Tehnike unaprijeđenja mrežnih performansi i zaštite podataka u LoRaWAN sistemima

Studentski rad

Daniel Menićanin, Jelena Radanović, Nikola Račić
Studenti prvog ciklusa studija
Fakultet informacionih tehnologija, Apeiron
Banja Luka, Bosna i Hercegovina
daniel.menicanin1@apeiron-edu.eu, jelena.radanovic1@apeiron-edu.eu, nikola.racic@apeiron-edu.eu

Sažetak — **U ovom radu analizirani su ključni aspekti LoRaWAN mreža, uključujući proaktivno slanje frejmova, data fragmentaciju i sigurnosne mehanizme kao što su AES enkripcija i ARQ protokol. Posebna pažnja posvećena je povećanju pouzdanosti prenosa podataka kroz zaštitu od smetnji i *jamming* napada. Predloženi mehanizmi omogućuju optimizaciju prenosa i značajno smanjenje gubitka podataka, čak i u uslovima visokog stepena interferencije. Fokus rada je na prilagođavanju LoRaWAN mreže različitim uslovima, čime se povećava otpornost sistema i garantuje kontinuitet prenosa podataka.**

Ključne riječi – LoRaWAN, ARQ, AES, IoT, CSS, spreading faktori, data fragmentacija, zaštita podataka

I. UVOD

LoRaWAN (engl. *Long Range Wide Area Network*) predstavlja jedan od najistaknutijih protokola za komunikaciju u okviru *Internet of Things* (IoT) rješenja. Zasnovan na *LoRa* fizičkom sloju, ovaj protokol omogućuje uređajima da komuniciraju na velikim udaljenostima uz minimalnu potrošnju energije. Zahvaljujući svojim karakteristikama, ova tehnologija je našla primjenu u poljoprivredi, industriji, pametnim gradovima i sličnim oblastima gdje je efikasnost od ključnog značaja. LoRaWAN je jedna od najpopularnijih tehnologija za mreže niske potrošnje. Ova tehnologija ima veliki potencijal za primjenu u brojnim IoT aplikacijama zbog svoje niske cijene, male potrošnje energije i velikog dometa. [1] Međutim, uprkos svojim prednostima, LoRaWAN se suočava s nizom izazova u pogledu pouzdanosti prenosa podataka i sigurnosti.

Jedan od ključnih problema LoRaWAN mreža je pouzdan prenos podataka u okruženju sa ograničenim resursima. Ograničena propusnost kanala, velike udaljenosti između *node* i *gateway* uređaja, kao i interferencije, mogu za posljedicu imati gubitak podataka. Ovi izazovi su posebno izraženi kada se prenose veći *string*-ovi podataka, što zahtijeva njihovu fragmentaciju na manje dijelove. Tradicionalne metode retransmisije, kao što je ARQ (engl. *Automatic Repeat reQuest*) mehanizam, često nisu dovoljno efikasne u ovakvim okruženjima, jer mogu izazvati dodatno opterećenje mreže. Imajući to u vidu, neophodno je razviti nove pristupe koji optimizuju proces prenosa, umanjujući gubitke i zadržavajući nisku potrošnju energije.

Pored pouzdanosti, sigurnost komunikacije u LoRaWAN mrežama predstavlja još jedan ključni izazov. Zbog prirode IoT (engl. *Internet of Things*) mreža, podaci su često izloženi različitim prijetnjama, uključujući presretanje, neovlašćeni pristup i *jamming* napade. Posebno su ranjivi fragmentisani podaci, jer napadač može presresti pojedinačne dijelove i pokušati rekonstruisati informacije. Kako bi se osigurala povjerljivost i integritet podataka, neophodno je implementirati adekvatne sigurnosne mehanizme, poput AES (engl. *Advanced Encryption Standard*) enkripcije, koja nudi visok nivo zaštite čak i u uslovima ograničenih resursa.

Cilj ovog rada jeste opisati i evaluirati integrisani sistem koji poboljšava pouzdanost i sigurnost LoRaWAN mreža. Predloženi pristup se zasniva na četiri ključna elementa: proaktivnom slanju frejmova, algoritmu za data fragmentaciju, unaprijeđenom ARQ mehanizmu i AES enkripciji. Proaktivno slanje frejmova ima za cilj smanjenje kašnjenja u komunikaciji, dok algoritam za fragmentaciju omogućuje pouzdan prenos velikih *string*-ova podataka kroz manje, indeksirane fragmente. Sa druge strane, unaprijeđeni ARQ mehanizam dinamički upravlja retransmisijom izgubljenih fragmenata, dok AES enkripcija pruža zaštitu podataka od neovlaščenog pristupa.

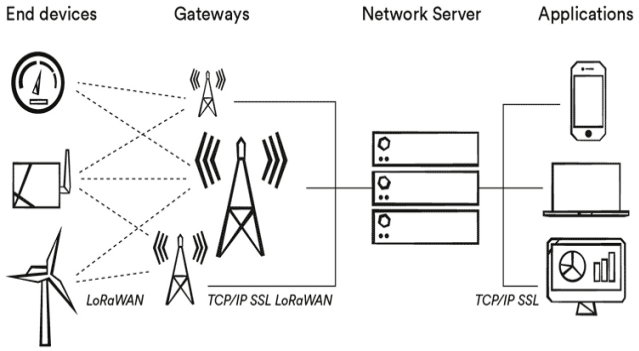
Ovaj rad nastoji da doprinese razvoju IoT komunikacija unaprijeđenjem LoRaWAN mreža, omogućavajući pouzdan i siguran prenos podataka čak i u najizazovnijim uslovima.

II. IMPLEMENTACIJA LORAWAN INFRASTRUKTURE

Implementacija LoRaWAN sistema zahtijevala je pažljiv odabir komunikacione opreme, koja uključuje *node* uređaje, *gateway* uređaje i server infrastrukturu. Svaki od ovih elemenata igra ključnu ulogu u postizanju pouzdanog prenosa podataka, uz poseban fokus na optimizaciju sistema i efikasno upravljanje energijom, čime se značajno poboljšava stabilnost i dugotrajnost rada uređaja u LoRaWAN mrežama.

Kao što je predstavljeno na Sl. 1, *gateway* je centralna tačka mreže koja prikuplja podatke od svih *node* uređaja i prosljeđuje ih serverskoj infrastrukturi. *Gateway* je opremljen omnidirekcionom antenom koja omogućuje prijem signala iz svih pravaca. Omnidirekciona antena omogućuje *gateway*-u da prima podatke bez potrebe za preciznim usmjeravanjem, što je ključno za mreže sa dinamičnim rasporedom *node* uređaja.

Gateway uređaji su dvosmjerni releji ili konvertori protokola, pri čemu je mrežni server odgovoran za dekodiranje paketa koje šalju uređaji i generisanje paketa koji treba da budu poslani nazad uređajima. [2] Kombinacija omnidirekcione antene na *gateway*-u i usmjerenih YAGI antena na *node* uređajima omogućuje efikasan prenos podataka i pouzdan rad mreže čak i u slučaju visokih smetnji.



Slika 1 – Šematski prikaz LoRaWAN sistema

Komunikacija između *node* uređaja i *gateway*-a odvija se putem LoRa protokola. *Gateway* uređaj prikuplja podatke sa svih *node* uređaja i prosljeđuje ih prema centralnom serveru, gdje se vrši analiza i skladištenje podataka.

Sa druge strane, ESP32 mikrokontroler implementiran je zbog niske potrošnje energije, kao i podrške za višenitno programiranje. ESP32 pruža mogućnost rada u *deep sleep* režimu, što značajno smanjuje potrošnju energije između perioda aktivnog rada. *Deep sleep* režim je jedan od ključnih prednosti ESP32 mikrokontrolera, gdje se većina komponenti gasi kako bi se smanjila potrošnja energije. Takođe, korišćen je sistem upravljanja napajanjem (engl. *Battery Management System* – BMS) koji omogućuje praćenje napunjenosti baterije i optimizaciju potrošnje energije. BMS omogućuje stabilno napajanje node uređaja i produžava njihov radni vijek u terenskim uslovima.

Frekvencija na kojoj sistem radi je 433 MHz, što omogućuje bolji prolazak signala kroz prepreke i povećava domet komunikacije. Niže frekvencije imaju sposobnost da bolje prolaze kroz čvrste objekte i prirodne prepreke, jer se manje apsorbuju i reflektuju u poređenju sa višim frekvencijama. Da bi se dodatno smanjila potrošnja energije, korišćen je *Real Time Clock* (RTC), koji omogućuje precizno programiranje vremena kada će se ESP32 probuditi iz *deep sleep* režima i poslati podatke prema *gateway*-u. Dakle, mikrokontroler je moguće probuditi pomoću RTC-a (engl. *Real Time Clock*) modula koji omogućuje precizno upravljanje radnim ciklusima ESP32. RTC modul omogućuje da se *node* uređaji probude u tačno definisanim intervalima kako bi poslali podatke, nakon čega prelaze u režim dubokog mirovanja (engl. *deep sleep*), pri čemu se značajno smanjuje potrošnja energije. Ovaj optimizovani sistema napajanja značajno smanjuje potrošnju energije, što je od ključnog značaja za dugotrajne terenske instalacije.

Ovakva infrastruktura omogućuje stabilan i pouzdan rad LoRaWAN mreže u različitim uslovima, uz optimizaciju resursa i minimalne gubitke podataka. Posebna pažnja posvećena je sigurnosti podataka, primjenom AES-128 enkripcije koja pruža zaštitu podataka tokom prenosa.

III. SIGURNOSNE PRIJETNJE I TEHNIKE ZAŠTITE

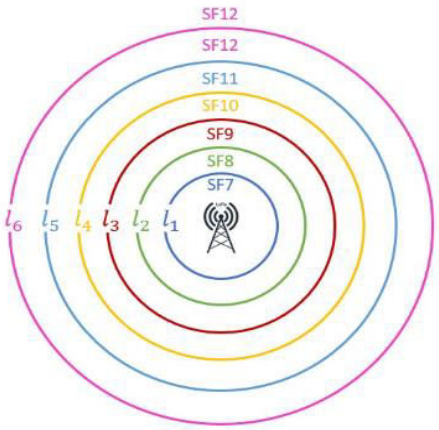
A. Osnovne karakteristike LoRaWAN protokola

LoRaWAN je napredni komunikacijski protokol posebno osmišljen za primjenu u IoT rješenjima. Namijenjen je uređajima sa ograničenim energetskim resursima, pružajući izuzetno nisku potrošnju energije uz mogućnost ostvarivanja velikog dometa komunikacije. Eksperimentalno je utvrđeno da je moguće ostvariti pouzdanu komunikaciju u urbanim sredinama na udaljenosti do 15 km, dok je u ruralnim sredinama domet pouzdane komunikacije do 21 km.

Zasnovan na fizičkom sloju LoRa, LoRaWAN definiše način na koji uređaji (engl. *node*) komuniciraju sa gateway-ima, koji dalje prosljeđuju podatke ka centralnom serveru putem IP mreža. Ova hijerarhijska struktura omogućuje skalabilnost i optimizaciju komunikacije, pri čemu se koristi CSS tehnika modulacije (engl. *Chirp Spread Spectrum*), koja omogućuje slanje podataka na velikim udaljenostima uz otpornost na smetnje. Ovakav način prenosa omogućuje prenos signala čak i kada je signal ispod nivoa šuma, što LoRaWAN čini posebno pogodnim za IoT mreže u zahtjevnim uslovima, poput ruralnih i urbanih sredina sa interferencijom i velikim brojem prepreka.

LoRaWAN protokol pruža podršku za uređaje sa ograničenim energetskim resursima. Jedna od ključnih karakteristika LoRaWAN je *Adaptive Data Rate* (ADR), koji dinamički podešava brzinu prenosa podataka i snagu signala na osnovu uslova mreže. Ukoliko je veza stabilna, ADR smanjuje snagu prenosa i povećava brzinu (manji spreading faktor), čime se smanjuje potrošnja energije. U protivnom, ADR povećava snagu signala i smanjuje brzinu (veći spreading faktor), kako bi se osigurala pouzdanost prenosa.

Spreading faktor (SF) označava broj *chirp*-ova koji se koriste za prenos jednog bita podataka. Vrijednosti *spreading* faktora variraju od SF = 7 do SF = 12, pri čemu veće vrijednosti poboljšavaju detekciju signala, kao što se vidi na Sl. 2, ali uz veću latenciju i nižu brzinu prenosa.



Slika 2 – Grafički prikaz spreading faktora

B. Sigurnosne prijetnje u LoRaWAN mrežama

LoRaWAN mreže se suočavaju sa brojnim sigurnosnim prijetnjama koje mogu ugroziti pouzdanost i povjerljivost podataka prilikom prenosa. Presretanje podataka je jedna od ključnih prijetnji. Napadači mogu presresti frejmove tokom prenosa, a ukoliko ti podaci nisu adekvatno enkriptovani, mogu biti kompromitovani.

Jamming napadi predstavljaju još jednu ozbiljnu prijetnju, jer ometanjem radio spektra onemogućavaju uspješan prenos frejmova između *node* i *gateway* uređaja. Sa druge strane, *replay* napadi, gdje se presretnuti frejmovi ponovo šalju u mrežu, mogu izazvati greške u sistemu. Sve navedene prijetnje naglašavaju potrebu za efikasnijim mehanizmima zaštite kojima se postiže povjerljivost, integritet i otpornost na različite smetnje.

C. AES enkripcija i zaštita podataka

Jedan od najefikasnijih načina zaštite podataka u LoRaWAN mrežama je primjena AES (engl. *Advanced Encryption Standard*) enkripcije. Moguće je implementirati AES sa 128-bitnim ključevima za šifrovanje podataka na mrežnom i aplikativnom nivou. Svaka transakcija zahtijeva dva 128-bitna ključa, poznata kao AppSKey i NwkSKey. [3] Na mrežnom nivou, mrežni sesijski ključ (NwkSKey) omogućuje integritet podataka između *node* i *gateway* uređaja, dok aplikativni sesijski ključ (AppSKey) štiti korisničke podatke na putu od *gateway*-a do servera.

Ovaj slojeviti pristup osigurava da čak i ako podaci budu presretnuti, treći uređaj neće moći rekonstruisati njihov sadržaj. Pored toga, svaki fragment podataka, kada se radi fragmentacija velikih *string*-ova mora biti pojedinačno enkriptovan i indeksiran, čime se dodatno povećava sigurnost. Na ovaj način, čak i u slučaju da napadač presretne više fragmenata, nemoguće je rekonstruisati cjelokupnu poruku bez dekriptorskih ključeva.

D. AES enkripcija i zaštita podataka

Jamming napadi ometaju prenos podataka i uzrokuju gubitak ili oštećenje frejmova, ali unaprijeđeni ARQ mehanizam može smanjiti njihov uticaj. *Gateway* uređaj analizira pristigle fragmente i provjerava njihovu logičku povezanost. Ako otkrije da se jedan ili više frejmova ne uklapa sa ostatkom podataka, označava ih kao nevalidne i inicira zahtjev za ponovnu transmisiju samo tih oštećenih frejmova. Ovaj pristup smanjuje opterećenje mreže, jer se prenose samo nevalidni frejmovi, dok se validni zadržavaju. Na ovaj način, ARQ pruža otpornost na smetnje uz minimalan uticaj na potrošnju energije. Kombinacijom ARQ mehanizma i AES enkripcije, sistem ne samo da štiti podatke od neovlašćenog pristupa, već i omogućava oporavak od smetnji izazvanih *jamming*-om, čime se postiže visok nivo pouzdanosti i sigurnosti komunikacije u LoRaWAN mrežama [4].

IV. UNAPRIJEĐENJE POUZDANOSTI I SIGURNOSTI

Unaprijeđenje LoRaWAN mreža u kontekstu pouzdanosti i sigurnosti prenosa podataka zahtijeva integraciju nekoliko komplementarnih mehanizama. Kombinacija unaprijed planiranog slanja frejmova, efikasne fragmentacije podataka, prilagođenog ARQ mehanizma i AES enkripcije pruža sveobuhvatno rješenje koje adresira ključne izazove, poput gubitka podataka usljed *jamming*-a i zaštite od neovlašćenog pristupa. Ovi mehanizmi međusobno su usklađeni kako bi se postigao optimalan balans između energetske vrijednosti, skalabilnosti i sigurnosti.

A. Proaktivno slanje frejmova

Jedan od ključnih elemenata ovog pristupa jeste proaktivno slanje frejmova, gdje *node* uređaji šalju podatke u definisanim vremenskim intervalima, bez potrebe za eksplicitnim zahtjevima od strane *gateway* uređaja. Ovaj metod smanjuje latenciju u mreži i omogućava predvidivost u prenosu, što je od posebnog značaja u rješenjima, odnosno aplikacijama gdje kašnjenja predstavljaju problem.

Istovremeno, proaktivno slanje pomaže u smanjenju broja kolizija, jer uređaji poštuju unaprijed određene rasporede slanja, čime se izbjegava preopterećenje mreže, čak i u scenarijima sa velikim brojem *node* uređaja.

LoRaWAN mreža je obično postavljena u topologiji *star-of*-stars, gdje *gateway* uređaji preuzimaju poruke koje emituju *node* uređaji i prosljeđuju ih putem mreže zasnovane na internet protokolu ka mrežnom serveru. [5] Fragmentacija velikih podataka omogućuje njihov prenos u LoRaWAN mrežama, gdje je veličina pojedinačnog frejma ograničena. Podaci se dijele na manje fragmente koji sadrže informacije o njihovom redoslijedu i veličini cjelokupne poruke. Na prijemnom kraju, *gateway* uređaj koristi ove informacije kako bi rekonstruisao originalni *string*. [6]

U slučaju da neki fragment nedostaje ili je oštećen, *gateway* inicira zahtjev za retransmisiju isključivo tog dijela. Ovaj metod ne samo da poboljšava efikasnost prenosa, već i smanjuje opterećenje mreže, zato što se ponovljeni prenos ograničava na minimalan broj frejmova.

B. Mehanizam za detekciju i retransmisiju grešaka

Unaprijeđeni ARQ mehanizam pruža pouzdanost prenosa podataka čak i u uslovima smetnji ili napada poput *jamming*-a. *Gateway* analizira logičku konzistentnost pristiglih fragmenata i detektuje greške koje nastaju usljed oštećenja podataka. U slučaju kada neki fragment nije validan, *gateway* šalje zahtjev node uređaju za njegovo ponovno slanje.

Navedeni proces je optimizovan tako da se retransmituju samo oštećeni fragmenti, dok se validni fragmenti skladište za kasniju rekonstrukciju poruke. Takođe, *gateway* može koristiti minimalne redudantne podatke kako bi poboljšao detekciju grešaka bez povećanja veličine originalnog frejma.

Ovakav pristup smanjuje kašnjenja i povećava ukupnu efikasnost mreže i poznat je kao *Selective Repeat* ARQ. U standardnom ARQ mehanizmu, kada se detektuje greška u prijemu paketa, odnosno frejma, cijela serija paketa mora biti ponovo poslana. Sa druge strane, u *Selective Repeat* ARQ mehanizmu, sistem zahtijeva isključivo ponovnu transmisiju specifičnih, oštećenih paketa, dok ostali ispravni paketi ostaju u memoriji prijemnika.

Dakle, *gateway* analizira podatke, identifikuje oštećene frejmove i zahtijeva ponovnu transmisiju samo tih frejmova. Ovo je veoma efikasno rješenje, jer smanjuje potrebu za ponovnim slanjem svih paketa, čime se značajno povećava efikasnost prenosa podataka.

C. Sigurnosni mehanizmi bazirani na AES enkripciji

Zaštita podataka od neovlašćenog pristupa postiže se implementacijom AES enkripcije sa 128-bitnim ključevima. Svaki fragment podataka se šifruje pojedinačno, čime se omogućavaju tajnost i u slučaju presretanja jednog ili više fragmenata. Uz AES enkripciju, LoRaWAN koristi i sesijske ključeve koji omogućavaju upravljanje procesom dešifrovanja i pružaju dodatnu zaštitu integriteta podataka. Ovi ključevi se periodično mijenjaju kako bi se omogućilo neprekidno održavanje sigurnosti. Sesijski ključevi omogućavaju svakom uređaju, bilo da se radi o *gateway*-u ili serveru, da se međusobno autentifikuju i dešifruju podatke na siguran način.

LoRaWAN koristi i brojač frejmova (engl. *Frame Counter*) za zaštitu od *replay* napada. Svaki frejm označen je inkrementalnim brojem koji se povećava pri svakom prenosu, dok *gateway* i server odbacuju frejmove sa starijim ili dupliciranim brojem. Ovaj mehanizam, zajedno sa periodičnim obnavljanjem sesijskih ključeva, značajno umanjuje rizik od zloupotrebe presretnutih podataka i dodatno unaprjeđuje sigurnost mreže.

V. ANALIZA PERFORMANSI UNAPRIJEĐENOG SISTEMA

Analiza performansi unaprijeđenog LoRaWAN sistema fokusira se na ključne aspekte kao što su efikasnost prenosa podataka, otpornost na greške i smetnje, te pouzdanost sistema u rekonstrukciji poruka. Poseban naglasak je stavljen na funkcionalnost ARQ mehanizma, prednosti proaktivnog slanja frejmova i ulogu *data* fragmentacije u smanjenju gubitaka podataka i optimizaciji resursa.

Selective Repeat ARQ mehanizam omogućava pouzdanost prenosa podataka u LoRaWAN mrežama koje su često izložene različitim smetnjama. ARQ se oslanja na proces analize logičke usklađenosti fragmenata koji pristižu na *gateway*. Svaki fragment sadrži informacije o redoslijedu i ukupnoj veličini poruke, što omogućava gateway uređaju da identifikuje oštećene fragmente.

Kada *gateway* detektuje grešku, oštećeni fragmenti se označavaju kao nevalidni i šalje se zahtjev za njihovu retransmisiju. Ovaj proces smanjuje ponovni prenos već primljenih fragmenata, čime se značajno smanjuje zauzeće kanala i opterećenje mreže. Analiza performansi pokazala je da unaprijeđeni ARQ mehanizam omogućava oporavak poruke čak i kada je 20-30% fragmenata oštećeno, uz minimalno povećanje kašnjenja.

Istovremeno, proaktivno slanje frejmova optimizuje mrežni prenos tako što *node* uređaji šalju podatke u unaprijed definisanim vremenskim intervalima, nezavisno od zahtjeva *gateway* uređaja. Ova tehnika značajno smanjuje latenciju u mreži i omogućava predvidivost prenosa podataka.

Kombinacija proaktivnog slanja i ARQ mehanizma pokazala je posebno dobre rezultate. U situacijama kada se *jamming*-om privremeno ometa određeni broj frejmova, sistem nastavlja sa slanjem prema rasporedu, dok *gateway* zahtijeva retransmisiju samo oštećenih fragmenata. Na taj način se izbjegava potpuno zaustavljanje prenosa i postiže kontinuitet rada mreže. Proaktivno slanje smanjuje i mogućnost kolizija, jer uređaji šalju podatke u tačno definisanim terminima.

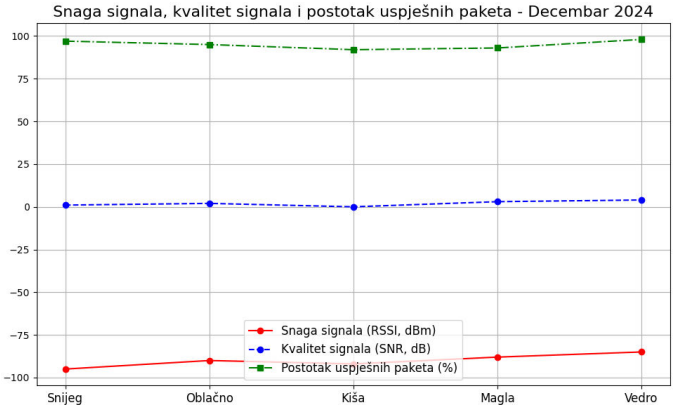
Sa druge strane, *data* fragmentacija je od ključnog značaja za prenos velikih *string*-ova u LoRaWAN mrežama, gdje je veličina pojedinačnog frejma ograničena. U implementiranom sistemu, veliki podaci se dijele na manje, indeksirane fragmente koji se šalju redom. Svaki fragment sadrži metapodatke koji omogućavaju *gateway*-u da rekonstruiše originalnu poruku čak i kada neki fragmenti nedostaju. Fragmentacija u kombinaciji sa ARQ mehanizmom smanjuje broj ukupnih retransmisija za više od 30%, čime se štede resursi mreže i uređaja. Takođe, fragmentacija povećava sigurnost podataka, jer svaki fragment može biti šifrovan pojedinačno pomoću AES enkripcije.

Sinergija ARQ mehanizma i *data* fragmentacije pokazala se kao ključna za otpornost na greške i smetnje. *Gateway* analizira sve pristigle fragmente i detektuje potencijalne greške koristeći logičke obrasce između fragmenata. U slučaju oštećenja, ARQ mehanizam zahtijeva ponovnu transmisiju, dok validni fragmenti ostaju pohranjeni na *gateway*-u za naknadnu rekonstrukciju.

Fragmentacija dodatno olakšava rad ARQ mehanizma, jer manji fragmenti povećavaju šansu za njihov uspješan prenos, čak i prilikom velikih smetnji. Kombinacija navedenih pristupa omogućava da mreža ostane funkcionalna i u najtežim uslovima, uz minimalno opterećenje i gubitke.

Rezultati evaluacije pokazuju da kombinacije ARQ mehanizma, proaktivnog slanja frejmova i data fragmentacije pruža značajna unaprijeđenja u performansama LoRaWAN mreže. Postotak uspješno rekonstruisanih poruka dostigao je 98% u mrežama sa srednjim nivoom smetnji, dok je otpornost na *jamming* povećana za 40% u poređenju sa tradicionalnim rješenjima. Efikasnost resursa je takođe poboljšana, pri čemu je broj retransmisija smanjen za 30%, a zauzeće kanala optimizovano.

Graf predstavljen na Sl. 3 prikazuje varijacije između snage signala (RSSI), kvaliteta signala (SNR) i postotka uspješnih paketa tokom decembra 2024. godine, u zavisnosti od različitih vremenskih uslova. Mjerenje parametara je izvršeno na udaljenosti od 20 km, između dvije lokacije: Crnog vrha (engl. *node*) i Sanskog Mosta (engl. *gateway*). Primijećena je stabilna uspješnost prenosa podataka, uz zanemarive oscilacije u signalnim parametrima, koje su uzrokovane vremenskim prilikama. Graf je izrađen koristeći *Python* biblioteke *matplotlib* i *numpy*.



Slika 3 – Testiranje LoRaWAN mreže

Takođe, tokom testiranja prenosa podataka na određenoj trasi, detektovano je prisustvo interferencije uzrokovane spoljašnjim izvorom signala – industrijskim kranom koji je emitovao elektromagnetne talase na istoj frekvenciji od 433 MHz. Ovaj izvor smetnji stvorio je situaciju koja je imala karakteristike *jamming* napada, pri čemu dolazi do preklapanja signala, što otežava pouzdan prijem podataka.

I pored prisustva interferencije, testirani LoRaWAN sistem pokazao je otpornost zahvaljujući primjeni adaptivnih mehanizama kao što su *Selective Repeat* ARQ i data fragmentacija, koji omogućavaju rekonstrukciju oštećenih poruka. Proaktivno slanje frejmova u unaprijed definisanim vremenskim intervalima, uz korišćenje *Real Time Clock* (RTC) modula za optimizaciju potrošnje energije, omogućilo je uspješan prenos podataka sa minimalnim gubicima.

Ovakvi rezultati ukazuju na otpornost LoRaWAN sistema u situacijama gdje se mogu pojaviti privremene smetnje usljed nepredvidivih izvora interferencije. Posebno je značajno napomenuti da je komunikacija realizovana uz nisku potrošnju energije, što potvrđuje primjenjivost ovog sistema u različitim okruženjima. Smanjeni broj retransmisija i efikasno korišćenje dostupnog spektra ukazali su na sposobnost sistema da ostane funkcionalan i u uslovima povećanog elektromagnetnog šuma, čime se omogućava kontinuitet rada IoT mreža [7].

VI. ZAKLJUČAK

Primjena LoRaWAN tehnologije pokazala se kao efikasan način prenosa podataka na velikim udaljenostima, čak i u uslovima prisustva smetnji i ograničenih infrastrukturnih resursa. Tokom eksperimentalnih ispitivanja, analizirana je otpornost sistema na interferenciju, optimizacija potrošnje energije i pouzdanost prenosa podataka u različitim okruženjima. Implementacija ESP32 mikrokontrolera, zajedno sa *Real Time Clock* (RTC) modulom i *Battery Management System*-om (BMS), omogućila je dugotrajan rad *node* uređaja, dok su YAGI i omnidirekcione antene obezbijedile stabilnu i pouzdanu komunikaciju.

Posebno je važno naglasiti otpornost sistema u scenarijima sa spoljnim interferencijama, gdje je korišćenjem naprednih mehanizama, poput ARQ retransmisije i adaptivnog upravljanja brzinom prenosa, obezbijeđena pouzdanost mreže uz očuvanje energetske efikasnosti. Ispitivanja su pokazala da LoRaWAN mreže omogućavaju visok stepen fleksibilnosti i prilagodljivosti u uslovim promjenljive radiofrekvencijske okoline, što ih čini pogodnim za primjenu u *Smart City* rješenjima [8], industrijskim IoT mrežama, kao i udaljenim ruralnim područjima.

Dobijeni rezultati ukazuju na potrebu daljeg unaprijeđenja tehnika otkrivanja i ispravljanja grešaka u realnom vremenu, kako bi se dodatno povećala otpornost sistema na smetnje. Pored toga, optimizacija potrošnje energije ostaje ključni faktor u razvoju IoT mreža, naročito u rješenjima koja zahtijevaju dugoročno autonomno funkcionisanje uređaja.

Implementirani sistem pokazao je da LoRaWAN tehnologija nudi održivo rješenje za bežični prenos podataka u okruženjima sa ograničenima resursima. Niska potrošnja energije, otpornost na smetnje i mogućnost prilagođavanja različitim uslovima čine ovu tehnologiju jednim od najperspektivnijih rješenja za razvoj modernih IoT aplikacija. [9]

ZAHVALNICA

Autori izražavaju zahvalnost doc. dr Draženu Marinkoviću za mentorsku podršku i nesebično izdvojeno vrijeme prilikom izrade ovog rada. Njegova stručnost i savjeti značajno su doprinijeli kvalitetu istraživanja i završnoj realizaciji rada.

LITERATURA

[1] M. N. Bin Che Kamarudin, A. B. Ayob, A. B. Hussain, S. Ansari, M. G. M. Abdolrasol, and M. H. B. Md Saad, "Review of LoRaWAN: Performance, Key Issues and Future Perspectives," *Jurnal Kejuruteraan*, vol. 36, no. 2, Mar. 2024.

[2] A. Augustin, J. Yi, T. Clausen, and W. M. Townsley, "A study of LoRa: Long range & low power networks for the Internet of Things," *Sensors*, vol. 16, no. 9, 2016.

[3] M. Rizzi, P. Ferrari, A. Flammini, and E. Sisinni, "Evaluation of the IoT LoRaWAN Solution for Distributed Measurement Applications," *IEEE Transactions on Instrumentation and Measurement*, vol. 66, no. 11, pp. 2851-2860, Nov. 2017.

[4] A. Marahatta, Y. Rajbhandari, A. Shrestha, and A. Singh, "Evaluation of a LoRa mesh network for smart metering in rural locations," *Electronics*, vol. 10, no. 6, p. 751, Mar. 2021.

[5] R. Chevillon, G. Andrieux, L. Clavier, and J.-F. Diouris, "Stochastic geometry-based analysis of the impact of underlying uncorrelated IoT networks on LoRa coverage," *IEEE Access*, Jan. 2022.

[6] A. Lavric and A. I. Petrariu, "LoRaWAN communication protocol: The new era of IoT," in *Proc. 14th Int. Conf. Development and Application Systems*, Suceava, Romania, May 24-26, 2018.

[7] A. Povalac, J. Kral, H. Arthaber, O. Kolar, and M. Novak, "Exploring LoRaWAN traffic: In-depth analysis of IoT network communications," *Sensors*, vol. 23, no. 17, p. 7333, Aug. 2023.

[8] M. Alkhayyal and A. Mostafa, "Recent developments in AI and ML for IoT: A systematic literature review on LoRaWAN energy efficiency and performance optimization," *Sensors*, vol. 24, no. 14, p. 4482, Jul. 2024.

[9] M. Nowak, R. Rózycki, G. Waligóra, J. Szewczyk, A. Sobiesierski, and G. Sot, "Data processing with predictions in LoRaWAN," *Energies*, vol. 16, no. 1, p. 411, Dec. 2022.

ABSTRACT

This paper analyzes key aspects of LoRaWAN networks, including proactive frame transmission, data fragmentation and security mechanisms such as AES encryption and the ARQ protocol. Special attention is given to improving data transmission reliablity through protection against interference and jamming attacks. The proposed mechanisms optimize data transfer and significantly reduce data loss, even under high interference conditions. The focus of the paper is on adapting the LoRaWAN network to various conditions, thereby increasing system resilience and ensuring continuity of data transmission.

TECHNIQUES FOR ENHANCING NETWORK PERFORMANCE AND DATA PROTECTION IN LoRaWAN SYSTEMS

Daniel Menićanin
Jelena Radanović
Nikola Račić