Satakunnan ammattikorkeakoulu
Satakunta University of Applied Sciences

TOMI SAINE

LoRaWAN-verkko sensoridatan hyödyntämiseen

TIETOJENKÄSITTELYN KOULUTUSOHJELMA

2020

Tekijä(t) Saine, Tomi	Julkaisun laji Opinnäytetyö, AMK	Päivämäärä toukokuu 2020
	Sivumäärä 27	Julkaisun kieli suomi

Julkaisun nimi
LoRaWAN-verkko sensoridatan hyödyntämiseen

Tutkinto-ohjelma
Tietojenkäsittelyn koulutusohjelma

Tiivistelmä
LoRaWAN (Low Power Wide-Area Network) -verkko on vähätehoiseen tiedonsiirtoon tarkoitettu langaton tiedonsiirtoverkko, joka perustuu LPWAN (Long Range Wide-Area Network) -verkkoteknologiaan. Se on yksi monista käytettävissä olevista LPWAN-verkoista. Langeton LoRaWAN-verkko toimii tietyllä taajuusalueella, joka tarjoaa muutamia eri datanopeuksia. Liikenne päätelaitteiden ja verkon välillä turvataan salausavaimilla. Työn tavoitteena oli rakentaa LoRaWAN-verkko, jonka kautta päätelaitteena toimiva sensori lähettäisi dataa tietokantaan. Työ toteutettiin yhteistyössä WiseNetwork Oy:n kanssa. Työssä käytettiin Digitan IoT-verkkoa ja Actility ThingPark –sovellusta, joka vastaanotti sensorin lähettämän datan kymmenen minuutin välein. Data lähetettiin edelleen WiseNetworkin MySQL-tietokantaan. LoRaWAN-verkko saatiin toimimaan ja lähettämään dataa tavoitteiden mukaisesti.

Alueverkot, langattomat verkot, esineiden internet

Author(s)
Saine, Tomi

Type of Publication
Bachelor's thesis
ThesisAMK

Date
May 2020

Number of pages
27

Language of publication:
Finnish

Title of publication
LoRaWAN network for sensor data utilization

Degree programme
Degree Programme in Business Information Systems

Abstract
LoRaWAN (Low Power Wide-Area Network) is a wireless communication network based on LPWAN (Long Range Wide-Area Network) technology intended for a low powered data transmission. It is one of many available LPWAN networks. The wireless LoRaWAN network operates on a certain frequency band that offers a few different data rates. Traffic between end devices and the network is secured by encryption keys. The aim of this thesis was to build a LoRaWAN network through which a sensor acting as an end device would send data into a database. This thesis was conducted in cooperation with WiseNetwork Oy. Digita's IoT network and Actility ThingPark application were utilized in the thesis. Actility ThingPark received data from the sensor every ten minutes. The data was then forwarded to WiseNetwork's MySQL database. The LoRaWAN network worked and sent data in accordance with the objective.

Wide area networks, wireless networks, Internet of things

SISÄLLYS

1 JOHDANTO

LPWAN-verkkoteknologiaan (Low Power Wide-Area Network) perustuvat langattomat tiedonsiirtoverkot, kuten LoRaWAN (Long Range Wide-Area Network) ovat yleistyneet viime vuosina esineiden internetin (Internet of Things, IoT) ansiosta. Näiden verkkojen hyötyjä ovat niiden alhainen virrankulutus, pitkä toimintakantama ja hyvä kustannustehokkuus. Verkon liikenne turvataan salausavaimilla, mikä takaa sen päätelaitteiden ja palvelimen välisten viestien autenttisuuden. LoRaWANin lisäksi on olemassa muita samankaltaisia LPWAN-teknologiaan perustuvia verkkoja, kuten Ingenu, Sigfox ja Narrowband IoT, joista jokaisella on erilaisia käyttötapauksia ja vahvuuksia. LPWAN soveltuu monen eri osa-alueen kohteisiin, kuten kaasu- ja vesimittaukseen, katulamppujen toimintaan ja maatalouden seurantamittaukseen.

Tässä työssä rakennetaan LoRaWAN-verkko tarkoituksena lähettää dataa sensorin ohi kulkeneiden lukumäärästä tietokantaan. Sensori toimii LoRaWAN-päätelaitteena, ja kerää sen ohi kulkeneiden lukumäärän ja lähettää datan kymmenen minuutin välein LoRaWAN-verkon kautta tietokantaan.

Työ tehdään yhteistyössä porilaisen tietotekniikkayrityksen WiseNetwork Oy:n kanssa. WiseNetwork perustettiin vuonna 2012. Yrityksen pääasiallinen tuote on asiakkuudenhallinnan CRM-järjestelmä, joka pyrkii helppokäyttöisyyteen ja suoraviivaisuuteen. Yrityksen tuotekehityksessä työskentelee 17 henkilöä kahdessa eri toimipisteessä Porissa ja Mikkelissä. (WiseNetwork, yrityksen taustat)

LoRaWAN valikoitui aiheeksi WiseNetworkin kautta, jolla oli toimeksiantona kävijälaskurin hankkiminen. Tutustuessa aiheeseen tarkemmin päädyttiin LoRaWAN-verkon rakentamiseen. Esineiden internet on nostanut kysyntää erilaisille kustannustehokkaille ja virtaa säästäville ratkaisuille etenkin kaupunkialueilla. Tällaisten älysovellusten tarve on todettu esimerkiksi terveydenhuollon, kaupunginhallinnan ja teollisuuden

aloilla. Esineiden internetiä on käytetty keräämään dataa älytelevisioista matkapuhelimiin ja jopa sähköhammasharjoihin. Dataa hyödyntäen esimerkiksi hammasharjavalmistajat voivat kehittää tuotettaan kuluttajille. LoRaWAN soveltuu hyvin erilaisten mittausten tekemiseen, kuten vaikka jonkin tapahtuman tai vastaavan kävijöiden laskemiseen.

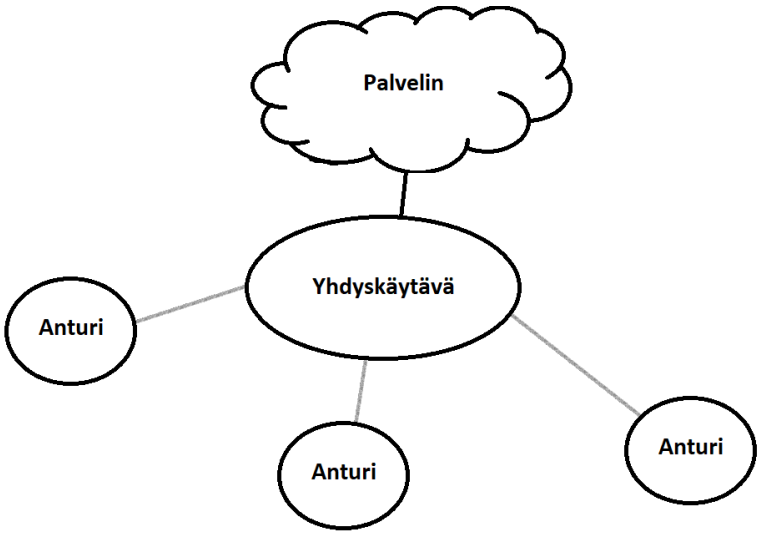
Suomessa verkko-operaattori Digita tarjoaa LoRaWAN-yhteensopivaa IoT-verkkoa, jota käyttääkseen se tulee tilata. LoRaWAN-verkko rakennetaan Digitan Actility Thingpark –verkkoalustaa apuna käyttäen. Verkkoalusta mahdollistaa sensorin liittämisen LoRaWAN-verkkoon ja datan eteenpäin lähettämisen WiseNetworkin MySQL-tietokantaan. Sensorilaitteen ainutlaatuiset tunnistamiskoodit on peitetty punaisella palkilla, jotta niistä ei tulisi julkisia.

2 LORAWAN-VERKKO

LoRaWAN (Long Range Wide-Area Network) on vähätehoiseen tiedonsiirtoon tarkoitettu langaton tiedonsiirtoverkko. Se on tarkoitettu erityisesti pienten datamäärien lähettämiseen ja vastaanottamiseen. LoRaWAN on maailmanlaajuinen ja avoimeen lähdekoodiin perustuva standardi, joka koostuu LoRa-päätelaitteista ja -reitittimistä sekä sovelluksista ja palvelimista. Se perustuu LPWAN-verkkoteknologiaan (Low Power Wide-Area Network). LoRaWANia hallinnoi voittoa tavoittelematon teknologialiitto LoRa Alliance. LoRa (Long Range) on irrallinen modulaatioratkaisu, jota käytetään päätelaitteiden ja reitittimien keskinäisessä viestinnässä. LoRaWAN-verkkoa käyttävät tietoa keräävät anturit ovat kevyitä, joissa käytettävä akku tai paristo saattaa kestää jopa kymmenen vuotta. Data liikkuu yleensä päätelaitteesta eli anturista palvelimelle päin. (Digita LoRaWAN-teknologia)

2.1 Verkon rakentaminen

LoRaWAN-verkko rakennetaan yleensä kohdennetusti jollekin alueelle, tai sitten koko maanlaajuisesti. Tarjolla on sekä julkisia että yksityiseen käyttöön tarkoitettuja verkkoja. (Digita LoRaWAN-teknologia) Verkkoarkkitehtuuri toteutetaan monesti star-of-stars-topologiana, jossa anturit ovat liitettynä langattoman LoRa-yhteyden kautta yhdyskäytävään, joka puolestaan on liitettynä etäpalvelimeen IP-verkon kautta (Bankov, Horov & Ljahov 2016, 2). LoRaWAN-päätelaitteet (anturit) eivät käytä IP-protokollaa, joten ne ovat täysin Internetistä erillään olevassa verkossa. Anturit lähettävät dataa yhteen tai useampaan yhdyskäytävään, jonka kautta data jatkaa palvelimelle. (Digita LoRaWAN-teknologia) Kuvassa 1 on esitelty yksinkertainen hahmotelma LoRaWAN-verkon rakenteesta.



Kuva 1. LoRaWAN-topologia.

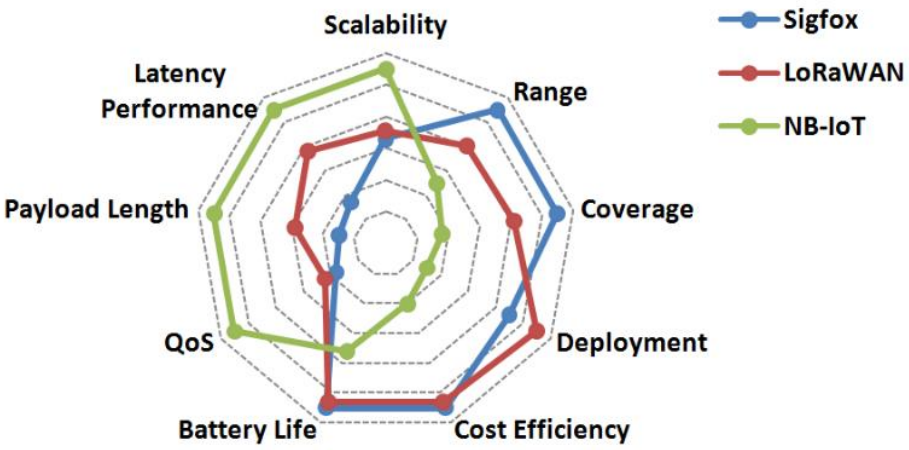
2.2 Tiedonsiirto

LoRa-teknologia perustuu matkapuhelinteknologiassakin käytettävään hajaspektrimodulaatioon, joka on vähätehoinen ja omaa suuren häiriönsietokyvyn, mikä vaikuttaa positiivisesti signaalin toimintakykyyn pitkilläkin matkoilla. LoRaWAN-tiedonsiirto on joko yksi- tai kaksisuuntaista, ja se on ositettu eri nopeuksille ja taajuuskanaville. Anturin ja verkkopalvelimen etäisyys sekä datamäärä vaikuttavat tiedonsiirtonopeuden valintaan. Siirtonopeus on tavallisesti 0,3-50 kilobittiä sekunnissa ja yksittäisen

tiedonsiirron datamäärä vain noin muutaman kymmenen tavua. (Digita LoRaWAN-teknologia)

2.3 Muita LPWAN-toteutuksia

LoRaWANin lisäksi on olemassa myös muita Low-Power Wide-Area Network –teknologioita, kuten Ingenu, Sigfox, sekä Weightless W, N ja P. (Adelantado ym. 2017, 1) Jokaisella LPWAN-toteutuksella on omat vahvuutensa, joita on vertailtu kuvassa 2. Seuraavissa luvuissa käsitellään näitä tarkemmin.



Kuva 2. Vertailu eri LPWAN-teknologioiden vahvuuksista. (Bajic, Chaxel, Mekki & Meyer 2018, 417)

2.3.1 Ingenu

Ingenu on kehittänyt patentoidun Random Phase Multiple Access (RPMA) -teknologiaan perustuvan LWPAN-toteutuksen, tarkoituksenaan tarjota machine-to-machine (M2M) -teollisuusratkaisuja ja yksityisiä verkkoja. Ingenun valttina on sen korkea enintään 624 kb/s datanopeus nousevassa linkissä (uplink) ja 156 kb/s laskevassa linkissä (downlink). Toisaalta tämä aiheuttaa virrankulutuksen kasvua, ja lisäksi sen kantama on lyhyempi sen käyttämän korkean taajuusalueskaalan vuoksi. (Adelantado ym. 2017, 1)

2.3.2 Sigfox

Sigfox on yksi suosituimmista LPWAN-teknologioista. Se on patentoitu Ultra Narrowband (UNB) -teknologiaan perustuva ratkaisu, joka operoi 869 MHz:n (Eurooppa) ja 915 MHz:n (Pohjois-Amerikka) taajuusalueilla. Sigfox perustuu Random Frequency and Time Division Multiple Access (RFTDMA) -teknologiaan ja sen signaali on erittäin kapeakaistainen 100 Hz:n kaistanleveydellä. Sigfox omaa tiukkoja rajoituksia: sen datanopeus on vain noin 100 b/s uplinkissä eikä sama laite voi lähettää yli 14 pakettia päivässä. Lisäksi yhtiön liiketoimintamalliin kuuluu, että Sigfox omistaa verkon, joten nämä asiat yhdessä ovat saaneet käyttäjät kääntymään avoimemman ja joustavamman LoRaWANin puoleen. (Adelantado ym. 2017, 1)

2.3.3 Weightless W, N ja P

Weightless Special Interest Group on kehittänyt kolme erilaista avointa LPWAN-toteutusta: Weightless-W, Weightless-N ja Weightless-P. Weightless-W on kaksisuuntainen ratkaisu, joka perustuu kapeakaistaisiin taajuusjakokanavoinnin (FDMA) kanaviin. Sen datanopeus vaihtelee 1 kb/s:stä 1 Mb/s:iin ja sen akunkesto on noin 3-5 vuotta. Weightless-N kehitettiin parantamaan Weightless-W:n kantamaa ja vähentämään sen virrankulutusta nostaen akunkestoa noin kymmeneen vuoteen. Tämä laski datanopeutta 1 Mb/s:sta 100 kb/s:iin. Weightless-N perustuu UNB-teknologiaan ja se toimii 800-900 MHz:n ultra high frequency (UHF) -taajuusalueella. Se tarjoaa vain uplink-tyyppistä viestintää. Weightless-P on huipputehoinen kaksisuuntainen ratkaisu, joka kykenee toimimaan useilla eri taajuusalueilla. Sille päätelaitteet ovat kuitenkin kalliita ja sillä on korkeampi virrankulutus mitä Weightless-N:llä omaten noin 3-8 vuoden akunkeston. (Adelantado ym. 2017, 1)

2.3.4 Narrowband IoT

Toinen LoRaWANin kaltainen pienitehoinen LPWAN-verkko on Narrowband IoT (NB-IoT), jonka on kehittänyt yhdysvaltalainen 3GPP-standardiorganisaatio. 3GPP on erikoistunut eritoten matkapuhelinverkkojen rakentamiseen. LoRaWANin käyttäessä avoimeen lähdekoodiin perustuvaa lupavapaata ISM-taajuusaluetta NB-IoT käyttää

matkapuhelinverkkojen taajuusaluetta, jonka lisenssimaksut ovat niin korkeita, että vain harvalla toimijalla on siihen varaa. Oheisessa taulukossa on vertailtu LoRaWA-Nia ja NB-IoTia keskenään (Taulukko 1).

Taulukko 1. LoRaWAN ja NB-IoT –vertailu. (Digita 10 faktaa)

Verkko	LoRaWAN	NB-IoT
Standardi	Avoin lähdekoodi	Maksullinen
Toteutusvaihtoehdot	Julkinen tai yksityinen	Julkinen
Protokolla	Asynkroninen	Synkroninen
Virrankulutus lähetys	18 mA – 84mA	100 mA – 220 mA
Virrankulutus vastaan-otto	5 mA	40 mA
Tiedonsiirtonopeus	293 b/s – 50 kb/s	Enintään 250 kb/s

2.4 Päätelaitteet

LoRaWAN-päätelaitteet (anturi tai toimilaite) on jaettu A-, B- ja C-luokan laitteisiin. A-luokan laitteet mahdollistavat kaksisuuntaisen viestinnän eli lähetyksen ja vastaan-ottamisen. Lähetykseen laitteet käyttävät asettamatonta suorasaantia (random access). Vastaanottaminen tapahtuu vain tarkoin määriteltyjen aikavälien aikana, onnistunei-den lähetysten jälkeen. A-luokan laitteet kuluttavat luokista vähiten virtaa verkon kuormituksen ollessa alhainen. B-luokassa viestintä toteutetaan ennalta määrättyjen vastaanottoaikojen kautta. Vastaanottoaikojen ilmoittaminen tapahtuu yhdyskäytävän lähettämien signaalien avulla. C-luokan laitteissa yhteys ei koskaan katkea, sillä ne kuuntelevat kanavaa jatkuvasti. Tämä tarjoaa alhaisimman viiveen lataukselle, mutta se kuluttaa myös eniten virtaa. (Bankov, Horov & Ljahov 2016, 2)

LoRaWAN-päätelaitteet viestivät yhdyskäytävien kanssa LoRa-teknologian avulla. Se perustuu Chirp-Spread Spectrum (CSS) -modulaatioon, joka kehitettiin alun perin 1940-luvulla tutkia varten. CSS:ää on käytetty esimerkiksi sotilaallisessa viestinnässä sen vähävirtaisuuden ja signaalin häiriönestokyvyn vuoksi. LoRan CSS-tekniikka sal-lii merkkien luomisen perustuen spreading factorin (SF, bittien määrä per kooditettu merkki) arvoon. (Bankov, Horov & Ljahov 2016, 3; Azevedo & Fialho 2018, 2)

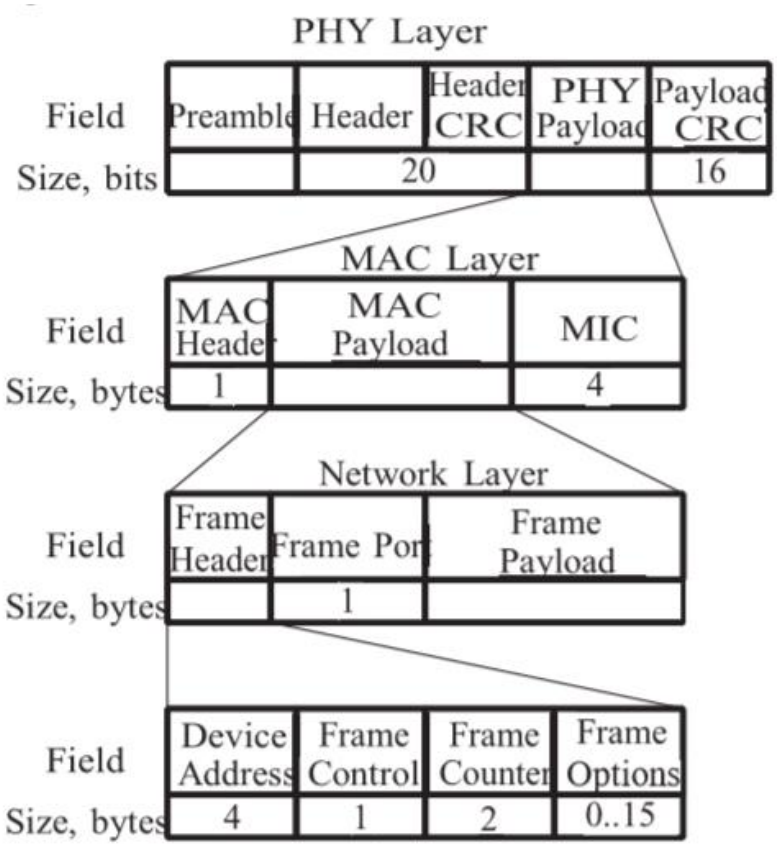
Seuraavassa taulukossa on esitetty Euroopan unionin (EU) alueella saatavissa olevat datanopeudet 863-880 MHz ISM (Industrial, Scientific and Medical) -taajuusalueella (Taulukko 2).

Taulukko 2. Datanopeudet EU:n alueella. (Bankov, Horov & Ljahov 2016, 4)

#	Spreading factor	Kanavan leveys, kHz	Koodiaste	PHY-bittinopeus b/s	RF-herkkyys, dBm
0	12	125	4/6	250	-137
1	11	125	4/6	440	-136
2	10	125	4/5	980	-134
3	9	125	4/5	1760	-131
4	8	125	4/5	3125	-128
5	7	125	4/5	5470	-125
6	7	250	4/5	11000	-122

2.5 Fyysisen kerroksen viestin koostumus

Koska LoRaWAN ei käytä raskasta TCP/IP-pinoa, se on kevyt protokolla, jota sensori- ja anturisovellukset voivat käyttää suoraan yhdyskäytävän kanssa viestimiseen. Fyysisessä kerroksessa (PHY layer) LoRaWAN-kehys (katso kuva 3) alkaa johdanto-osalla, joka määrittelee paketin modulaatioskeeman ja sisältää synkronisointifunktion. Johdanto-osaa seuraavat PHY-otsikko ja CRC-otsikko, jotka ovat yhdessä 20 bittiä pitkiä. PHY-otsikko kertoo myös hyötykuorman (payload) pituuden ja tiedon siitä, onko kehyksessä mukana hyötykuorman 16-bittinen CRC, joka LoRaWAN-verkossa on mukana vain uplink-kehyksissä. (Bankov, Horov & Ljahov 2016, 4)

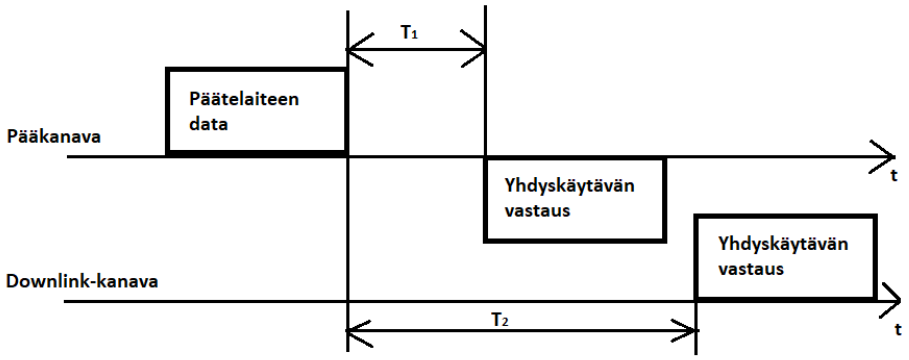


Kuva 3. LoRaWAN-kehyksen muoto. (Bankov, Horov & Ljahov 2016, 4)

Hyötykuorman koostumus on seuraavanlainen: yksibittinen MAC-tunniste kertoo protokollan version ja viestin tyypin, esimerkiksi onko se data- tai käsittelykehys, onko se lähetetty uplink- vai downlink-muodossa, tai onko viestiä tarkoitus tunnustaa. MAC-tunnistetta seuraa kehystunniste, joka sisältää laitteen osoitteen, verkon valvontatiedon, sekvenssinumeron, kehysvaihtoehdot ja kehysportin. Laitteen osoite on kaksiosainen: sen ensimmäiset kahdeksan bittiä tunnistavat verkon, ja loput bitit luodaan dynaamisesti verkkoon liityttäessä. Verkon valvontatieto on yksibittinen ja se kertoo esimerkiksi, että käytetäänkö uplink-lähetykseen yhdyskäytävän määrittelemää datanopeutta, tunnustaako viesti edellisen viestin vastaanottamisen, tai onko yhdyskäytävällä lisää dataa päätelaitetta varten. Kehysvaihtoehdot voivat sisältää komentoja datanopeuden vaihtamiseen, lähetystehon säätämiseen tai yhteyden vahvistamiseen. Kehysportti sisältää arvon, jonka avulla erotetaan yhdyskäytävän ja päätelaitteen välillä kulkevat datavirrat toisistaan. Jos sen arvo on nolla (0), viesti sisältää MAC-komentoja käyttäjädatan sijaan. (Bankov, Horov & Ljahov 2016, 5)

2.6 Taajuuskanavat

LoRaWAN-verkon käyttämät taajuuskanavat määritellään yhdyskäytävän konfiguraatiossa. Käyttövarattujen kanavien lukumäärä riippuu alueellisista rajoituksista ja verkkoasetuksista. Jotkut kanavat on varattu datan lähettämiseen (pääkanavat) ja yksi kanava (downlink-kanava) on varattu yhdyskäytävän kehysten vastauksille. Lisäksi päätelaitteet käyttävät joitakin kanavia lähettäessään liittymispyyntöjä yhdyskäytävälle. (Bankov, Horov & Ljahov 2016, 5) Kuvassa 4 on esitelty A-luokan laitteiden kulku kanavalle.



Kuva 4. LoRaWANin kanavaan pääsy. (Bankov, Horov & Ljahov 2016, 6)

Kun päätelaite on valmis lähettämään dataa, se valitsee yhden pääkanavista satunnaisesti ja lähettää kehyksen yhdyskäytävälle varaamattomassa ALOHA-tilassa ilman tahdistusta tai kantoaallon tunnistusta. Lähetyksen jälkeen päätelaite avaa kaksi lyhyttä vastaanottoikkunaa: ensimmäisen uplink-lähetystä käyttävälle kanavalle, ja toisen downlink-kanavalle. Virran säästämisen vuoksi vastaanottoikkunoita ei avata samaan aikaan: toinen vastaanottoikkuna avataan sekunti ensimmäisen jälkeen. (Bankov, Horov & Ljahov 2016, 6)

2.7 Tietoturva

Koska LoRaWAN-yhteys on langaton, se on teoriassa avoinna kenelle tahansa urkkijalle. Lisäksi sen viestipakettien autenttisuus, eli toisin sanoen, tuleeko paketti aiotusta kohteesta, voidaan vaarantaa. LoRaWAN käyttää kahta eri avainta, verkkoavainta

NwkSKey ja sovellusavainta AppSKey, yhteyden turvaamiseen. NwkSKey turvaa yhteyden IoT-laitteen ja verkon välillä, ja AppSKey turvaa päästä päähän -yhteyden. Viestin lähtiessä sovelluspalvelimelle AppSKey salakirjoittaa ensin sen hyötykuorman. Datan luottamuksellisuuden turvaa lohkosalausalgoritmi, jota operoidaan CTR-tilassa. (Doerr, Karampatzakis, Kuipers & Yang 2018, 2) Taulukossa 3 on vertailtu eri LoRaWAN-avaimia.

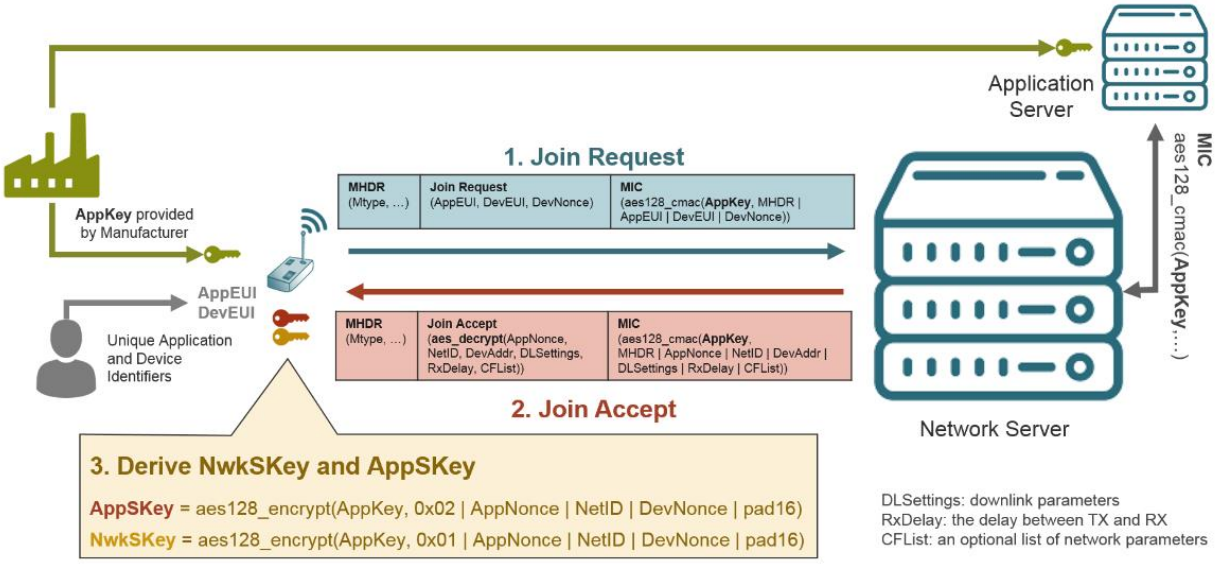
Taulukko 3. LoRaWAN-avaimet. (Yang 2017, 11)

Nimi	Pituus	Luoja	Käyttö
AppKey	128 bittiä	Sovellus	MIC-tunniste join-viesteille, salakirjoittaa join acceptin, luo sessioavaimet
AppSKey	128 bittiä	AppKey	Salakirjoittaa viestit
NwkSKey	128 bittiä	AppKey	MIC-tunniste viesteille, salakirjoittaa MAC-komentoviestit

2.7.1 Aktivointimenettelyt

Koska viestin lähettämiseen tarvitaan kaksi avainta, tarvitaan jokin keino ladata avaimet IoT-laitteille. LoRaWAN tarjoaa kahta eri aktivointimenettelyä: Over-The-Air-Activation (OTAA) ja Activation by Personalization (ABP). (Doerr, Karampatzakis, Kuipers & Yang 2018, 2)

OTAA-menettelyssä päätelaite lähettää ensin liittymispyynnön (Join Request), joka sisältää kolmebittisen satunnaisen numeron DevNonce. Tämän jälkeen verkkopalvelin tarkistaa voiko päätelaitetta hyväksyä, ja lähettää hyväksytylle laitteelle Join Accept –viestin, joka sisältää verkkopalvelimen luoman kolmebittisen AppNonce-numeron. Hylätyille laitteille ei lähetetä minkäänlaista viestiä. Kun päätelaite saa AppNonce-numeron, laite ja palvelin muodostavat verkko- ja sovellusavaimet yhdessä. OTAA tuottaa verkko- ja sovellusavaimet salakirjoittamalla datan 16-bittisen AppKeyn avulla, joka on päätelaitteen uniikki avain. Näin estetään yhteyden salakuuntelijoita luomasta NwkSKey ja AppSKey –avaimia. (Doerr, Karampatzakis, Kuipers & Yang 2018, 2-3) Kuvassa 5 on esitetty aktivoinnin kulku OTAA-menettelyssä.

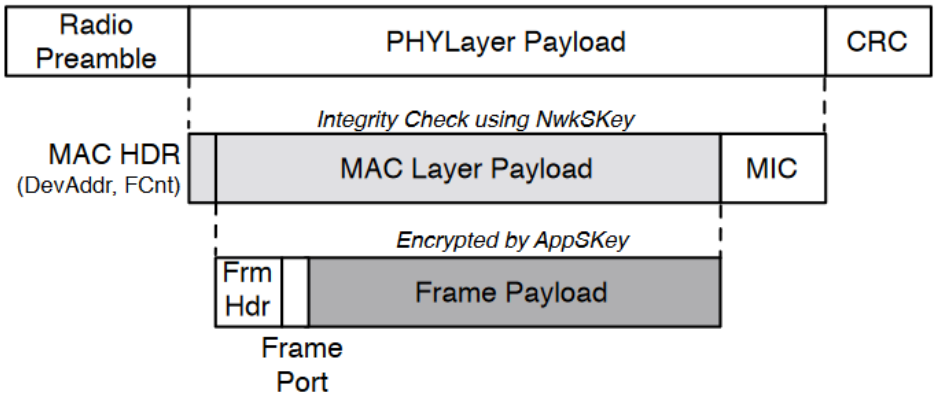


Kuva 5. OTAA-menettely. (Butun, Eldefrawy, Gidlund, Pereira 2019, 5)

APB-menettelyssä ei vaihdeta join-viestejä. Päätelaitteelle määrätään ennen aktivointia kolme ainutlaatuista parametria, DevAddr, NwkSKey ja AppSKey, jotka tallennetaan palvelimelle. Päätelaite lähettää viestejä suoraan sen yrittäessä viestiä palvelimen kanssa. Nämä viestit salakirjoitetaan ja allekirjoitetaan siten, että vain niiden vastaanottajaksi määritelty palvelin voi lukea niitä. ABP-menettelyllä määriteltyjä laitteita käytettäessä NwkSKey ja AppSKey –avaimia käytetään kaikissa istunnoissa, kunnes ne päivitetään laitteeseen. (Doerr, Karampatzakis, Kuipers & Yang 2018, 3)

2.7.2 Viestien eheyden ja autenttisuuden tarkistus

LoRaWAN käyttää message integrity code (MIC) -tunnistetta tarkistamaan tiedon eheyden MAC-headerissä ja payloadissa. MIC luodaan NwkSKeyn ja AES-CMAC –algoritmin avulla. Kun viesti saapuu verkkopalvelimelle, palvelin tarkistaa viestin eheyden ja läpäistessä tarkistuksen lähettää sen edelleen sovelluspalvelimelle. Liittymispyynnöille MIC luodaan NwkSKeyn sijaan AppKeyllä. (Doerr, Karampatzakis, Kuipers & Yang 2018, 3) Kuvassa 6 vaaleanharmaata aluetta turvaa NwkSKey:stä luotu MIC ja tumman harmaa alue on salakirjoitettu AppSKeyn avulla.



Kuva 6. Viestin eheys tarkistetaan MAC-headerissä ja payloadissa. (Doerr, Karampatzakis, Kuipers & Yang 2018, 3)

2.7.3 Laskurien käsittely

Jokaisella päätelaitteella on kaksi laskuria FCntUp ja FCntDown, jotka laskevat uplink- ja downlink-viestejä päätelaitteen ja verkon välillä. Jotta viestit pysyvät synkronoituna, on olemassa huippuraja-arvo MAX_FCNT_GAP. Jos ero uplink- ja downlink-viestien välillä on suurempi kuin MAX_FCNT_GAP, seuraavat viestit hylätään. Laskurien arvoja käytetään sala- ja allekirjoituksessa eikä samaa arvoa tulisi käyttää enempää kuin kerran. Jos laskurin tila ylittyy, laskuri nollataan LoRaWAN-määrittelyn mukaisesti. (Doerr, Karampatzakis, Kuipers & Yang 2018, 2; Yang 2017, 16-17)

2.7.4 Hyökkäykset LoRaWANia kohtaan

Hyökkääjät voivat käyttää erilaisia haavoittuvuuksia LoRaWANissa kaapatakseen yhteyden verkossa. Hyökkäyksiin kuuluvat replay-hyökkäys, salakuuntelu, bit flipping ja ACK-huijaus. (Yang 2017, 66)

Replay-hyökkäyksessä käytetään hyväksi haavoittuvuutta ABP-aktivointimetodissa ja laskurihallinnassa. Hyökkääjä pystyy uudelleenkäyttämään viestejä, minkä vuoksi palvelin jättää huomiotta todellisia viestejä päätelaitteelta. Salakuuntelussa hyökkääjä käyttää haavoittuvuutta laskurihallinnassa ja LoRaWANin salakirjoitusmenetelmässä. Tässä hyökkäyksessä hyökkääjä voi protokollapuutteiden takia purkaa LoRa-viestejä.

Bit flipping -hyökkäyksessä hyökkääjä pystyy muokkaamaan viestejä verkko- ja sovelluspalvelimen välillä. ACK-huijauksessa hyökkääjä voi muunnella ACK-viestejä tunnustamaan muita kuin alkuperäisiä sovellukselle lähetettyjä viestejä. (Doerr, Karampatzakis, Kuipers & Yang 2018, 4-7)

Radiohäirintä on yksi IoT-laitteiden ongelmista. Hyökkääjä voi lähettää vahvaa radiosignaalia laitteiden läheisyydessä ja häiritä tällä tavoin tiedonsiirtoa. LoRaWANissa käytetty CSS-modulaatio on tunnettu vankasta häirinnänestokyvystään, mutta rinnakkaisissa LoRa-lähetyksissä samaa taajuutta ja spreading factoria käyttävät lähetykset voivat häiritä toisiaan. Tämä antaa hyökkääjälle mahdollisuuden tukkeuttaa LoRa-verkon. Vaikka tällaista hyökkäystä on vaikea ehkäistä, koko taajuuden tukkivat häirinnät on helppo havaita, sillä kaikki sillä taajuudella toimivat laitteet häviäisivät verkosta. Tällöin järjestelmän ylläpitäjä voisi estää häirinnän vaikutukset, esimerkiksi vaihtamalla käytettävää taajuutta. (Aras, Lawrence, Hughes & Ramachandran 2017, 5)

2.8 Käyttötarkoitukset

LoRaWAN-teknologiaa voi käyttää useissa esineiden internetin (Internet of Things, IoT) ratkaisuissa. Se sopii etenkin pienten datamäärien lähettämiseen ja vastaanottamiseen. LoRaWAN on myös tietoturvallinen ratkaisu, sillä sen tiedonsiirto on salattu ja se kulkee verkon kolmessa eri kerroksessa. Lisäksi päätelaitteella ja sen käyttämällä sovelluksella on omat salausavaimensa, mikä takaa tiedonsiirron turvallisen kulun yhdyskäytävällä. (Digita LoRaWAN-teknologia)

LoRaWAN soveltuu hyvin esimerkiksi maatalouden, vuodonetsinnän ja ympäristönhallinnan sovelluksiin, sillä niiden viiverajoitukset ovat lieviä ja jaksollisia tai jaksottomia viestejä on vähän. Toisaalta laajalle levitetyt päätelaitteet aiheuttavat sen, että viestintäkantaman tulee olla tarpeeksi pitkä, jotta yhteys toimisi. LoRaWAN soveltuu tällaisiin sovellusratkaisuihin hyvin, kunhan yhdyskäytävät on sijoiteltu niin, että ne kattavat kaikki päätelaitteet. Toisaalta teollisuusautomaatio tarvitsee reaaliaikaista toiminnallisuutta, johon LoRaWAN pitkine viiveaikoineen ei sovellu. Siitä huolimatta pieni LoRaWAN-verkko voi toimia sovelluksissa, jotka tarvitsevat datan poimintaa esimerkiksi joka sekunti. Toimiakseen tällaisen verkon spreading factor tulee olla

mahdollisimman pieni eli toisin sanoen yhdyskäytävän pitää olla tarpeeksi lähellä päätelaitteita. Lisäksi kanavien lukumäärä pitää tarkoin määritellä ristiriitojen mahdollisuuden minimoimiseksi. (Adelantado ym. 2017, 4)

LoRaWAN on toiminut hyvin niin sanottujen älykaupunkien sovelluksissa. LoRaWAN-toteutuksilla on kerätty dataa esimerkiksi kaupunkien valaistuksesta, pysäköimisestä ja jätehuollosta. Näihin se soveltuu hyvin, sillä viestinnän määrä päivässä on yleensä vähäistä: esimerkiksi pysäköintiä tarkkaileva sovellus ilmoittaa vain, kun se havaitsee muutoksen parkkipaikan tilassa. Jätehuollon ja valaistukseen liittyvissä sovelluksissa viive ja synkronointivirheet eivät ole ongelma. Toisaalta esimerkiksi kaupungin valaistusta kontrolloivassa sovelluksessa auringonnousu ja –lasku toimivat laukaisimena samanaikaisesti monen eri päätelaitteen kanssa, mikä aiheuttaa suuren vyöryn viestejä verkossa. (Adelantado ym. 2017, 5)

Logistiikan ja kuljetusalan-, sekä videovalvonnan sovelluksiin LPWAN-verkot eivät sovi hyvin. Kuljetukseen liittyviä ongelmia ovat LoRaWAN-verkon liian pieni kantama ja näiden sovellusten mahdollinen sietokyvyttömyys viive- ja synkronointivirheille. Videovalvonnassa taas LoRaWANin 0,3 – 50 kb/s datanopeus on riittämätön, kun alhaislaatuista kuvaa lähettävälle videoyhteydelle suositellaan vähintään 130 kb/s datanopeutta, ja teräväpiirtoista kuvaa lähettävälle yli 4 Mb/s datanopeutta. (Adelantado ym. 2017, 5)

3 TOTEUTUKSESSA KÄYTETYT LAITTEET JA OHJELMISTOT

3.1 Päätelaite

Päätelaitteena toteutuksessa käytettiin sensoria, joka laskee sen ohi kulkeneiden ihmisten määrän tietyllä aikavälillä. Sensori on sveitsiläisen Parametric-yhtiön valmistama laite OCR2-OD Outdoor People Counter, tuotekoodiltaan PCR2-EU868-OD. Laite on A-luokan LoRaWAN-laite, ja se käyttää tasavirtaista 5-12V:n virtalähdettä. Se asennetaan ruuveilla kiinni esimerkiksi seinään tai kattoon. Se kykenee laskemaan sekä vasemmalta oikealle että oikealta vasemmalle laitteen ohi kulkeneet.

Sensorin hyötykuorman syntaksi on seuraava: 0a<ltr>16<rtl>01<tmp>, jossa 0a, 16 ja 01 ovat selitteitä, <ltr>, <rtl> ja <tmp> objekteja, jotka sisältävät sensorin lähettämää dataa. Ltr kertoo vasemmalta oikealle, ja rtl oikealta vasemmalle kulkeneiden lukumäärän, ja tmp lämpötilan heksadesimaalina. (Taulukko 4)

Taulukko 4. Sensorin hyötykuorma. (Parametric Quick Start Guide)

Objekti	Tyyppi	Vaihtelu-väli	Esimerkki
0a	Selite vasemmalta oikealle	-	-
<count>	Vasemmalta oikealle ohi kulkeneiden lukumäärä	0000...ffff	0010 = 16 henkilöä vasemmalta oikealle edellisen uplink-lähetyksen jälkeen
16	Selite oikealta vasemmalle	-	-
<count>	Oikealta vasemmalle ohi kulkeneiden lukumäärä	0000...ffff	0014 = 20 henkilöä oikealta vasemmalle edellisen uplink-lähetyksen jälkeen
01	Selite lämpötilalle	-	-
<tmp>	Sisäinen lämpötila celsiusasteissa	0000...ffff	ff9a = -10,2 celsiusastetta

Sensori konfiguroidaan Parametricin kotisivuilta ladattavalla asennustyökalulla. Työkalussa on tietoja laitteesta, kuten malli- ja sarjanumero, lämpötila ja LoRaWAN-status. Työkaluun määritellään kaksi (2) kappaletta LoRaWAN-salausavaimia, jonka jälkeen laitteen vilkkuva LED-merkkivalo sammuu, jos yhteys on onnistunut. Työkalussa asetetaan aika siitä, kuinka usein laite lähettää dataa palvelimelle. Aikaväli on mahdollista asettaa 1-1440 minuuttiin, eli maksimissaan 24 tuntiin. Tuona aikana laite laskee sensorin ohi kulkeneet ja lähettää ne ajan päätyttyä palvelimelle, minkä jälkeen laskuri nollataan. Laitteen voi konfiguroida myös lähettämään dataa jokaisen sensorihavainnon jälkeen, tai olla lähettämättä mitään, jos laskurin tulos on nolla. Muita asetuksia ovat muun muassa sensorin herkkyyden asettaminen prosenteissa, hyötykuorman tyypin valinta ja kanavien valinta. (Parametric Quick Start Guide)

Laitteen toimintatiloja on kolmenlaisia: Timespan, NotZero ja Trigger. Timespan-tilassa laite laskee sensorin ohi kulkeneita objekteja ja lähettää havaintojen summat määritellyn aikavälin jälkeen. NotZero on muuten sama kuin Timespan, mutta se ei lähetä mitään, jos summat ovat nolla. Trigger lähettää tiedot jokaisen havainnon jälkeen; tätä voi säätää käyttämällä Trigger Hold Off –asetusta lähettämään tietoja 1-600 sekunnin välein. Hyötykuorman tyyppejä on kahta erilaista: oletusarvona Parametricin payload-formaatti ja vaihtoehtoisesti Cayenne LPP –yhteensopiva formaatti. Sensorin herkkyyttä pystyy säätämään 10-100 prosentin välillä. (Parametric Quick Start Guide)

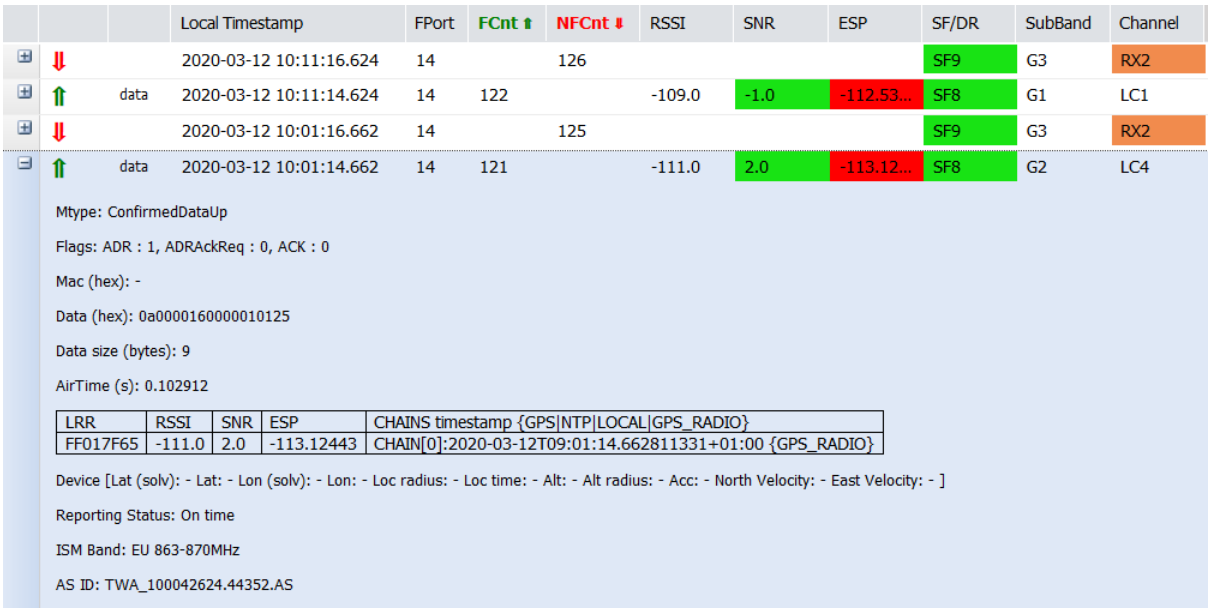
Koska laite on Over-The-Air-Activation (OTAA) -mallinen, sen LoRaWAN-asetuksissa on määritelty laitteen DevEUI, AppEUI ja AppKey. Jokaisella LoRaWAN-laitteella on uniikki 64-bittinen DevEUI, joka on valmistajan määrittelemä. Se tunnistaa laitteen LoRaWAN-verkossa liittymispyynnön aikana. AppEUI on myös 64-bittinen uniikki tunniste, joka tunnistaa join-palvelimen liittymispyynnön yhteydessä. AppKey on 128-bittinen tunniste, jonka tehtävänä on salakirjoittaa data liittymispyynnön aikana. (ThingPark Wireless, 7-8)

3.2 Actility Thingpark -verkkoalusta

Digitan IoT-verkkoa käyttääkseen tarvitaan Actility Thingpark –verkkoalusta. Thingpark-portaaliin kirjaudutaan verkkoselaimessa. Käyttäjätunnukset ovat Digitan luomia. Thingparkin työkaluihin kuuluvat Device Manager, Wireless Logger ja Network Manager.

Device Managerissa lisätään ja muokataan LoRaWAN-päätelaitteita, määritellään sovelluspalvelimet (application servers) ja reititysprofiilit. Wireless Logger –moduulissa on esillä kaikki liikenne. Uplink- ja downlink-viestit on eroteltu toisistaan vihreillä (uplink) ja punaisilla (downlink) nuolilla. Lisäksi viesteistä on luettavissa niiden hyötykuorma, MAC-komennot ja radioparametrit: Spreading factor (SF), signaalinvoimakkuus (RSSI), signaalikohinasuhde (SNR) ja ESP-arvo (Evaluated Signal Power). Network Manager näyttää mahdolliset tukiasemat, jotka Digita on määritellyt yleensä valmiiksi. Digitan IoT-verkko käyttää REST-API –rajapintaa, mikä tarkoittaa, että se

lähettää päätelaitteelta saadut viestit HTTP POST –kutsuina. Lisäksi päätelaitteen tulee käyttää Trusted Authority –mallista SSL-sertifikaattia. Sovelluspalvelimelle määritellään päätelaitteen URL-osoite, jonne paketit menevät joko JSON- tai XML-muodossa. (Digita LoRaWAN-ohje) Kuvassa 7 on kuvattu Wireless Loggerin toimintaa.



		Local Timestamp	FPort	FCnt	NFCnt	RSSI	SNR	ESP	SF/DR	SubBand	Channel
⇓		2020-03-12 10:11:16.624	14		126				SF9	G3	RX2
⇑	data	2020-03-12 10:11:14.624	14	122		-109.0	-1.0	-112.53...	SF8	G1	LC1
⇓		2020-03-12 10:01:16.662	14		125				SF9	G3	RX2
⇑	data	2020-03-12 10:01:14.662	14	121		-111.0	2.0	-113.12...	SF8	G2	LC4

Mtype: ConfirmedDataUp

Flags: ADR : 1, ADRAckReq : 0, ACK : 0

Mac (hex): -

Data (hex): 0a0000160000010125

Data size (bytes): 9

AirTime (s): 0.102912

LRR	RSSI	SNR	ESP	CHAINS timestamp {GPS|NTP|LOCAL|GPS_RADIO}
FF017F65	-111.0	2.0	-113.12443	CHAIN[0]:2020-03-12T09:01:14.662811331+01:00 {GPS_RADIO}

Device [Lat (solv): - Lat: - Lon (solv): - Lon: - Loc radius: - Loc time: - Alt: - Alt radius: - Acc: - North Velocity: - East Velocity: -]

Reporting Status: On time

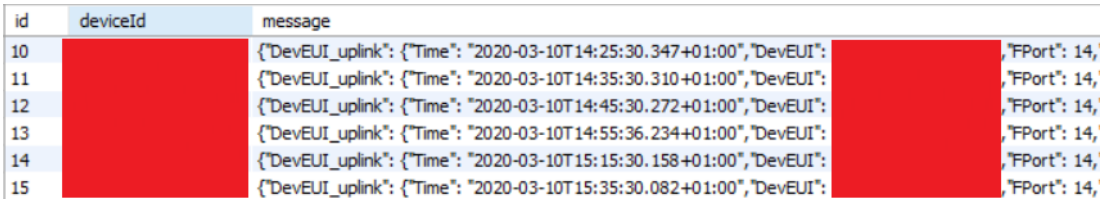
ISM Band: EU 863-870MHz

AS ID: TWA_100042624.44352.AS

Kuva 7. ThingParkin Wireless Logger –lokiin tulevaa dataa.

3.3 MySQL Workbench

MySQL on avoimen lähdekoodin tietokanta, jota käytetään esimerkiksi Facebookissa, Twitterissä ja YouTubessa (Oracle MySQL). MySQL on lyhenne sanoista My, joka on sen kehittäjän tyttären nimi, ja SQL eli Structured Query Language, joka on ohjelmointikieli, jolla voidaan käsitellä dataa relaatiotietokannassa (Kinsta). MySQL Workbench on tietokantasuunnitteluun tarkoitettu työkaluohjelma MySQL-tietokantajärjestelmälle. Ohjelmalla voidaan luoda, muokata ja tarkastella tietokantatauluja. Kuvassa 8 on esimerkki tässä toteutuksessa käytetyn taulun riveistä.



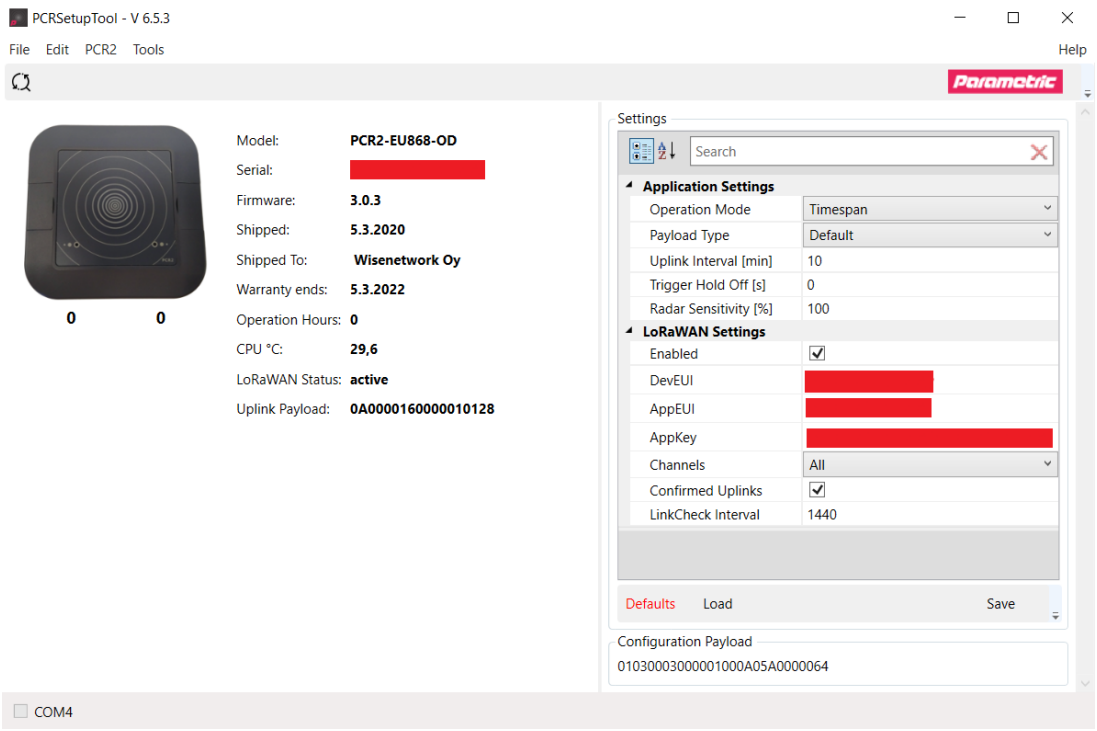
id	deviceId	message
10	[redacted]	{"DevEUI_uplink": {"Time": "2020-03-10T14:25:30.347+01:00","DevEUI": [redacted] ,"FPort": 14,
11		{"DevEUI_uplink": {"Time": "2020-03-10T14:35:30.310+01:00","DevEUI": [redacted] ,"FPort": 14,
12		{"DevEUI_uplink": {"Time": "2020-03-10T14:45:30.272+01:00","DevEUI": [redacted] ,"FPort": 14,
13		{"DevEUI_uplink": {"Time": "2020-03-10T14:55:36.234+01:00","DevEUI": [redacted] ,"FPort": 14,
14		{"DevEUI_uplink": {"Time": "2020-03-10T15:15:30.158+01:00","DevEUI": [redacted] ,"FPort": 14,
15		{"DevEUI_uplink": {"Time": "2020-03-10T15:35:30.082+01:00","DevEUI": [redacted] ,"FPort": 14,

Kuva 8. Anturilta saatua dataa MySQL Workbench –ohjelmassa.

4 VERKON TOTEUTUS

4.1 Anturin käyttöönotto

Anturilaitteen kansi oli kiinni neljällä ruuvilla, jotka irrotettiin laitteeseen pääsemiseksi. Laite konfiguroitiin laittamalla se kiinni tietokoneeseen USB-kaapelilla. Laitteen valmistajan verkkosivuilta oli ladattavissa asennustyökalu PCR Setup Tool, jota käytettiin laitteen konfigurointiin. Asennustyökalu tunnisti laitteen ja kertoi siitä oleellisia tietoja, kuten malli- ja sarjanumeron, takuuajan päättymisen ja laitteen sisäisen lämpötilan, joka oli noin 30 celsiusastetta. Työkalulla laitteen asetuksia oli mahdollista säätää. Asetuksissa määriteltiin laitteen toimintatila, hyötykuorman tyyppi, uplinkin aikaväli, laukaisimen viivytys ja sensorin herkkyysaste. Sovellusasetuksiin jätettiin oletusarvot eli toimintatilaksi Timespan, hyötykuorman tyypiksi oletus, uplinkin aikaväliksi 10 minuuttia ja sensorin herkkyydeksi 100 prosenttia; laukaisimen viivytys oli nolla, mutta koska Trigger-toimintatilaa ei käytetty, se ei vaikuttanut testaukseen. Sovellusasetusten lisäksi laitteeseen tuli konfiguroida LoRaWAN-asetukset. Näihin kuuluivat DevEUI, AppEUI ja AppKey (kuva 9).



Kuva 9. Sensorin konfigurointityökalun asetukset.

4.2 Application Serverin asennus

ThingParkissa luotiin Application Server, jonka tyypiksi valittiin oletuksena ollut HTTP Application Server (LoRaWAN), ja sisällön tyypiksi JSON. Sille määriteltiin reitti ja määränpää, joka oli palvelimella sijaitseva PHP-tiedosto. Tämän jälkeen luotiin Application Serverin reititysprofiili. Anturi yhdistettiin reititysprofiiliin, jonka jälkeen saatiin luettua dataa PHP-tiedostoon, ja sieltä edelleen MySQL-tietokantaan.

4.3 MySQL-taulun luonti ja siihen datan lisääminen

Anturilta tulevaa dataa varten luotiin MySQL-tietokantaan uusi IoTMessageLog-taulu, johon tehtiin sarakkeet id, deviceId ja message, joissa id on viestin järjestysnumero, deviceId laitteen tunnistusnumero ja message itse JSON-muotoinen viesti anturilta (Kuva 9). MySQL-taulun luontiin käytettiin MySQL Workbench –ohjelmaa. Anturilta tuleva data lisättiin tauluun palvelimelle luodulla PHP-tiedostolla. PHP-tiedostoon asetettiin rajoite, joka sallii vain tietyistä IP-osoitteista tulevien viestien välittämisen tietokantaan. Luvalliset viestit lisättiin tietokantaan vikasietoisesti try-catch-lauseella, joka nappaisi ja raportoisi mahdolliset virheet lokiin. Virheettömät kyselyt lisäävät tietokantataulun uuden rivin, jossa on eritelty deviceId ja message erikseen. Kuvassa 10 on esitelty kyseisen PHP-tiedoston koodi kokonaisuudessaan. Tässä kohtaa toteutusta opiskeltiin melko laajasti PHP-ohjelmointia, jotta data saataisiin ajettua tietokantaan onnistuneesti.

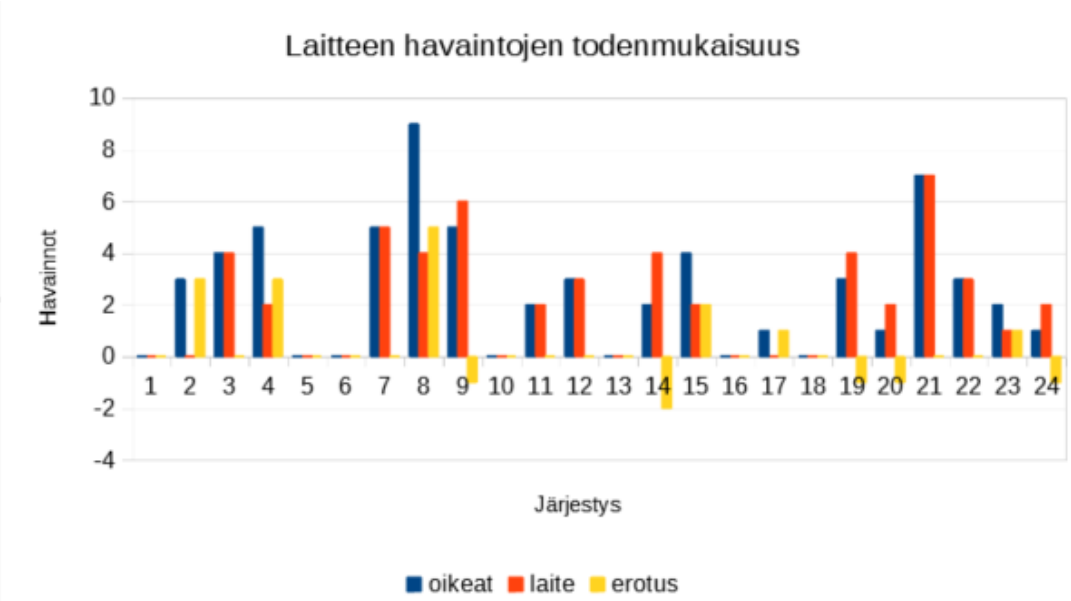
```php
<?php
/**
 * IotMessages Listener Service.
 * The Service will push incoming JSON POST data into IotMessageLog table.
 */

ini_set('display_errors', 0);
date_default_timezone_set('Europe/Helsinki');

$allowedIPs = [redacted]

if(!in_array($_SERVER['REMOTE_ADDR'], $allowedIPs)) {
    exit('Not allowed');
    error_log('IP '.$_SERVER['REMOTE_ADDR'].' blocked');
}

include __DIR__.'/ProceduralDB.php';

$postStr = file_get_contents("php://input");
$postObj = json_decode($postStr);

// push to database
try {
    $result = query([
        'query' => 'insert into IoTMessageLog (deviceId, message) values (?,?)',
        'types' => 'ss',
        'deviceId' => $postObj->DevEUI_uplink->DevEUI,
        'message' => $postStr
    ], $db);
    if($result) {
        $success = true;
        $db->commit();
    } else {
        $success = false;
        $db->rollback();
    }
} catch(\Exception $e) {
    error_log($e->getMessage());
    $success = false;
}
echo intval( $success );
```

Kuva 10. PHP-tiedosto, jolla data siirrettiin tietokantaan.

4.4 Testaus

Sensori asennettiin testausta varten WiseNetworkin toimistolle oviaukon läheisyyteen ensin pöydälle vaakatasoon. Sensorin antama data ei vastannut kovin hyvin reaalimaailmaa, joten se siirrettiin oven päälle katon suuntaisesti. Testauksessa simuloitiin myös pyöröovea, ja todettiin, että se tulisi häiritsemään datan oikeellisuutta. Laitteen ohi todellisuudessa kulkeneista ja toisaalta sen havaitsemista kulkemisista pidettiin kirjaa, ja todettiin, että laitteen antama tieto pitää pääosin paikkaansa. Eroavaisuudet datan ja havaintojen välillä voivat johtua sensorin korkeasta herkkyysasteesta tai sitten kirjaa

pitäneen virheistä havainnoissa. Mittaustuloksista voidaan laskea erinäisiä lukuja, kuten keskiarvon, keskihajonnan ja virhetermin MSE (mean squared error), joka kertoo erotuksen neliöiden keskiarvon. MSE mittaa laskelmien laatua ja se on aina positiivinen luku; mitä lähempänä MSE on nollaa, sen parempi. Erotuksen keskiarvo oli 0,875, keskihajonta 1,296 ja MSE 2,375. Kuvassa 11 on kirjattu havainnot yhden päivän ajalta pylväsdiagrammiin.



Kuva 11. Laitteen havainnot päivän aikana.

5 YHTEENVETO

Esineiden internetin ansiosta erilaiset langattomat tiedonsiirtoverkot ovat nousseet viime vuosina suosioon. LoRaWAN-verkko soveltuu muiden LPWAN-verkkojen tavoin pieniä datamääriä lähettäviin kevyisiin sovelluksiin. Sen vahvuuksia ovat alhainen virrankulutus, kohtuullisen pitkä kantama ja hyvä kustannustehokkuus. Liikenne verkon ja päätelaitteiden välillä salakirjoitetaan salausavaimilla, ja verkon viestien eheys ja autenttisuus tarkistetaan. LoRaWAN-verkon käyttötapauksia ovat etenkin erilaiset älykaupunkien sovellukset, kuten katulamppujen valaistus, jätehuollon seuranta ja auton pysäköinnin seuranta, kun taas hyvin pitkää kantamaa tai suurta tiedonsiirtonopeutta tarvitseviin applikaatioihin se ei sovellu.

Tässä työssä rakennettiin oma LoRaWAN-verkko, jotta voitaisiin tarkastella dataa sensorilta, joka laskee sen ohi kulkeneiden objektien määrän. LoRaWAN-laitteena toiminut sensori oli siis käytännössä kävijälaskuri. Työ tehtiin yhteistyössä tietotekniikkayritys WiseNetwork Oy:n kanssa. LoRaWAN-verkko rakennettiin Digitan IoT-verkon avulla: Digita tarjosi Actility Thingpark –verkkoalustan, jossa määriteltiin verkon asetukset ja laitteet. Kävijälaskuri konfiguroitiin ja sitten yhdistettiin verkkoalustan kautta LoRaWAN-verkkoon ja alkoi lähettää dataa kymmenen minuutin välein verkkoalustalle, josta se lähetettiin edelleen WiseNetworkin palvelimella olevaan MySQL-tietokantaan. Sensori asennettiin WiseNetworkin toimistolle oven lähettyville ensin vaakatasoon pöydälle. Dataa tarkastellessa huomattiin eroavaisuuksia datan ja todellisuudessa sen ohi kävelleiden määrän kanssa, joten laite siirrettiin kattoon oven yläpuolelle. Havaintojen yhdenmukaisuus parantui, mutta data ei ollut täysin vastaava reaalimaailmaa. Tämä saattoi johtua sensorin herkkyysasteesta, joka oli asetettu sataan prosenttiin, tai sitten inhimillisistä tekijöistä, kuten tarkkailijan eli allekirjoittaneen huolimattomuudesta havaintoja tehdessä. Joka tapauksessa verkko todettiin toimivaksi ja työn tavoitteet täyttyneeksi.

Ennen toteutusta LPWAN-verkot olivat itselleni täysin tuntematon aihe. Sitä tutkiessa opin LoRaWAN-verkon lisäksi myös esineiden internetistä, ja muista LPWAN-verkoista ja niiden eroavaisuuksista. Aihe oli hyvin mielenkiintoinen varsinkin sen tietoturvan osalta, josta voisi kirjoittaa kokonaan oman toteutuksen. Käytännön työssä piti hyödyntää montaa eri työkalua ja ohjelmaa, mutta se ei tuottanut suurempia ongelmia. Datan saanti tietokantaan oli toteutuksen haastavin osuus, sillä siinä tarvittu PHP-ohjelmoinnin tietämys oli melko suppea.

Tulevaisuudessa erilaisten IoT-sovellusten määrän ja käytön ennustetaan nousevan huimasti. Vuonna 2018 arvioitiin, että vuoden 2020 lopulla IoT-laitteiden määrä olisi yli 20 miljardia, ja niillä olisi 3 miljardia käyttäjää. Vuoteen 2021 mennessä LPWAN-verkkojen markkinaosuuden arvioidaan olevan noin 24,5 miljoonaa Yhdysvaltain dollaria eli noin 22,4 miljoonaa euroa. (Butun, Pereira, Gidlund 2019, 1) Varsinkin urbaaneilla alueilla erilaisten älysovellusten tarve esimerkiksi terveydenhuollon, kaupunginhallinnan ja teollisuuden alalla on kasvanut. LoRaWAN tarjoaa kustannustehokkaan vaihtoehdon alhaisemman datanopeuden kustannuksella. (You ym. 2018, 28)

LoRaWAN 1.0:n turvallisuusuhat johtivat uudemman version, LoRaWAN 1.1:n, käyttöönottoon, mikä ei toki korjannut kaikkia uhkia. IoT-laitteiden ja LPWAN-verkkojen kehittyessä LoRaWANin uuden päivitetyn version julkaisu on väistämätöntä.

LÄHTEET

Adelantado, F. ym. 2017. Understanding the Limits of LoRaWAN. IEEE Communications Magazine. Viitattu 6.3.2020. https://arxiv.org/pdf/1607.08011.pdf

Aras, E., Lawrence, P., Hughes, D. & Ramachandran, G. S. 2017. Exploring the Security Vulnerabilities of LoRa. Viitattu 16.3.2020. https://core.ac.uk/download/pdf/84932416.pdf

Azevedo, F. & Fialho, V. 2018. Wireless Communication Based on Chirp Signals for LoRa IoT Devices. Viitattu 17.3.2020. PDF ladattavissa. http://journals.isel.pt/index.php/i-ETC/article/download/51/57

Bankov, D., Horov, J., Ljahov A. 2016. On the Limits of LoRaWAN Channel Access. Venäjän tiedeakatemia. Viitattu 3.3.2020. https://www.researchgate.net/publication/312485284_On_the_Limits_of_LoRaWAN_Channel_Access

Bajic, E., Chaxel, F., Mekki, K., Meyer, F. 2018. Overview of Cellular LPWAN Technologies for IoT Deployment: Sigfox, LoRaWAN, and NB-IoT. Viitattu 16.3.2020. https://ieeexplore.ieee.org/abstract/document/8480255

Butun, I., Eldefrawy, M., Gidlund, M., Pereira, N. 2019. Formal Security Analysis of LoRaWAN. Computer Networks. Viitattu 16.3.2020. http://www.diva-portal.org/smash/get/diva2:1269488/FULLTEXT01.pdf

Butun, I., Pereira, N., Gidlund, M. 2019 Security Risk Analysis of LoRaWAN and Future Directions. Viitattu 4.5.2020. https://www.mdpi.com/1999-5903/11/1/3

Digita 10 faktaa. Viitattu 3.3.2020. https://www.digita.fi/etusivu/palvelut-yrityksille/iot/lorawan-teknologia/10-faktaa-lorawan-ja-nb-iot-tekniikasta/

Digita LoRaWAN-ohje. Tekninen kuvaus ja ohje – ThingPark:n käyttö / Rajapinnat ja FAQ. Yrityksen sisäinen PDF. Viitattu 5.3.2020.

Digita LoRaWAN-teknologia. Viitattu 3.3.2020. https://www.digita.fi/etusivu/palvelut-yrityksille/iot/lorawan-teknologia/

Doerr, C., Karampatzakis, E., Kuipers, F & Yang, X. 2018. Security Vulnerabilities in LoRaWAN. 2018 IEEE/ACM Third International Conference on Internet-of-Things Design and Implementation (IoTDI). Viitattu 16.3.2020. https://pure.tudelft.nl/portal/files/46032668/IoTDI2018.pdf

Kinsta. Viitattu 11.3.2020. https://kinsta.com/knowledgebase/what-is-mysql/

Oracle MySQL. Viitattu 11.3.2020. https://www.oracle.com/mysql/

Parametric Quick Start Guide. Viitattu 4.3.2020. http://www.parametric.ch/downloads/PCR2_OD_R2_Quickstart_Guide_en-05.pdf

ThingPark Wireless. ThingPark Wireless Advanced Developer Guide. PDF. Viitattu 10.3.2020. https://partners.thingpark.com/sites/default/files/2017-11/AdvancedThingParkDeveloperGuide_V4.pdf

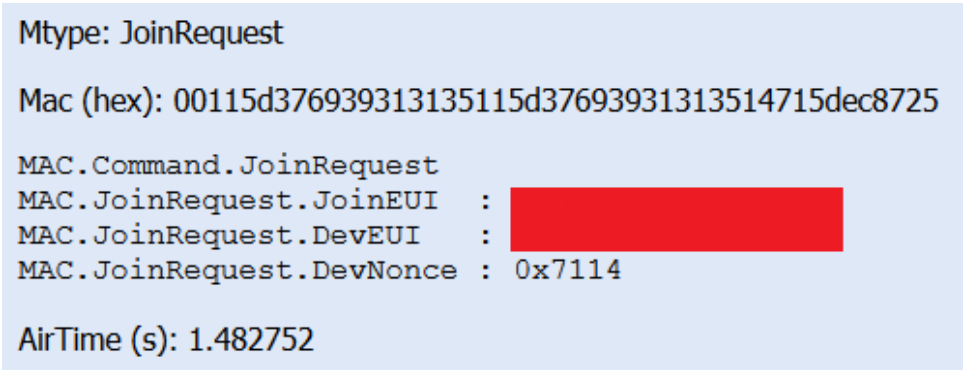
WiseNetwork, yrityksen taustat. Viitattu 7.5.2020. https://wisenetwork.fi/fi-fi/yritys/61/

Yang, X. 2017. LoRaWAN: Vulnerability Analysis and Practical Exploitation. Viitattu 16.3.2020. https://projets-ima.plil.fr/mediawiki/images/0/05/Thesis_Xueying_P27.pdf

You, I. ym. 2018. An Enhanced LoRaWAN Security Protocol for Privacy Preservation in Iot with a Case Study on a Smart Factory-Enabled Parking System. Viitattu 6.5.2020. https://www.mdpi.com/1424-8220/18/6/1888

```
{
    "DevEUI_uplink": {
        "Time": "2020-03-10T13:35:28.999+01:00",
        "DevEUI": [redacted]
        "FPort": 14,
        "FCntUp": 27,
        "ADRbit": 1,
        "MType": 4,
        "FCntDn": 29,
        "payload_hex": "0a000416000001012c",
        "mic_hex": "758f0e73",
        "Lrcid": "00000201",
        "LrrRSSI": -113.000000,
        "LrrSNR": -6.000000,
        "SpFact": 12,
        "SubBand": "G2",
        "Channel": "LC7",
        "DevLrrCnt": 2,
        "Lrrid": "FF017F65",
        "Late": 0,
        "LrrLAT": 61.488132,
        "LrrLON": 21.789967,
        "Lrrs": {
            "Lrr": [{
                    "Lrrid": "FF017F65",
                    "Chain": 0,
                    "LrrRSSI": -113.000000,
                    "LrrSNR": -6.000000,
                    "LrrESP": -119.973228
                }, {
                    "Lrrid": "FF017D42",
                    "Chain": 0,
                    "LrrRSSI": -114.000000,
                    "LrrSNR": -9.000000,
                    "LrrESP": -123.514969
                }]
        },
```


Osa uplink-viestin JSON-datasta.



Kuva: OTAA-menettelyssä päätelaite lähettää liittymispyynnön palvelimelle

oikeat	laite	erotus	erotuksen neliöt
0	0	0	0
3	0	3	1,732051
4	4	0	0
5	2	3	1,732051
0	0	0	0
0	0	0	0
5	5	0	0
9	4	5	2,236068
5	6	1	1
0	0	0	0
2	2	0	0
3	3	0	0
0	0	0	0
2	4	2	1,414214
4	2	2	1,414214
0	0	0	0
1	0	1	1
0	0	0	0
3	4	1	1
1	2	1	1
7	7	0	0
3	3	0	0
2	1	1	1
1	2	1	1
	keskiarvo	0,875	
	keskihaj	1,295897	
	neliösum	57	
	MSE	2,375	

Toteutuksessa pylväsdiagrammina kuvatut havainnot Excel-taulukossa.