TAMPEREEN
AMMATTIKORKEAKOULU

LANGATON IOT

Anne Nurmi

Opinnäytetyö
Toukokuu 2018
Tietotekniikka
Tietoliikennetekniikka ja tietoverkot

TIIVISTELMÄ

Tampereen ammattikorkeakoulu
Tietotekniikka
Tietoliikennetekniikka ja tietoverkot

ANNE NURMI:
Langaton IoT

Opinnäytetyö 30 sivua, joista liitteitä 2 sivua
Toukokuu 2018

Tämän opinnäytetyön tarkoituksena oli tutustua esineiden Internetiin (lyhyemmin IoT), eritysesti langattomuuden näkökulmasta, koska langattomien IoT-laitteiden määrä kasvaa jatkuvasti ja niiden kirjo on valtava.

Aluksi työssä tutkittiin IoT:tä ilmiönä yleisesti, käytiin läpi historiaa, palveluntarjoajia ja käyttökohteita, sekä perusteltiin langattomuutta. Seuraavaksi jaoteltiin langattomat IoT-tekniikat kantaman mukaan pitkän ja lyhyen kantaman tekniikoihin ja tutustuttiin niistä käytetyimpiin. Lopuksi tutkittiin tietoturvaan liittyviä ongelmia ja miten niitä kannattaisi huomioida käytännössä.

Todettiin, että langattomia IoT-tekniikoita on paljon eri tarkoituksiin ja niitä kehitetään lisää jatkuvasti. Kuitenkin tietoturvan nykytila saattaa muodostua ongelmaksi, jos siihen ei panosteta nykyistä enemmän, koska laitteet altistuvat jatkuvasti liian monille uhille, jotka vähentävät niiden käyttämisen mielekkyyttä.

Asiasanat: esineiden internet, langattomuus, tietoturva

ABSTRACT

Tampereen ammattikorkeakoulu
Tampere University of Applied Sciences
Degree Programme in ICT Engineering
Telecommunications and Networks

ANNE NURMI:
Wireless IoT

Bachelor's thesis 30 pages, appendices 2 pages
May 2018

The purpose of this thesis was to collect information about Internet of Things (IoT) and especially wireless IoT. There are many wireless IoT technologies and the amount of them is growing fast.

At first, IoT was studied generally, it's history, service providers and use cases. It was also explained, why wireless IoT devices are used so frequently. Next IoT technologies were divided into two groups: long range and short range technologies, and those that are mostly used, were introduced. Finally, some IoT security problems were presented and how they should be considered in practice.

It was discovered, that there are various IoT technologies for many different uses and they are continuously developed more. After all, the present state of information security can be a problem if it is not considered better, because devices are vulnerable for too many threats, and that can decrease the willingness to use IoT devices.

Key words: internet of things, wireless, information security

SISÄLLYS

LYHENTEET JA TERMIT

2G	2nd Generation, toisen sukupolven matkapuhelinteknologia
3G	3rd Generation, kolmannen sukupolven matkapuhelinteknologia
3GPP	3rd Generation Partnership Project -standardointijärjestö
4G	4th Generation, neljännen sukupolven matkapuhelinteknologia
5G	5th Generation, viidennen sukupolven matkapuhelinteknologia
CPS	Cyber Physical System, kyberfyysinen järjestelmä
CSS	Chrip Spread Spectrum, chirp-hajaspektritekniikka
EC-GSM-IoT	Extended GSM Internet of Things, GSM-tekniikasta laajennettu IoT-tekniikka
IoE	Internet of Everything, kaiken Internet
IIoT	Industrial Internet of Things, teollinen Internet
IoT	Internet of Things, asioiden Internet
LoRa	Long Range, pitkän kantaman IoT-tekniikka
LoRaWAN	Long Range Wide Area Network, pitkän kantaman laajaverkko
LPWAN	Low-Power Wide Area Network, vähätehoinen laajaverkko
LTE-M	LTE Machine, koneiden välinen 4G-viestintä
M2M	Machine-to-Machine, koneiden välinen viestintä
NB-IoT	Narrow Band IoT, kapeakaistainen IoT
NFC	Near Field Communication, lähiluenta
RFID	Radio Frequency Identification, radiotaajuuksilla toimiva tunnistustekniikka
UNB	Ultra Narrow Band, kapeakaistainen modulaatiomenetelmä
UPnP	Universal Plug ‘n Play Protocol, kytke-ja-käytä -protokolla
WLAN	Wireless Local Area Network, langaton lähiverkko

1 JOHDANTO

Tämän opinnäytetyön tarkoituksena on esitellä yleisimmät langattoman IoT:n tekniikat, niiden ominaisuudet ja käyttökohteet. Lisäksi työn loppuosassa pohditaan IoT:n tietoturvaa ja kuinka sitä voitaisiin parantaa tulevaisuudessa.

IoT, eli esineiden Internet on jatkuvasti kasvava tekniikan ala, jossa laitteet liitetään verkkoon, jotta niitä voidaan ohjata etänä ja niiden keräämät tiedot saadaan tallennettua esimerkiksi pilvipalveluun myöhempää käyttöä varten. Langattomuus on helppo ja halpa tapa saada tietoliikenneyhteys toimimaan laitteen ja pilvipalvelun välillä.

Langattomia IoT-tekniikoita on paljon erilaisiin tarkoituksiin ja niitä kehitellään jatkuvasti lisää kysynnän kasvaessa. Tässä työssä esitellään niistä osa, koska ei olisi mielekästä eritellä kaikkia niiden samankaltaisuuden ja suuren lukumäärän takia. Tekniikoiden kirjo ja yhä useampien laitteiden liittyminen verkkoon saattaa lisätä ongelmia esimerkiksi toisten laitteiden aiheuttamien häiriöiden muodossa, koska useat laitteet käyttävät samoja taajuusalueita.

Tietoturva on IoT:n osalta huonolla mallilla. Koska yhä erilaisemmat laitteet liittyvät Internetiin, myös uhat ovat uudenlaisia, eikä niiden tunnistaminen ole aivan yksinkertaista. Ongelmaksi muodostuu myös käyttäjien tietämättömyys uhista ja siitä, miten niiltä suojaudutaan. Toisaalta taas valmistaja ei pysty varautumaan laitteen suunnittelussa kaikkeen ja osa turvallisuudesta jää väkisin käyttäjän käsiin.

Lopuksi työssä pohditaan, miltä IoT:n tulevaisuus näyttää ja mitä tiedonsiirrolle tapahtuu tämän kehityksen myötä.

2 IOT YLEISESTI

IoT (Internet of Things), eli asioiden Internet on nykypäivänä monien ihmisten ja yritysten mielessä. Se kuulostaa monen mielestä tulevaisuuden utopialta ja suurelta mullistukselta ihmisten elämässä, ja vaikka se sitä osaltaan onkin, niin todellisuudessa IoT on arkipäivää jo useimpien ihmisten kohdalla. IoT:n historia alkaa vuodesta 1999, jolloin Kevin Ashton (2009) ehdotti englanninkielistä termiä Internet of Things käytettäväksi.

ITU-T:n suosituksen (Y.2060 2012) mukaan IoT on tietoyhteiskunnan maailmanlaajuinen infrastruktuuri, joka mahdollistaa virtuaalisten ja fyysisten asioiden yhdistämisen, perustuen olemassa olevaan ja yhteentoimivaan informaatioon, sekä tietoliikennetekniikoihin.

Termi IoT viittaa yleisesti siihen, kuinka laitteet, myös ne, jotka aiemmin eivät ole olleet verkossa, liitetään verkkoon, jotta niitä voidaan seurata ja ohjata etänä ja jotta ne voivat kommunikoida jopa keskenään. Useimmin IoT-laitteissa on erilaisia sensoreita, joilla kerätään dataa laitteen toiminnasta ja käytöstä, tai vallitsevista olosuhteista. Yleensä kerätty data lähetetään verkon kautta pilvipalveluun, jossa käyttäjä pääsee käsiksi laitteen keräämiin tietoihin ja jopa itse laitteeseen, riippumatta laitteen fyysisestä sijainnista.

2.1 Termit

Tässä työssä käytetään termiä IoT, mutta käytössä on paljon muitakin nimiä. IoT:llä viitataan monesti ilmiöön yleisesti, tai sillä voidaan tarkoittaa kuluttajien yksityiseen käyttöön tarkoitettuja laitteita. Toinen vastaava termi on IoE (Internet of Everything), eli kaiken Internet. Tätä termiä käyttää enimmäkseen verkkoyhtiö Cisco.

Teollisuudessa IoT tunnetaan paremmin nimellä teollinen internet. Englanniksi tämä termi on Industrial Internet of Things, eli IIoT. Toisaalta teolliseen internetiin viittaavat myös käsitteet M2M (Machine-to-Machine), joka viittaa koneiden keskinäiseen kommunikointiin, Saksassa syntynyt Industrie 4.0 eli Teollisuus 4.0, sekä CPS (Cyber Physical System), eli kyberfyysinen järjestelmä. (Collin & Saarelainen 2016, 29-33.)

2.2 Käyttökohteet

Tällä hetkellä IoT on käytössä niin teollisuudessa, kuin yksityisillä käyttäjilläkin. Uusissa laitteissa tarvittavat anturit on asennettu valmiiksi, mutta esim. jo käytössä oleviin tehdaslaitteisiin voidaan asentaa jälkikäteen tarvittavat anturit. Laitteista kerätään käytönaikaista tietoa, jota kerätään pilvipalveluun, johon käyttäjällä on pääsy. Tämä mahdollistaa laitteen etäseurannan. Toisaalta yhteys toimii myös toiseen suuntaan, eli käyttäjä voi tehdä muutoksia laitteen asetuksiin ja jopa käyttää laitetta etänä.

Laitteista kerättyjä tietoja voidaan hyödyntää monin eri tavoin. Esimerkiksi laitteiden hajoamisen saattaa pystyä ennustamaan kerättyjen tietojen pohjalta, ja näin välttämään hajoamisen huoltamalla laitteen ennakkoon. Näin voitetaan aikaa ja mahdollisesti parannetaan turvallisuutta. Joitakin huoltotoimia voidaan myös tehdä etänä. Esimerkiksi älypuhelimen päivitykset voidaan hoitaa verkon välityksellä ilman, että puhelin pitäisi viedä huoltoon.

Yksityishenkilöillä on käytössä esimerkiksi kodinvalvontalaitteita, joiden avulla voidaan tarkastella kodin tilannetta verkon välityksellä vaikkapa puhelimen sovelluksen avulla. Samalla sovelluksella voi esimerkiksi tarkistaa lämpötilan ja tarvittaessa säätää lämmitystä.

Puhelimissa on nykyisin erilaisia antureita, joiden keräämää dataa voidaan käyttää sovelluksissa hyödyksi. Esim. kiihtyvyysanturin avulla sovellus voi laskea, montako askelta käyttäjä on ottanut päivän aikana ja tämän tiedon perusteella ehdottaa vaikkapa liikunnan lisäämistä, jotta askelia tulisi otettua enemmän.

Teollisuudessa IoT mahdollistaa mm. koneiden tehokkaamman käytön. Etäohjattavuus ja -seuranta saattaa vähentää työvoimaa. Vaaralliselle tai hankalalle alueelle ei tarvitse välttämättä tarvitse mennä ollenkaan, tai vain huollon ajaksi. Viat voidaan huomata ja korjata ennakoivasti, jolloin niihin on varauduttu etukäteen, eikä yllättävä koneen hajoaminen sekoita tarkkaan määriteltyä, monesti tiukkaakin aikataulua.

IoT:n avulla tuotteen valmistajan ja asiakkaan välillä on mahdollista, että yhteys jatkuu ostohetken jälkeenkin. Tällöin valmistaja saa tietoa siitä, miten asiakas käyttää tuotetta ja pystyy kehittämään tuotettaan, sekä saattaa huomata viallisen tuotteen jo ennen asiakasta.

Näin esim. reklamaatiotilanteessa voidaan todentaa, onko kyseessä valmistusvirhe, tai onko tuotetta käytetty väärin.

Käyttömahdollisuuksia IoT:lle kehitetään jatkuvasti lisää. On vain mielikuvituksesta kiinni, mihin kaikkeen sitä voidaan hyödyntää. Tulevaisuudessa kaikkien esineiden käyttö, samoin kuin yritysten liiketoiminta ja eritoten ammatit tulevat kokemaan radikaalin muutoksen IoT:n myötä.

2.3 Langattomuus

IoT:n toteuttamiseen on monia eri tekniikoita. Monissa tapauksissa toteutus tehdään langattomasti, sillä se mahdollistaa laitteen joustavamman käytön. Jo olemassa oleviin järjestelmiin voi olla mahdotonta jälkikäteen asentaa verkkokaapeleita ja esimerkiksi liikkuvissa laitteissa langaton yhteys on ainoa vaihtoehto.

Suurissa paikallaan pysyvissä kohteissa verkkoyhteys voidaan toteuttaa langallisesti. Muissa tapauksissa langaton toteutus voi olla vaivattomampi, sekä halvempi toteutustapa, kun ei tarvitse suunnitella ja asentaa verkkokaapelointia. Langattoman tekniikan valintaan vaikuttaa mm. käyttöetäisyys, turvallisuus ja energiankulutus.

Tulevaisuudessa verkkoon liitettävien laitteiden ja esineiden määrä kasvaa huomattavasti, mikä myös puoltaa langattomuuden puolesta helppoudellaan. Käytön ja tarpeen lisääntyessä langattomien tekniikoiden hinta on romahtanut, mikä sekin osaltaan vauhdittaa langattomuuden yleistymistä.

Langattomien tekniikoiden lisääntyessä myös ongelmia saattaa ilmetä. Eri tekniikat käyttävät samoja taajuusalueita, jolloin kaista ruuhkautuu helposti. Toisaalta taas laitteilta vaaditaan tukea usealle eri tekniikalle, mikä saattaa vaikeuttaa laitteiden suunnittelua. Langattomuus tuo myös oman hankaluutensa tietoturvan saralla, kun laitteet ovat etähallittavia, mutta jollakin tavalla pitäisi estää asiattomien pääsy laitteen asetuksiin ja tietoihin.

2.4 Palveluntarjoajat

Jotta asioiden Internet toimisi mahdollisimman saumattomasti, tarvitaan useiden eri alojen osaamista. Tietoliikenne-, ohjelmisto- ja elektroniikkaosaamisen lisäksi tarvitaan kullakin alalla omaa erityistietämystä, jotta pystytään keräämään tarvittavat tiedot ja hyödyntämään niitä mahdollisimman hyvin. Kerätty data on usein monimutkaista, ja sen tulkitseminen vaatii erikseen data-analyysia.

Helpointa on ottaa yhdeltä palveluntarjoajalta valmis IoT-paketti, jossa kaikki tietämys ja IoT:n osa-alueet on yhdistetty valmiiksi usein muokattavissa olevaksi kokonaisuudeksi. Tällöin kaikki osa-alueet varmasti toimivat yhteen ja kaikki asiat hoituvat samassa paikassa. Tällaisia paketteja Suomessa tarjoavat mm. teleoperaattorit Elisa ja Telia, sekä verkkoyhtiö Digita. Monet yritykset ovat kehitelleet omaan käyttöön oman pakettinsa.

IoT:n myötä on syntynyt lisätarvetta sen osa-alueisiin keskittyneille yrityksille, kuten anturivalmistajille, verkkotekniikoiden kehittäjille, ohjelmistoyrityksille ja data-analyytikoille. Jokaiselta osa-alueelta löytyy suurempia tekijöitä, mutta myös pieniä startup-yrityksiä, kuten mittausjärjestelmiä suunnitteleva TreLab, ohjelmisto- ja analytiikkayhtiö Quva, sekä verkkoratkaisuja kehittäneet Wirepas ja Tosibox (Collin & Saarelainen 2016, 54).

3 PITKÄN KANTAMAN TEKNIIKAT

Pitkän kantaman IoT-tekniikat voidaan jakaa kahteen osaan: LPWAN-verkkoihin ja 3GPP-standardoituihin perinteisiin mobiiliverkkoihin (Nokia, 2015). Käyttökohteita ovat esim. älykkäät kaupungit ja suuret teollisuusalueet, joissa tarvitsee kattaa suuri alue.

3.1 LPWAN-verkot

LPWAN-verkot (Low Power Wide Area Network) useimmiten toimivat vapailla taajuuksilla ja niistä tunnetuimmat tekniikat ovat LoRa ja Sigfox. Tunnusomaisia ominaisuuksia LPWAN-verkoille ovat mm. pitkä akunkesto, halpa hinta, harva lähetysväli sekä lyhyet viestinpituudet.

3.1.1 LoRa

LPWAN-verkkoihin kuuluvan LoRan (Long Range) linkkibudjetti on suurempi, kuin millään muulla standardoidulla tietoliikenneteknologialla. Yhdellä tukiasemalla voidaan kattaa kokonainen kaupunkialue tai satoja neliökilometrejä, riippuen ympäristöstä. Samankaltaista teknologiaa on käytetty aiemmin sotilaskäytössä ja avaruudessa, mutta LoRa on ensimmäinen kaupalliseen käyttöön, erityisesti IoT:lle ja M2M:lle tarkoitettu modulaatiomenetelmä. (LoRa Alliance, 2015, 3-4.)

LoRa käyttää chirp-hajaspektritekniikkaa (CSS), mikä mahdollistaa vähäisen virrankulutuksen ja pitkän kantaman myös rakenteiden läpi. Sen ominaisuuksia on myös hyvä häiriönsieto, sekä diffraktion ja heijastumien pieni vaikutus signaaliin. Verkon topologiana käytössä on tähtitopologia, jolloin verkko on mahdollisimman yksinkertainen ja käyttää vähiten virtaa. Verkon noodit ovat epäsynkronisia ja ne lähettävät dataa vain silloin, kun se on ennalta määritelty lähetettäväksi, joko tietyin väliajoin, tai tietyn tapahtuman aikaan. Tyypillisesti viestien lähetystiheydet ovat 15 ja 60 minuutin välillä (Digita). Tämä ominaisuus tekee tekniikasta käytännölliseksi erilaisiin anturinluku- tai ohjaussovelluksiin.

Euroopassa LoRan käytössä on kolme kaistaa 868 MHz:n kaistalla. Kanavia yhdyskäytävillä on käytössä tyypillisesti kahdeksan ja päätelaitteiden pitää tukea vähintään 16:tta kanavaa. Yhden kanavan kaistanleveys on 125 kHz. Pohjois-Amerikassa käytössä on 915 MHz:n kaista. Uplink-suuntaan kanavia on käytössä 64 + 8 ja downlink-suuntaan on käytössä kahdeksan kanavaa. Lähetysnopeus vaihtelee välillä 0,3 – 5 kbit/s.

Parhaiten LoRa sopii käytettäväksi paristoilla toimiviin antureihin, älykkäisiin kaupunkeihin, teollisuusalueille, katuvalojen ohjaamiseen ja vaikkapa maatalouteen. Se on halpa, kuluttaa vähän virtaa ja vaatii hyvin vähän huoltoa pitkän akunkeston ansiosta.

LoRaa kehittää LoRa Alliance, johon voi liittyä kuka tahansa. LoRa on avoin tekniikka, jota saa hyödyntää mikä vain laitevalmistaja. Kuitenkin ainoa LoRa:lle soveltuvia radiomoduuleita valmistava yritys on Semtech (Schatz, 2016). Suomessa Digita kehittää ja valvoo LoRaWAN-verkkoa jatkuvasti ja nykyään verkko kattaa Suomessa jo suurimmat kaupungit (Digita).

3.1.2 Sigfox

Sigfox on samannimisen ranskalaisyhtiön luoma IoT-verkkoratkaisu. Se muistuttaa ominaisuuksiltaan LoRaa ja on näin kilpaileva teknologia LPWAN-verkkojen saralla. Sigfox on vähän virtaa kuluttava ja halpa ratkaisu IoT:n toteuttamiseksi. Kuten LoRalla, myös Sigfoxilla kantama on laaja, yhdellä tukiasemalla voidaan kattaa 10-15 neliökilometrin alue (Isohanni, 2017).

Modulaationa Sigfox käyttää Ultra Narrow Band -modulaatiota (UNB), mikä mahdollistaa häiriösietoisen signaalin, joka läpäisee rakenteet hyvin ja kuuluu pitkälle. Tämäkin tekniikka hyödyntää vapaita taajuuksia, Euroopassa 868 MHz kaistaa, Pohjois-Amerikassa 902 MHz kaistaa ja Etelä-Amerikassa, sekä Australiassa ja Uudessa-Seelannissa 920 MHz kaistaa.

Dataa Sigfox-laitteet lähettävät harvoin ja lähetettävät paketit ovat pieniä, maksimissaan 12 tavua. 24 tunnin aikaikkunan aikana Sigfox-laite voi lähettää enintään 140 viestiä 100

bit/s tiedonsiirtonopeudella. Tukiasema voi samassa ajassa lähettää 4 viestiä Sigfox-laitteelle, mutta viestin koko on vain 8 tavua, koska viestien tarkoitus on pelkästään muuttaa Sigfox-laitteen asetuksia. (Isohanni, 2017.)

Koska yhteys Sigfox-laitteen ja tukiaseman välillä on epäsymmetrinen, sopii Sigfox parhaiten sellaiseen käyttöön, jossa laite lähettää tukiasemalle harvoin pieniä lähetyksiä. Esimerkkinä tästä ovat erilaiset hälytykset tai mittaustulokset. (Schatz, 2016.)

Sigfox-verkko kattaa Suomessa jo 85 % väestöstä (Connected Finland) ja maailmanlaajuisesti 727 miljoonaa henkilöä kuuluu verkon kuuluvuusalueelle, yhteensä 36 eri maassa (Sigfox). Siinä missä LoRa Allianceen voi liittyä kuka vaan, Sigfox huolehtii omasta verkostaan ja myy sen palveluna muille yrityksille, joista tulee tämän ostettuaan oman alueensa Sigfox-operaattoreita (Schatz, 2016). Suomessa verkkoa ylläpitää Sigfox-operaattori Connected Finland.

3.2 Mobiiliverkot

Mobiiliverkkojen käyttäminen IoT:n toteuttamisessa on suosittua, sillä mobiiliverkot kattavat valmiiksi suurimman osan maailmasta, joten valmiina olevaa tekniikkaa voidaan vain jatkokehittämällä hyödyntää asioiden internetin käyttötarkoituksiin. IoT:tä varten on jatkokehitetty GSM- ja LTE-tekniikoita (Nokia, 2015), 3G-tekniikkaa ei enää tähän tarkoitukseen käytetä virtasyöppöytensä takia (Collin & Saarelainen, 2016, 175). Tulevassa 5G-tekniikassa IoT on otettu jo suunnitteluvaiheessa huomioon.

3.2.1 EC-GSM-IoT

EC-GSM-IoT (Extended Coverage GSM Internet of Things) on eGPRS:stä jatkokehitetty tekniikka, joka mahdollistaa pitkän, jopa 10 vuoden akunkeston ja laajan kantaman. Kyseinen tekniikka voidaan toteuttaa vain ohjelmistopäivityksellä jo olemassa olevaan GSM-verkkoon ja se toimii näin sekä 2G-, 3G-, että 4G-verkossa.

Koska tiedonsiirtonopeus on pieni, maksimissaan 140 kb/s, soveltuu EC-GSM-IoT parhaiten esimerkiksi mittaustulosten lähettämiseen, jolloin tietoa ei tarvitse siirtää paljoa.

Kaistanleveys tekniikalla on 200 kHz, eli kohtalaisen kapea, mikä mahdollistaa hyvän läpäisykyvyn materiaaleille. Kun yhdistää tähän laajan kantaman, voidaan tekniikkaa käyttää myös huonomman kuuluvuuden alueilla, kuten maaseudulla. (Nokia, 2017)

3.2.2 NB-IoT

NB-IoT (Narrow Band IoT) on 3GPP:n kehittämä 4G-mobiilistandardi. Kuten LPWAN-tekniikoillakin, myös NB-IoT:llä on tarkoitus siirtää pieniä datamääriä kerrallaan, 250 kb/s siirtonopeudella. Muina aikoina laite on lepotilassa, mikä lisää akunkestoa. (Telia)

Kapean kaistan, 180 kHz, ansiosta NB-IoT soveltuu hyvin käytettäväksi myös alueilla, joilla kuuluvuus on huono, kuten esimerkiksi kellareissa. Koska NB-IoT käyttää omaa lisensoitua taajuuskaistaansa, eivät muut laitteet aiheuta turhia häiriöitä. NB-IoT-signaali voidaan sijoittaa sekä GSM-, että LTE-verkon spektriin.

3.2.3 LTE-M

LTE-M (LTE Machine) tunnetaan myös nimellä eMTC (enhanced Machine Type Connection) on LTE:stä jatkokehitetty tekniikka. Se on hyvin samankaltainen kuin NB-IoT, mutta kaistanleveys on hieman leveämpi, 1,08 MHz. Toisin kuin NB-IoT, LTE-M toimii vain LTE-verkon taajuuksilla. (Nokia, 2017)

Nimensä mukaisesti LTE-M on tarkoitettu M2M-tyyppiseen viestintään. Akunkesto on 10 vuotta, kuten muillakin pitkän kantaman tekniikoilla. NB-IoT:hen verrattuna anturien hinta on hieman korkeampi.

3.2.4 5G

5G:n odotetaan vastaavan IoT:n tarpeita paremmin kuin nykyiset mobiiliverkkotekniikat. Se tulee olemaan kokoelma erilaisia tekniikoita ja se tulee tukemaan monipuolisemmin erilaisia sovelluksia. Nokia (2017, 10-11) odottaa 5G:n mahdollistavan mm. etäkirurgiaa, autonomiset kulkuneuvot ja teollisuusrobotit.

Suomessa verkkorakentaja Eltel on kehittänyt 5G-testiverkon erääseen senioriasuntokohteeseen Ouluun, jossa käytetään NB-IoT-tekniikkaa laitteiden välisten yhteyksien luomiseen. (Uusiteknologia.fi, 2017)

4 LYHYEN KANTAMAN TEKNIIKAT

Lyhyen kantaman tekniikoiden käyttökohteita ovat mm. älykkäät kodit ja erilaiset henkilökohtaiset älylaitteet, jotka eivät vaadi signaalin pitkää kantamaa.

4.1 Bluetooth

Bluetooth on yksi yleisimmistä tavoista toteuttaa IoT langattomasti. Sen suosio perustuu enimmäkseen siihen, että Bluetooth-tuki löytyy monista kulutuslaitteista, kuten älypuhelimista ja puettavista älylaitteista valmiiksi. Näin ollen on loogista käyttää valmiiksi saatavilla olevaa tekniikkaa. Myös anturin pieni koko ja edullinen hinta edistää tekniikan suosiota.

IoT:n tarkoituksiin on kehitetty kahta eri Bluetooth-tekniikkaa: BLE ja Bluetooth Mesh, jotka molemmat ovat kehittyneempiä versioita alkuperäisestä Bluetoothista. BLE kuluttaa vähemmän virtaa, mutta sen heikkous on verkon topologia, joka ei pysty kilpailemaan toisten mesh-verkkoja hyödyntävien IoT-tekniikoiden kanssa. Bluetooth Mesh vastaa tähän tarpeeseen käyttämällä verkkotopologianaan mesh-verkkoa, jolloin signaalin kantama laajenee ja näin käyttökohteet lisääntyvät.

4.1.1 BLE

BLE eli Bluetooth Low Energy, joka tunnetaan myös nimellä Bluetooth Smart, on vähemmän virtaa kuluttava versio Bluetoothista. Se on kehitetty nimenomaan IoT:n tarkoituksiin sopivaksi. BLE-piiri on pienikokoinen ja edullinen ja se on yhteensopiva mm. älypuhelinten tekniikan kanssa, joten siihen on helppo saada yhteys ilman erillisiä laitteita.

BLE toimii 2,4 GHz:n taajuudella ja sen kantama on muutamia kymmeniä metrejä. Tiedonsiirtonopeus BLE:llä on 1 Mb/s. Kovin suuria paketteja Bluetoothilla ei voida siirtää, vaan parhaiten BLE toimii pienten datamäärien siirtämiseen (Design Spark). Collin & Saarelaisen mukaan vähävirtaisuuden ansiosta BLE:llä voidaan saavuttaa parin vuoden akunkesto.

4.1.2 Bluetooth Mesh

Bluetooth Mesh nimensä mukaisesti hyödyntää mesh-verkkoa pystyäkseen kilpailemaan muiden vastaavien tekniikoiden kanssa, mitä edeltäjänsä BLE ei ole pystynyt tekemään. Yhdistämällä BLE:n ominaisuuksiin mesh-verkot, saadaan joustavampi ja pidemmällä kuuluvuudella varustettu teknologia, jolla saavutetaan lisää käyttökohteita.

Bluetooth Mesh on parhaimmillaan älykkäissä kodeissa ja rakennusautomaation eri käyttökohteissa, mutta se voi laajennetun kantamansa ansiosta päätyä käytettäväksi yhä enemmän myös teollisuudessa. (Kolderup, 2017.)

4.2 Zigbee

Zigbee on Zigbee Alliancen kehittämä avoin langaton standardi. Sen kehitys aloitettiin 90-luvun lopussa tarjoamaan vaihtoehto Wi-Fille ja Bluetoothille (Frenzel, 2012). Nykyisin versio Zigbee 3.0 kokoaa kaikki aiemmat Zigbee-standardit yhdeksi erilliseksi standardiksi (Design Spark).

Zigbee toimii vapaalla 2,4 GHz:n taajuusalueella ja sen tiedonsiirtonopeus on 250 kb/s. Verkkotopologiana toimii mesh-verkko, mikä mahdollistaa kommunikoinnin sujumisen, vaikka jokin verkon noodeista ei pystyisi välittämään liikennettä. Zigbee tukee jopa 65000 noodia.

Kantama vaihtelee 10 ja 100 m välillä ja vähäisen virrankulutuksen takia Zigbee Alliance lupaa seitsemän vuoden akunkeston. Turvallisuudesta on huolehdittu usealla tavalla: Zigbee käyttää mm. AES-128 -salausta, laite- ja verkkoavaimia, sekä kehyslaskureita. (Zigbee Alliance)

Standardi on joustava, mikä mahdollistaa sen käytön monissa erilaisissa käyttökohteissa ja monen eri valmistajan tuotteissa. Zigbeetä käytetään mm. älykkäissä kodeissa, älykkäässä valaistuksessa, sekä erilaisissa mittauskohteissa. (Zigbee Alliance)

4.3 Z-Wave

Zigbeetä toiminnallisesti muistuttava Z-Wave on alun perin Zensysin kehittämä langaton standardi. Toisin kuin useimpien langattomien standardien tapauksessa, Z-Wave ei ole avoin, vaan vaatii Sigma Designsilta saatavan lisenssin. Kuitenkin kuka tahansa voi liittyä Z-Wave -allianssiin, jonka tarkoitus on valvoa, että eri valmistajien Z-Wave -tuotteet ovat yhteensopivia keskenään. Standardi tukee myös IPv6-verkkoa, joten tekniikka todella on joustava ja yhteensopiva monien erilaisten laitteiden kanssa. (Z-Wave Alliance)

Kuten Zigbee, myös Z-Wave käyttää mesh-verkkotopologiaa, jossa voi olla jopa 232 noodia yhtä aikaa toiminnassa. Z-Wave sopii pienten pakettien lähettämiseen, tiedonsiirtonopeus on 100 kb/s. Tiedonsiirto tapahtuu sub-1GHz -taajuuksilla, joten muut langattomat tekniikat, kuten Wi-Fi eivät pääse häiritsemään yhteyttä. Zigbeen tavoin Z-Wave käyttää AES-128 -salausta. (Z-Wave Alliance)

Z-Wave soveltuu parhaiten älykkään kodin tarpeisiin, jossa lähetetään mittaustuloksia tai ohjauskäskyjä laitteille. Tekniikka kuluttaa vähän virtaa, joten laitteen akunkesto on pitkä. Kuuluvuus Z-Wavella on noin 30 m, eli käytännössä yhteys kattaa normaalikokoisen asuinhuoneiston kokonaan.

4.4 RFID ja NFC

RFID (Radio Frequency Identification) tarkoittaa radiotaajuuksilla toimivaa tunnistamiseen tarkoitettua tekniikkaa. Tekniikka toimii hieman kuten viivakoodi, jolla pystytään yksilöimään esine, mutta RFID-tunniste ei vaadi näköyhteyttä tietojen lukemiseksi ja sen sisältämiä tietoja voidaan muokata myöhemmin (RFIDLab Finland ry).

RFID on kokonaisuus, joka muodostuu tunnisteista, ns. RFID-tageista, jotka sisältävät lähetys- ja vastaanottoantenneja, sekä lukijalaitteista, joilla tietoa siirretään taustajärjestelmään ja joilla voidaan muokata tunnisteissa olevia tietoja. Koska näköyhteyttä tietojen lukemiseen ei tarvita, voidaan tunnisteiden tiedot lukea esimerkiksi suuremmissa erissä, viemällä ne luentaportin läpi. Näin vältytään tuotteiden yksittäiseltä siirtelyltä tietojen lukemiseksi.

Tunnisteita on kahdenlaisia, aktiivisia ja passiivisia. Passiiviset RFID-tunnisteet vain lähettävät tietoja, mutta aktiiviset tunnisteet sekä lähettävät, että vastaanottavat radiokyselyitä. Passiiviset tunnisteet ovat ohuita ja niiden kantama on vain muutaman metrin. Aktiiviset ovat noin kolikon kokoisia ja niiden kantama pidempi, muutamia kymmeniä metrejä. (Collin & Saarelainen, 2016, 180-181.) Tunnisteet ovat halpoja, ja niitä voidaan kiinnittää tuotteeseen sekä valmistusvaiheessa, että jälkikäteen.

Käyttökohteita RFID:llä on jo pitkään ollut mm. logistiikassa. IoT:n näkökulmasta tunnisteita voidaan hyödyntää esimerkiksi kaupoissa, jolloin tuotteissa voisi olla esimerkiksi antureita, jotka mittaavat vallitsevia olosuhteita ja tallentavat tietoa RFID-tunnisteeseen. Myös sairaaloissa voidaan kiinnittää tunnisteita vaikkapa sänkyihin ja pyörätuoleihin, jolloin voidaan seurata, missä mikäkin tarvike sijaitsee.

4.4.1 NFC

NFC (Near Field Communication) perustuu RFID-tekniikkaan. NFC-teknologiaa on mm. useimmissa matkapuhelimissa valmiina, eikä sen käyttämiseen tarvita erillistä sovellusta. Kuten RFID-tekniikassa yleisesti, myös NFC-siru voidaan kiinnittää haluttuun tuotteeseen myös jälkikäteen tarralla. Kuuluvuusalue on lyhyt tietoturvasyistä, vain muutamia senttimetrejä.

Tällä hetkellä tärkeimpiä käyttökohteita NFC:llä ovat mobiilimaksaminen ja mobiilimatkaliput. Se kuitenkin mahdollistaa myös kuvien ja tiedostojen siirtämisen NFC-laitteesta toiseen ilman kosketusta. NFC on tämänhetkisistä langattomista tekniikoista vähiten virtaa käyttävä. (Faulkner, 2017.)

4.5 WLAN

WLAN (Wireless Local Area Network), eli langaton lähiverkko, kaupalliselta nimeltään Wi-Fi, on luonnollinen ratkaisu moneen IoT-sovellukseen laajan saatavuutensa ja nopeutensa takia. Tällä hetkellä Wi-Fistä on käytössä 802.11ac-standardi.

Tiedonsiirtonopeus on tyypillisesti 150 – 200 Mbit/s ja kuuluvuus n. 100 m. WLAN toimii 2,4 GHz:n ja 5 GHz:n vapailla taajuuksilla, joten liikenteen ruuhkautuminen on potentiaalinen ongelma. Lisäksi signaali ei läpäise kovin hyvin rakenteita ja virrankulutus on IoT:n käyttötarkoituksiin erittäin suuri. (Design Spark.)

4.5.1 Wi-Fi HaLow

Uusi WLAN-standardi 802.11ah, eli Wi-Fi HaLow on kehitetty erikseen IoT- ja M2M-käyttöä varten. Wi-Fi HaLow toimii alle 1 GHz taajuuksilla ja sen kantama on jopa tuplasti pidempi, kuin nykyisellä WLAN-tekniikalla. Lisäksi signaalin rakenteiden läpäisykyky on parempi ja virrankulutus pienempi, mikä mahdollistaa sen käytön laajemmin IoT-sovelluksissa. (Wi-Fi Alliance.)

4.6 6LoWPAN ja Thread

6LoWPAN (IPv6 Low-power Wireless Personal Area Network) on IPv6-pohjainen verkkoprotokolla, joka ei tue ollenkaan IPv4-protokollaa. 6LoWPAN on eritoten suunniteltu koti- ja rakennusautomaation tarpeisiin, joissa tarvitaan pientä virrankulutusta ja kapeaa kaistaa. (Design Spark.)

Topologiana 6LoWPAN käyttää mesh-verkkoa ja se voi olla kytkettynä muihin IP-verkkoihin reitittimen avulla. Tämä tekniikka on yksinkertaisempaa kytkeä muihin verkkoihin, kuin vaikkapa Zigbee, joka vaatii monimutkaisemman yhdyskäytävän erilaisten verkkojen välille. (Olsson, 2014.)

4.6.1 Thread

Thread on Thread Groupin kehittämä protokolla, joka perustuu 6LoWPAN-protokollaan. Myös Threadin topologiana toimii mesh-verkko ja kuten 6LoWPAN, myös Thread on suunniteltu kodin automaation tarpeisiin.

Thread kykenee käsittelemään jopa 250 laitetta kerrallaan ja se toimii 2,4 GHz:n taajuusalueella. 802.15.4 -laitteissa Threadin käyttämiseksi vaaditaan vain yksinkertainen ohjelmistopäivitys. (Thread Group)

5 TIETOTURVA

5.1 Nykytila

Eräs IoT:n suosiota hidastava tekijä on tietoturvan nykytila IoT-laitteissa. Mediassa nousee ajoittain esiin uutisia käyttäjää vakoilevista IoT-laitteista, kuten esimerkiksi äly-TV tai lasten lelut. Tutkijat, kuten myös hakkerit, ovat löytäneet vakavia puutteita laitteiden salauksessa. Usein samat ongelmat koskevat myös kilpailijoiden vastaavia tuotteita, koska yleensä valmistajat käyttävät jo olemassa olevia ohjelmistoja tai avointa lähdekoodia.

Tällaisten uutisten ja omien kokemusten perusteella käyttäjät ovat huolestuneita yksityisyydestään. Samaan aikaan vähemmän asiaan perehtyneet käyttäjät eivät edes osaa kuvitella, mitä kaikkia uhkia laitteiden liittämisessä Internetiin voi ilmetä. Nämä seikat vähentävät ihmisten halukkuutta liittää yhä useampia laitteita verkkoon ja tätä kautta altistaa itsensä useammille tuntemattomille uhille.

5.2 Ongelmat

Tietoturvaan liittyviä ongelmia IoT:ssä on monia. Sekä käyttäjät, että laitteiden suunnittelijat ja valmistajat voisivat parantaa monessa asiassa. Kuitenkin samaan aikaan yhä erilaisempien laitteiden liittyessä Internetiin myös uhkia tulee lisää ja niiden tunnistaminen on osa ongelmaa. Mahdollisten uhkien arviointi ja estäminen on lähes mahdotonta, kun kukaan ei osaa edes ajatella, mitä kaikkea voi tapahtua.

Mahdollisesti suurin ongelma on se, että ihmiset eivät ymmärrä, kuinka verkot toimivat ja mitä kaikkea tulisi huomioida tietoturvan osalta. Kodeissa WLAN:n salasana on se, joka laitteen takana lukee, tai pahimmassa tapauksessa salasanaa ei ole asetettu ollenkaan. Tällöin kuka vain voi liittyä verkkoon ja pääsee myös käsiksi muihin verkossa oleviin laitteisiin. Kuitenkaan käyttäjät eivät huomaa huolestua yksityisyydestään, vaan huolenaiheena on vain vaikutus kaistaan tai se, käyttäkö joku ilmaiseksi maksullista Internetyhteyttä.

Teollisuudessa ongelmaksi on noussut se, että kuvitellaan, että laitteet eivät ole yhteydessä Internetiin, vaikka ne epäsuorasti ovat kuitenkin. Toisaalta tietoturvan puutteita perustellaan sillä, että hakkerit eivät ymmärrä teollisuudessa käytettävistä järjestelmistä tarpeeksi pystyäkseen aiheuttamaan vahinkoa. Teollisuuslaitoksessa kenelläkään ei välttämättä ole tarkkaa tietoa siitä, millainen verkkotopologia kokonaisuudessaan laitoksessa on ja eri laitteet saattavat käyttää eri verkkoyhteyksiä, jolloin yhteyksien kirjo muuttuu myös tietoturvauhaksi. (Collin & Saarelainen, 2016, 242 - 245)

Laitteiden suunnittelijoiden kohtaama ongelma on se, mikä on laitevalmistajan ja mikä käyttäjän vastuulla. Rajanveto saattaa olla vaikeaa ja käyttäjä helposti olettaa tuotteen olevan turvallinen, vaikka sen liittäisi suojaamattomaan langattomaan lähiverkkoon. Ihmiset eivät usein lue käyttöohjeita ja käyttöehtoja, joten tämäkin osaltaan vaikeuttaa rajanvetoa, kun toinen osapuoli ei edes ota selvää omista velvollisuuksistaan. Toisaalta taas käyttäjällä ei välttämättä ole tarpeeksi teknistä ymmärtämystä, eikä velvollisuudet selviä, vaikka kyseiset tekstit olisikin luettu.

IoT-laitteiden oletetaan yleensä olevan käyttövalmiita ns. plug-and-play -mallin mukaisesti. Käyttäjän kannalta tämä on hyvä, koska teknistä osaamista ei tarvita, mutta turvallisuuden kannalta tämä on erittäin huono asia. Pahimmillaan laitteet yhdistyvät verkkoon käyttämällä UPnP-protokollaa, joka löytää muut samaa protokollaa käyttävät laitteet ja muodostaa yhteyden niihin automaattisesti. Tämä tapahtuu käyttäjälle näkymättömästi ja myös sellaiset laitteet, joiden ei haluta olevan yhteydessä, pystyvät kommunikoimaan keskenään käyttäjän tietämättä. (Gilchrist, 2017, 50-51)

Laitevalmistajan kannalta ongelman tuottaa nykymarkkinat, joiden takia moni tuote viedään kauppoihin mahdollisimman nopeasti, usein jopa keskeneräisenä. Yleensä laite toimii kyllä, mutta sen testaus esimerkiksi tietoturvan osalta on kesken, jolloin saattaa jäädä huomaamatta vakavatkin puutteet. Kuitenkin tällainen testaaminen voi kestää kauan ja pahimmillaan laite saattaa jäädä kokonaan myymättä, jos testaamista jatketaan liian pitkään. Toisaalta tietoturva saattaisi olla myyntivaltti, jota kilpailijat eivät pystyisi kopioimaan. (Gilchrist, 2017, 66-67)

Laitteiden ohjelmistot aiheuttavat myös tietoturvauhkia monella tapaa. Tosiasia on, että monissa käytössä olevissa verkkoon liitetyissä laitteissa on käytössä vanhentunut käyttö-

järjestelmä ja vanhoja ohjelmistoversioita. Laitesuunnittelussa yleinen käytäntö on käyttää valmista koodia, johon luotetaan sokeasti, koska kaikki muutkin ovat käyttäneet samaa aikaisemmin, eikä kaikki haavoittuvuudet tule välttämättä ilmi, vaikka koodin tutkisi useampikin ammattilainen (Gilchrist, 2017, 77-78). Toinen ongelma ohjelmistoissa on erilaiset ajurit ja laiteohjelmat. Niiden päivitykset ovat ladattavissa Internetistä vapaasti, eikä niissä ole minkäänlaista tarkastusmekanismia lähteen tai muutosten osalta. Näin ollen hakkerit voivat vapaasti muokata ohjelmistoja ja jakaa niitä uusina versioina verkossa.

5.3 Mitä valmistaja voi tehdä

IoT-laitteen valmistajan tulisi jo suunnitteluvaiheessa ottaa huomioon tietoturva, määrittää mahdolliset uhat ja päättää mitä vastaan tulee suojautua. Pohdintaan liittyy myös se, mikä on oikeasti mahdollista. Käytännössä mihin tahansa IoT-laitteeseen voi murtautua, jos siihen pääsee käsiksi ja ymmärtää tarpeeksi sen toiminnasta, mutta monesti tärkeämpää on suojautua hyökkäyksiltä, jotka tapahtuvat esimerkiksi lähiverkon ulkopuolelta.

Tuotteen suunnitteluvaiheessa tulisi huolehtia, että salasanat ja lähetettävä data on salattua. Järkevää on myös miettiä, tarvitseeko laite kaksisuuntaista datayhteyttä, vai onko sen tarkoitus pelkästään lähettää keräämäänsä dataa, jolloin laitteen suuntaan ei tarvitse lähettää mitään.

Mahdollisesti hankalin osuus on se, miten määritellään, mitkä laitteet voivat luottaa toisiinsa ja voivatko ne olla yhteydessä käyttäjän huomaamatta. Samalla valmistajan tulee pohtia, mitä kaikkea tietoa kerätään ja lähetetäänkö sitä esimerkiksi kolmannelle osapuolelle ja kulkeutuuko kerätty data esimerkiksi toisten IoT-laitteiden kautta vielä eteenpäin.

5.4 Mitä käyttäjä voi tehdä

Käyttäjän tulee huolehtia verkon turvallisuudesta. On tärkeää, että kuka vain ei pääse verkkoon ja tätä kautta saa yhteyttä kaikkiin sen laitteisiin. Tämän mahdollistamiseksi salasanat tulee olla kunnossa ja palomuuri, sekä virusturva käytössä. Jos mahdollista, IoT-laitteet voisi liittää eri verkkoon, kuin vaikkapa puhelimet, tabletit ja tietokoneet. (Rashid, 2017)

Olisi tärkeää, että käyttäjä tutustuu tarkasti kaikkien IoT-laitteidensa toimintoihin ja ymmärtää mitä ne tekevät. Käyttöohjeen ja käyttöehtojen lukeminen on ensimmäinen asia, mikä tulisi tehdä. Laitteiden toiminnoista ne, joita ei tarvita, kannattaisi estää, samoin laitteen etähallinta, jos vain mahdollista.

Kuitenkin on ymmärrettävää, että kaikki ihmiset eivät ole perehtyneet tarpeeksi tekniikkaan, jotta he pystyisivät muuttamaan monimutkaisia asetuksia ja ymmärtämään kaikkia uhkaavia vaaroja. Tässä kohtaa pallo onkin taas laitteen valmistajalla, jonka tulisi tehdä tarpeeksi helppokäyttöinen laite ja siihen kattavat käyttöohjeet, sekä mahdollisesti tarjota käyttäjälle toimiva asiakaspalvelu vielä tuotteen käytön tueksi. Kaikkien näiden vaatimusten täyttäminen voi kuitenkin olla mahdotonta.

6 POHDINTA

Työssä tutkittiin eri tekniikoita, joilla liitetään IoT-laitteet Internetiin. Työssä kävi selväksi melko nopeasti, että tekniikoita on valtavasti, minkä takia työssä esiteltiin vain tärkeimmät ja käytetyimmät tekniikat. Lisäksi tarkasteltiin tietoturvaa IoT:n kannalta, koska nykypäivänä tietoturvan taso on huono, ja se uhkaa hidastaa laitteiden liittämistä verkkoon.

IoT:llä on monia käyttökohteita niin teollisuudessa, kodeissa, kuin kaupungeissakin ja perustelut eri laitteiden liittämiseen verkkoon vaihtelevat käytännön tarpeen ja silkan mukavuudenhalun välillä. Toiset laitteet parantavat turvallisuutta, toiset tehostavat ajankäyttöä ja toiset ovat vain mukavia leikkikaluja. Laitteiden määrän kasvaessa myös eri alojen ammattilaisille on kysyntää ja työssä todettiinkin, että työpaikkoja IoT:n saralla tulee olemaan paljon, vaikka se toisaalla saattaa niitä myös vähentää.

Eri tekniikoiden osalta todettiin, että samoihin käyttötarkoituksiin on useita eri tekniikoita ja on laitevalmistajan mielenkiinnosta kiinni, minkä tekniikan kuhunkin sovellukseen haluaa valita. Useimmat tekniikat käyttävät vapaita taajuuksia, joten häiriöiden määrä ja kaistan ruuhkautuminen saattaa muodostua ongelmaksi tulevaisuudessa laitteiden lisääntyessä.

Tietoturva osoittautui olevan huonolla mallilla ja todettiin, että uhkien määrä lisääntyy jatkuvasti ja uudenlaisia uhkia muodostuu, kun verkkoon liitettävien laitteiden laatu muuttuu. Kuitenkaan valmistajat eivät yksin pysty takaamaan laitteen täysin tietoturvallista käyttöä, vaan esimerkiksi verkon suojaaminen jää käyttäjälle. Ongelmana kuitenkin on, että tietoturvasta huolehtiminen saattaa olla vaikeaa tekniikkaan perehtymättömille käyttäjille.

Työtä olisi voinut vielä jatkaa esimerkiksi käytännön esimerkin avulla, mutta ajanpuutteen takia se jäi tekemättä. Tietoturva osoittautui niin laaja-alaiseksi aiheeksi, että siitä saisi aivan oman työnsä. Kuitenkin tästä työstä käy tutuksi tärkeimmät osa-alueet ja langattomasta IoT:stä muodostuu hyvä pohjakäsitys.

LÄHTEET

Ashton, K. 2009. RFID Journal. That 'Internet of Things' Thing. Luettu 18.12.2017. http://www.rfidjournal.com/articles/view?4986

Collin, J & Saarelainen, A. 2016. Teollinen internet. Helsinki: Talentum Media Oy.

Connected Finland. Olemme osa maailman laajinta IoT-verkkoa. Luettu 28.12.2017. http://www.connectedfinland.fi/fi/

Design Spark. 11 Internet of Things (IoT) Protocols You Need to Know About. Luettu 18.4.2018
https://www.rs-online.com/designspark/eleven-internet-of-things-iot-protocols-you-need-to-know-about

Digita. Mikä on LoRaWAN? Luettu 27.12.2017
https://www.digita.fi/yrityksille/iot/mika_on_lorawan

Faulkner, C. 2017. Techradar. What is NFC? Everything you need to know.
https://www.techradar.com/news/what-is-nfc

Frenzel, L. 2012. Electronic Design. What's The Difference Between ZigBee And Z-Wave?
http://www.electronicdesign.com/communications/what-s-difference-between-zigbee-and-z-wave

Gilchrist, A. 2017. IoT Security Issues. Boston/Berlin: Walter de Gruyter Inc.

Isohanni, J. 2017. Centria Bulletin. Sigfox – maailmanlaajuinen IoT-verkkoliittymä.
https://centriabulletin.fi/sigfox-maailmanlaajuinen-iot-verkkoliittyma/

ITU-T. 2012. Recommendation Y.2060. Overview of the Internet of things.
https://www.itu.int/ITU-T/recommendations/rec.aspx?rec=y.2060

Kolderup, K. 2017. Bluetooth Blog. Introducing Bluetooth Mesh Networking.
https://blog.bluetooth.com/introducing-bluetooth-mesh-networking

Liew, C. 2015. IoTnow. The Smart Home Radio Protocols War.
https://www.iot-now.com/2015/08/10/35653-the-smart-home-radio-protocols-war/

LoRa Alliance. 2015. LoRaWAN. What is it? A technical overview of LoRa and LoRaWAN.
https://docs.wixstatic.com/ugd/eccc1a_ed71ea1cd969417493c74e4a13c55685.pdf

Nokia. 2015. White Paper. LTE evolution for IoT connectivity.
https://onestore.nokia.com/asset/200178/Nokia_LTE_Evolution_for_IoT_Connectivity_White_Paper_EN.pdf

Nokia. 2017. White Paper. IoT connectivity – understanding the options and choices.
https://onestore.nokia.com/asset/201050/Nokia_IoT_Connectivity_White_Paper_EN.pdp

Olsson, J. 2014. Texas Instruments. 6LoWPAN demystified.
http://www.ti.com/lit/wp/swry013/swry013.pdf
Rashid, F. Y. 2017. Tom's Guide. How to Secure Your (Easily Hackable) Smart Home
https://www.tomsguide.com/us/secure-smart-home-how-to,news-19380.html

RFIDLab Finland ry. Mitä on RFID? Luettu 17.4.2018
http://www.rfidlab.fi/rfid-teknologia/mita-on-rfid/

Schatz, G. 2016. Link Labs. SigFox Vs. LoRa: A Comparison Between Technologies & Business Models.
https://www.link-labs.com/blog/sigfox-vs-lora

Sigfox. Our key figures. Luettu 28.12.2017.
https://www.sigfox.com/en

Telia. NB-IoT. Luettu 10.1.2018.
https://www.telia.fi/yrityksille/tuotteet/liittymat/iot-ratkaisut/nb-iot

Thread Group. What is Thread. Luettu 18.4.2018.
https://www.threadgroup.org/What-is-Thread

Uusiteknologia.fi. 2017. Eltel rakentaa Ouluun 5G-IoT-testiverkkoa.
https://www.uusiteknologia.fi/2017/11/27/eltel-rakentaa-ouluun-5g-iot-testiverkkoa/

Wi-Fi Alliance. Wi-Fi HaLow. Luettu 18.4.2018.
https://www.wi-fi.org/discover-wi-fi/wi-fi-halow

Zigbee Alliance. Zigbee for Developers. Luettu 17.1.2018.
http://www.zigbee.org/zigbee-for-developers/

Z-Wave Alliance. Luettu 29.1.2018.
https://z-wavealliance.org/

LIITTEET

Liite 1. LoRan ja mobiiliverkkotekniikoiden vertailu. (Nokia, 2017)

	LoRa	GSM (Rel.8)	EC-GSM-IoT (Rel. 13)	LTE (Rel. 8)	eMTC (Rel. 13)	NB-IoT (Rel.13)
LTE user equipment category	N/A	N/A	N/A	Cat.1	Cat.M1	Cat.NB1
Max.Coupling Loss	160 dB	144 dB	164 dB	144 dB	156 dB	164 dB
Spectrum	Unlicensed <1GHz	Licensed GSM bands	Licensed GSM bands	Licensed LTE bands In-band	Licensed LTE bands in-band standalone	Licensed LTE in-band guard-band standalone
Bandwidth	<500KHz	200KHz	200KHz	LTE band carrier bandwidth (1.4-20MHz)	1.08MHz (1.4MHz carrier bandwidth)	180kHz (1.4kHz carrier bandwidth)
Max. data rate*	<50kbps (DL/UL)	<500 kbps (DL/UL)	<140kbps (DL/UL)	<10Mbps(DL) <5Mbps(UL)	<1Mbps (DL/UL)	<170 kbps (DL) <250 kbps (UL)

Liite 2. Älykodin tekniikoiden vertailu (Liew, 2015)

Variable	Wi-Fi	Z-Wave	ZigBee	Thread	BLE
Year first launched in Market	1997	2003	2003	2015	2010
PHY/MAC Standard	IEEE 802.11.1	ITU-T G.9959	IEEE 802.15.4	IEEE 802.15.4	IEEE 802.15.1
Frequency Band	2.4 GHz	900 MHz*	2.4 GHz	2.4 GHz	2.4 GHz
Nominal Range (0 dBm)	100 m	30 – 100 m	10 – 100 m	10 – 100 m	30 m
Maximum Data Rate	54 Mbit/s	40-100 kbit/s	250 kbit/s	250 kbit/s	1 Mbit/s
Topology	Star	Mesh	Mesh	Mesh	Scatternet
Power Usage	High	Low	Low	Low	Low
Alliance	Wi-Fi Alliance	Z-Wave Alliance	ZigBee Alliance	Thread Group	Bluetooth SIG