tehnologija koja je posebno dizajnirana za Internet stvari (IoT) i aplikacije koje zahtijevaju nisku potrošnju energije, velik domet i pouzdanu dvosmjernu komunikaciju. Tehnologija je temeljena na protokolu otvorenog standarda, omogućujući široku primjenu u pametnim gradovima, industriji, poljoprivredi i drugim sektorima.

Jedan od ključnih elemenata LoRaWAN-a je modulacija s proširenim spektrom poznata kao CSS (Chirp Spread Spectrum). CSS omogućuje otpornost na smetnje i visoku osjetljivost prijema, čime se osigurava pouzdana komunikacija na velikim udaljenostima uz vrlo nisku potrošnju energije.

2. Struktura LoRaWAN Mreže

LoRaWAN mreža sastoji se od četiri osnovne komponente: krajnjih uređaja (end devices), pristupnih točaka (gateways), mrežnog poslužitelja (network server) i aplikacijskog poslužitelja (application server). Krajnji uređaji šalju podatke putem pristupnih točaka do mrežnog poslužitelja, koji potom prosljeđuje podatke aplikacijskom poslužitelju za daljnju obradu. Zahvaljujući svojoj energetskoj učinkovitosti, velikom dometu (do nekoliko kilometara u urbanim područjima i preko 15 kilometara u ruralnim područjima) te niskim troškovima implementacije, LoRaWAN je postao jedna od najperspektivnijih tehnologija za IoT aplikacije.



Slika 1 LoRaWAN struktura

3. Chirp Spread Spectrum (CSS)

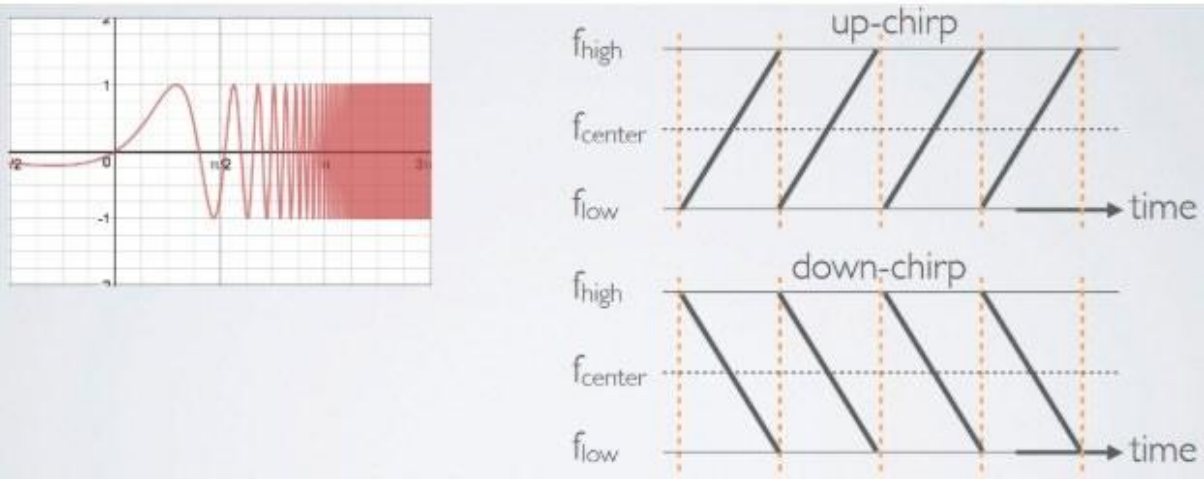
CSS je tehnika modulacije koja koristi linearno promjenjive frekvencije, poznate kao chirp signali. Ova modulacija pruža visoku otpornost na šum, interferencije i multipath efekte, što je ključno za komunikacijske sustave s velikim dometom. U CSS-u, signal se širi preko većeg spektra frekvencija, čime se poboljšava pouzdanost prijenosa podataka čak i pri niskim snagama signala. Osnovna karakteristika CSS-a je sposobnost kodiranja podataka koristeći promjene frekvencije unutar chirp signala. Na taj način postiže se:

- Otpornost na Dopplerov efekt.
- Povećana robusnost signala u prisutnosti šuma.
- Efikasno korištenje spektra za prijenos informacija.

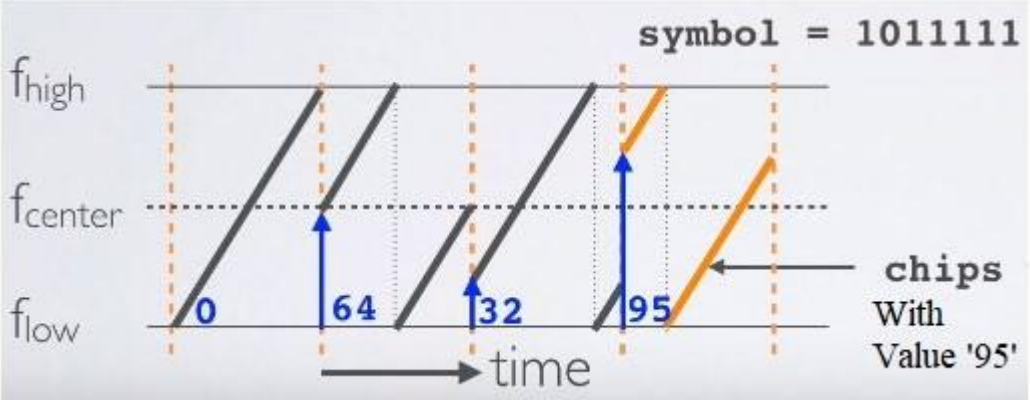
CSS je osobito pogodan za IoT aplikacije zbog svoje energetske učinkovitosti i velikog dometa. Signal može premostiti velike udaljenosti uz vrlo nisku snagu prijenosa, što ga čini idealnim za uređaje s baterijskim napajanjem.

4. LoRa CSS Tehnologija

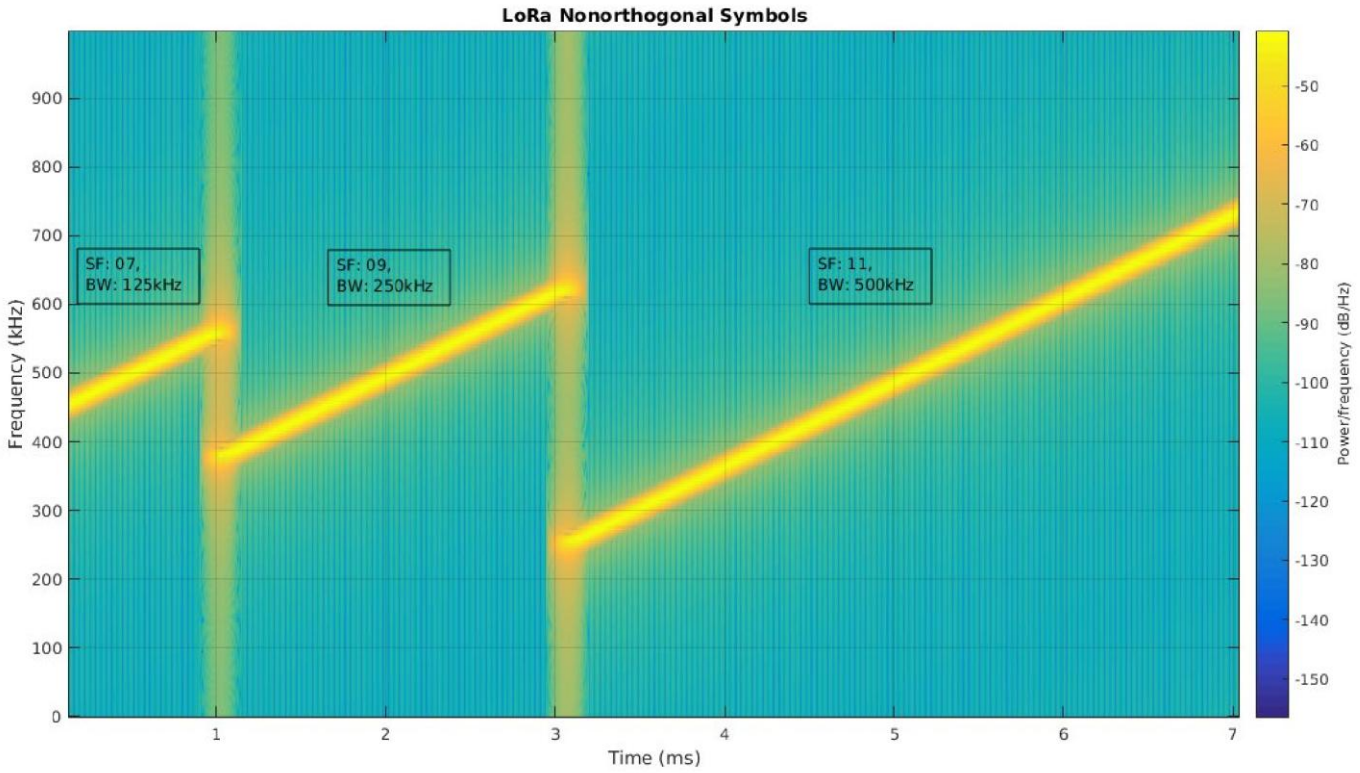
Lora je tehnika modulacije s proširenim spektrom, u vlasništvu tvrtke Semtech Corporation, a izvedena je iz postojeće tehnologije Chirp Spread Spectrum (CSS). Nudi kompromis između osjetljivosti i brzine prijenosa podataka, pri čemu radi u kanalima fiksne širine pojasa od 125 kHz do 500 kHz. LoRa predstavlja isključivo fizički (PHY) sloj, u skladu s OSI sedmoslojnim modelom mreža. Tehnologija Chirp Spread Spectrum (CSS), koju koristi LoRa, omogućuje niske troškove i malu potrošnju energije te ne zahtijeva visoko precizan referentni signal takta. U LoRaWAN sustavima vremenski i frekvencijski pomaci između predajnika i prijamnika su ekvivalentni, što značajno pojednostavljuje dizajn prijamnika. LoRa modulacija podržava ukupno šest faktora širenja signala (SF7 do SF12). Veći faktor širenja omogućuje prijenos signala na veće udaljenosti bez pogrešaka u prijemu od strane RF prijamnika.



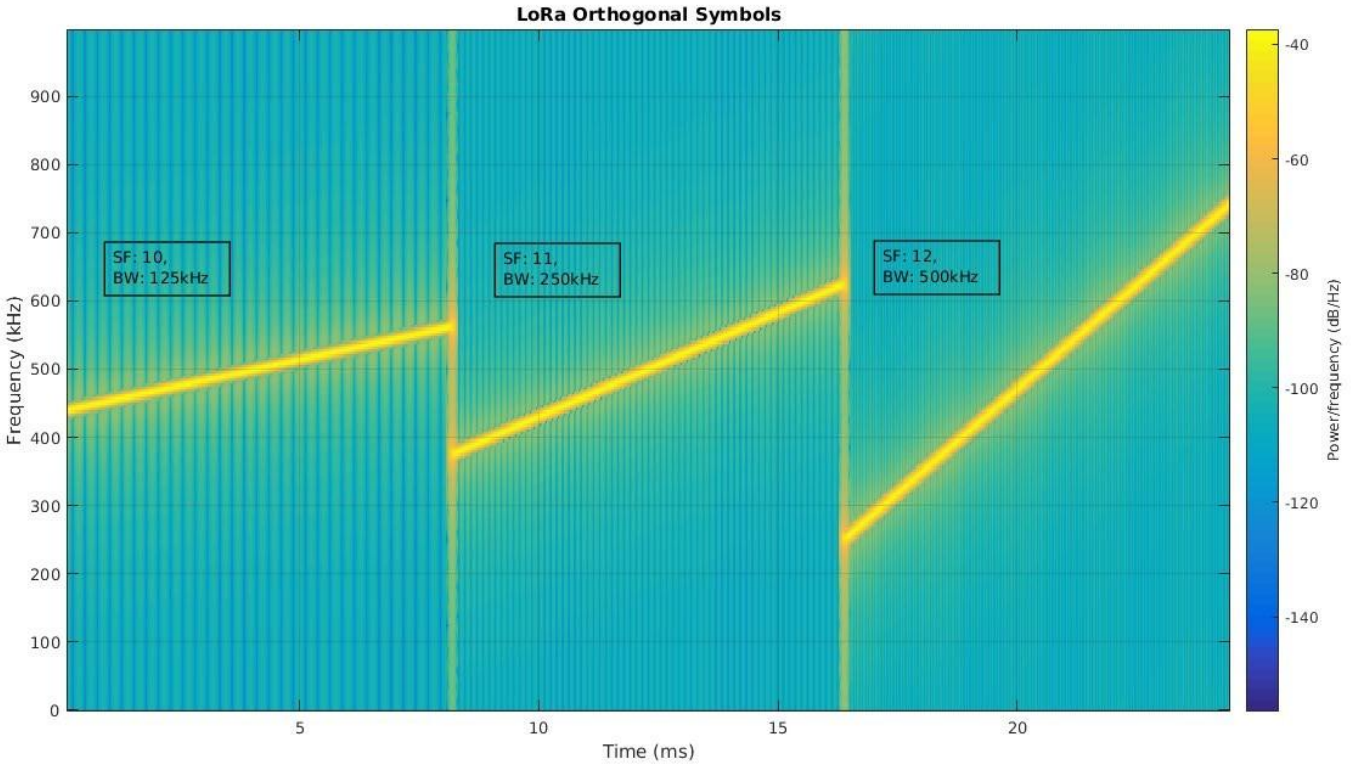
Slika 2 LoRa CSS u vremenskoj domeni



Slika 3 LoRa CSS simboli



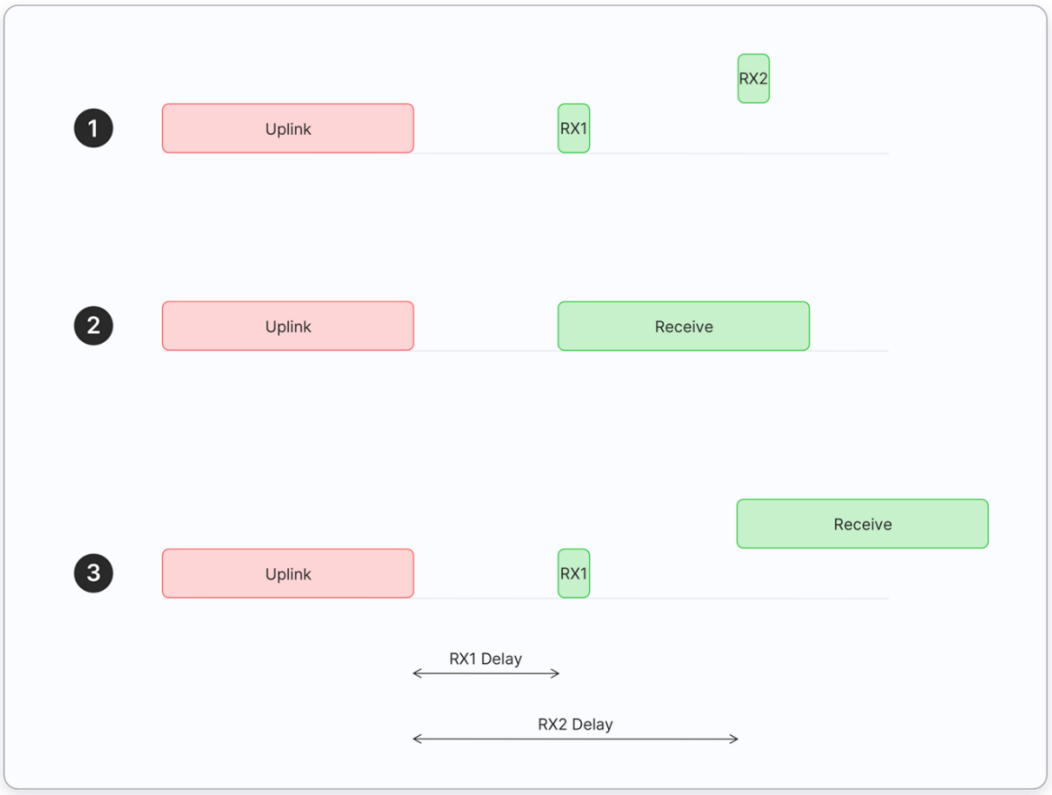
Slika 4 Neortogonalni CSS simboli



Slika 5 Ortogonalni CSS simboli

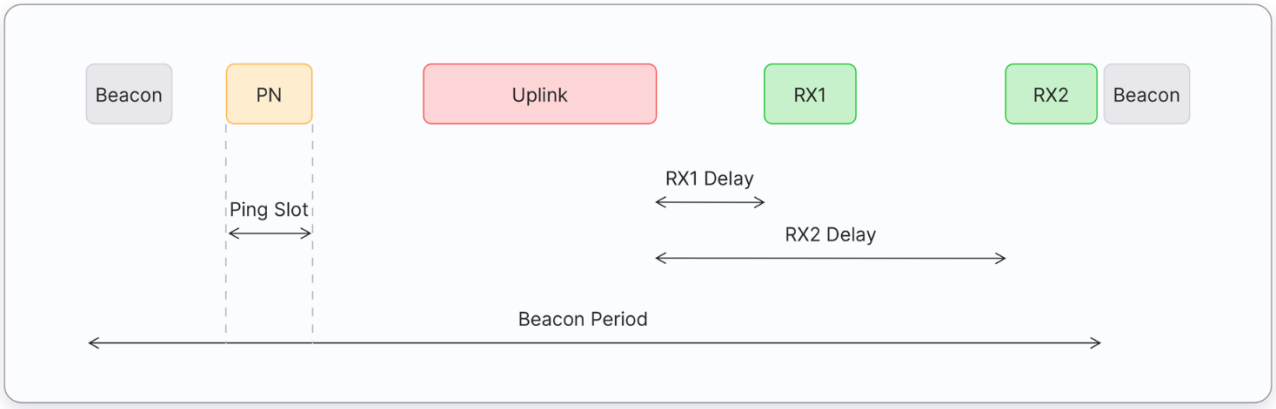
5. Klase uređaja u LoRaWAN mreži

U LoRaWAN mrežama način komunikacije između krajnjeg uređaja i mreže ovisi o klasi kojoj uređaj pripada. Klasa uređaja definira kada i koliko često uređaj sluša poruke s mreže te izravno utječe na potrošnju energije, latenciju i trajanje baterije. Standard LoRaWAN definira tri osnovne klase uređaja: Class A, Class B i Class C. Svaka od njih namijenjena je različitim primjenama, ovisno o zahtjevima sustava i dostupnom napajanju.



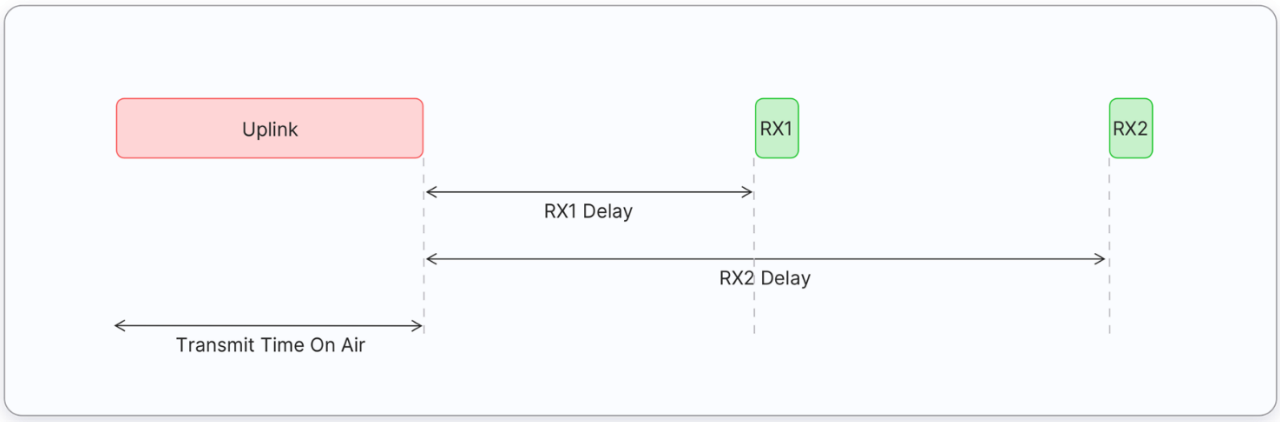
Slika 6 Class A uređaji

Class A je osnovna i obavezna klasa koju mora podržavati svaki LoRaWAN uređaj. Uređaj u ovoj klasi otvara prijemne prozore samo nakon slanja uplink poruke, čime se postiže minimalna potrošnja energije. Downlink poruke mogu se primiti isključivo unutar ta dva kratka prijemna prozora. Zbog toga Class A ima najveću latenciju, ali omogućuje višegodišnji rad na bateriju. Najčešće se koristi kod senzora i mjernih uređaja.



Slika 7 Class B uređaji

Class B proširuje funkcionalnost Class A dodavanjem sinkroniziranih prijemnih intervala. Uređaj se sinkronizira s gatewayem pomoću beacon signala i periodički otvara dodatne prijemne prozore. Na taj način mreža može predvidjeti kada je uređaj dostupan za downlink komunikaciju. Time se smanjuje latencija u odnosu na Class A, ali se povećava potrošnja energije. Class B se koristi kod uređaja koji povremeno trebaju primati naredbe, poput aktuatora i pametne rasvjete.



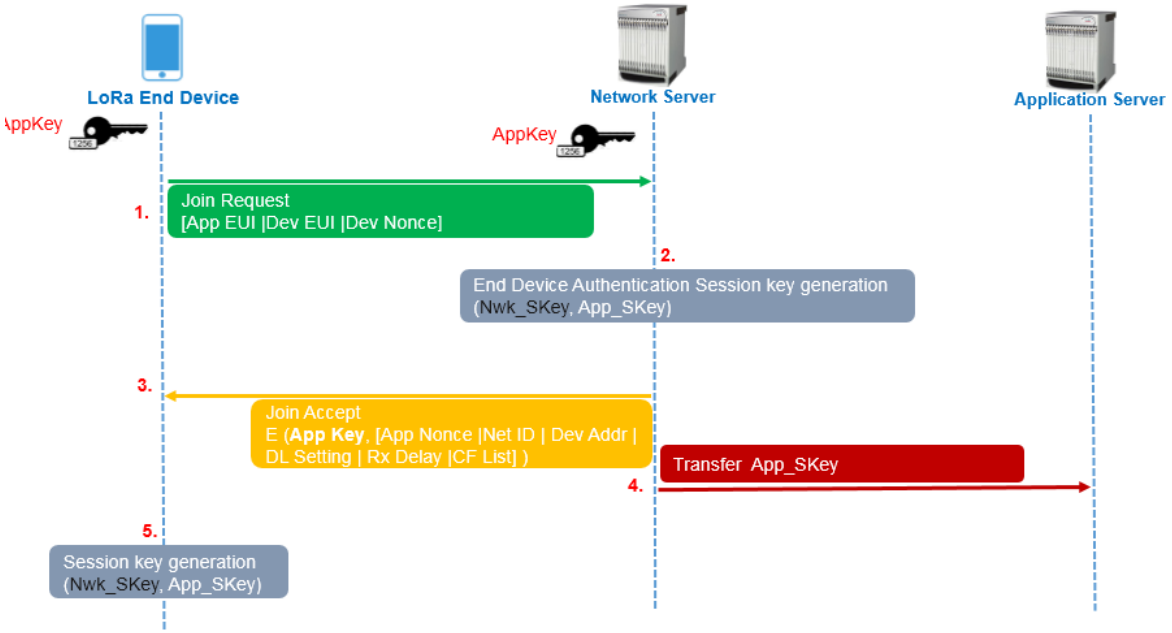
Slika 8 Class C uređaji

Class C omogućuje gotovo stalno aktivan prijemni kanal, osim tijekom slanja uplink poruka. Uređaj je u svakom trenutku spreman za primanje downlink poruka, što osigurava minimalnu latenciju. Zbog stalnog rada prijemnika, potrošnja energije je vrlo velika. Ova klasa je prikladna isključivo za uređaje s trajnim napajanjem. Najčešće se koristi u industrijskim sustavima upravljanja i nadzora.

6. Spajanje uređaja na LoRaWAN mrežu

U LoRaWAN mrežama postoje dva osnovna načina spajanja uređaja na mrežu: OTAA (Over-The-Air Activation) i ABP (Activation By Personalization). Kod OTAA metode uređaj se dinamički prijavljuje u mrežu pomoću sigurnosnog postupka razmjene poruka i generiranja sesijskih ključeva, dok se kod ABP metode sigurnosni parametri unaprijed ručno upisuju u uređaj. Zbog veće sigurnosti i mogućnosti promjene ključeva, OTAA se danas smatra preporučenim načinom spajanja na LoRaWAN mrežu.

6.1 Postupak spajanja pomoću OTAA metode



Slika 9 Postupak spajanja pomoću OTAA metode

Kod OTAA metode krajnji uređaj najprije šalje mreži poruku Join Request, koja sadrži identifikatore AppEUI, DevEUI i nasumični broj DevNonce. Ova poruka nije enkriptirana, ali je zaštićena MIC kodom koji se računa pomoću tajnog ključa AppKey, čime se omogućuje provjera autentičnosti uređaja.

Nakon primitka Join Request poruke, mrežni server provjerava ispravnost MIC-a, identitet uređaja i jedinstvenost DevNonce vrijednosti. Ako su svi podaci valjani, server započinje postupak generiranja sesijskih ključeva za komunikaciju.

Zatim mrežni server šalje uređaju poruku Join Accept, koja sadrži mrežne parametre, adresu uređaja i dodatne komunikacijske postavke. Ova poruka je u potpunosti enkriptirana pomoću AppKey-a, što znači da je može dekriptirati isključivo legitimni uređaj koji posjeduje odgovarajući ključ.

Istovremeno mrežni server prosljeđuje aplikacijskom serveru aplikacijski sesijski ključ AppSKey, koji se koristi za dekripciju korisnih podataka. Na taj način aplikacijski server može pristupiti sadržaju poruka, dok mrežni server prvenstveno brine o prijenosu i sigurnosti prometa.

Nakon primitka i dekripcije Join Accept poruke, uređaj pomoću AppKey-a, DevNonce-a i podataka iz poruke samostalno izračunava sesijske ključeve NwkSKey i AppSKey. Time se osigurava da se stvarni ključevi ne šalju preko mreže, već se neovisno generiraju na obje strane.

Od tog trenutka sva korisna komunikacija između uređaja i mreže odvija se sigurno. Korisni podaci se enkriptiraju pomoću AppSKey-a, dok se integritet poruka provjerava pomoću NwkSKey-a. Time se sprječava neovlašteno čitanje i izmjena podataka tijekom prijenosa.

7. DoS napad na LORAWAN mrežu

7.1 Opis razvijenog proizvoda

Razvijeni sustav predstavlja eksperimentalno i istraživačko okruženje za analizu sigurnosti LoRaWAN bežičnih mreža u kontroliranim uvjetima. Sustav je namijenjen isključivo za laboratorijsku i akademsku uporabu te omogućuje ispitivanje ponašanja LoRaWAN mreže tijekom pasivnog nadzora komunikacije i simulacije odabranih scenarija napada.

Sustav se sastoji od funkcionalne LoRaWAN infrastrukture koja uključuje krajnji uređaj, pristupni uređaj (gateway) i mrežni poslužitelj, kao i dodatne alate za pasivno praćenje i analizu LoRaWAN prometa pomoću SDR tehnologije. Poseban naglasak stavljen je na mogućnost promatranja reakcije mreže na namjerne radio-frekvencijske smetnje i nepravilnosti u komunikacijskim postupcima, poput postupka pridruživanja mreži i prijenosa potvrđenih poruka.

Razvijeni proizvod ne predstavlja gotov komercijalni sustav, već istraživačku platformu koja služi za demonstraciju sigurnosnih ograničenja i evaluaciju postojećih sigurnosnih mehanizama LoRaWAN protokola u realističnom, ali kontroliranom okruženju.

7.2 Tehničke značajke

7.2.1 Arhitektura sustava

Razvijeni sustav temelji se na standardnoj LoRaWAN arhitekturi, proširenoj dodatnim komponentama za pasivni nadzor i aktivno sigurnosno testiranje u kontroliranom okruženju. Sustav se sastoji od legitimnih LoRaWAN komponenti, testnih napadačkih uređaja te neovisnog SDR prijamnog sustava za analizu radio-sloja.

Legitimni dio sustava uključuje LoRaWAN krajnji uređaj temeljen na LA66 USB adapteru, LoRaWAN gateway realiziran pomoću WM1302 koncentratora i Raspberry Pi 5 platforme te mrežni poslužitelj temeljen na ChirpStack programskom paketu. Ovaj dio sustava omogućuje uspostavu i normalan rad LoRaWAN komunikacije u EU868 frekvencijskom području.

Za provođenje aktivnih sigurnosnih eksperimenata koriste se dodatni testni uređaji koji nisu dio LoRaWAN mreže. To uključuje modificirani LA66 uređaj s prilagođenim firmwareom te LoStik USB uređaj, koji se koriste za generiranje vremenski usklađenih radio-frekvencijskih smetnji i simulaciju odabranih napadnih scenarija, poput ometanja postupka pridruživanja mreži i potvrđenih uplink poruka.

Pasivni nadzor komunikacije ostvaruje se pomoću SDR prijamnika temeljenog na RTL-SDR platformi. SDR sustav omogućuje neinvazivno praćenje LoRa signala na fizičkom sloju, ne sudjelujući u LoRaWAN mreži i ne utječući na njezin rad. Prikupljeni podaci obrađuju se u GNU Radio okruženju te se koriste za daljnju analizu i dekodiranje LoRaWAN paketa.

Ovakva arhitektura omogućuje istovremenu analizu ponašanja LoRaWAN mreže s mrežnog, aplikacijskog i radio-frekvencijskog aspekta, čime se osigurava cjelovit uvid u sigurnosna ograničenja sustava tijekom eksperimentalnih testiranja.

7.2.2 Hardverske komponente

Razvijeni sustav sastoji se od više hardverskih komponenti koje zajedno omogućuju uspostavu LoRaWAN mreže, pasivni nadzor radiokomunikacije te provođenje aktivnih sigurnosnih eksperimenata u kontroliranom okruženju.

7.2.2.1 Raspberry Pi 5

Raspberry Pi 5 koristi se kao središnja računalna platforma sustava. Na uređaju je instaliran Linux operacijski sustav te pokrenuto ChirpStack okruženje koje obavlja funkciju LoRaWAN mrežnog i aplikacijskog poslužitelja. Raspberry Pi također služi kao komunikacijsko sučelje prema LoRaWAN gatewayu i ostalim perifernim uređajima.

Slika 10Raspberry Pi 5

7.2.2.2 WM1302 LoRa koncentrator

WM1302 LoRa koncentrator koristi se kao LoRaWAN gateway i povezan je s Raspberry Pi 5 platformom putem Pi-HAT sučelja. Koncentrator omogućuje istovremeni prijem više LoRa paketa različitih parametara, uključujući različite spreading faktore i širine pojasa, u EU868 frekvencijskom području. Time se osigurava realističan rad LoRaWAN mreže sukladan stvarnim implementacijama.

Slika 11 WM1302 LoRa koncentrator

7.2.2.3 LA66 USB LoRaWAN adapter

LA66 USB LoRaWAN adapter temeljen na ASR6601 platformi koristi se kao legitimni LoRaWAN krajnji uređaj unutar mreže. Uređaj podržava OTAA postupak pridruživanja mreži te prijenos uplink i downlink poruka. Zahvaljujući dostupnom razvojnome SDK-u, omogućena je izmjena i ponovno prevođenje firmwarea, čime se postiže precizna kontrola ponašanja uređaja tijekom sigurnosnih eksperimenata. Modificirani LA66 uređaj s prilagođenim firmwareom koristi se kao testni uređaj za simulaciju specifičnih sigurnosnih scenarija. Ovaj uređaj nije registriran kao legitimni član LoRaWAN mreže, već se koristi za generiranje namjernih radio-frekvencijskih smetnji i kontroliranih nepravilnosti u komunikaciji, primjerice tijekom postupka pridruživanja mreži.

Slika 12 LA66 USB LoRaWAN adapter

7.2.2.4 LoStik USB LoRa uređaj

LoStik USB uređaj, temeljen na Microchip RN2483 LoRa transceiveru, koristi se kao namjenski testni uređaj za provođenje aktivnih radio-frekvencijskih smetnji. Uređaj se upravlja putem serijskog sučelja korištenjem AT naredbi te omogućuje precizno definiranje parametara prijenosa, uključujući frekvenciju, spreading faktor i izlaznu snagu. U okviru projekta LoStik se koristi za vremenski usklađeno ometanje komunikacije tijekom kritičnih faza LoRaWAN prijenosa, poput potvrđenih uplink poruka i prijemnih prozora RX1 i RX2.

Slika 13 LoStik USB LoRa

7.2.2.5 RTL-SDR v4 prijamnik

RTL-SDR v4 prijamnik koristi se za pasivni nadzor LoRa radio-signala. Prijamnik omogućuje neinvazivno praćenje komunikacije na fizičkom sloju bez sudjelovanja u LoRaWAN mreži. Time se osigurava da proces nadzora ne utječe na ponašanje sustava, a istovremeno omogućuje detaljna analiza emitiranih LoRa signala.

Slika 14 RTL-SDR v4

7.2.3 Softverske komponente

Softverski dio sustava obuhvaća programske pakete i vlastite alate koji omogućuju upravljanje LoRaWAN mrežom, pasivni nadzor radio-komunikacije te analizu i dekodiranje LoRaWAN paketa prikupljenih tijekom eksperimentalnih testiranja.

7.2.3.1 Operacijski sustav i osnovni servisi

Na Raspberry Pi 5 platformi koristi se Linux operacijski sustav koji osigurava stabilno izvođenje mrežnih servisa, upravljanje USB i SPI uređajima te mrežnu povezanost potrebnu za rad LoRaWAN infrastrukture i SDR alata.

7.2.3.2 ChirpStack LoRaWAN poslužitelj

ChirpStack programski paket koristi se kao mrežni i aplikacijski poslužitelj LoRaWAN mreže. Sustav obuhvaća Gateway Bridge, Network Server i Application Server te omogućuje upravljanje krajnjim uređajima, provedbu OTAA postupka, generiranje i upravljanje sesijskim ključevima, kao i evidentiranje uplink i downlink poruka. ChirpStack služi kao referentna točka za praćenje ponašanja mreže tijekom normalnog rada i tijekom sigurnosnih testiranja.

7.2.3.3 Gateway softver za WM1302

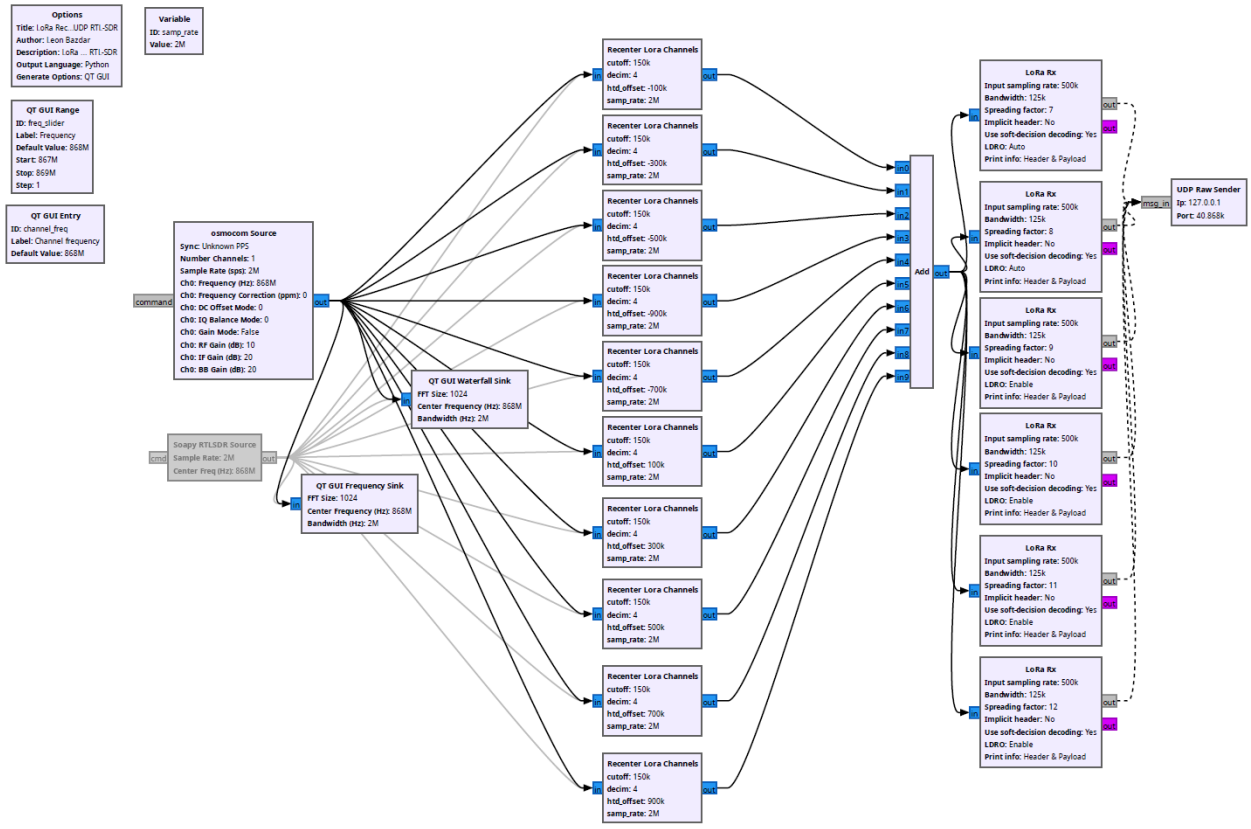
Za upravljanje WM1302 LoRa koncentratorom koristi se odgovarajući gateway softver kompatibilan s ChirpStack okruženjem. Softver omogućuje prijem LoRa paketa na više kanala i njihovo prosljeđivanje mrežnom poslužitelju putem UDP ili MQTT sučelja.

7.2.3.4 GNU Radio

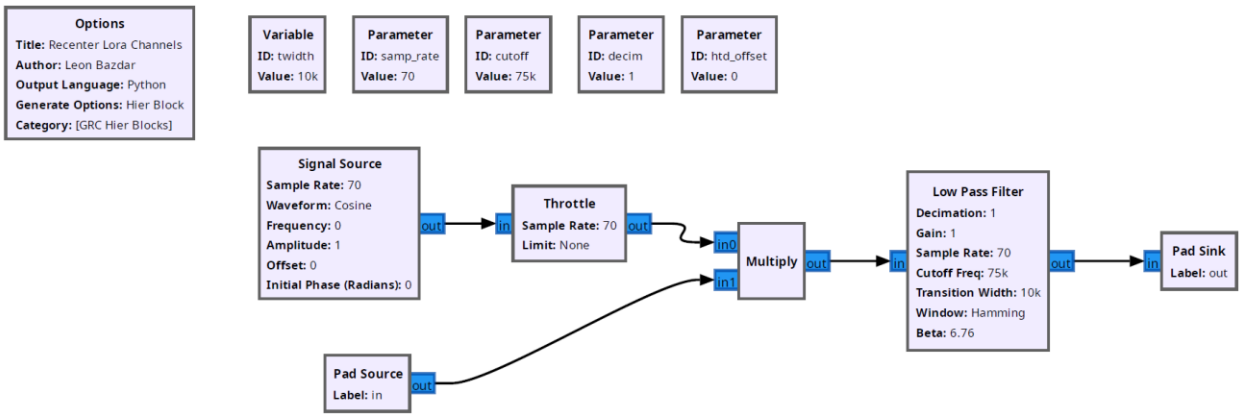
GNU Radio koristi se kao osnovno okruženje za digitalnu obradu signala primljenih putem RTL-SDR prijamnika. Sustav omogućuje konfiguraciju prijamnih parametara, filtriranje signala i daljnju obradu primljenih LoRa okvira na fizičkom sloju.

7.2.3.4.1 Gr-lora_sdr i LoRaCraft moduli

Open-source moduli gr-lora_sdr i LoRaCraft koriste se unutar GNU Radio okruženja za demodulaciju i dekodiranje LoRa signala. Moduli omogućuju izdvajanje LoRaWAN paketa iz sirovih IQ uzoraka te njihovo prosljeđivanje u digitalnom obliku prema vanjskim aplikacijama putem UDP sučelja. Za pasivni nadzor i dekodiranje LoRaWAN komunikacije korišteni su prilagođeni GNU Radio flowgrafovi temeljeni na open-source modulima gr-lora_sdr i LoRaCraft. Flowgrafovi omogućuju prijem sirovih IQ uzoraka s RTL-SDR prijamnika, njihovu obradu na fizičkom sloju te izdvajanje LoRaWAN paketa u digitalnom obliku.



Slika 15- GNU Radio postav za prijem LoRaWAN paketa RTL-SDR v4 prijemnikom



Slika 16-Blok za centriranje primljenog signala u osnovni pojas

7.2.3.5 Vlastiti alati za dekodiranje i analizu

Razvijene su vlastite Python skripte za prijem LoRaWAN paketa putem UDP sučelja iz GNU Radio okruženja. Alati omogućuju parsiranje LoRaWAN zaglavlja i dekodiranje aplikacijskog payload-a korištenjem poznatih sesijskih ključeva. Na taj način omogućena je usporedba podataka prikupljenih pasivnim nadzorom s podacima evidentiranim na LoRaWAN mrežnom poslužitelju.

7.2.3.6 Razvojni alati za LA66 i LoStik

Za razvoj i prilagodbu firmwarea LA66 uređaja koristi se službeni razvojni SDK za ASR6601 platformu. LoStik uređaj upravlja se putem serijskog sučelja korištenjem AT naredbi, uz mogućnost automatizacije putem skripti na računalu domaćinu.

7.3 *Funkcionalne značajke sustava*

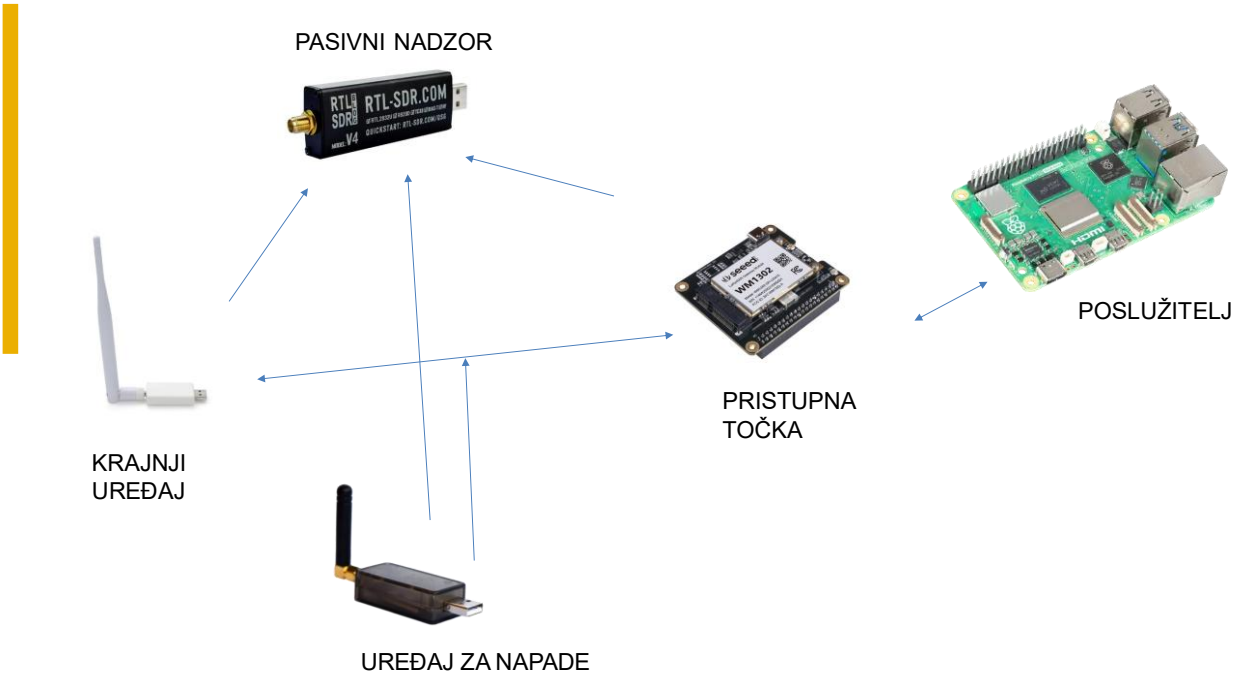
Razvijeni sustav pruža skup funkcionalnosti namijenjenih analizi sigurnosti LoRaWAN mreža u kontroliranom laboratorijskom okruženju. Funkcionalnosti su raspoređene tako da omogućuju istovremeni rad legitimne LoRaWAN infrastrukture, pasivni nadzor radio-komunikacije i provođenje aktivnih sigurnosnih eksperimenata.

Sustav omogućuje:

- uspostavu i rad funkcionalne LoRaWAN mreže temeljene na ChirpStack poslužitelju, LoRaWAN gatewayu i krajnjem uređaju,
- provedbu OTAA postupka i razmjenu uplink i downlink poruka između krajnjeg uređaja i mrežnog poslužitelja,
- pasivni nadzor LoRaWAN komunikacije na fizičkom sloju pomoću SDR prijamnika bez sudjelovanja u mreži,
- prijem, demodulaciju i dekodiranje LoRa signala različitih parametara korištenjem GNU Radio okruženja,
- izdvajanje i obradu LoRaWAN paketa prikupljenih pasivnim nadzorom,
- dekodiranje aplikacijskog payload-a LoRaWAN poruka uz poznate sesijske ključeve,
- simulaciju odabranih sigurnosnih scenarija, uključujući ometanje postupka pridruživanja mreži i potvrđenih uplink poruka,
- provođenje aktivnih radio-frekvencijskih smetnji korištenjem LoStik USB uređaja i modificiranog LA66 uređaja,
- prikupljanje i usporedbu podataka dobivenih pasivnim nadzorom i podataka evidentiranih na LoRaWAN mrežnom poslužitelju,
- analizu ponašanja LoRaWAN mreže tijekom normalnog rada i tijekom sigurnosnih eksperimenata.

Navedene funkcionalnosti omogućuju cjelovitu analizu sigurnosnih ograničenja LoRaWAN sustava s aspekta mrežnog, aplikacijskog i radio-frekvencijskog sloja.

7.4 *Provođenje aktivnih sigurnosnih eksperimenata pomoću LoStik uređaja*



Slika 17 Pregledni prikaz spajanja uređaja

LoStik USB uređaj koristi se za provođenje aktivnih radio-frekvencijskih smetnji pomoću Python skripti koje se pokreću iz terminala. Smetnje se ostvaruju slanjem posebno oblikovanih LoRa okvira s maksimalnom duljinom payload-a, često ispunjenih konstantnom vrijednošću (npr. 0xFF), čime se namjerno zauzima radio-kanal tijekom kritičnih prijemnih prozora RX1 i RX2.

Skripte upravljaju LoStik uređajem putem serijskog sučelja korištenjem AT naredbi te precizno tempiraju trenutak slanja smetajućeg okvira u odnosu na detektirani uplink prijenos krajnjeg uređaja. Nakon slanja uplink poruke, LoRaWAN krajnji uređaj otvara dva vremenski definirana prijemna prozora (RX1 i RX2) u kojima očekuje downlink odgovor mreže. Slanjem dugotrajnog LoRa okvira u tom vremenskom intervalu dolazi do preklapanja signala na fizičkom sloju, čime se onemogućava ispravan prijem legitimne downlink poruke.

Korištenjem payload-a s velikim brojem ponavljajućih vrijednosti (npr. 0xFF) postiže se maksimalno trajanje prijenosa za odabrani spreading faktor i širinu pojasa. Time se povećava vjerojatnost da će prijemni prozor krajnjeg uređaja biti u potpunosti prekriven smetajućim signalom. Posljedica toga je neuspješan prijem join-accept poruke tijekom postupka pridruživanja mreži ili neuspješan prijem potvrde (ACK) za potvrđene uplink poruke.

Ovakav oblik ometanja predstavlja napad uskraćivanja usluge (Denial of Service - DoS) na fizičkom sloju komunikacije. Napad ne zahtijeva poznavanje kriptografskih ključeva niti sudjelovanje u LoRaWAN mreži, već se temelji isključivo na poznavanju vremenskog ponašanja protokola i karakteristika LoRa modulacije. Zbog dugog trajanja prijenosa pri većim spreading faktorima, čak i relativno jednostavan napadački uređaj može učinkovito degradirati dostupnost komunikacijskog kanala.

U kontekstu LoRaWAN sustava, ovakvi napadi mogu dovesti do povećane potrošnje energije krajnjih uređaja zbog ponovljenih pokušaja prijenosa, gubitka poruka te nemogućnosti uspješnog pridruživanja mreži. To je posebno kritično u aplikacijama s ograničenim energetskim resursima i zahtjevima za visoku pouzdanost komunikacije.

7.4.1 Interferencija potvrđenih uplink poruka

Kod ovog tipa napada cilj je onemogućiti uspješnu razmjenu potvrđenih uplink poruka između krajnjeg uređaja i mreže. Napadač generira vremenski usklađene radio-frekvencijske smetnje tijekom RX1 i RX2 prijemnih prozora krajnjeg uređaja. Time se sprječava ispravan prijem potvrde o primitku poruke (ACK) koju šalje mrežni server. Budući da uređaj ne prima potvrdu, smatra da prijenos nije bio uspješan te ponavlja slanje iste poruke, što povećava potrošnju energije i opterećenje mreže. Dugotrajna primjena ovog napada može dovesti do ubrzanog pražnjenja baterije i smanjenja pouzdanosti komunikacije.

7.4.2 Interferencija postupka pridruživanja mreži

Ovaj napad usmjeren je na ometanje postupka pridruživanja krajnjeg uređaja LoRaWAN mreži pomoću OTAA metode. Napadač stvara radio-frekvencijske smetnje tijekom slanja Join Request poruka ili tijekom prijema Join Accept odgovora. Time se onemogućuje uspješna razmjena ključnih poruka potrebnih za autentifikaciju uređaja. Posljedica je neuspješno pridruživanje mreži, zbog čega uređaj ostaje izvan komunikacije i ne može započeti normalan rad. Uređaj u tom slučaju kontinuirano pokušava ponoviti postupak pridruživanja, što dodatno povećava potrošnju energije i produžuje vrijeme nedostupnosti sustava.

Literatura

Hessel, F. P. LoRaWAN Security Analysis: An Experimental Evaluation of Attacks. Master Thesis, Technische Universität Darmstadt, 2019.
URL: https://tuprints.ulb.tu-darmstadt.de/17550/
Datum pristupa: 19.12.2025.

Dudek, S. Low Powered but High Risk: Evaluating Possible Attacks on LoRaWAN Devices. Trend Micro Research, 2021.
URL: https://www.trendmicro.com/en_gb/research/21/a/Low-Powered-but-High-Risk-Evaluating-Possible-Attacks-on-LoRaWAN-Devices.html
Datum pristupa: 19.12.2025.

Trend Micro Research. The Current State of LoRaWAN Security. Technical brief,
URL:
https://documents.trendmicro.com/assets/pdf/The%20Current%20State%20of%20LoRaWAN%20Security.pdf
Datum pristupa: 19.1.2026.

Seeed Studio. WM1302 Pi HAT - Wiki. URL: https://wiki.seeedstudio.com/WM1302_Pi_HAT
Datum pristupa: 19.12.2025.

ChirpStack. chirpstack-concentratord: Hardware support. URL: https://www.chirpstack.io/docs/chirpstack-concentratord/hardware-support.html
Datum pristupa: 19.12.2025.

Y-Security (y-security.de). Security of LoRaWAN. URL: https://www.y-security.de/news-en/security-of-lorawan/
Datum pristupa: 19.12.2025.

Dragino. Compile and Upload Code to ASR6601 Platform (LA66 LoRaWAN Module). URL:
https://wiki.dragino.com/xwiki/bin/view/Main/User%20Manual%20for%20LoRaWAN%20End%20Nodes/LA66%20LoRaWAN%20Module/Compile%20and%20Upload%20Code%20to%20ASR6601%20Platform/
Datum pristupa: 7.12.2025.

Dragino (GitHub). LA66 repository. URL: https://github.com/dragino/LA66
Datum pristupa: 7.12.2025.

Ronoth (GitHub). LoStik repository. URL: https://github.com/ronoth/LoStik
Datum pristupa: 19.11.2025.

Tapparelj (GitHub). gr-lora_sdr repository. URL: https://github.com/tapparelj/gr-lora_sdr/tree/master
Datum pristupa: 19.11.2025.

PentHertz (GitHub). LoRa_Craft repository. URL: https://github.com/PentHertz/LoRa_Craft
Datum pristupa: 11.11.2025.

GNU Radio. GNU Radio Wiki. URL: https://wiki.gnuradio.org/index.php
Datum pristupa: 11.11.2025.