SVEUČILIŠTE U ZAGREBU
FAKULTET ELEKTROTEHNIKE I RAČUNARSTVA

SEMINAR

Sigurnosni izazovi u ostvarivanju interneta stvari

Lovre Mitrović
Voditelj: *Ante Đerek*

Zagreb, svibanj 2023.

SADRŽAJ

POPIS SLIKA

1. Uvod

Internet stvari (eng. Internet of Things, IoT) je relativno novi i popularni koncept i nekolicinom definicija koje su se pojavile tokom vremena [2]:

- Globalna infrastruktura za informacijsko društvo koja omogućava povezanost (fizičkih i virtualnih) stvari baziranih na informacijskim i komunikacijskim tehnologijama.
- Mreža međusobno povezanih objekata koji su jedinstveno označeni te koriste inteligentna sučelja za povezanost u kontekstu društva, okoliša i raznih korisnika.
- Povezanost fizičkih objekata opremajući ih senzorima i sredstvima za povezivanje na internet.
- Žična ili bežična mreža jedinstveno označenih uređaja koji imaju mogućnost obrade podataka i mogućnost međusobne komunikacije bez ili s ljudskom uključenošću u proces.

U suštini internet stvari nam omogućava da dosad izolirane stvari u fizičkom svijetu opremimo senzorima koji očitavaju trenutno stanje i uz pomoć nekog komunikacijskom protokola razmjenjujemo i skupljamo podatke. Te ih naknadno po potrebi skladištimo i obrađujemo.

Procjenjeno je da se danas u 2023 na svijetu nalazi oko 15 milijardi uređaja spojenih na internet stvari [3]. Tako velik broj ne iznenađuje jer je primjena interneta stvari široka i raznolika od industrije do potrošačkih uređaja. Tako se internet stvari već primjenjuje u pametnoj proizvodnji gdje senzori opažaju stanje u procesu proizvodnje te na osnovu njihovih očitavanja neki inteligentni sustav donosi daljnje odluke. Zatim u infrastrukturi pametnih gradova gdje senzori očitavaju zauzeće parkirnih mjesta, kvalitetu vode ili pak kvalitetu zraka. Slično prethodnom postoji primjena i u pametnom uzgoju gdje su plantaže opremljene senzorima za vlagu zraka ili kvalitetu tla. Također internet stvari je našao svoju primjenu i u domaćinstvima u obliku nadzornih kamera koje se spajaju na internet ili žarulja kojima je moguće upravljati koristeći pametni

telefon. Što se tiče potrošačkim uređajima (eng. business to consumer) uglavnom se radi o uređajima za praćenje lokacije, unosa kalorija i sličnih. [2]

U nastavku se razmatraju potrošački uređaji jer potrošači često imaju malo utjecaja na kvalitetu proizvoda koji kupuju te imaju malo ili nemaju uopće znanja o tehnologiji u pozadini. A proizvođači ulažu malo vremena i resursa u razvoj kako bi što prije lansirali proizvod na tržište po što nižoj cijeni što dovodi do manjka brige o sigurnosti. Takvi uređaji su već zbog svoje primjene izuzetno ograničeni svojom računarskom moći jer je nužno da budu mali, prijenosi, jeftini i da troše što manje energije. Takve specifikacije same po sebi predstavljaju izazov u implementaciji kvalitetne sigurnosti. Za razliku od računala koje imaju računarske moći, memorijskog kapaciteta i energije u izobilju za potrebe implementacije sigurnosti. [2]

1.1. Model sigurnosne arhitekture

Kako bi uspješno razmatrali sigurnost u internetu stvari predstavljamo model sigurnosne arhitekture u kojem razdvajamo odgovornosti po slojevima apstrakcije.[4]

Model koji Gartner predstavlja orijentiran na tehničku perspektivu i sastoji se od:

- Sigurnosti oblaka (eng. Cloud Security)
- Sigurnosti aplikacije (eng. Application Security)
- Sigurnosti krajnje točke (eng. Endpoint Security)
- Sigurnosti mreže (eng. Network Security)

U nastavku razmatramo sigurnost mreže koja je jedan od najbitnijih aspekata u internetu stvari.

2. Komunikacijski protokoli u internetu stvari

U radu se fokusiramo na mrežni sloj OSI modela i na protokole koji se koriste, a posebno na LoRa WAN protokol verzije 1.0.2.

Mrežni protokoli koji se koriste razlikuju se u brzini prijenosa podataka, udaljenosti koju mogu pokriti, broju uređaja koje podržavaju, dostupnosti na određenom geografskom području, skalabilnosti i konačno cijeni.

Sljedeći popis sadržava tehnologije koji se koriste u primjeni te njihove prednosti i mane.[2]

- **Low Energy Bluetooth (BLE)** je jeftin i koristi malo energije te podržava visoku brzinu (1 Mbps) i u teoriji neograničen broj uređaja. Ali ima izuzetno ograničen domet (50 m) te zahtjeva prijestupnu točku koja ima pristup mreži.
- **ZigBee (802.15.4e)** je jeftin, koristi malo energije te podržava velik broj uređaja (do 65000) ali je ograničen u brzini (250 kbps) i dometu (100 m).
- **IEEE 802.11.ah** je preinaka postojeće WiFi specifikacije (IEEE 802.11) za potrebe interneta stvari. Pruža velike brzine (do 346 Mbps) i podržava do 8000 uređaja također koristi malo energije i ima srednji domet (do 1.5 km). Nedostatak su cijena i činjenica da koristi 900 MHz koji za razliku od 2.4 MHz nije globalno nelicencirani spekatar.
- **3G i 4G** su globalno prisutni i pružaju visoke brzine ,ali glavni nedostatak je cijena. Oprema je skuplja i koristi se licencirani spektar također koristi više energije.
- **NB IoT** je podskup LTE standarda te je kao takav široko prisutan i radi u licenciranom spektru ali ima ograničenu brzinu na 250 kbps zbog svoje propusnosti. Koristi malo energije i relativno je jeftin.

U nastavku se fokusiramo isključivo na LoRa WAN protokol.

3. Protokol LoRaWAN

LoRaWAN je LPWAN (Low Power Wide Area Network) osmišljen u svrhu bežičnih uređaja napajanih baterijom u sklopu interneta stvari. LoRa je bežična modulacija razvijena od strane Semtecha koja koristi nelicencirani radijski spektar. U usporedbi s prethodnim tehnologijama je jeftinija, koristi izuzetno malo energije i ima relativno dalek domet (15 km). Ali ima ograničenu brzinu (50kbps na kratke udaljenosti i oko 300bps na duge udaljenosti) i trenutno ne postoji dovoljno razvijena i raspršena infrastruktura.[2]

LoRaWAN mreža je ostvarena u topologiji zvijezdze u kojoj gateway uređaji izmjenjuju poruke između krajnjih uređaja i mrežnog servera. Komunikacija između servera i gatewaya se odvija IP protokolom dok krajnji uređaji komuniciraju LoRa komunikacijom s jednim ili više gatewaya.

Kako bi bili bolje upoznati s ranjivostima u nastavku ovog poglavlja su izdvojeni bitni dijelovi specifikacije LoRaWAN protokola.

3.1. Fizički format poruke

LoRa terminologija razlikuje dvije vrste poruke. To su **uplink** koje šalje krajnji uređaj ,a prima mrežni server i **downlink** koje šalje mrežni server ,a prima krajnji uređaj. [1]

3.1.1. Uplink poruke

Uplink poruke su sastavljene od fizičkog zaglavlja (**PHDR**), CRC zaglavlja (**PHDR_CRC**), **CRC** polja koju štiti integritet poruke i sadržaja (**PHY Payload**).

Slika 3.1: Format uplink poruke

Preambula	PHDR	PHDR_CRC	PHY Payload	CRC

3.1.2. Downlink poruke

Downlink poruke su sastavljene od fizičkog zaglavlja (**PHDR**), CRC zaglavlja (**PHDR_CRC**) i sadržaja poruke (**PHY Payload**).

Slika 3.2: Format downlink poruke

3.2. MAC format poruke

Navedeni sadržaj poruke (**PHY Payload**) sadržava MAC zaglavlje veličine jednog okteta (**MHDR**) koje u sebi sadrži oznake za tip poruke i tip verzije. Zatim sadržaj (**MAC Payload**) i na kraju **MIC** polje veličine 4 okteta koje služi za zaštitu integriteta. [1]

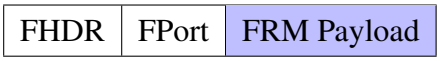
MIC polje se računa koristeći ključ mrežne sjednice (**NwkSKey**) u AES128-CMAC algoritmu nad poljima MHDR i MAC payload. Nakon provedbe algoritma uzimaju se najniža 4 okteta i spremaju u MIC polje.

Slika 3.3: Format MAC poruke

Sadržaj MAC poruke nadalje sadrži zaglavlje okvira (**FHDR**) koje sadržava adresu uređaja (**DevAddr**), oktet za kontrolu okvira(**FCtrl**), polje od 2 okteta za brojač okvira (**FCnt**), i polje veličine do 15 okteta za opcije okvira (**FOpts**). Nakon zaglavlja okvira dolazi polje za port (**FPort**) veličine 2 okteta i sadržaj okvira (**FRMPayload**).

FRM Payload polje se enkriptira koristeći AES128 koristeći ključ mrežne sjednice (**NwkSKey**) u slučaju kada je FPort postavljen na 0 ,a inače ključ aplikacijske sjednice (**AppSKey**).

Slika 3.4: Format MAC sadržaja



3.3. Aktivacija uređaja

Nakon aktivacije uređaja sljedeće informacije trebaju biti pohranjene na uređaju [1]:

- adresa uređaja u trenutnoj mreži veličine 32 bita (**DevAddr**)
- globalno jedinstvena oznaka aplikacije (**AppEUI**)
- ključ mrežne sjednice (**NwkSkEy**) jedinstven za krajnji uređaj koji koriste i krajnji uređaj i mrežni server te služi za izračun i potvrdu **MIC** polja kao i za šifriranje i dešifriranje sadržaja MAC poruke ukoliko je FPort postavljen na 0
- ključ aplikacijske sjednice (**AppSKey**) jedinstven za krajnji uređaj koji služi za osiguravanje enkripcije s kraja na kraj između krajnjeg uređaja i aplikacijskog servera koji se nalazi iza mrežnog servera. Koristi se za šifriranje i dešifriranje sadržaja MAC poruke ukoliko je FPort bilo što osim 0

Protokol definira dva načina za aktivaciju krajnje uređaja OTAA (Over the Air Activation) i ABP (Activation by Personalization). [1]

3.3.1. ABP

ABP je primitivniji način aktivacije gdje se u uređaj hardcodiraju adresa (**DevAddr**) i dva ključa sjednice (**NwkSKey** i **AppSKey**). Valja napomenuti da oba ključa trebaju biti jedinstvena kako kompromitiranje jednog uređaja ne bi ugrozilo druge. Također preporuča se da ključevi ne bi trebali biti izvedeni iz javno dostupnih informacija poput adrese uređaja. [1]

3.3.2. OTAA

OTAA je nešto kompliciraniji način aktivacije uređaja u kojem je potrebno proći proceduru pridruživanja (eng. join procedure) prije razmjene podataka sa mrežnim serverom. Krajni uređaj prije početka navedene procedure mora biti opremljen sljedećim informacijama globalnim identifikatorom uređaja (**DevEUI**), identifikatorom aplikacije (**AppEUI**) i AES128 ključem (**AppKey**). Pokretanjem procedure pridruživanja krajnji uređaj mrežnom serveru šalje identifikator uređaja (**DevEUI**), i aplikacijski identifikator (**AppKey**) zajedno sa **DevNounce**. Server pamti navedene informacije i uređaju šalje adresu (**DevAddr**) zajedno sa **AppNounce** i **NetID** te još nekim dodatnim informacijama. Navedeni **AppNounce** i **NetID** su bitni jer zajedno s aplikacijskim ključem (**AppKey**) sudjeluju u izračunu ključeva sjednice **NwkSKey** i **AppSKey**. [1]

4. Sigurnosne prijetnje

U ovom dijelu razmatramo koje su to općenite prijetnje sustavu koji implementira internet stvari. Navedene prijetnje su razmatrana s većeg nivoa apstrakcije te su manje specifične LoRaWAN protokolu ,a više općenite za sustav interneta stvari.

4.1. Prisluškivanje poruka

Bilo tko bi mogao kupiti jeftini uređaj koji sluša poruke koje se šalju LoRa tehnologijom te na taj način izvršiti napad na povjerljivost informacija. Moguće je pročitati poruke koje se šalju čistim tekstom, koje koriste loš algoritam enkripcije ili imaju implementiran ranjiv proces razmjene ključeva.

4.2. Izmjena poruka

Prijetnja predstavlja napad na integritet poruke gdje napadač presretne poruku, izmjeni ju te je pošalje zadanom primatelju.

4.3. Reprodukcija poruka

Poruke je također moguće snimiti zatim ponovno reproducirati. Na primjer snimim poruku koja se šalje dok je parkirno mjesto zauzeto i reproduciram je jačim signalom dok je ono slobodno te na taj način sustav zabilježi slobodno mjesto kao zauzeto.

4.4. Neovlašteno ili neautorizirano slanje poruka

Prijetnja opisuje scenarij u kojem se krajnji uređaj ili gateway prihvaća konekciju nekog trećeg neovlaštenog ili neautentificiranog uređaja. Dodatni problem je taj što često u internetu stvari ne možemo garantirati fizičku sigurnost uređaja.

4.5. Nedostatak izoliranosti mreže

Prijetnja opisuje scenariji u kojemu uređaji na mreži nisu izolirani i zlonamjerni napadač se već nalazi u mreži. Ova prijetnja ne predstavlja problem u globalnim mrežama koje su javne i imlementirane na većem području već u slučaju kada želimo izgraditi privatnu mrežu. Slično kao što postoje LAN mreže.

4.6. Gubitak povezanosti s mrežom

Povezanost uređaja može biti prekinuta zbog interferencije signala ili prestanka rada infrastrukture zbog ljudske greške ili prirodne katastrofe.

5. Zaštitne mjere

U ovom poglavlju razmatramo zaštitne mjere koje su poduzete na razini LoRaWAN protokola. Prijetnje od 4.1 do 4.4 su uzete u razmatranje tijekom izrade protokola te on nudi zaštitne mjere protiv navedenih prijetnji. Za prijetnje 4.5 i 4.6 protokol ne nudi nikakve zaštitne mjere te se one neće razmatrati ni u ovom niti u sljedećim poglavljima.

5.1. Povjerljivost podataka

Kako bi se osigurala povjerljivost podataka kao zaštita od prisluškivanja potrebno je šifrirati podatke snažnim kriptografskim algoritmom tako da i u slučaju kada je poruka presretnutna da napadač ne može isčitati nikakve značajne informacije iz nje. U slučaju LoRaWAN protokola polje **FRM Payload** je šifrirano koristeći simetrični algoritam enkripcije, AES s ključem duljine 128 bitova. Dva ključa se koriste u enkripciji: ključ aplikacijske sjednice **AppSKey** ukoliko se radi o podacima aplikacije i ključ mrežne sjednice **NwkSKey** ukoliko se radi o porukama za administraciju mreže.

Simetrični algoritam enkripcije je odabran umjesto asimetričnog zbog svoje manje računarske složenosti. Jer su krajnji uređaji najčešće napajani baterijom i imaju malu računarsku moć.

Također valja naglasiti da ostala polja nisu zaštićena enkripcijom: MHDR,FHDR, FPort i MIC kao niti poruke u proceduri pridruživanja.

5.2. Integritet podataka

Primatelj poruke mora biti u stanje detektirati je li poruka došla od izvora do odredišta nepromjenjena kako bi se zaštitili od neovlaštene izmjene poruka. Osim zaštite integriteta podataka koji se šalju u **FRM Payload** potrebno je zaštititi i kontrolna polja. Protokol zato implementira kod za zaštitu integriteta u **MIC** polju koje štiti MAC zaglavlje (**MHDR**) i cijeli njegov sadržaj (**MAC Payload**). Za njegov izračun koristi se ključ mrežne sjednice (**NwkSKey**) kao što je opisano u 3.2.

5.3. Zaštita od reprodukcije

Ova mjera je usmjerena kako bi detektirali poruke koje su neovlašteno snimljene i zatim ponovno reproducirane u svrhu zavaravanja sustava . Razmatramo dva scenarija prvi je reprodukcija tijekom procesa OTAA ,a drugi je reprodukcija tijekom regularne komunikacije.

Tijekom OTAA procesa krajnji uređaj šalje zahtjev koji sadržava **DevNounce** ,a on se za taj uređaj pamti na mrežnom serveru te će server u budućnosti odbaciti zahtjeve tog uređaja za aktivacijom ukoliko ponovno pokuša poslati isti nounce.

U drugom scenariju tijekom regularne komunikacija obrana od ove prijetnje je ostvarena koristeći polje **FCnt** (Frame Count) koje se ponaša kao brojač koji se inkrementira svakom poslanom porukom. Te će se odbaciti svaka poruka koja sadržava manji ili jednak broj od posljednjeg zapamćenog.

5.4. Autentifikacija uređaja

Potrebno je omogućiti mehanizam kojim se svaki uređaj na mreži autentificira prije slanja podataka kako bi se onemogućila konekcija s neovlaštenim uređajima. LoRaWAN protokol definira ključeve koji autentificiraju uređaj. Ključ mrežne sjednice (**NwkSKey**) autentificira sam uređaj dok ključ aplikacijske sjednice (**AppSKey**) autentificira aplikaciju ili pretplatnika. Prije procesa aktivacije ključ **AppKey** služi u obje svrhe.

6. Sigurnosne ranjivosti

Ovo poglavlje razmatra koje su to ranjivosti i slabosti koje i dalje postoje u protokolu nakon što je protokol definirao zaštitne mjere. Mreža se sastoji od čvorova i veza u slučaju LoRaWAN protokola čvorovi su krajnji uređaji u gateway uređaji dok su veze ostvarene konekcije između njih. Naglasak u ovom poglavlju stavljamo na ranjivosti veza.

6.1. Nesigurna aktivacija

LoRaWAN protokol definirao je dva načina aktivacije uređaja ABP (3.3.1) i OTAA (3.3.2). Nakon aktivacije uređaj zadovoljava zaštitnu mjeru za autentifikacijom na mreži. U slučaju ABP pošto su ključevi hardcodirani te ne postoji način ponovnog generiranja ključeva ukoliko je to potrebno. Ako su ključevi na bilo koji način kompromitirani uređaj je trajno ranjiv zbog nemogućnosti obnove ključeva. Zato se ABP smatra manje sigurnim načinom aktivacije.

6.2. Ranjivost DevNouncea

DevNounce je nasumična vrijednost koja se šalje krajnjem uređaju tijekom procesa pridruživanja. Tijekom slanja ta poruka nije šifrirana ta je moguće snimiti poruku i jednostvano isčitati DevNounce. Razlog zašto poruka nije šifrirana je zato što još nisu stvoreni potrebni ključevi za enkripciju. Prisluškivanjem DevNounce vrijednosti moguće je dobiti uvid kako funkcionira generator pseudo nasumičnih brojeva koji će zbog manjka računarska moći biti relativno loš. Drugi problem DevNounce je što protokol ne specificira koliko ih je unazad potrebno pamtiti. Ako se pamti velik broj prethodnih vrijednosti server će ignorirati veći broj zahtjeva za aktivacijom te će usluga na trenutke biti uskraćena. Ako se pak odluči pamtiti manji broj prethodnih vrijednosti tada se povećava vjerojatnost napada reprodukcijom. Ova slabost bi se ublažila kada bi se povećala veličina DevNounce te se tako spriječila vjerojatnost kolizije.

6.3. Ranjivost brojača

Brojač je uveden kao zaštitna mjera protiv napada reprodukcijom. Međutim u dizajnu brojača postoje dvije ranjivosti.

Prva obuhvaća uređaje koji su aktivirani ABP načinom. Naime kada se reserira uređaj aktiviran ABP načinom brojač se vraća na 0. Također kriptografski ključevi se ne mijenjaju kod uređaja aktiviranim ABP načinom. Što znači da se resetiranjem ponovno koriste isti ključevi s istim vrijednostima brojača. Stoga ako je poruka krajnjeg uređaja snimljena prije restarta ona se može ponovno reproducirati i biće prihvaćena kao ispravna od strane mrežnog servera. Jer ta poruka ima vrijednost brojača veću od nula dok je pravi brojač na krajnjem uređaju i mrežnom serveru nula. Kada je takva poruka prihvaćena mrežni server uvećava svoj brojač i posljedično odbacuje legitimne poruke krajnjeg uređaja jer one imaju manju vrijednost brojača. Osim što je u ovom napadu reproducirana poruka došlo je i do uskraćivanja usluge.

Druga ranjivost obuhvaća uređaje aktivirane i ABP načinom i OTAA načinom. Naime brojač je implementiran kao 16 bitno ili 32 bitno polje. Jednom kada je dosegnuta maksimalna vrijednost dolazi do preljeva i brojač ponovno kreće od nule. Što znači da napadač koji je prethodno snimio poruke može ih uspješno reproducirati.

6.4. Wormhole napad

Protokol je po dizajnu ranjiv na tzv. Wormhole napad. Takav napad se sastoji od tri koraka. U prvom koraku se osluškuje komunikacija između krajnjeg uređaja i gateway uređaja. Drugi korak je ometanje signala krajnjeg uređaja. I na kraju u trećem koraku reproduciramo signal na drugoj lokaciji spojeni na neki drugi gateway. Signal ćemo moći uspješno reproducirati na drugoj lokaciji sve dok ga ometamo na prvoj lokaciji. S obzirom da protokol ne sadržava nikakvu vremensku oznaku signal se može uspješno reproducirati u nedogled. Primjer ovakvog napada bi bio sustav za praćenje koji određuje lokaciju na osnovu LoRa signala. Ovakvu ranjivost je moguće ukloniti dodavajući vremensku oznaku u protokol kao i implementiranje nadzora od strane operatora mreže koji bi detektirao Wormhole napad ukoliko se signal brzo pojavi na lokaciji koja je previše udaljena od prethodne.

6.5. Dekripcija poruka ABP uređaja

Uređaji aktivirani ABP načinom aktivacije dodatno posjeduju ranjivost koja omogućava dešifriranje poruka pod određenim okolnostima.

Jednom kada je uređaj aktiviran poruke se šifriraju AES128 enkripcijom u CTR načinu. Nad porukom se provodi XOR operacija s bitovima generiranim iz inicijalnog vektora. Taj inicijalni vektor je upravo brojač koji se inkrementira svakom sljedećom porukom. Pošto se radi CTR načinu kada bi uspjeli natjerati uređaj da dvaput koristi isti inicijalni vektor mogli bi dešifrirati poruke uz posjedovanje nekog znanja o sadržaju. Vjerojatnost uspještnosti dešifriranje poruka se povećava ako su korišteni isti kriptografski ključevi što je upravo slučaj kod ABP aktivacije uređaja. A brojač koji koristimo kao inicijalni vektor možemo postaviti na nulu resetirajući uređaj ili uzrokovanjem preljeva. Sama ranjivost brojača je opisana u odjeljku 6.3.

6.6. Napad grubom silom na MIC polje

Integritet svake poruke u LoRaWAN protokolu je zaštićen MIC poljem koje mogu izračunati jedino uređaji na krajevima komunikacije koji posjeduju ključ mrežne sjednice (NwkSKey). Ranjivost je uvedena jer je MIC polje premalo za današnje kriptografske standarde. Veličina polja je 4 okteta što znači da postoji ukupno 4 292 967 296 mogućnosti. U prosjeku napadač treba isprobati pola od toga. Koristeći suvremeni procesor s 8 jezgri moguće je izračunati ispravnu MIC vrijednost za projesčno 1.5 sekundu [5]. Napadač može presresti poruku izmjeniti je i izračunati ispravnu MIC vrijednost te je predstaviti kao legitimnu.

6.7. Bit-Flipping napad

Bit Flipping napad označava napad u kojem napadač mijenja bitove u šifratu koji uzroruju predvidljivu promjenu čistom tekstu. AES128 u CTR načinu kakav se koristi u LoRaWAN protokolu je ranjiv na ovakav napad. Zaštitna mjera koja je predložena je miješanje bitova tako da napadač ne može pogoditi poziciju odgovarajućeg bita u šifratu. Dodatno je ovaj napad olakšan jer je kod za zaštitu integriteta (MIC) jednostavan za pogađanje napadom grube sile kao što je opisano u 6.6

7. Zaključak

LoRaWAN je jedan od protokola razvijen upravo za internet stvari. Osmišljen je da bude lako dostupan zajednici stoga koristi LoRa tehnologiju koja funkcionira u nelicenciranom spektru. Navedena tehnologija je jeftina i koristi malo energije što je čini pogodnom za baterijski napajane uređaje. Ali ima ograničenu brzinu što ograničava njezinu primjenu i dostupnost što onemogućava korištenje na određenom geografskom području. LoRaWAN protokol definira dva načina aktivacije uređaja ABP i OTAA. OTAA način je preporučeni način jer je fleksibilniji i sigurniji od ABP načina koji ne mijenja svoje jednom postavljene kriptografske ključeve. Protokol LoRaWAN je i dalje ranjiv usprkos poduzetim zaštitnim mjera koje nameće protokol zato što je namjenjen krajnjim uređajima koji su napajani baterijom i imaju malu računarsku moć i ograničenu mogućnost prijenosa podataka. Zbog štednje prijenosa podataka protokol koristi brojač relativno ograničene veličine što dovodi do mogućnosti preljeva u nekom trenutku koji otvara mogućnost narušavanja intergriteta i tajnosti te reprodukcije snimljenih poruka.

Zbog svoje ograničenosti protokol ne bi trebali koristiti u primjenama gdje je sigurnost kritična poput financijske industrije. Ali je njegova primjena sasvim zadovoljavajuća za neke projekte nadzora gdje nam sigurnost nije kritična i gdje je mali rizik od napada poput nadzora kvalitete tla manjih poljoprivrednih zemljišta.

8. Literatura

[1] Lorawan® specification v1.0.2, Nov 2022. URL https://lora-alliance.org/resource_hub/lorawan-specification-v1-0-2/.

[2] Vojtech Brtnik. Security risk assessment of lorawan, 2017.

[3] Fabio Duarte. Number of iot devices (2023-2030), Feb 2023. URL https://explodingtopics.com/blog/number-of-iot-devices.

[4] Gartner. Internet of things (iot) security market worth 29.02 billion usd by 2022, 2017.

[5] JungWoon Lee, DongYeop Hwang, JiHong Park, i Ki-Hyung Kim. Risk analysis and countermeasure for bit-flipping attack in lorawan. U *2017 International Conference on Information Networking (ICOIN)*, stranice 549–551, 2017. doi: 10.1109/ICOIN.2017.7899554.

9. Sažetak

Razmatraju se predložene definicije interneta stvari te se daje kratki uvod u primjenu. Predstavljaju se tehnologije koje se koriste u praksi te se posebna pažnja daje LoRaWAN protokolu koji koristi LoRa tehnologiju. Objašnjava se način prijenosa poruka i aktivacije uređaja onako kako ih definira protokol. Razmatraju se potencijalne prijetnje sustavu te se obrađuju zaštitne mjere koje uvodi protokol kao odgovor na prijetnje. Obrađuje se nekolicina relevantnih ranjivosti koje postoje u dizajnu protokola usprkos zaštitnim mjerama.