Tampereen yliopisto

Juho Lommi

LORAWAN-TEKNOLOGIAN SOVELTUVUUS KRIITTISEN TIEDON VÄLITTÄJÄNÄ

Kandidaattitutkielma
Informaatioteknologian ja viestinnän tiedekunta
Tarkastajat: Matti Monnonen
Heinäkuu 2023

TIIVISTELMÄ

Juho Lommi: LoRaWan-teknologian soveltuvuus kriittisen tiedon välittäjänä
Kandidaattitutkielma
Tampereen yliopisto
Tieto- ja sähkötekniikan kandidaattiohjelma
Heinäkuu 2023

Langattomien verkkoteknologioiden ja verkkoon kytkettävien laitteiden määrä on kasvanut räjähdysmäisesti viime vuosikymmenien aikana. Laitteiden verkkoon kytkemisen seurauksena myös huoli niiden tietoturvasta on kasvanut etenkin tilanteissa, joissa uusia teknologioita sovelletaan kriittisen tiedon välittämiseen. Long Range (LoRa) on pitkän kantaman hajaspektrimodulaatioon perustuva radioteknologia, joka toimii lisenssivapailla radiotaajuuksilla. Low Power Wide Area Network (LoRaWan) on LoRan päälle rakennettu verkkoteknologia, jonka avulla voidaan lähettää pieniä datamääriä päätelaitteilta sovelluspalvelimille. LoRaWan on saavuttanut suuren suosion sen hyvän kuuluvuuden, päätelaitteiden halpojen valmistuskustannusten sekä hyvän akunkeston vuoksi.

Tässä tutkielmassa tarkastellaan LoRaWan-verkkoteknologiaa ja sen soveltuvuutta kriittisen tiedon välittäjänä. Tutkielman tarkoituksena on selvittää, voidaanko LoRaWan-teknologiaa hyödyntää tilanteissa, joissa välitettävä tieto on kriittistä ja mitä asioita tulee ottaa huomioon, jotta teknologiaa voidaan hyödyntää turvallisesti. Tutkielma toteutettiin kirjallisuuskatsauksena ja sen lähteiksi valittiin tuoreita LoRaWan-teknologiaa ja siihen kohdistuvia tietoturvauhkia käsittelevää tieteellistä kirjallisuutta sekä laitevalmistajien teknisiä dokumentaatioita. Tutkielmaan valitun kirjallisuuden perusteella on koottu yhteen yleisimmät teknologiaan kohdistuvat uhat ja tavat miten niiltä on mahdollista suojautua. Tutkielman lopuksi teknologiaan ja sitä koskeviin uhkiin liittyvät havainnot kootaan yhteen ja tehdään päätelmä siitä, soveltuuko LoRaWan kriittisen tiedon välittämiseen.

Tutkielma osoittaa, että LoRaWanin hyödyntämiseen kriittisen tiedon välittäjänä on syytä suhtautua varauksella. Havaintojen mukaan se on muiden verkkoteknologioiden tavoin altis häirinnälle ja siihen kohdistuu myös useita muita tietoturvauhkia, mikä vaarantaa kriittisen tiedon välittämisen. Käsiteltyjen uhkien perusteella suurimmat riskit rajoittuvat viestin saatavuuteen. Lisäksi kirjallisuuden perusteella viestin manipulointi ja purkaminen on joissain tapauksissa mahdollista. Kirjallisuuden mukaan suurin osa teknologiaan kohdistuvista haavoittuvuuksista on korjattu LoRaWan-versioissa 1.0.4 ja 1.1. Tulosten perusteella teknologiaa ei kannata käyttää tilanteissa, joissa viestin perille pääsy on erityisen tärkeää. Muissa tapauksissa viestin välittäminen on varsin turvallista, mikäli laitteet on suojattu asianmukaisesti ja verkosta on käytössä jokin uusimmista versioista.

Avainsanat: LoRaWan, LoRa, Tietoturva, Esineiden internet

Tämän julkaisun alkuperäisyys on tarkastettu Turnitin OriginalityCheck -ohjelmalla.

SISÄLLYSLUETTELO

1. Johdanto 1
2. Teknologia 3
2.1 LoRa 3
2.2 LoRaWan 5
3. LoRaWanin tietoturva 8
3.1 Salaus 8
3.2 Laitteiden rekisteröinti 9
4. LoRaWan tiedetyt haavoittuvuudet 11
4.1 LoRaWan-verkon häritseminen 11
4.2 Uudelleentoistohyökkäys ABP-aktivoiduilla laitteilla 12
4.3 Salakuuntelu 12
4.4 Bitinkääntöhyökkäys 13
4.5 ACK-huijaus 14
4.6 ADR-huijaus 14
4.7 Fyysiset hyökkäykset 15
4.8 Muita tiedossa olevia hyökkäyksiä 16
5. Yhteenveto 17
Lähteet 19

LYHENTEET JA MERKINNÄT

ABP	LoRaWan-päätelaitteen aktivointitapa, jossa parametrit on asetettu etukäteen päätelaitteelle (engl. Activation By Personalization)
AES	Edistynyt salausstandardi (engl. Advanced Encryption System)
MIC	Viestin eheyskoodi (engl. Message Integrity Code)
IoT	Esineiden internet (eng. Internet of Things)
ACK	Vastaus (engl. Acknowledgement) on viestityyppi, jolla LoRaWan-liikenteessä vahvistetaan vastaanottaminen
CTR	Edistyneen salausstandardin salaustapa (engl. Counter mode)
OTAA	LoRaWan päätelaitteen aktivointitapa, jossa aktivointi tapahtuu verkon yli
Up-Link	Viesti joka välitetään päätelaitteelta verkkopalvelimelle

1. JOHDANTO

Langattomien verkkoteknologioiden huima kehitys viime vuosikymmenien aikana on saanut aikaan sen, että yhä useampi tekninen laite on yhdistetty verkkoon. Tämä niin kutsuttu esineiden internet (engl. Internet of Things, IoT) on mahdollistanut sen, että asuntojen lämpötiloja voidaan mitata ja säätää etänä, rahtiliikenteessä yksittäisten rullakoiden sijaintia voidaan seurata lähes reaaliajassa kartalta ja laitevalmistaja voi kerätä arvokasta dataa kehittämiensä laitteiden käytöstä ja hyödyntää tätä oman päätöksentekonsa tukena. Esineiden internetin huima kasvu on saanut aikaan sen, että Ericson mobility arvioi, että verkkoon kytkettyjä IoT-laitteita olisi vuonna 2021 verkossa noin 14,6 miljardia ja vuonna 2027 noin 30,2 miljardia [6]. Hurjimpien arvioiden mukaan on arvioitu, että IoT-laitteita olisi kytketty verkkoon vuonna 2030 jopa 500 miljardia [12].

Laitteiden lukumäärän kasvaessa on markkinoille ilmestynyt myös monenlaisia uusia teknologioita, jotka pyrkivät tarjoamaan oman ratkaisunsa eri käyttötilanteista riippuen. Tällaisia teknologioita ovat muun muassa ZigBee, NB-IoT, SIGFOX sekä LoRaWan, jonka toimintaperiaatteeseen ja turvallisuuteen syvennytään myöhemmin tässä tutkielmassa [6].

Teknologioiden ja laitteiden määrän kasvun seurauksena myös tietoturvaan tulee kiinnittää aiempaa enemmän huomiota. Laitteiden kytkeminen internetiin muodostaa aina riskin, mikä tulisi ottaa huomioon etenkin silloin, kun laitteita ja niiden tarjoamia mahdollisuuksia hyödynnetään esimerkiksi teollisuudessa tai kriittisen infrastruktuurin hallinnassa.

Tässä työssä tutkitaan LoRaWan-teknologiaa ja sen soveltuvuutta kriittisen tiedon välittäjänä. Tutkielman tavoitteena on selvittää, soveltuuko LoRaWan-verkko kriittisen tiedon välittämiseen ja mitä asioita tulisi ottaa huomioon, jotta teknologiaa voidaan hyödyntää turvallisesti. Tästä työstä on rajattu kokonaan pois verkon hyödyntäminen tilanteissa, joissa siirrettyä dataa ei voida pitää kriittisenä. Tutkielmassa esille tulevia asioita on mahdollista kuitenkin soveltaa myös näihin tilanteisiin.

Tämä tutkielma on toteutettu kirjallisuuskatsauksena kokoamalla tietoa eri lähteistä yhdeksi kokonaisuudeksi, jonka avulla pyritään vastaamaan tutkimuskysymykseen. Lähteinä työssä käytetään ensisijaisesti Tampereen yliopiston Andor-hakupalveluista hankittuja vertaisarvioituja tieteellisiä artikkeleja sekä LoRaWan-verkon kehittäjien ja teknologiaa

hyödyntävien laitteiden jälleenmyyjien luomia teknisiä dokumentaatioita.

LoRaWanista on olemassa useita eri versioita tällä hetkellä käytettäväksi suositeltujen versioiden 1.1 ja 1.0.4 lisäksi. Tässä työssä käsitellään yleisesti LoRaWan-verkon hyödyntämistä kriittisen tiedon välittäjänä ja koska lähes kaikkia versioita hyödyntäviä laitteita on markkinoilla edelleen, ei työssä rajata ulkopuolelle yksittäisiä versioita. Jos esimerkiksi jokin tietoturvauhka löytyy vain vanhemmista versioita, mutta se on korjattu uudemmissa versioissa, mainitaan tästä kyseistä uhkaa käsiteltäessä.

Tutkielmassa käsitellään aluksi LoRa-radioteknologiaa ja sen toimintaperiaatetta, jonka jälkeen syvennytään LoRaWan-verkkoon. Kolmannessa luvussa käsitellään LoRaWan-teknologian salausta, avaintenhallintaa ja laitteiden rekisteröimistä verkkoon. Neljännessä luvussa käsitellään jo tiedossa olevia teknologiaan kohdistuvia tietoturvauhkia, jotka voivat vaikuttaa tiedonsiirron turvallisuuteen. Uhkia käsiteltäessä käydään myös läpi, miten näiltä hyökkäyksiltä on mahdollista suojautua. Viidennessä luvussa kootaan yhteen työssä käsiteltyjä aiheita ja tehdään niistä yhteenveto.

2. TEKNOLOGIA

LoRaWan-verkkoteknologia on monimutkainen kokonaisuus, joka koostuu monesta eri osasta ja sen lisäksi siitä on olemassa useita eri versioita. Teknologian perustana toimii LoRa-modulaatioteknologia, joka mahdollistaa fyysisesti viestien siirron päätelaitteilta reitittimille. Tässä luvussa perehdytään syvällisemmin LoRa-modulaatioteknologiaan ja sen rajoitteisiin sekä LoRaWan-teknologiaan, sen arkkitehtuuriin ja eri versioihin.

2.1 LoRa

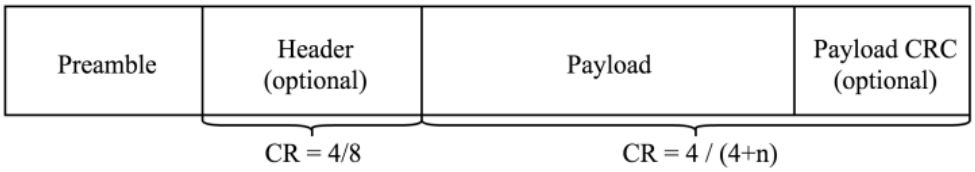
LoRa on pitkän matkan hajaspektrimodulaatioon perustuva modulaatioteknologia, jonka on kehittänyt ranskalainen Cycleo ja jonka on myöhemmin patentoinut Semtech. Se käyttää hyödykseen lupavapaita teolliseen, tieteelliseen ja lääkinnälliseen käyttöön tarkoitettuja (engl. Industrial, Scientific and Medical, ISM) -taajuuksia ja Euroopassa LoRa-verkko toimii 868 MHz taajuudella.[3] Teknologia on otettu vastaan myönteisesti laitteiden halpojen valmistuskustannusten, vähäisen energiankulutuksen ja hyvän häiriönkestävyyden vuoksi [2].

LoRa-teknologia sopii hyvin sellaiseen käyttöön, jossa siirrettävät datamäärät ovat pieniä ja tarvetta jatkuvalle tiedonsiirrolle ei ole. Vapailla ISM-taajuuksilla toimivien laitteiden pulssisuhde on EU-maiden alueella rajoitettu yhteen prosenttiin. Tämä tarkoittaa esimerkiksi sitä, että mikäli laitteen lähetysaika on yksi sekunti, tulee tämän jälkeen seurata 99 sekunnin aika, jolloin laite ei lähetä mitään. Rajoitusten avulla pyritään vähentämään taajuuksilla tapahtuvaa päällekkäisyyttä. Euroopan Unionin (EU) rajoitusten takia LoRa-radioteknologia ei sovi jatkuvaan tiedonsiirtoon vaan on omiaan sellaisissa tilanteissa, joissa tietoa täytyy siirtää vain muutamia kertoja päivässä. [2][3]

Maksimitiedonsiirtonopeus LoRa:n avulla voi olla jopa 50 kilobittiä sekunnissa, mutta yleensä nopeus on huomattavasti tätä hitaampi. Nopeuteen, kantamaan ja häiriönkestävyyteen voidaan vaikuttaa seuraavilla parametreilla: kaistanleveydellä, leviämistekijällä ja koodinopeudella. Näistä tärkein parametri on kaistanleveys, sillä yksinään sitä muuttamalla voi vaikuttaa merkittävästi tiedonsiirtonopeuteen. Karkeasti kaistanleveyden kaksinkertaistaminen tuplaa myös tiedonsiirtonopeuden. Kaistanleveyden tai leviämistekijän muuttaminen vaikuttaa merkittävästi myös vastaanottimen herkkyyteen. Kaistanleveyden nostaminen heikentää vastaanottimen herkkyyttä, kun taas leviämistekijä vahvistaa si-

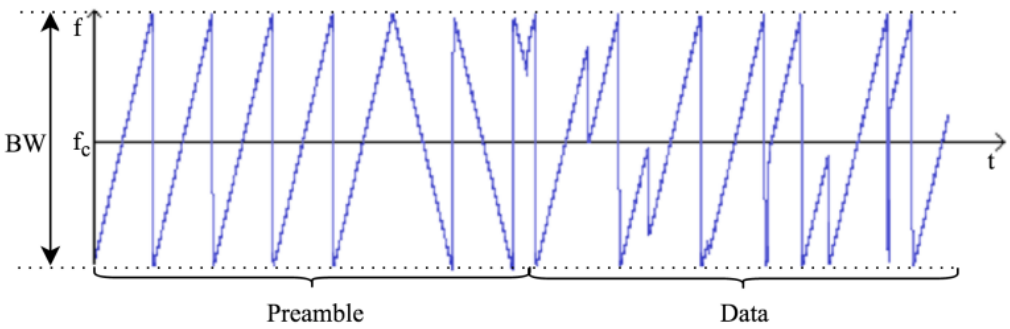
tä.[2]

Vaikka Lora-modulaation yli voidaan lähettää minkälaisia kehyksiä tahansa, on Semtech määritellyt oman kehyksensä omille laitteilleen kuvan 2.1 mukaisesti. Tätä kehystä käytetään myös LoRaWanin viestinvälityksen perustana. Semtechin määritelmässä LoRa-kehys koostuu esiviestistä, ylätunnisteesta, tietosisällöstä ja tietosisällön tarkistusummasta. [2]



Kuva 2.1. *Semtechin määrittelemä kehys LoRa-tiedonsiirtoon. [2].*

LoRa-kehys alkaa esiviestillä, joka koostuu tasaisesta sarjasta ylöspäin suuntautuvia pulsseja, joiden sijainti kehyksessä on kuvassa 2.1 merkitty kohtaan esiviesti (engl. preamble). Kahta viimeistä pulssia voidaan käyttää kahden samalla taajuudella toimivan LoRa-verkon erottamiseen toisistaan, jolloin laitteet, jotka on konfiguroitu toiseen verkkoon, lakkaavat kuuntelemasta viestiä. Ylöspäin suuntautuvien pulssien jälkeen seuraa muutama alaspäin suuntautuva pulssi, jotka päättävät esiviestin. Kuvasta 2.2 voidaan erottaa ylös- ja alaspäin suuntautuvat pulssit esiviestissä. [2]



Kuva 2.2. *LoRa lähettimen signaalin taajuusvaihtelu ajan suhteen. [2].*

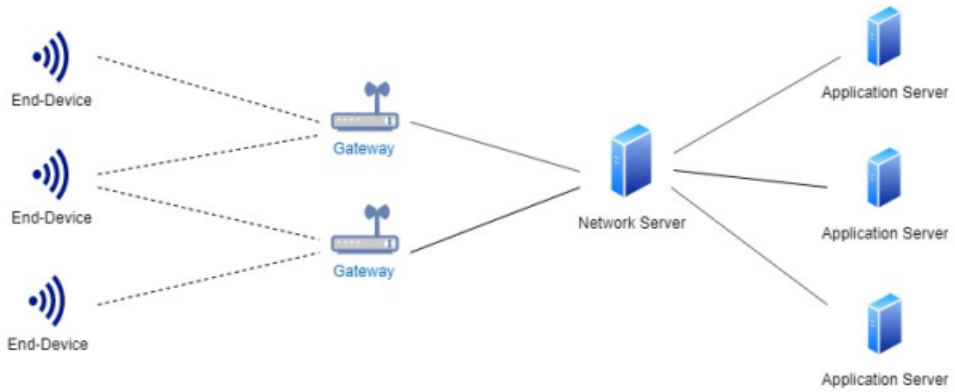
Esiviestin jälkeen seuraa vapaaehtoinen ylätunniste, joka on merkitty kuvassa 2.1 kehykseen kohtaan ylätunniste (engl. header). Esiviesti ilmaiseen sen, kuinka suuri tietosisältö viestillä on ja mitä koodinopeutta käytetään sekä onko viestin virheellisyyden varmistava tarkistussumma käytössä. Ylätunnisteen jälkeen seuraa tietosisältö, jossa siirrettävä data lähetetään. Tämä on merkitty kuvassa 2.1 kehykseen kohtaan tietosisältö (engl. payload). Viimeisenä kehyksen rakenteessa sijaitsee vapaaehtoinen tarkistussumma, jolla tarkistetaan, että lähetetty tietosisältö ei sisällä virheitä. Tämä on merkattu kuvan 2.1 kehyksessä kohtaan tarkistussumma (engl. Payload CRC). [2]

2.2 LoRaWan

LoRaWan on ohjelmistoviestintäprotokolla, joka on kehitetty fyysisen LoRa-kerroksen päälle. LoRaWan-verkko rakennetaan yleensä tähti-verkkotopologian mukaan ja se koostuu päätelaitteista, yhdyskäytävästä, verkkopalvelimesta, sovelluspalvelimesta sekä liityntäpalvelimesta. Näitä laitteita hyödyntäen tiedonsiirto päätelaitteelta onnistuu muualle verkkoon. [1]

LoRaWan-teknologiaa hallinnoi LoRa Alliance. Ensimmäinen versio 1.0 julkaistiin vuonna 2015. Yhteensä versioita on julkaistu kuusi kappaletta, joista viimeisin 1.0.4 vuonna 2020. LoRaWan-versioiden välillä on eroja ja etenkin vanhemmista versioista on löydetty useita tietoturvauhkia, joita on paikattu myöhemmissä päivityksissä. Kuitenkin vuonna 2021 iso osa markkinoilla olevista laitteista hyödynsi jotain muuta LoRaWan-versioita kuin 1.1 tai 1.0.4, joita suositellaan käytettäväksi tällä hetkellä uusissa järjestelmissä. Fyysisten laitteistovaatimusten muutoksien takia vanhoja laitteita ei voida päivittää käyttämään uudempia LoRaWan-versioita. [5]

Vuosina 2015 ja 2016 julkaistut LoRaWan-versiot 1.01 ja 1.0.2, eivät tuoneet merkittäviä muutoksia verrattuna aikaisempaan versioon 1.0. Näissä versiossa pyrittiin tarkentamaan dokumentaatiossa muutamia epäselvyyksiä sekä keskityttiin parantamaan joitain siirtoyhteyskerroksen (engl. Medium Access Control, MAC) komentoja. Vuonna 2017 julkaistu versio 1.1 muutti verkon arkkitehtuuria lisäämällä uuden liittymispalvelimen (Join Server), jonka tehtävänä on hallita verkon yli tapahtuvia aktivointeja ja hallita istuntoavaimia. Lisäksi versiossa 1.1 korjattiin aikaisempien versioiden haavoittuvuuksia. Vuosina 2018 ja 2020 julkaistut versiot 1.0.3 ja 1.0.4 toivat käyttöön joitakin ominaisuuksia versiosta 1.1 sekä muuttivat hieman komentoja. Versiossa 1.0.4 tuotiin myös joitakin tietoturvaan liittyviä parannuksia. [6]



Kuva 2.3. *LoRaWan verkon arkkitehtuuri. [7] .*

LoRaWan-verkko perustuu yleensä tähti-verkkotopologiaan, jossa päätelaitteet välittävät viestejä verkossa oleville reitittimille kuvan 2.3 mukaisesti. Päätelaitteet eivät ole yhtey-

dessä yksittäisiin reitittimiin, joten sama viesti voi päätyä useammalle reitittimelle. Reitittimien tehtävä on vastaanottaa saapunut viesti ja välittää se IP-protokollaa hyödyntäen verkkopalvelimelle, joka on LoRaWan-verkon aivot. Verkkopalvelimen tehtävä on analysoida jokainen saapunut viesti ja välittää se oikealle sovelluspalvelimelle. Sovelluspalvelimen tehtävä on käsitellä saapunut viesti sen käyttötarkoituksen mukaisesti. Verkkopalvelin myös analysoi ja poistaa virheelliset viestit sekä kaksoiskappaleet, mikäli päätelaitteen viestin on vastaanottanut useampi reititin. [7] LoRaWan-versiossa 1.1 verkon topologiaan lisättiin myös liittymispalvelin, joka on yhteydessä verkkopalvelimeen. Liittymispalvelimen tehtävänä on varmistaa päätelaitteen aitous ja toimittaa istunnon avaimet laitteen rekisteröintivaiheessa. [7].

LoraWan päätelaitteet on jaettu kolmeen eri luokkaan A, B ja C sen perusteella miten ne toimivat MAC-verkkokerroksella. Näiden eri luokkien laitteiden välillä on eroja muun muassa akunkeston ja viiveen suhteen. Päätelaitteiden jakaminen eri luokkiin mahdollistaa sen, että eri luokkien laitteita voidaan soveltaa eri tilanteisiin. Jossain tilanteissa lyhyt viive on tärkeämpää, kuin sähkönkulutus, toisissa tilanteissa taas laitteilta vaaditaan pidempää akunkestoa. [2]

Luokan A päätelaitteet lähettävät viestin (Up-Link) reitittimelle ja lähettämisen jälkeen avaavat kaksi vastaanottoikkunaa, jolloin päätelaite voi vastaanottaa palvelimelta tulevia viestejä. Luokan A laitteet ovat yleensä paristoilla toimivia ja erittäin energiatehokkaita. Luokan B päätelaitteet toimivat pitkälti samalla tavalla A luokan laitteet, mutta kahden vastaanottoikkunan lisäksi on erikseen mahdollista ajastaa vielä erillinen ikkuna, jolloin voidaan vastaanottaa verkkopalvelimelta tulevia viestejä. Luokan C laitteet ovat lähes jatkuvassa vastaanottovalmiudessa, mikä lisää niiden energiankulutusta huomattavasti. Siitä syystä ne ovatkin yleensä kytkettynä verkkovirtaan. Luokan C laitteet pystyvät vastaanottamaan viestejä jatkuvasti, jolloin viive palvelimen ja päätelaitteen välillä pienenee merkittävästi.[7][10]

LoRaWan-protokollapino koostuu jo aiemmin mainitusta fyysisestä LoRa-kerroksesta, MAC-kerroksesta sekä sovelluskerroksesta. MAC-kerroksen kehys alkaa MAC-otsikolla, joka määrittää viestin tyypin sekä kehyksen muodon. MAC-hyötykuorma taas sisältää käyttäjän datan, käytössä olevan LoRaWan-version sekä viestin tyypin. Kehyksen lopussa olevaa viestin eheyskoodin (engl. Message Integrity Code, MIC) -arvoa käytetään MAC-otsikon ja hyötykuorman eheyden tarkistamiseen, jotta voidaan varmistua siitä, että kehyksen sisältö tai lähde ei ole muuttunut matkan aikana. [10]

LoRaWan-protokollapinon sovelluskerroksen kehys sisältää seuraavat kentät: kehyksen ylätunniste (FHDR), valinnainen porttikenttää (FPort) ja valinnainen kehyksen hyötykuorma (FRMPayload). Kehyksen ylätunniste sisältää osoitteen, jonka avulla päätelaite voidaan tunnistaa. Otsikkokenttä sisältää myös kontrolli- ja kehyslaskurikentän, joiden avulla voidaan hallita esimerkiksi datan nopeutta ja pitää lukua lähetettyjen Up-Link ja Down-

Link viestien määrästä. Otsikon viimeisen kentän avulla voidaan lähettää erinäisiä MAC-komentoja. Otsikon lisäksi valinnainen porttikenttä määrittelee, sisältääkö kehys pelkästään MAC-komentoja vai myös muuta dataa. Kehyksen viimeinen kenttä sisältää itse kehyksen viestin salatussa muodossa. [10]

3. LORAWANIN TIETOTURVA

LoRaWan-verkkoteknologiassa on panostettu tietoturvaan usealla eri tasolla, jotta viestien vaihto olisi mahdollisimman turvallista. Keskeisimmät teknologiaan liittyvät tietoturvatoimenpiteet liittyvät yhteyksien salaukseen ja päätelaitteiden rekisteröintiin. Tässä luvussa perehdytään tarkemmin näihin aihepiireihin ja sen lisäksi käydään läpi mahdollisia tietoturvauhkia, jotka voivat vaikuttaa näiden osa-alueiden turvallisuuteen.

3.1 Salaus

LoRaWan-teknologian salaus perustuu 128-bittiseen Advanced Encryption Standardiin (AES), joka on toteutettu kahdessa kerroksessa salaten näin koko yhteyden päätelaitteelta sovelluspalvelimelle. AES-128 salausta voidaan toistaiseksi pitää vielä turvallisena, mutta on esitetty epäilyksiä siitä, että kvanttitietokoneiden tarjoaman lisääntyneen laskentakyvyn vuoksi 128-bittinen salaus voitaisiin purkaa jopa lähitulevaisuudessa. Tätä voidaan pitää riskinä LoRaWanin tietoturvalle, kun otetaan huomioon laitteiden suunniteltu pitkä akunkesto ja käyttöikä. On arvioitu, että Grooverin algoritmin avulla AES-128 salaus voitaisiin purkaa tilanteessa, jossa kvanttitietokoneen laskentateho olisi 2 953 kubittia [14].

Vuoteen 2022 mennessä teknologiayhtiö IBM on julkistanut 433 kubittisen prosessorin ja se tavoittelee yli 4 158 kubitin laskentatehoa jo vuonna 2025. Toteutuessaan 4 158 kubitin laskentateho aiheuttaisi vaaran LoRaWanin salaukselle jo varsin nopeasti, mikäli kvanttitietokoneita haluttaisiin käyttää salauksien murtamiseen. AES-128 salauksesta AES-256 salaukseen siirtyminen kasvattaisi laitteiden energiankulutusta sekä hidastaisi salauksen nopeutta. Se myös tarkoittaisi merkittäviä päivityksiä verkkoarkkitehtuuriin, vaikka nykyinen LoRaWan-kehys sallisi myös korkeampitasoisen salauksen. [9][15]

Teknologian kaksikerroksinen salaus perustuu kahteen vaiheeseen, jossa salataan liikenne päätelaitteen ja verkkopalvelimen välillä sekä päätelaitteen ja ohjelmistopalvelimen välillä. Eheys ja luotettavuus päätelaitteen ja ohjelmistopalvelimen välissä saavutetaan sovellusistunnon avaimen (AppSKey) avulla. Eheys ja todennus taas tapahtuu verkkopalvelimen ja päätelaitteen välillä hyödyntäen verkkoistunnon avainta (NwkSKey). Mikäli laite tukee yli ilman aktivointia (engl. Over The Air Authentication, OTAA) on laitteella myös sovellusavain (AppKey), jota käytetään laitteen aktivointiprosessissa. Päätelaite ei

voi kuitenkaan liittyä verkkoon ilman erillistä aktivointia. [15]

3.2 Laitteiden rekisteröinti

Jotta LoRaWan-verkon reitittimet pystyvät lähettämään viestejä päätelaitteelta verkkopalvelimelle, tulee laitteiden olla rekisteröityneenä verkkoon. Ilman päätelaitteen rekisteröintiä päätelaitteiden lähettämät viestit eivät reitity verkossa verkkopalvelimelta eteenpäin. LoRaWan-päätelaitteiden rekisteröintiin on olemassa kaksi eri tapaa: yli ilman aktivointi (OTAA) sekä aktivointi personoimalla (engl. Activation By Personalization, ABP). [8]

OTAA-aktivointia voidaan lähtökohtaisesti pitää kaikissa tilanteissa parempana tapana rekisteröidä laite LoRaWan-verkkoon, sillä ABP-aktivointiin kohdistuu paljon ongelmia, jotka voivat aiheuttaa tietoturvariskejä. ABP-aktivointia ei suositella ollenkaan teollisiin sovellutuksiin sen heikon tietoturvan takia. [11]

Jokaisella LoRaWan-verkkoon kytkeytyvällä laitteella on oma 32-bittinen osoite (engl. Device Address, DevAddr), jolla laite pystytään tunnistamaan verkossa. Tämä osoite on joko ennalta määritetty tai se luodaan aktivointivaiheessa laitteelle. Osoite ei ole uniikki ja useammalla laitteella voi olla sama osoite, sillä laitteiden identifioiminen verkossa tapahtuu yhdistämällä DevAddr-osoite ja verkkoistunnon avain, joka on jokaisella laitteella uniikki. [8]

Aktivoinnissa personoimalla laite on tiukasti kytketty ennalta määritettyyn verkkoon ja sen vaihtaminen verkosta toiseen voi olla vaikeaa tai jopa mahdotonta. Siinä laitteen osoite ja istunnon avaimet on ennalta asetettu laitteelle, jolloin laite on automaattisesti rekisteröity verkkoon eikä erillistä ilman yli aktivointia tarvita. Yli ilman aktivoinnissa taas laitteen osoitetta tai istunnon avaimia ei ole määritelty ennalta, vaan istunnon avaimet generoidaan verkkopalvelimella tai liittymispalvelimella ja palautetaan sitten päätelaitteelle yhdessä muun informaation kanssa. [8]

ABP-aktivoinnissa on paljon erilaisia ongelmia verrattuna OTAA-aktivointiin ja siksi OTAA-aktivointia suositellaan käyttämään ensisijaisena aktivointitapana. ABP-päätelaitteissa istunnon avaimet on tallennettu suoraan laitteeseen, joten mikäli ne pääsevät vuotamaan, voi se aiheuttaa todellisen riskin verkon turvallisuudelle. OTAA-aktivointiin verrattuna myös ABP-laitteiden kehyslaskurit ovat ongelmallisia, sillä päätelaitteet voivat lähettää ja vastaanottaa kehyksiä vain rajallisen määrän. Maksimimäärän ylittäessä päätelaitetta ei voi enää käyttää ilman laskureiden alustusta, joka ei kaikissa laitteissa ole mahdollista ja alustamisen salliminen voi aiheuttaa tietoturvariskin. OTAA-aktivoinnissa laitteen yhdistyessä verkkoon, kehyslaskurit nollataan. Kehyslaskureita käytetään tietoturvasyistä, sillä niiden avulla sekä verkkopalvelin että päätelaite pystyvät seuraamaan lähetettyjen viestien määrää ja näin pyrkimään estämään uudelleenlähetyshyökkäykset. [13][5]

Aktivoinneissa ja salausavaimissa on hieman eroja LoRaWan versioiden 1.0.x ja 1.1 välil-

lä. LoRaWan versiossa 1.1 lisättiin arkkitehtuuriin erillinen liittymispalvelin, joka käsittelee päätelaitteiden liittymispyynnöt verkkopalvelimen toimiessa vain liittymisviestien välittäjänä. Tämän lisäksi myös istuntoavaimien määrää lisättiin kolmella. FNwkSIntKeyllä ja SNwkSIntKeyllä, joita käytetään MIC-arvon laskemiseen viestin eheyden varmistamiseksi ja NwkSEncKeytä, jota käytetään MAC-komentojen salaamiseen viestin luotettavuuden turvaamiseksi. [8]

4. LORAWAN TIEDETYT HAAVOITTUVUUDET

Tutkimuksissa on ilmennyt, että LoRaWan-verkkoon kohdistuu useita eri tietoturvauhkia, jotka voivat aiheuttaa riskin välitettyjen viestien luottamuksellisuudelle, yhteneväisyydelle ja saatavuudelle. Osa käsitellyistä uhista on korjattu teknologian myöhemmissä versioissa. Tässä luvussa käydään läpi yleisimpiä tiedossa olevia LoRaWan-verkkoon kohdistuvia uhkia sekä keinoja, miten niiltä on mahdollista suojautua, mikäli se on mahdollista.

4.1 LoRaWan-verkon häritseminen

Kuten lähes kaikki langattomat tietoverkot, myös LoRaWan on altis verkon häirinnälle. Häirinnällä tarkoitetaan tilannetta, jossa samalla taajuudella verkon peitealueella lähetetään vahvempaa signaalia, jonka tarkoituksena on sekoittaa tai pahimmassa tapauksessa estää päätelaitteen mahdollisuus lähettää viestejä reitittimelle. Verkon häirintä koskee kaikkia LoRaWan-versioita, sillä ne toimivat samalla taajuusalueella ja verkot rakennetaan versiosta riippumatta pitkälti samalla tavalla. Tutkimuksissa on havaittu, että häirintää on mahdollista tehdä myös halvoilla markettilaitteilla, mikä voi lisätä pahimmassa tapauksessa häirinnän määrää. [5]

Verkon häirintään on olemassa useita eri tapoja jatkuvan häirinnän lisäksi:

- **Aktivoituva häirintä**: Radioliikennettä seurataan jatkuvasti ja häirintää tapahtuu vasta sitten, kun verkossa havaitaan liikettä.[4].
- **Reagoiva häirintä**: Radioliikennettä seurataan jatkuvasti samalla kun viestejä vastaanotetaan. Laitteisto analysoi tulevat viestit siltä osin kuin ne ovat luettavissa ja käynnistää häirinnän vain, jos se täyttää ennalta määritellyt ehdot. Häirinnän jälkeen laite palaa taas vastaanottotilaan odottamaan seuraavaa ehdot täyttävää viestiä. [4].
- **Madonreikä hyökkäys**: Laitteisto on kykenevä vastaanottamaan sekä häiritsemään samaan aikaan. Tämä mahdollistaa sen, että viesti voidaan kaapata ja sitä voidaan säilyttää niin kauan, kunnes nähdään tarve lähettää viesti sen oikealle alkuperäiselle vastaanottajalle. [4].

Verkon häiritsemisen tehokkuus riippuu paljon verkon rakenteesta, sillä se riippuu pitkälti siitä pystytäänkö yhteyttä päätelaitteen ja reitittimien välillä häiritsemään. Mikäli yksikin

reititin pystyy vastaanottamaan päätelaitteen viestin, on silloin verkon häirintä tehotonta. Häirintää pystytäänkin ehkäisemään luomalla mahdollisimman tiheä verkko, jossa reitittimien kuuluvuusalueet ovat osittain päällekkäin ja siten useamman reitittimen on mahdollista vastaanottaa päätelaitteen viesti ja ohjata se eteenpäin verkkopalvelimelle. Madonreikä hyökkäys voidaan välttää pienentämällä taajuutta ja paketin kokoa, jolloin pienempi lähetysaika pystyy voittamaan häirintälaitteiston. Verkon häirintä ei aiheuta uhkaa viestin luottamuksellisuuteen tai yhteneväisyyteen, mutta sen vaikutus saatavuuteen on erittäin korkea. [5]

4.2 Uudelleentoistohyökkäys ABP-aktivoiduilla laitteilla

Kuten aikaisemmin on mainittu, LoRaWan-verkkoon ABP-aktivoiduissa laitteissa käytetään aina ennalta asetettuja istuntoavaimia sekä laitteen osoitetta. Tämä aiheuttaa haavoittuvuuden uudelleentoistohyökkäyksille tilanteissa, joissa kehyslaskuri nollaantuu. Uudelleentoistohyökkäyksessä on tarkoituksena kaapata päätelaitteen ja verkkopalvelimen välisestä keskustelusta viesti, jossa kehyslaskurin arvo on mahdollisimman korkea. [5]

LoRaWan versioon 1.0.3 asti sallittiin päätelaitteiden kehyslaskureissa käytettävän haihtumatonta NVM-muistia, joka ei pysty säilyttämään tietoa muistissaan tilanteissa, joissa virta muistipiirille katkeaa [5]. Virran katketessa päätelaitteen kehyslaskuri nollaantuu ja lähetettyjen sekä vastaanotettujen kehysten laskeminen alkaa alusta. Kehyslaskurin nollaantuminen on mahdollista havaita, sillä nollaantuminen välitetään verkkopalvelimelle selkokielisenä tekstinä. Kun aikaisemmasta keskustelusta kaapattu viesti korkealla kehyslaskurin arvolla lähetetään uudelleen verkkopalvelimelle, merkitsee verkkopalvelin nykyiseksi kehyksen arvoksi juuri saapuneen arvon. Tämän jälkeen verkkopalvelin hylkää päätelaitteelta tulevat oikeat viestit niin kauan, kunnes saapuvan viestin kehyslaskurin arvo on suurempi kuin arvo, joka kaapatun viestin avulla verkkopalvelimelle asetettiin. [4]

Tämä hyökkäys vaikuttaa erityisesti viestien saatavuuteen, sillä sen avulla voidaan estää yksittäisten viestien vastaanottaminen päätelaitteilta pitkäksi aikaa. Hyökkäykseen ei myöskään tarvita erityisen kallista ammattilaislaitteistoa, vaan muutamien satojen eurojen välineet, joilla pystytään vastaanottamaan sekä lähettämään viestejä LoRaWan-verkossa riittävät. [16] Hyökkäys on korjattu LoRaWan versioissa 1.1 ja 1.0.4 estämällä kokonaan mahdollisuus kehyslaskurin nollaamiselle laitteen elinkaaren aikana. Versio 1.1 on kuitenkin edelleen haavoittuvainen hyökkäykselle, mikäli päätelaitetta ajetaan taaksepäin yhteensopivassa tilassa. [5]

4.3 Salakuuntelu

LoRaWanin salaus perustuu AES-salaukseen laskuri (engl. Counter Mode, CTR) -tilassa, jossa salauksen syötteenä käytetään kehyslaskurin arvoa. Koska ABP-aktivoiduissa pää-

telaitteissa osoite ja istuntoavaimet eivät muutu, käytetään lohkosalausmenetelmässä aina laitteen uudelleenkäynnistyessä samaa avainmateriaalia. Tätä materiaalia hyväksikäyttäen hyökkääjän on mahdollista purkaa samalla avainmateriaalilla salattu toinen viesti. Hyökkäyksen onnistumiseen vaaditaan kuitenkin se, että hyökkääjä pystyy päättelemään ensimmäisen viestin sisällön selkokielisenä. Ilman tätä tietoa toista samalla avainmateriaalilla salattua viestiä ei voi purkaa. Mitä enemmän päätelaitteen uudelleenkäynnistyksiä tehdään ja samoja avainmateriaaleja käytetään, sitä helpompaa viestien purkamisesta tulee. [4]

Viestien salakuuntelu on mahdollista vain LoRaWan versioon 1.0.3 asti ja versiossa 1.1 mikäli päätelaitetta ajetaan taaksepäin yhteensopivassa tilassa. Riskiä sille, että viestin luottamuksellisuus vaarantuisi hyökkäyksen takia voidaan pitää varsin pienenä, sillä ensimmäisen viestin arvaaminen selkokielisenä vaatii todella hyvän ymmärryksen hyökkäyksen kohteena olevasta järjestelmästä tai arvauksen siitä mitä MAC-komentoa päätelaitteelta lähetetään. [4]

Hyökkäykseltä on myös mahdollista suojautua käyttämällä OTAA-aktivointia päätelaitteita aktivoitaessa. Mikäli ABP-aktivointia kuitenkin käytetään, on perusteltua käyttää LoRaWan-teknologian uudempia versioita, joista on poistettu kokonaan mahdollisuus kehyslaskureiden nollaantumiselle [8]. Vanhoja versioita käytettäessä voi olla myös järkevää suojata laite siten, että sen sähkönsaanti on turvattu, jolloin riski kehyslaskurin nollaantumiselle pienenee. Tällä tavoin salakuunteluhyökkäksen toteuttamisesta tulee huomattavasti haastavampaa, kun samoja avainmateriaaleja käytetään vähemmän. [5]

4.4 Bitinkääntöhyökkäys

Vaikka LoRaWanissa on pyritty huolehtimaan viestin eheydestä sekä luottamuksellisuudesta, puuttuu teknologiasta silti kokonaan viestin eheyden tarkistus päätelaitteen ja sovelluspalvelimen välillä. Tämä johtaa siihen, että ainoastaan viestin saapuessa päätelaitteelta verkkopalvelimelle, tarkastetaan viestin eheys. Viestin jatkaessa matkaa verkkopalvelimelta sovelluspalvelimelle, ei viestin sovelluspalvelin voi kuitenkaan varmistua viestin eheydestä. Tämä altistaa LoRaWanin kautta kulkevat viestit bitinkääntöhyökkäykselle (engl. bit flipping attack). [4]

LoRaWan verkon AES-salausta käytetään CTR-moodissa, jossa salausta käytetään avainmateriaalin luomiseen ja luotua materiaalia hyödynnetään sen jälkeen viestin salauksessa. Salausta näin käytettäessä ei yksittäisen bitin muuttaminen normaalista AES-salauksesta poiketen kuitenkaan aiheuta lumivyöryefektiä, jossa yksittäisen bitin muokkaaminen sekoittaisi koko viestin sisällön. Tämä aiheuttaa sen, että hyökkääjän on varsin helppo muokata lähetetyn viestin sisältöä, mikäli lähetetyn viestin rakenne on tiedossa. Tutkimuksissa on onnistuttu muokkaamaan esimerkiksi päätelaitteen osoitetta, yksittäisen sensorin lähettämää lämpötilaa tai kehyslaskurin lukuarvoa. Kuten aiemmin on mai-

nittu, kehyslaskurin lukuarvoa nostamalla voidaan estää kokonaan päätelaitteen lähettämien viestien vastaanottaminen verkkopalvelimella. [16]

Bitinkääntöhyökkäykselle ovat alttiita kaikki LoRaWan-versiot ja sitä voidaan pitää varsin merkittävänä tietoturvauhkana, sillä eheyden varmistuksen puutteesta johtuen nykyisillä versiolla ei ole mahdollista varmistaa, että viestiä ei ole muutettu verkko- ja sovelluspalvelimen välillä. Hyökkäys vaatii kuitenkin onnistuakseen sen, että palvelimien välinen yhteys ei ole turvallinen. Mikäli salauksesta on palvelimien välillä huolehdittu ja verkkopalveluntarjoajaan voidaan luottaa, ei suurta riskiä bitinkääntöhyökkäykselle ole. [4]

4.5 ACK-huijaus

Vastaanottoviestihyökkäyksessä (engl. Acknowledgement, ACK) on tarkoitus hyödyntää LoRaWanin ongelmaa, jossa päätelaitteelta lähetetyn viestin ja verkkopalvelimelta palaavan ACK-viestin välillä ei ole yhteyttä. ACK-viesti on viesti, joka välitetään verkkopalvelimelta reitittimen kautta päätelaitteelle ja se sisältää tiedon siitä, että viesti on vastaanotettu onnistuneesti. Tässä hyökkäyksessä hyödynnetään valikoivaa häirintää ja ACK-viestin kehyslaskuria, joka sisältää arvon siitä, montako viestiä verkkopalvelimelta on lähetetty päätelaitteelle. [4]

Hyökkäys kohdistuu tilanteeseen, jossa päätelaitteen lähettämä viesti on saapunut verkkopalvelimelle ja verkkopalvelin kuittaa saapuneen viestin ACK-viestillä ja lähettää sen takaisin. Hyödyntäen valikoivaa häirintää ACK-viesti kaapataan reitittimen ja päätelaitteen välillä ja häiritsemällä estetään viestin saapuminen päätelaitteelle. Päätelaite yrittää tämän jälkeen lähettää viestin uudestaan, mutta lopulta päättelee tämän jälkeen viestin olevan kadonnut. Kun päätelaitteelta lähetetään uusi viesti, voidaan viestin saapuminen estää häiritsemällä, jolloin verkko- ja sovelluspalvelimet eivät koskaan vastaanota viestiä. Hyökkääjä voi kuitenkin tässä tilanteessa toistaa kaapatun ACK-viestin, jolloin päätelaite luulee, että viesti vastaanotettiin onnistuneesti. [16]

Hyökkäystä voidaan pitää haitallisena tilanteissa, joissa estetään kriittisen datan välittyminen verkkopalvelimelle. Tällä hyökkäyksellä ei kuitenkaan ole vaikutusta esimerkiksi viestin eheyteen tai luottamuksellisuuteen ja se on estetty LoRaWanin versiossa 1.1. Mikäli käytetään aikaisempia versiota tai versiota 1.1 taaksepäin yhteensopivassa tilassa tulisi huolehtia siitä, että kriittiset viestit lähetetään useaan kertaan ja ohjelmisto rakennetaan siten, että se ei luota liikaa saapuviin ACK-viesteihin. [5]

4.6 ADR-huijaus

Mukautuvan tiedonsiirtonopeuden (Adaptive Data Rate, ADR) hyökkäyksessä on tarkoituksena huijata päätelaitetta käyttämään heikkoa lähetystehoa sekä tiedonsiirtonopeutta ja siten pyrkiä aiheuttamaan tilanne, jossa lähetetyt viestit eivät päädy päätelaitteelta rei-

tittimelle liian heikon lähetystehon takia. [5]

LoRaWanin ADR-ominaisuuden tarkoituksena on löytää sopiva lähetysteho ja lähetysaika päätelaitteen ja reitittimen välille. Hyökkäyksessä pyritään häiritsemään ja kaappaamaan päätelaitteen lähettämä ADR-alustusviesti ja muokkaamaan sen metadataa siten, että verkkopalvelimen analysoinnin jälkeen se asettaisi paluuviestiin mahdollisimman heikot lähetysparametrit. Kun hyökkääjä on kaapannut viestin ja muokannut sen sisältämää dataa, lähetetään viesti eteenpäin verkkopalvelimelle. Palvelin lähettää dataan perustuen takaisin päätelaitteelle ADR-vastausviestin, joka sisältää päätelaitteelle asetettavat lähetysparametrit. Päätelaite ottaa käyttöön verkkopalvelimelta tulleet asetukset ja tämän jälkeen lähetysteho on niin heikko, että reititin ei pysty enää vastaanottamaan päätelaitteen viestejä. [5]

Tällä hyökkäyksellä on vakavat vaikutukset saatavuuteen, sillä sen avulla voidaan estää kokonaan yksittäisen päätelaitteen lähettämät viestit. Haavoittuvuutta ei ole myöskään korjattu uudemmissa LoRaWan-versioissa ja ainoa keino hyökkäykseltä puolustautumiseen on ottaa ADR-ominaisuus kokonaan pois käytöstä ja asettaa lähetysparametrit manuaalisesti.[5]

4.7 Fyysiset hyökkäykset

LoRaWan-päätelaitteita käytetään monesti laajalla alueella ja osa laitteista ei välttämättä ole suojattu siten, että hyökkääjä ei voisi päästä niihin fyysisesti käsiksi. Vaikka fyysisistä hyökkäyksistä suoraan johtuvat ongelmat eivät olekaan varsinaisesti teknologiasta johtuvia, voivat nekin aiheuttaa isoja riskejä viestien saatavuudelle ja luotettavuudelle. Esimerkiksi päätelaitteiden vanhemmissa versioissa sähkönsyötön katkaiseminen aiheuttaa NVM-muistin nollaantumisen ja sitä kautta myös riskin uudelleentoistohyökkäykselle ABP-aktivoiduilla laitteilla. Muita fyysisiä hyökkäyksiä ovat muun muassa varastaminen tai laitteen vahingoittaminen, turvaparametrien varastaminen tai laiteohjelmiston päivittäminen. [5]

Päätelaitteelle suurin fyysinen uhka tulee todennäköisesti hajoamisesta tai varastamisesta. Päätelaitteita säilytetään monesti paikoissa, joissa ne ovat alttiita sääolosuhteille tai ihmisen vahingolliselle tai tahalliselle toiminnalle. Joku päätelaitteesta tietämätön ihminen saattaa vahingossa poistaa sen käytöstä tai rankkasade voi rikkoa päätelaitteen herkät elektroniikat. Päätelaitteen katoaminen tai hajoaminen aiheuttaa vakavan riskin saatavuudelle ja se voi esimerkiksi johtaa tilanteeseen, jossa jonkin sensorin tietoja ei enää pystytä vastaanottamaan. [4]

Turvaparametrien varastamisessa hyökkääjä yrittää päästä käsiksi sarjaportin kautta päätelaitteelta lähetettyyn dataan sillä päätelaitteissa ei ole sisäänrakennettua salausta. Sarjaportin kautta hyökkääjä voi myös asentaa laitteeseen päivitetyn vahingollisen laiteohjel-

miston, joka voi pahimmassa tilanteessa mahdollistaa avainten uudelleenkäytön. Avainten uudelleenkäyttöä hyväksikäyttäen hyökkääjän on mahdollista päästä käsiksi esimerkiksi sensoridataan sekä syöttää päätelaitteen kautta verkkoon virheellisiä viestejä. Tämä hyökkäystapa on riski viestien luottamuksellisuudelle. [5]

Fyysisiltä hyökkäyksiltä on mahdollista suojautua varsin helposti sijoittamalla päätelaitteet turvallisiin paikkoihin ja sääolosuhteilta suojaan. Laitteet kannattaa suojata siten, että hyökkääjän on vaikeaa päästä fyysisesti käsiksi laitteen sarjaporttiin tai mikropiireihin. Mikäli päätelaitteisiin käsiksi pääseminen on tehty vaikeaksi, on niihin hyökkääminenkin vaikeampaa ja enemmän aikaa vievää ja siten suojaa verkkoa paremmin. [5]

4.8 Muita tiedossa olevia hyökkäyksiä

Edellä käytyjä hyökkäystapoja voidaan pitää yleisimpinä sekä vaarallisimpina LoRaWaniin kohdistuvina hyökkäyksinä ja nämä hyökkäykset toistuvat myös eniten tutkimuksissa ja tieteellisessä kirjallisuudessa. Teknologiaan kohdistuu kuitenkin huomattavasti laajempi määrä erilaisia hyökkäyksiä, jotka on joko vasta löydetty, niitä ei ole vielä keretty tutkia tai niiden ei nähdä aiheuttavan niin suurta riskiä teknologian turvallisuudelle. Seuraavaksi on listattu lyhyesti muita hyökkäyksiä, joita teknologiaan voi kohdistua.

- **Sivukanavahyökkäys (engl. Side-channel attack)**: Tutkimuksissa on todettu, että päätelaitteen elektromagneettista säteilyä seuraamalla ja tietoa LoRaWan-protokollan toiminnasta hyväksikäyttämällä, voidaan AppSKey muodostaa päätelaitteesta alle 100 viestin lähetyksen jälkeen, kun päätelaite on rekisteröity ABP-tilassa. [5]
- **LoRaWan B-luokan laitteisiin kohdistuvat hyökkäykset**: LoRaWan-teknologian B-luokan laitteisiin voidaan kohdistaa hyökkäyksiä, joiden avulla on mahdollista selvittää tai huijata reitittimen sijainti tai lisätä päätelaitteen virran kulutusta lisäämällä turhien sensoriherätysten määrää.
- **Verkon tulvaaminen**: LoRaWan-verkkoon lähetetään yksittäiseltä päätelaitteelta viestejä suuria määriä, joiden tarkoitus on hidastaa verkon toimintaa lisäämällä aikaa, joka turhien viestien käsittelyyn kuluu. [5]
- **Verkon liikenteen seuraaminen**: Hyökkääjä voi seurata liikennettä ottamalla käyttöön oman reitittimen, jonka tarkoituksena on seurata LoRaWan-verkossa liikkuvia viestejä. Viestiliikennettä analysoimalla voidaan muodostaa joitakin tietoja esimerkiksi viestien sisällöstä. [5]

5. YHTEENVETO

Tässä kirjallisuuskatsauksessa tutkittiin LoRaWan-verkkoteknologian soveltuvuutta kriittisen tiedon välittäjänä. Tutkielmassa käytiin lyhyesti läpi perustiedot teknologiasta, sen salauksesta sekä perehdyttiin syvällisemmin tiedossa oleviin LoRaWania koskeviin tietoturvauhkiin. Jokaisen tarkemmin läpi käydyn tietoturvauhan kohdalla käsiteltiin myös sitä, miten hyökkäykseltä on mahdollista puolustautua ja millaiset vaikutukset sillä on teknologian tietototurvaan luottamuksellisuuden, yhteneväisyyden ja saatavuuden näkökulmasta.

Tutkielmassa havaittiin, että muiden langattomien tiedonsiirtoteknologioiden tavoin myös LoRaWan on altis häirinnälle ja siihen kohdistuu paljon myös muita tietoturvauhkia. Suurin osa näistä uhista koskee viestin saatavuutta, mutta myös viestin manipulointi ja muuttaminen selkokieliseksi on jossain tapauksissa mahdollista. Osa hyökkäyksistä on mahdollista toteuttaa ilman kalliita ammattilaisvälineitä ja monessa tapauksessa vain muutaman sadan euron tarvikkeet riittävät. Tutkielmassa kuitenkin havaittiin, että salattujen viestien muuttaminen selkokieliseksi on mahdollista vain harvoissa tapauksissa ja näissäkin tilanteissa hyökkääjällä täytyy olla jonkinlainen käsitys hyökkäyksen kohteena olevasta verkosta sekä siitä, millaisia viestejä verkossa liikkuu.

Tutkielma osoittaa, että LoRaWan-teknologian hyödyntämiseen kriittisen tiedon välittäjänä on syytä suhtautua varauksella. Etenkin tilanteissa, joissa viestin saatavuus on erittäin tärkeää ja viestin tulee saavuttaa vastaanottajansa jokaisessa tilanteessa, ei välttämättä kannata hyödyntää LoRaWania tai muutakaan langatonta verkkoteknologiaa. Mikäli teknologiaa halutaan kuitenkin käyttää, tulisi verkko rakentaa uudempien LoRaWan-versioiden 1.0.4 tai 1.1 varaan sekä suojata päätelaitteet siten, että niihin ei pääse kohdistumaan fyysistä uhkaa. Suurin osa tässä tutkielmassa käsitellyistä teknologiaa koskevista tietoturvauhista on korjattu uudemmissa versioissa. Häirinnältä on mahdollista suojautua jossain määrin sijoittamalla reitittimiä siten, että niiden kuuluvuusalueet ovat hieman toistensa päällä. Näin yhden reitittimien ollessa häirinnän kohteena, jokin toinen kuuluvuusalueella oleva reititin voi vastaanottaa päätelaitteen viestin.

LoRaWan on omiaan tilanteissa, joissa päätelaitteilta vaaditaan hyvää kuuluvuutta, akunkestoa ja halpaa hintaa. Sen takia teknologiaa hyödynnetäänkin nykyään esimerkiksi sähkö- ja vesimittareissa sekä erilaisten sensorien lukemien välittämisessä. Tällaisissa

tilanteissa yksittäisen viestin katoaminen ei ole maailmanloppu ja toisaalta myöskään viestien sisältö ei ole sellainen, että hyökkääjät käyttäisivät sen murtamiseen resursseja. Koska LoRaWan-viestin muuttaminen selkokielelle on nykyisen tutkimustiedon valossa hankalaa, uskaltaa verkkoa hyödyntää myös kriittisempien viestien lähettämiseen. Kuitenkin teknologian soveltamisessa esimerkiksi kriittisten järjestelmien kuten patojen tai pumppujen ohjaamiseen kannattaa suhtautua varauksella, sillä on mahdollista, että päätelaitteelta lähetetty viesti ei koskaan päädy vastaanottajalle.

LÄHTEET

[1] LoRa Alliance™. ”LoRaWAN™ 1.1 Specification” (2017). URL: https://lora-alliance.org/resource_hub/lorawan-specification-v1-1/.

[2] Aloÿs Augustin et al. ”A Study of LoRa: Long Range amp; Low Power Networks for the Internet of Things”. *Sensors* 16.9 (2016). ISSN: 1424-8220. DOI: 10.3390/s16091466. URL: https://www.mdpi.com/1424-8220/16/9/1466.

[3] Guillaume Ferré ja Audrey Giremus. ”LoRa Physical Layer Principle and Performance Analysis”. Teoksessa: *2018 25th IEEE International Conference on Electronics, Circuits and Systems (ICECS)*. 2018, s. 65–68. DOI: 10.1109/ICECS.2018.8617880.

[4] Frank Hessel, Lars Almon ja Matthias Hollick. ”LoRaWAN Security: An Evolvable Survey on Vulnerabilities, Attacks and their Systematic Mitigation”. eng. *ACM transactions on sensor networks* (2023). ISSN: 1550-4859.

[5] Franz Kuntke et al. ”LoRaWAN security issues and mitigation options by the example of agricultural IoT scenarios”. eng. *Transactions on emerging telecommunications technologies* 33.5 (2022). ISSN: 2161-3915.

[6] Slim Loukil et al. ”Analysis of LoRaWAN 1.0 and 1.1 Protocols Security Mechanisms”. *Sensors* 22.10 (2022). ISSN: 1424-8220. DOI: 10.3390/s22103717. URL: https://www.mdpi.com/1424-8220/22/10/3717.

[7] Poliana de Moraes ja Arlindo Flavio da Conceição. ”A Systematic Review of Security in the LoRaWAN Network Protocol”. eng. *arXiv.org* (2021). ISSN: 2331-8422.

[8] The Things Network. *Learn about LoRaWAN®*. URL: https://www.thethingsnetwork.org/docs/lorawan/ (viitattu 15. 05. 2023).

[9] IBM Newsroom. *BM Unveils 400 Qubit-Plus Quantum Processor and Next-Generation IBM Quantum System Two*. 2022. URL: https://newsroom.ibm.com/2022-11-09-IBM-Unveils-400-Qubit-Plus-Quantum-Processor-and-Next-Generation-IBM-Quantum-System-Two (viitattu 15. 05. 2023).

[10] Hassan Noura et al. ”LoRaWAN security survey: Issues, threats and possible mitigation techniques”. eng. *Internet of Things* 12 (2020), s. 100303–. ISSN: 2542-6605.

[11] Ondrej Pospisil et al. ”Testbed for LoRaWAN Security: Design and Validation through Man-in-the-Middle Attacks Study”. eng. *Applied sciences* 11.16 (2021), s. 7642–. ISSN: 2076-3417.

[12] Amir Rahmani, Suleyman Bayramov ja Behnam Kiani Kalejahi. ”Internet of Things Applications: Opportunities and Threats”. *Wireless Personal Communications* 122 (tammikuu 2022). DOI: 10.1007/s11277-021-08907-0.

[13] The Things Stack. *ABP vs OTAA*. 2023. URL: https://www.thethingsindustries.com/docs/devices/abp-vs-otaa/ (viitattu 15. 05. 2023).

[14] Tsuyoshi Takagi. ”Applying Grover’s Algorithm to AES: Quantum Resource Estimates”. eng. Teoksessa: *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*. Vol. 9606. Lecture Notes in Computer Science. Switzerland: Springer International Publishing AG, 2016, s. 29–43. ISBN: 3319293591.

[15] Phithak Thaenkaew, Bruno Quoitin ja Ahmed Meddahi. ”Evaluating the cost of beyond AES-128 LoRaWAN security”. Teoksessa: *2022 International Symposium on Networks, Computers and Communications (ISNCC)*. 2022, s. 1–6. DOI: 10.1109/ISNCC55209.2022.9851811.

[16] Xueying Yang et al. ”Security Vulnerabilities in LoRaWAN”. Teoksessa: *2018 IEEE/ACM Third International Conference on Internet-of-Things Design and Implementation (IoTDI)*. 2018, s. 129–140. DOI: 10.1109/IoTDI.2018.00022.