SAVONIA

OPINNÄYTETYÖ - **AMMATTIKORKEAKOULUTUTKINTO**
TEKNIIKAN JA LIIKENTEEN ALA

KNX JA IOT-MAAILMAN TUTKIMUS

TEKIJÄ: Petteri Lammi

SAVONIA-AMMATTIKORKEAKOULU

OPINNÄYTETYÖ
Tiivistelmä

Koulutusala Tekniikan ja liikenteen ala	
Koulutusohjelma/Tutkinto-ohjelma Sähkötekniikan tutkinto-ohjelma	
Työn tekijä(t) Petteri Lammi	
Työn nimi KNX ja IOT-maailman tutkimus	
Päiväys 10.11.2020	Sivumäärä/Liitteet 54/10
Ohjaaja(t) Pekka Aho (AH-Talotekniikka), Tossavainen Mika (AH-Talotekniikka), Heikki Laininen (Savonia), Arto Toppinen (Savonia)	
Toimeksiantaja/Yhteistyökumppani(t) AH-Talotekniikka (AH Elens Oy)	

Tiivistelmä
Opinnäytetyön aihe oli selvittää KNX automaatiojärjestelmän sekä tulevaisuuden IoT-maailman yhteensovittamista.

Työntavoitteena oli selvityksen lisäksi rakentaa demolaitteisto, jossa jo olemassa olevan langattoman standardin laitteita käytettäisiin kaksisuuntaisesti KNX järjestelmän sekä laitteiden välillä. Tämä voisi mahdollistaa halvan sensori verkoston käyttämistä KNX taloautomaatiojärjestelmän ohjaukseen. Työssä tutustuttiin nykyisiin langattomiin IoT verkkoihin, niiden ominaisuuksien sekä yhteensopivuuden määrittämiseksi. Jonka lisäksi perehdyttiin KNX tulevaisuuden KNX IoT verkkoon. Ajatuksena oli myös tehdä vertailu puhtaan KNX-järjestelmän sekä KNX järjestelmän ja kolmannen järjestelmän sensoriverkon hinta eroa, sekä säätömahdollisuuksien suhteen. Tätä ei kuitenkaan lopulta toteutettu, sillä työn aikana ilmeni, että useat standardit olivat vielä hyvin kehittyvässä vaiheessa sekä tuomassa uusia versioita markkinoille muutaman vuoden sisällä. Tällöin taloautomaation vaatima varmuus sekä laitteiden yhdistäminen, laitteiden käyttötapa sekä laitteiden hinnat muuttuisi hyvin nopeasti työn valmistumisen jälkeen. Työn aikana ilmestyikin uusia versioita sekä standardien välisiä uusia yhteistyö kuvioita.

Opinnäytetyön tuloksena saatiin rakennettu toimiva demolaitteisto, jolla KNX ja IoT laitteet saatiin toimimaan toistensa järjestelmistä, lisäksi saatiin yleistätietoa mihin KNX standardina tulevaisuudessa tähtää, ja millä langattomilla standardeilla se mahdollisesti jatkossa toimii.

Avainsanat
KNX, IoT

SAVONIA UNIVERSITY OF APPLIED SCIENCES

THESIS
Abstract

Field of Study Technology, Communication and Transport			
Degree Programme Degree Programme in Electrical Engineering			
Author(s) Petteri Lammi			
Title of Thesis Research on Integration between KNX and IoT			
Date	10 November 2020	Pages/Appendices	54/10
Supervisor(s) Pekka Aho (AH-Talotekniikka), Tossavainen Mika (AH-Talotekniikka), Heikki Laininen (Savonia), Arto Toppinen (Savonia)			
Client Organisation /Partners AH-Talotekniikka (AH Elens Oy)			

Abstract

The purpose of this thesis was to research integration of KNX building automation and future IoT systems.

The aim of the thesis in addition to the research, was to build a demonstration hardware, consisting of two-way communication between an existing wireless sensor system and KNX building automation. This could allow to utilize a cheap sensor network to be used with KNX building automation. The thesis explored current wireless IoT systems to determine their viability and compatibility with KNX, and KNX plans for the future of KNX IoT. Originally the idea was to compare the cost and controlling possibilities between a traditional KNX system and a KNX system with IoT devices. But it was not carried out since those IoT systems were still in a developing state and new versions were to be published in a few years. In this case the configuration, devices and prices would have changed shortly after finishing the thesis. During the thesis work there were new versions and new co-operations between systems.

As a result, a working demonstration hardware that allows operation between KNX devices and IoT devices was build. The research also gave general knowledge where KNX as a standard is aiming to advance in the future, and with which wireless standards it could operate.

Keywords
KNX, IoT

SISÄLTÖ

LYHENNELUETTELO

M2M	MACHINE TO MACHINE
ISM	INDUSTRIAL, SCIENTIFIC AND MEDICAL
OSI-MALLI	OPEN SYSTEMS INTERCONNECTION REFERENCE MODEL
SPOF	SINGLE POINT OF FAILURE
ITU	INTERNATIONAL TELECOMMUNICATION UNION
SRI	SMART READINESS INDICATOR
COAP	CONSTRAINED APPLICATION PROTOCOL
MQTT	MESSAGE QUEUING TELEMETRY TRANSPORT
AMPQ	ADVANCED MESSAGE QUEUING PROTOCOL
EHS	EUROPEAN HOME SYSTEMS PROTOCOL
EIB	EUROPEAN INSTALLATION BUS
IOT	INTERNET OF THINGS
OFDMA	ORTHOGONAL FREQUENCY-DIVISION MULTIPLE ACCESS
MIMO	MULTIPLE-INPUT AND MULTIPLE-OUTPUT

1 JOHDANTO

Kiinteistöautomaatiojärjestelmät ovat kehittyneet vuosikymmenten aikaan nopeasti relepohjaisista järjestelmistä moderneihin väyläpohjaisiin järjestelmiin. Tulevaisuuden näköpiirissä on kuitenkin suuri muutos tuntemattomaan, kun väyläpohjaisista automaatiojärjestelmistä siirrytään IoT maailmaan.

Opinnäytetyön tilaaja toimii AH-talotekniikka (AH Elens Oy), joka tilasi tutkielman aiheesta KNX ja IoT maailman tutkimus. Tarkoituksena oli selvittää tämän hetken KNX järjestelmän ja IoT:n yhteen sovittamista, sekä tutkita uusia mahdollisuuksia kiinteistöautomaation suhteen IoT:n avulla. Aihe liittyy vahvasti alati muuttuvaan kiinteistöautomaation mahdollisiin uusiin suuntauksiin, jossa myös AH-talotekniikka haluaa pysyä mukana. Tarkoituksena oli myös selvittää kustannuksia puhtaan KNX järjestelmän sekä yhdistetyn järjestelmän välillä. Tavoitteena oli kerätä yleistä tietoa IoT:n liittämisestä KNX järjestelmään ja tavoitteena on tehdä yleistieto paketti aiheesta tulevaisuuden insinööri sukupolvien käytettäväksi.

2 KNX

2.1 Yleistä

KNX on avoin väyläpohjainen hajautettu kiinteistöautomaatiojärjestelmä. Se perustettiin 2000- luvun alussa ”uutena” kiinteistöautomaatiojärjestelmänä, mutta se perustuu jo 1990-luvun alussa Belgiassa 15 tunnetun eurooppalaisen sähköyhtiöiden perustamaan EIB (European Installation Bus) standardiin, jonka tavoite oli perustaa yhteinen väyläteknologia, jota valmistajat voivat hyödyntää omissa tuotteissaan, sekä kiinteistöautomaatiossa, säilyttäen yhteensopivuuden muiden laitevalmistajien laitteiden kanssa. EIB protokolla perustui parikaapelin käyttöön, joka on myös säilynyt yhdeksi KNX käytetyimmäksi käyttötavaksi.
Vuonna 1997 kolme standardia, EIB (European Installation Bus), EHS (European Home Systems Protocol) sekä Batibus päättivät yhdistyä ja perustaa KNX:n. Vuonna 2002 julkaistiin ensimmäinen KNX spesifikaatio ja samalla KNX sertifiointi järjestelmä käynnistettiin. Jokainen KNX laite täytyy sertifioida, jotta laitteen markkinoinnissa voidaan käyttää KNX nimeä tai logoa hyödyksi. Sertifiointia hoitaa useat riippumattomat laboratoriot ympäri maailmaa. Vuonna 2003 KNX protokolla, käyttäen parikaapelia sekä datasähköä, hyväksyttiin eurooppalaiseen CENELEC standardiin EN 50090. Myöhemmin myös langaton KNX RF (Radio Frequency) protokolla hyväksyttiin KNX standardiin. Vuonna 2007 KNX hyväksyttiin myös kansainväliseen ISO/IEC 14543-3, sekä Kiinalaisen GB/Z 20965 standardiin. Samana vuonna myös KNX IP hyväksyttiin KNX standardiin. (KNX Association, 2013)

KNX- järjestelmän tavoite on yhdistää kiinteistön sähköisiä toimintoja toimimaan yhden järjestelmän sisällä, parantamaan rakennuksen energiatehokkuutta, parantamaan rakennuksen käyttömukavuutta sekä muokattavuutta.

2.2 Toimintaperiaate

KNX toiminta perustuu KNX laitteista löytyviin mikrokontrollereihin, jotka kommunikoivat väyläpohjaisesti eri laitteiden välillä. KNX-järjestelmä myös tukee Parikaapelia, IP pohjaisia verkkoja, Powerline eli sähkönkaapelissa tapahtuvaa tiedonsiirtoa, sekä KNX RF langatonta verkkoa. KNX-järjestelmässä parikaapelilla ainoa kielletty topologia on ”suljettu” rengastopologia, jolla pyritään estämään saman käskyn kiertämistä uudestaan väylän sisällä. Muuten parikaapelia käytettäessä sallittuja topologioita ovat linja, puu tai tähti. Pienin mahdollinen KNX järjestelmä sisältää anturin, yhden toimilaitteen, teholähteen sekä laitteiden välisen väyläkaapeloinnin

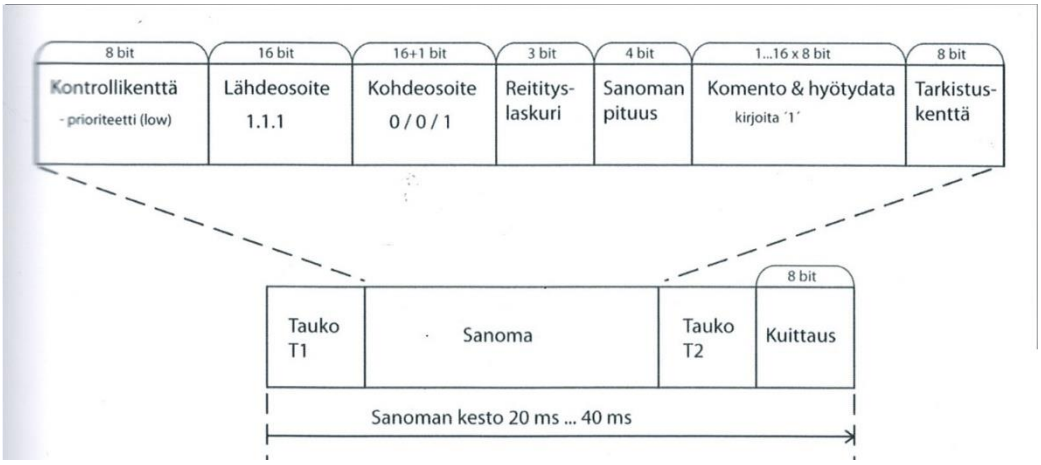
Anturi voi kerätä tietoa ympäristöstään esimerkiksi lämpötilan muutoksesta, painikkeen painamista tai valoisuuden muutoksesta. Tämän jälkeen anturi lähettää sanoman ympäristönmuutoksesta väylään. Anturit vievät tyypillisesti hyvin vähän virtaa (alle 300mW), jolloin niille ei tarvitse vetää omaa virtajohtoa vaan laite voi hyödyntää väyläkaapelin virtaa.
Toimilaitteita toimivat fyysisesti annettujen sanomien mukaan, niitä voivat olla esimerkiksi valaistuksen himmennys, lämmittimen ohjaus tai sähkölaitteiden ohjaus. Toimilaitteet kytketään lähes poikkeuksetta rakennuksen sähköverkkoon, sillä usein väyläkaapelista saatavilla oleva virta ei riitä toimilaitteiden käyttämiseen.

Teholähde tuottaa väyläkaapelin toiminnan vaadittavan tehon (30VDC). Tyypillinen KNX-järjestelmän tehonlähde ei vastaanota taikka lähetä sanomia väylältä. Vaan tuottaa vain väylän vaatiman tehon. KNX-järjestelmän tehonlähteet ovat standardoituja, joissa standardi vaatii teknisiä erityisvaatimuksia, eikä sitä korvaamaan voi käyttää yleiskäyttöisiä teholähteitä. (Härkönen, 2015)

KNX järjestelmässä olemassa kahdenlaisia osoitteita, ryhmäosoite sekä yksilöllinen osoite. Lähes jokaiselle väylän laitteelle ohjelmointi hetkellä annetaan yksilöllinen osoite, ainoa poikkeukset ovat teholähteet. Yksilöllisen osoitteen esitysmuoto on kolmen pisteellä erotetun luvun sarja. Yksilölliselle osoitteelle on varattu 16 bittiä, joista ensimmäisten kahden luvun välillä 4 bittiä, joka mahdollistaa luvut 0-15, ja kolmannelle luvulle 8 bittiä, joka mahdollistaa luvut 0-255. Yksilöllisiä osoitteita käytetään vain käyttöönottovaiheessa. KNX-järjestelmän ollessa käynnissä, ei yksilöllisiä osoitteita käytetä. Ryhmäosoitetta käytetään väylällä olevien laitteiden välisessä tietoliikenteessä. Ryhmäosoitteen esitys tapoja on kolme, kolmen tason, kahden tason tai vapaa esitystapa. Vapaata esitystapaa ei suositella, sillä monet visualisointiohjelmat tunnistavat vain kolmen tason esitystavan.
Ryhmäosoitteen koko on myös 16 bittiä, jotka jakautuvat eri tavoin riippuen esitystavasta. Kolme tason esitystavassa on kolme sarjaa, joista ensimmäisessä sarjassa on pääryhmä (5 bittiä, 0-31), toisessa sarjassa keskiryhmä (3 bittiä, 0-7), ja viimeisessä sarjassa alaryhmä (8 bittiä 0-255). Ryhmäosoite voi olla esimerkiksi muotoa 2/1/6, ryhmäosoitteita voi täten olla yhteensä 32 767

SANOMA

KNX järjestelmässä on kahdentyyppisiä sanomia, täsmälähetys- sekä ryhmälähetyssanomia. Täsmälähetyssanoma on tarkoitettu vain yhdelle laitteelle, kun taas ryhmälähetyssanoma on tarkoitettu yhdelle tai usealle vastaanottajalle. Esimerkkinä ryhmälähetyssanomaa voidaan käyttää huoneen kaikkien valojen ohjaukseen yhdellä sanomalla, tai täsmälähetyssanomaa voidaan käyttää lämpötilan lähetystä lämmitinlaitteelle.
Itse sanoma sisältää seuraavat kentät; Kontrollikenttä, joka vaikuttaa sanomien väliseen järjestykseen viestien törmäystilanteessa, mikäli KNX järjestelmässä välitetään hälytystoimintoihin liittyviä sanomia, voidaan niille antaa etusija. Lähdeosoite, joka kertoo mistä sanoma on lähetetty. Kohdeosoite, joka sisältää joko ryhmäosoitteen tai yksilöllisenosoitteen riippuen onko sanoma ryhmälähetys vai täsmälähetys. Reitityslaskuri, joka on sanoman mukana kulkeva numero. Sanoman lähtiessä arvo on 6, joka kerta kun sanoma kulkee yhdistimen tai toistimen kautta numero pienenee yhdellä.



Kuva 1, KNX sanoma (Härkönen, 2015)

Kun numero on 0 poistaa yhdistin tai toistin sanoman väylästä. Tällä ehkäistään ”haamu” viestin kulkeminen loputtomasti ympäri väylää. Loput viestissä on käyttökelpoista dataa, joka voi sisältää komennon tai hyötydatan. Viimeisenä on tarkastuskenttä, joka sisältää lähetetyn viestin tarkastussumman, tällä tavoin voi vastaan ottanut laite tarkistaa lähetetyn sanoman, mahdollisten tiedonsiirtovirheiden varalta. Kuvassa 1 löytyy esitettynä KNX sanoma.

KNX sanomat kulkevat väylässä vuorotellen, väylä laite kuuntelee edeltävän sanoman kuittauksen odottaa ajan T1 jonka jälkeen se alkaa lähettämään omaa viestiään. Mikäli kaksi laitetta aloittaa viestin lähettämisen samaan aikaa, keskeyttää myöhemmin aloittanut laite viestin välityksen. Tämä riippuu myös kontrollikentän arvosta. Parikaapelissa viestit kulkevat 9600 bittiä/s, joka vastaa yhdessä väylässä noin 20 sanomaa sekunnissa. Kuvassa 1 on esitettynä sanoma sekä sanoman liikkuminen väylässä taukoineen.

Yhdessä parikaapelilinjassa voi olla enintään 64 KNX laitetta. Tämä suurin laitemäärä riippuu laitteiden vaatimasta virrasta sekä KNX virtalähteestä. Linja voidaan myös jakaa enintään neljään linjasegmenttiin, käyttäen linjavahvistimia. Tällöin jokaisella segmentillä täytyy olla oma virtalähde ja suurin laitemäärä muuttuu väylän osalta 256 laitteeseen, mikäli käytetään 16 bittisiä osoitteita. Linjassa on myös muita rajoitteita, linjan pituus saa olla enimmillään olla 1 000 metriä sekä etäisyys virtalähteen ja kauimmaisen laitteen välillä saa olla enintään 350 metriä. Kahden laitteen välinen etäisyys saa olla enintään 700 metriä sekä virtalähteiden välinen etäisyys tulee olla vähintään 200 metriä.
Mikäli laitemäärä kasvaa yli 256 voidaan rakennuksen eri osia rakentaa omiksi väylikseen ja yhdistää ne päälinjaan linjayhdistimillä. Päälinja vaatii oman virtalähteensä ja siihen voidaan liittää enintään 15 linjaa, päälinjaa ei voida jakaa linjatoistimilla linjasegmenteiksi. Tällöin eri KNX väylät ovat yhteyksissä toisiin väyliin päälinjan kautta. Päälinjaan voidaan myös kytkeä lisää KNX laitteita, jolloin linjan teoreettinen laitemäärä kasvaa 3 840 laitteeseen. 15 päälinjaa puolestaan voidaan yhdistää runkolinjaan, jolloin laitemäärä kasvaa 57 375 laitteeseen. Parikaapelilla on kuitenkin rajoituksensa, eikä runkolinjaa suositella käytettäviksi todella suurissa KNX asennuksissa, joissa parikaapelilla toteutettu runkolinja voisi ruuhkautua. Parikaapelilla suurin rajoitus tiedonsiirtokapasiteetin lisäksi on 1 000 metrin suurin sallittu väylän pituus. Tätä voidaan kuitenkin parantaa, käyttämällä KNX IP verkkoa, tällöin KNX sanomat kulkevat hyvin pitkiä matkoja valokuitua pitkin. Tällöin myös tiedonsiirtokapasiteetti kasvaa jopa 1000 kertaiseksi parikaapeliin verrattaessa. KNX IP verkkoa voidaan myös käyttää väylä- tai runkolinjana. KNX TP sanomat kulkevat salaamattomina parikaapelissa, mikäli myös parikaapelin viestit halutaan salata, vaaditaan tähän KNX laitteilta tuki myös KNX Data Security standardille. Ennen KNX Data Securitya, ohjeistettiin suunnittelijoita sekä asentajia asentamaan laitteet sekä väylät siten, että niihin olisi hankala päästä kiinni. Teoriassa hyökkääjä voisi päästä KNX väylään kiinni ja alkaa ohjaamaan laitteistoja, mutta laitteiden tarkkaan ohjaukseen tarvittaisiin kuitenkin ETS semantiikka, tätä voidaan osittain kiertää kuuntelemalla väylän liikennettä. Ilkivalta tapauksessa myös KNX väylän oikosulkeminen voisi aiheuttaa väylän toimimattomuutta.

KNX RF laitteet liitetään TP/RF-rajapinnan kautta, jolloin jokainen langaton laite paritetaan rajapinnan kanssa. KNX RF toimii alle yhden gigahertsin taajuuksilla ja uusin vuonna 2010 julkaistu KNX RF standardi mahdollistaa kolmen nopean kanavan sekä kahden hitaan kanavan käytön. Nopeat kanavat mahdollistavat nopeamman tiedonsiirron, jota käytetään esimerkiksi ihmisten käyttämiin laitteiden kanssa, hitaat kanavat puolestaan sopivat esimerkiksi LVI laitteille, joiden viiveet saavat olla pidempiä. Uudistus on kuitenkin yhteensopiva vanhan vuoden 2003 standardin kanssa. RF laitteita on sekä yksisuuntaisena, että kaksisuuntaisena. Yksisuuntaiset laitteet paritetaan TP/RF-rajapinnan kanssa, mutta ne eivät saa omaa yksilöllistä osoitetta. Yksisuuntaisien laitteiden suuri ongelma on ollut luotettavuus, sillä lähettävä laite ei voi tietää menikö sanoma perille.
Kaksisuuntaiset laitteet sen sijaan saavat oman yksilöllisen osoitteen TP/RF-rajapinnan muodostamasta langaton linja. Kaksisuuntaiset laitteet voivat myös käyttää sanomatoistimia, joilla RF toimialue voi olla suhteellisen suuri. KNX RF toimii tähtitopologiassa, vaikkakin jokainen RF laite voi olla yhteydessä useampaan TP/RF-rajapinta laitteeseen, tämä tarkoittaa ettei kaksisuuntaisilla laitteilla ole samaa 64 laitteen rajoitusta mitä parikaapelilla, mutta koska kanavia on rajallinen määrä on uhkana, että RF verkko ruuhkautuu.

KNX PL laitteet toimivat olemassa olevan sähköverkon päällä se toimii 1200 bit/s nopeudella.
Koska PL laitteet vaativat joitakin muutoksia sähkökeskuksessa (kaistanestosuodatin, vaihesilta) ja koska sähköverkkojen omat häiriöt vaikeuttavat PL laitteiden viestintää, tehden viestinnästä epävakaata, on KNX PL laitteet lähes kokonaan poistuneet markkinoilta.

2.3 KNX ja IoT

NYKYINEN TILANNE KNX IOT

Nykyisellään KNX ja muiden IoT standardien yhteensovittamiseen on ollut tarjolla joko suoria yhdyskäytäviä, jotka yhdistävät eri standartit suoraan ilman internetin välitystä. KNX tulevaisuuden visiona on kuitenkin ollut suora internet pohjainen IoT tuki.
Nykyisin on olemassa keskitin ratkaisuja KNX:n sekä eri IoT standardien välillä, jolloin useat standardit voivat toimia samasta laitteesta käsin, eikä jokaisen valmistajan omaa yhdyskäytävää tarvitse ostaa ja liittää verkkoon erikseen. Näissä on kuitenkin omat ongelmansa, keskittimen konfigurointi vaatii yleensä internet yhteyden valmistajan palvelimille, jolloin riskinä on, että IoT laitteistojen tietoja vuotaa myös valmistajien palvelimille. Sekä uhka siitä, että laitevalmistaja lopettaa syystä tai toisesta tuen laitteellensa. Tällöin laitteisto toimisi niin pitkään, kunnes keskitin hajoaa tai kun verkkoon täytyisi tehdä muutoksia. Tällä hetkellä keskittimien konfigurointi vaatii internet yhteyttä laitteiden nopean muutoksien sekä laitteiden ohjelmistojen päivityksien myötä, jolloin laitteiden toiminnan takaamiseksi tarvitaan hakea keskittimen valmistajan palvelimilta tiedot laitteiden ohjelmistojen muutoksista. Suoraan KNX ja muita IoT standardeja tukee Zipaton Zipabox, jolla kuitenkin vaatii

konfigurointiin internet yhteyden valmistajan palvelimille. Muita yleisiä keskitin ratkaisuja ovat Samsungin SmartThings sekä suomalainen Cozify. Muihin IoT järjestelmiin verrattuna KNX järjestelmän kenties yksi heikkous on tietojen keräämättä jättäminen, jolloin historiatietojen perusteella voitaisiin kiinteistöä säätää tarkemmin.

KNX HAHMOTELMAT TULEVAISUUTEEN

KNX associationilla on pyritty varautumaan IoT kehitykseen, tekemällä IoT suunnitelman.
Ennen vuotta 2016 KNX-järjestelmän ratkaisuna oli tehdä KNXnet/IP standardi, jonka käyttö vaati turvallisen yhteyden IP-muuntimeen. Monet valmistajat loivat omia ei standardoituja malleja tämän käyttöön. Vaikka KNX järjestelmän ohjaus onnistuu KNXnet/IP:n ylitse ei se sisällä kiinteistön ohjaukseen vaadittavaa semantiikkaa. Tällöin ryhmäosoitteet ja laitteet täytyy tietää etukäteen ohjatakseen järjestelmän toimintaa, sekä ohjauskomentojen täytyy olla KNX sanomia.
Vuonna 2016 ilmestyi KNX Web Services, joka toi standardisoidun yhdyskäytävän KNX järjestelmän sekä IoT maailman väliin. Se sisälsi korjauksia edelliseen KNXnet/IP:n toimintaan tuomalla ETS ohjelmiston avulla tietoa kiinteistön KNX-järjestelmän semantiikasta. Jolloin yhdyskäytävän avulla myös täysin ulkopuoliset henkilöt voivat nähdä, mikäli heille on annettu oikeudet, mitä laitteita järjestelmässä on kiinni. ETS ohjelmistosta voidaan myös valita mitä laitteita yhdyskäytävän kautta voidaan ohjata.
KNX association ei kuitenkaan suositellut tätä käytettäväksi vielä kaupallisiin tarkoituksiin.
Vuonna 2018 tarkoituksena oli julkistaa KNX IoT 2.0, jonka tarkoituksena olisi saada ns. ”Plug and play” internettiin yhdistetty ”KNX web services”, ilman VPN yhteyksiä. Tällöin myös standardisoidut IoT pilvipalvelut olisivat käytettävissä. Kiinteistön KNX-järjestelmän semantiikka tuotaisiin selainpohjaisella työkalulla WS (Web services) yhdyskäytävästä.

Vuonna 2020 KNX aikoo lanseerata KNX IoT 3.0, jossa KNX laitteet toimivat nativisti IP verkon päällä, ja mikäli kiinteistö on uusi, ei perinteisiä KNX väyliä tarvita lainkaan. Yhteensopivuuden vanhoihin asennuksiin varmistetaan yhdyskäytävällä. Tällöin myös vanhoihin asennuksiin voidaan lisätä uusia IP-pohjaisia KNX laitteita. Samalla myös turvallisuutta lisätään IP-pohjaisten KNX laitteiden välillä. Uudet IP-pohjaiset KNX laitteet myös sisältävät itsessään semantiikkatietomallin, jolloin niiden ohjaaminen on mahdollista myös muilta laitteilta ja ne voivat mahdollisesti ohjata laitteita ilman tarvetta uudelleen ohjelmoimiseen. Vuoden 2020 jälkeen julkistettaisiin KNX IoT 4.0, jossa KNX laitteet olisivat itseoppivia. (KNX Association, 2016)

KNX on myös tuonut uusia turvallisuuskonsepteja, joita oletettavasti tullaan käyttämään myös tulevaisuudessa KNX IoT laitteissa. KNX IP Turva on protokolla, joka suojaa KNX IP yhdistimien keskinäisen sekä laitteiden välisen IP-pohjaisen tietoliikenneyhteyden. Tällöin kaikki liikenne, joka liikkuu IP-verkossa, on salattu eikä ulkopuoliset pääse näkemään salattua sisältöä. Kuitenkin muut väylän KNX laitteet näkevät lähetetyt KNX sanomat. KNX IP Turva vaatii, että jokainen KNX IP laite kykenee käyttämään KNX IP Turvaa. Verkkoja, joissa KNX IP Turva laitteita ja tavallisia KNX IP laitteita on sekoitettuna ei voida turvata käyttäen KNX IP Turvaa. KNX IP Turva käyttää AES 128 CCM salausta.

KNX Data Turva protokolla taas suojaa koko yhteyden kahden KNX laitteen välillä, teoriassa vaikkei KNX IP Turva ole käytössä, se suojaisi laitteiden välisen sanoman myös IP-verkossa. KNX Data Turva myös vaatii, että lähettävä ja vastaanottava laite tukevat KNX Data Turvaa, mutta kaikkien KNX verkossa olevien laitteiden ei tarvitse tukea sitä. (KNX Association)
KNX Data Turva käyttää myös AES 128 CCM salausta laitteiden välillä. Koska Data Turva ei voi salata kaikkea tietoja vaan KNX osoitteet täytyy säilyä luettavana, on Data Turva paketeissa myös laskuri, jottei hyökkäävätaho voi tallentaa käytettyä liikennettä ja hyödyntää tätä sanomaa myöhemmin. Varmennuskoodilla vastaanottava laite kykenee tunnistamaan, mikäli viestiä on koitettu muokata matkan aikana. Varmennuskoodi avataan laitekohtaisella salausavaimella, jolloin muut kuin haluttu vastaanottaja ei niitä voi nähdä.

3 ESINEIDEN INTERNET

3.1 IoT yleisesti

Esineiden internetillä tarkoitetaan hyvin yksiselitteisesti laitteita tai esineitä, jotka ovat yhteydessä toisiinsa, yleensä internetin välityksellä, siirtäen tietoja joko itsestään, toiminnastaan tai sensoreidensa havaitsemista asioista itsenäisesti, ilman ihmisten puuttumista tiedon kulkuun. Tällöin puhutaan siis M2M eli Machine to Machine protokollista. Tiedonsiirto laitteiden välillä on myös usein kaksisuuntaista, jolloin se mahdollistaa pelkän tiedonkeräyksen lisäksi myös laitteiden ohjaamisen. Yleisesti IoT laitteisiin luetaan vain aikaisemmin ”tyhmät” laitteet, jolloin esimerkiksi älypuhelinta tai tietokonetta ei lueta IoT laitteeksi.

IoT:lla ei ole virallista määritelmää, joten teoriassa siihen riittäisi vain, että laitteet ovat yhteydessä toisiinsa M2M tapaan, tällä tavoin myös KNX voitaisiin tietyin ehdoin luokitella IoT-järjestelmäksi. ITU (international Telecommunication Union) on määritellyt sen seuraavasti, “The IoT can be viewed as a global infrastructure for the information society, enabling advanced services by interconnecting (physical and virtual) things based on existing and evolving interoperable information and communication technologies (ICT).” (ITU, International Telecommunication Union)

3.2 IoT rakennusautomaatiossa.

Rakennusautomaatiossa IoT mahdollisuudet ovat lähes rajattomat, sensoroinnin lisääminen tuottaa valtavasti lisää tietoa kiinteistön tilasta, energiankulutuksesta sekä käytöstä.

Sensoroinnilla saadaan tietoa rakennuksen tilasta, lämpötilasta, vesivuodoista, kosteudesta, ilmanpaineesta, ilmanlaadusta. Näitä tietoja voidaan käyttää usealla eri tavalla, sekä estämään kiinteistön vaurioituminen, vesivuotoantureita voidaan sijoittaa vapaasti vesiputkien läheisyyteen sama anturi voi myös sisältää lämpötilan mittauksen, jolloin se voi myös hälyttää, mikäli putket uhkaavat jäätyä. Se voi myös samalla katkaista kyseisen piirin vedensyötön, jolloin mahdollinen vesivahinko jää pieneksi. Kosteusantureilla voidaan säätää ilmanvaihtoa siten, että ilmankosteuden taso on alle sallitun, niiden avulla voidaan myös talvella mitata kosteutta ja näillä tiedoilla mahdollisesti nostaa ilmankosteutta.
Ikkuna ja ovisensoreilla voidaan estää ovien tai ikkunoiden unohtumisen auki tai edes tarpeen avata ikkunoita, jos ikkunoita avataan useasti voi sitä koittaa ”ehkäistä” tehostamalla ilmanvaihtoa. Etenkin talvella auki jäänyt ikkuna voi aiheuttaa putkirikkoja.
Lämpöantureita voidaan asentaa usealle erikorkeuksille, jolloin nähdään ilmankerrostumaa, jota voidaan säädettävän puhaltimen avulla sekoittaa tarvittaessa lisää. Myös lämpötila-antureiden sijoitus itsessään voidaan muuttaa mittaamaan esimerkiksi keskeltä huonetta tai työpisteen läheisyydeltä. Lasten usein käyttämä lattiatason mittauksella voidaan varmistua, etteivät lapset kärsi liian kylmistä leikkipinnoista. Tällöin huoneiden säätö voidaan räätälöidä jokaiselle käyttäjälle sopivaksi.
Myös valaistauksen värilämpötilaa säätämällä voidaan saavuttaa etuja, talvisin kaamosaikaan voidaan värilämpötilaa muokata päivänvaloa vastaavaksi, myös sen aikaa voidaan säätää, jotta iltaisin

sinisen valon saanti vähenee. Laitteilla voidaan myös mitata ilmanlaatua sekä hiilidioksidin määrää ilmassa, suurin etu on, että se voidaan sijoittaa sinne missä ihmiset ovat, kouluissa pulpettien päälle, kokoustiloissa, työpisteissä pöydälle. Koska hiilidioksidi pysyy suhteellisen pitkään samalla paikalla ja on ilmaa raskaampi kaasu, ei katossa olevat sensorit välttämättä kerkeä reagoimaan epäsuotuisaan tasoon tarpeeksi nopeasti. Tällöin kiinteistö voisi periaatteessa ilmoittaa näitä tiloja käyttävälle, että tauko olisi paikallaan, ja alkaa tehostamaan ilmanvaihtoa sekä mahdollisesti säätää toimilaitetta puhaltamaan eri suuntiin, lopulta optimoiden suunnan, jonne puhaltaa. Pienimmissä pitoisuuksissa esimerkiksi ihmisten poistuttua syömään, voisi kiinteistö automaattisesti käyttäjien huoneistosta poistumisen jälkeen reagoida hiilidioksidipitoisuuteen tuulettamalla huonetta, kunnes tasot ovat laskeneet. Myös VOC sensoreilla voidaan tarkkailla kiinteistön sisäilmanlaatua, mikäli niiden tasot muuttuvat merkittävästi voidaan ruveta etsimään syytä jo ennen kuin kiinteistön käyttäjiltä alkaa saapua huomautuksia sisäilmaongelmista. Tallennetuilla tiedoilla voidaan myös osoittaa, mikä on ollut aikaisemmin normaali taso. IoT laitteet voisivat myös auttaa tuetussa asumisessa, esimerkkinä markkinoille on jo saapunut älykkäitä kamera- tai sensoripohjaisia järjestelmiä, jotka kykenevät tulkitsemaan ihmisten asennon. Jos käyttäjä kaatuu älykiinteistö voisi koittaa ”herätellä” henkilöä väläyttämällä valoja tai esimerkiksi palovaroitinta, mikäli käyttäjä on maannut esimerkiksi keittiön tai suihkuhuoneen lattialla yli määritellyn ajan. Mikäli henkilö ei reagoi näihin, voisi kiinteistö hälyttää paikalle ulkopuolista apua. Kiinteistö voisi myös kytkeä lieden pois päältä, mikäli käyttäjä poistuu huoneistosta, joka korvaisi perinteisen liesivahdin. Kiinteistö voisi myös automaattisesti säätää autojen talvella tarvitseman lämmityksen, analysoimalla käyttäjän päivärutiinin sekä auton käytön. Tällöin autoa voitaisiin lämmittää täsmälleen oikealla ajalla, jotta auto olisi lämmin käyttäjän lähtiessä. Myös tulevaisuudessa sähköautojen lataaminen tai lämmitys voitaisiin säätää kiinteistön avulla.

IoT tuo uusia mahdollisuuksia kiinteistönhoidolle, katolle voidaan asentaa sensorit mittaamaan katolla olevan lumen määrää, ilman paikallakäyntiä. Eri laitteet voivat ilmoittaa käyttötunneistaan, ja esimerkiksi valaisimet voivat ilmoittaa kiinteistönhoitajalle, kun niiden käyttöikä alkaa lähestymään valmistajan lupaamaa käyttöikää, jolloin valaisinten vaihtoon voidaan varautua etukäteen. Valaisin voisi myös itse kertoa, kun se on hajonnut. Tiedolla voidaan vertailla eri valmistajien tuotteiden kestoa, ja jos valaisin hajoaa ennen takuuajan loppumista, voisi kiinteistö ilmoittaa siitä automaattisesti myös valmistajalle. Myös sähkönkulutusta voidaan seurata, jolloin mahdollisesti viallinen laite voidaan löytää pelkästään yksittäisen pistorasian tai huoneiston sähkönkulutuksen muuttumisena. Tällöin kulutustietoa voidaan verrata aikaisempaan esimerkiksi tilanteessa, jossa kiinteistö on ollut tyhjillään, mutta sähköä kuluu historiatietoja enemmän. Samoin vedenkulutusta voitaisiin mitata, ja mikäli siinä tulisi poikkeuksellinen äkillinen muutos, voitaisiin asiaa tutkia, tai sulkea piirejä vesivuodon estämiseksi. Näiden lisäksi läsnäolotiedoista voitaisiin tarkastaa mitkä huoneet kaipaavat siivousta, ja kävijälaskurilla voitaisiin myös tarkkailla käytävän käyttöä, jolloin siivoja voisi tulla joko siivoamaan ja vahaamaan käytäviä etu- tai jälkikäteen, riippuen tilojen käyttömäärästä.

Kiinteistö voisi IoT:n tietojen perusteella sekä analysoinnilla ennustaa tulevien tuntien jopa päivien energiankulutusta. Tulevaisuuden sähköverkon mahdollistaessa tuntiperusteisen laskutuksen, voitaisiin kiinteistölle antaa tietyt parametrit lämmityksen, viilennyksen ja muun energiankäytöstä, joilla kiinteistö voisi itsestään ennakoinnilla säätää näitä arvoja ja täten säästää ”suhteellisen” normaalilla

toiminnalla sähkölaskuissa. Säästön suuruuteen vaikuttaa lopulta ennustuksen tarkkuus sekä sähkönhinta, todella suurissa hintapiikeissä säästö voisi teoriassa olla myös suuri. Riippuen annetuista parametreistä kiinteistön käyttäjät eivät välttämättä huomaisi eroa.

Kysyntäjousto saapuu tulevaisuudessa yhä pienemmille kiinteistöille, kantaverkko yhtiö Fingrid pilotoi jo 2019 syksyllä 1 MW minimitarjouskokoa säätösähkömarkkinoilla. Tämä tarkoittaa, että hyvin suuri kulutukselliset kiinteistöt voivat osallistua suoraan myös säästösähkömarkkinoille, sekä se helpottaa useiden pienten kiinteistöjen yhdistymistä yhdeksi virtuaaliseksi ”yksiköksi”. Energian säästöä saadaan myös huonekohtaisilla läsnäoloantureilla, jolloin energiaa säästetään vähentämällä käyttämättömien huoneiden lämmitystä tai viilennystä. Historiatietoja käyttämällä voidaan laskea lämmityksen vasteaika samoissa olosuhteissa, esimerkiksi mikäli huone on lämmennyt kolme astetta aikaisemmin yhdessä tunnissa, voidaan huoneiston historiatiedoista ennakoida, milloin käyttäjä saapuu paikalle ja aloittaa lämmitys juuri oikeaan aikaan. Tällöin teoriassa voidaan säästää lämmityksestä jopa yön yli tapahtuvasta lämmönpudotuksesta, mikäli huoneen vasteaika on tarpeeksi matala jäähtymisen sekä lämmityksen suhteen. Mikäli huoneistossa on myös ovianturi olisi mahdollista tiputtaa lämpötilaa vielä lisää, sillä lämpötilan tiputtaminen synnyttää myös vetoa, kun lämmin ilma pyrkii tasaamaan lämpötilan kylmän ilman kanssa. Mikäli ovi estää tämän ilmavirran, vähentää se vedontunnetta sekä lämmityksen tai viilennyksen siirtymistä muista huoneista ja täten parantaa säätövastetta. Tulevaisuudessa kiinteistö voi myös hakea sääennusteet tunneille tai päivälle, jolloin säädöstä saadaan vielä tarkempi.

Kiinteistön viilennyksessä ja lämmityksessä voidaan myös säästää avaamalla ja sulkemalla kaihtimia ja markiiseja, mikäli huoneistossa on tyhjillään. Tällöin kesällä jäähdytys kustannukset laskevat, kun auringon lämpö jää kiinteistön ulkopuolelle. Ja talvella vastaavasti auringon tuottamaa lämpöä voidaan ohjata sisälle lämmittämään huoneistoa, tiputtaen lämmityskustannuksia. Ikkunan ulkopuolelle voidaan asentaa valoisuus- sekä ilmanpaineanturit, joilla pystytään seuraamaan auringon tuottamaa lämpöä ja kiinteistöön kohdistuvan tuulen voimakkuutta, joilla kiinteistön lämmityksen säätäminen helpottuu. Tällöin myös markiisien ja kaihtimien käytöstä saadaan automaattista, eikä kiinteistön käyttäjät välttämättä huomaa näiden toimintaa.

Teoreettisesti myös jokaisen yksittäisen huoneiston sähkönkulutus voidaan mitata antureiden avulla, jolloin myös huoneistoa lämmittävien laitteiden vaikutus voidaan huomioida lämmityksen säädössä. Kiinteistön valaistuksen määrää voidaan myös mitata ja säätää, mikäli aurinko tuottaa tarpeeksi valoa huoneistoon, voidaan huoneiden valaistusta himmentää säästäen sähköä. Suurissa tiloissa tai käytävillä taas voitaisiin käyttää läsnäolonantureiden antamaa tietoa, missä on havaittu liikettä ja tällä tavoin sytyttää valot vain 5-10 metrin etäisyydellä käyttäjästä. Tällöin kiinteistö tuottaisi valoa vain siellä missä käyttäjä kulkee, valojen syttyessä ja sammuessa käyttäjän liikkeiden mukaan.

Mikäli kiinteistön tiedot annetaan oppivalle tekoälylle voisi se myös laskea optimaalisia asetuksia jokaiselle tunnille ja jokaiselle yksittäiselle huoneelle. Tämä on tarpeen etenkin siinä tilanteissa, mikäli huonekohtainen ilmastointi ei tue kuin yhtä anturia, tällöin tekoäly kykenisi laskemaan tarvittavan arvon käyttäen useita eri antureita. Tekoäly voisi myös tehdä ennustuksen kiinteistön kulutuksen tasosta jopa paikallisesti, vertailemalla aikaisempien vuosien lämmitystietoja sekä sääennustuksia toisiinsa.

Perinteisille KNX sensoreille vedetään Suomessa usein KNX parikaapeli, joka vähentää perinteisille sensoreille mahdollisen lisävirran vedon, mutta joka kuitenkin lisää parikaapelin verran asennettavaa. Langattomat ratkaisut mahdollistavat sekä kaapelinvedon vähentämisen, että sensoreiden sijoittamisen paikkoihin, joissa KNX sensorin tai laitteen asentaminen olisi kannattamatonta tai mahdotonta. Langattomien laitteiden etuna on myös jälkiasennukset, mikäli jostain syystä rakennuksen valmistumisen jälkeen tarvitaan johonkin kiinteistön osaan lisäominaisuuksia tai mikäli sensoreiden sijoittaminen ei ole onnistunut vaan alueita jää katveeseen. Tällöin on mahdollista lisätä langattomia sensoreita nopeasti ja edullisesti.
Myös muiden langattomien järjestelmien hinnat voivat olla KNX järjestelmiä halvempia, joka mahdollistaa useampien laitteiden käyttämistä samalla hinnalla kuin yhdellä KNX sensorilla. Halvempi hinta lopulta riippuu siitä, miten monta laitetta tulisi käyttöön, mitä enemmän langattomia laitteita on, sen vähemmän maksaa laitteiden vaatiman keskittimen suhteellinen osuus laitetta kohti. Lopulta yhdistämällä KNX sekä joitakin IoT-järjestelmiä olisi mahdollista saada hyvin kustannustehokas kokonaisuus ohjaamaan kiinteistöautomaatiota. Langattomissa ratkaisuissa on vielä ongelmana niiden akkuriippuvuudesta, joiden vaihtaminen on kallista käsityötä. Mutta markkinoille on myös alkanut ilmestymään täysin akuttomia laitteita, jotka keräävät tarvitsevansa energian ympäristöstään. Uusien piirien myötä myös virrankulutus on alkanut laskea, joka tarkoittaa akunkeston parantamista.

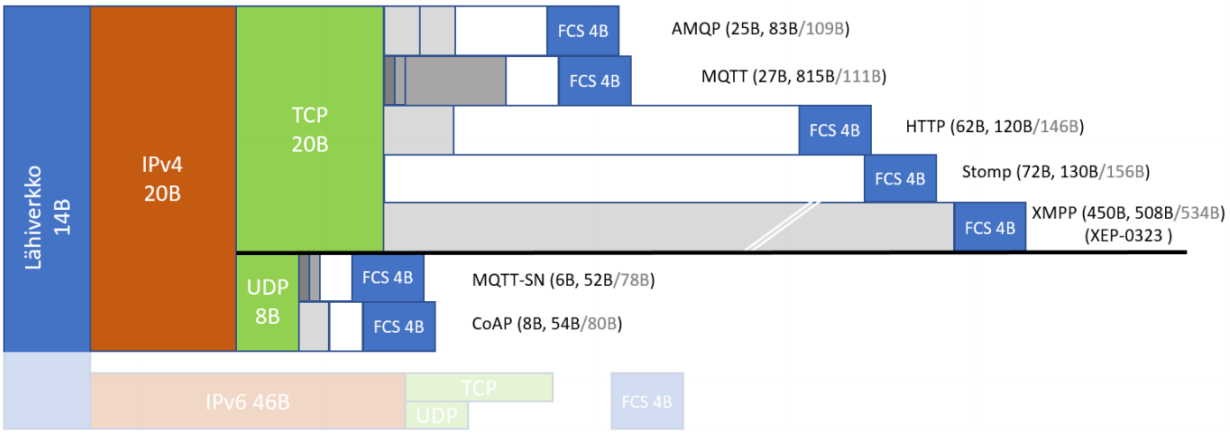
Myös EU on herännyt älykkäiden kiinteistöjen energiansäästö mahdollisuuksiin, osana EPBD direktiiviä on vapaaehtoinen, mutta koko EU:ta koskeva yhtenäisen rakennusten älykkyysindeksin SRI (Smart Readiness Indicator). SRI:ssä tarkastellaan kiinteistön kymmentä eri teknistä järjestelmää, lämmitys, lämmin käyttövesi, jäähdytys, ilmanvaihto, valaistus, rakennuksen dynaaminen vaippa, tehontarpeen tasaus, energian tuotanto, sähköajoneuvojen lataus sekä seuranta ja säätö. Vaikka SRI on vielä vapaaehtoinen, on mahdollista kenties jopa todennäköistä, että se tulee pakolliseksi uudisrakennuksiin ja lopulta myös muuhun rakentamiseen lähitulevaisuudessa.
KNX itsessään tulee täyttämään suurimman osan SRI pisteytyksessä, mutta langattomat IoT järjestelmät voisivat mahdollistaa vielä paremman SRI pisteytyksen. Toistaiseksi SRI indikaattoria ei vielä ole avattu, Euroopan komissiolta on odotettavissa indikaattorin määritelmä ja laskentatapa vuoden 2019 loppuun mennessä. Tämä tarkoittanee, että älykkäät IoT sekä KNX järjestelmät tulevat yleistymään kiinteistöautomaation käytössä.

3.3 Protokollat

Toimiakseen älylaitteet vaativat standardoituja protokollia, joiden avulla ne voivat kommunikoida keskenään ja pilvipalvelun välillä. Laitteiden ja pilvipalveluiden välillä pääasialliseksi tavaksi kommunikoida on internetin ylitse. Internet itsestään tarjoaa jo monipuolisesti erilaisia standardeja tiedon siirtämiseen esimerkkinä HTTP, SMTP, SSH. Standardeissa ongelmia IoT:n suhteen aiheuttaa se, ettei niitä ole luotu suoraan IoT:n tarpeisiin, vaan ne ovat suunniteltu tietokoneiden väliseen kommunikointiin.

Ongelmia aiheuttaa IoT:n vaatima hyvin alhainen virrankulutus, jolloin aikaisemmat keinot tietojen siirtämiseen eivät ole optimaalisia IoT:n laitteiden vaatimaan alhaisen virrankulutuksen tai siirrettävän tietomäärän suhteen. Mitä vähemmän protokollat käyttävät tilaa tiedonsiirrosta, sitä matalampi on myös virrankulutus, sillä samalla tiedonsiirron määrällä siirretään vähemmän tietoa.

Rami Ojala opinnäytetyössään kävi läpi muutaman eri protokollan viemän tilankulutuksen tiedonsiirrosta ja kuvassa 2 näkyy Ojalan tekemä arvio eri protokollien vaatimasta koosta. Kuvasta nähdään miten paljon pelkkä protokollan vaihto voi vähentää tiedonsiirron määrää.



Kuva 2, Protokollien vaatima koko tiedonsiirrosta. (Ojala, 2017)

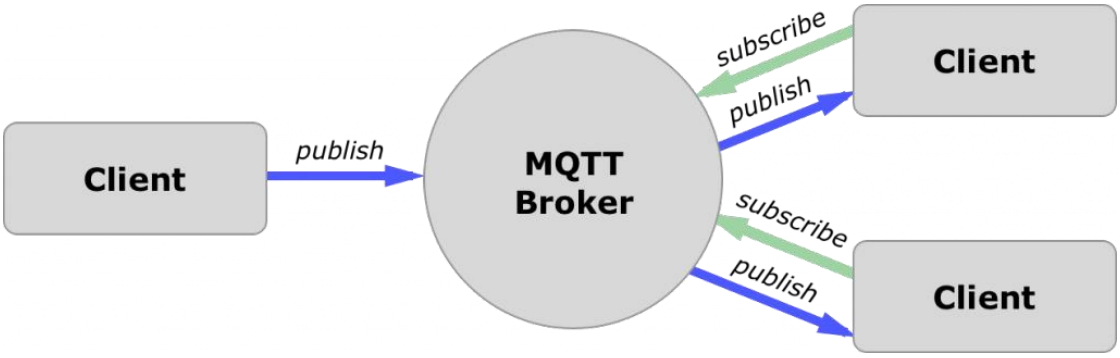
COAP

CoAP (Constrained Application Protocol) on avoin IFTF kehittämä tiedonsiirto protokolla, joka toimii OSI-mallin kuljetuskerroksessa. Se toimii REST-mallin mukaisesti hyvin saman tapaisesti kuin HTTP, mutta on HTTP:stä poiketen hyvin vähän tilaa vievä tiedonsiirtomenetelmä. CoAP toimii IP kerroksen UDP protokollan päällä ja se tukee DTLS suojausta, joten sen läpi tuleva tietoliikenne on mahdollista suojata. CoAP tukee tiedonsiirtoa joko yhdeltä yhdelle tai yhdeltä monelle.

CoAP hyväksyttiin IEFT RFC 7252 standardiksi vuonna 2013. (IETF, 2014)

MQTT

MQTT (Message Queuing Telemetry Transport) kehitettiin alun perin öljyputkien seurantaan satelliittiyhteyttä käyttäen jo vuonna 1999, tavoitteena oli luoda kevyt yksinkertainen protokolla, joka mahdollistaisi alhaisen virrankulutuksen, sekä alhaisen kaistanleveyden. Vuonna 2010 IBM julkaisi siitä parannellun version ja julkaisi sen avoimena protokollana, myöhemmin se myös hyväksyttiin OASIS-järjestössä virallisena standardina vuonna 2014. MQTT toimii TCP protokollan päällä.
(OASIS, 2014) (HiveMQ, 2015).



Kuva 2. MQTT toiminnallisuus (1sheeld)

MQTT toiminta perustuu keskitettyyn välittäjään (broker), joka välittää asiakkaiden (client) tuottaman (publish) tiedon ja välittää sen asiakkaille, jotka ovat tilanneet (subscribe) aihealueen (topic). Asiakkaiden määrää ei ole rajoitettu, jolloin useampi laite voi tuottaa ja tilata samalta aihealueelta. MQTT on myös saatavilla vielä tiiviimpänä MQTT-SN muodossa.

AMPQ

AMPQ (Advanced Message Queuing Protocol) on OASIS järjestön ylläpitämä standardi.
Protokolla käyttää tuottajia, käyttäjiä sekä välittäjiä, tuottajat lähettävät viestin välittäjille, joka puolestaan lähettää viestin tilaajille. Toiminta on hyvin saman kaltaista MQTT:n kanssa poikkeuksena yksi tärkeä kohta, joka on, että AMPQ välittäjä tallentaa tuottajan viestin, kunnes kaikki käyttäjät ovat sen saaneet. Vastaavasti MQTT protokollassa, jos asiakas ei ole kuulolla oikeaan aikaa voi viesti mennä ohi. AMPQ puolelta tämä tarkoittaa, että viestien välitys on hyvin luotettavaa, tuottajien sekä käyttäjien välillä. Monet suuret pankit käyttävätkin AMPQ tiedonsiirroissaan. (Wikipedia) (Microsoft).

3.4 Langattomat IOT sovellutukset

TAAJUUS

Langattomat IoT laitteet käyttävät hyväkseen useita eri taajuuksia, suosituimmat ovat ISM (Industrial, Scientific and Medical) taajuudet, osittain johtuen niiden maksuttomuudesta. Se myös samalla aiheuttaa ongelmia, sillä jos useat eri standartit ja laitteet käyttävät samaa taajuutta, voi taajuus alue ”tukkeuta”, jolloin laitteiden tiedonsiirto voi häiriintyä tai estyä kokonaan. Usein taajuuden tukkeutuessa, myös laitteiden välinen kuuluvuus heikkenee, mikä luo haasteita laitteistojen toimivuuden kannalta. ISM taajuudet eivät kuitenkaan ole joka mantereella samat, vaan ne voivat vaihdella riippuen alueiden sekä maiden lainsäädännöstä. Lähes kaikissa maissa 2,45 GHz sekä 5,8 GHz ovat sallittuja, jolloin laitevalmistajat voivat myydä samalla radiosiruilla sekä antenneilla varustettuja laitteita ympärimaailmaa. Etenkin alle yhden gigahertsin taajuuksilla sen sijaan sallitut taajuudet vaihtelevat erimaiden välillä. EU maiden välillä taajuudet ovat pääosin samat, mutta muualla maailmassa sallitut alle yhden gigahertsin taajuudet vaihtelevat. (ITU)

EU on aloittanut pääosin IoT laitteiden käyttämien (874-876 MHz ja 915-921MHz) taajuuksien harmonisoinnin jäsenmaiden lainsäädännössä. Ongelmana on, että osaa näistä taajuusalueista on käytetty jäsenmaissa sotilaskäyttöön sekä junien tiedonsiirtoon. Nopeaa maailman kattavaa taajuusaluetta alle gigahertsin taajuuksilla ei ole näkyvillä. (European Commission, 2018)

VAIMENNUS

Radiotaajuuden kuuluvuuteen vaikuttaa pääasiassa heijastuminen, vaimentuminen, diffraktio, vapaantilan eteneminen, hajonta sekä monitie-eteneminen. Suurimmat erot eri taajuuksien välillä liittyvät signaalin etenemiseen esteissä sekä ilmassa. Esteissä signaali voi joko heijastua vaimentua tai hajota.

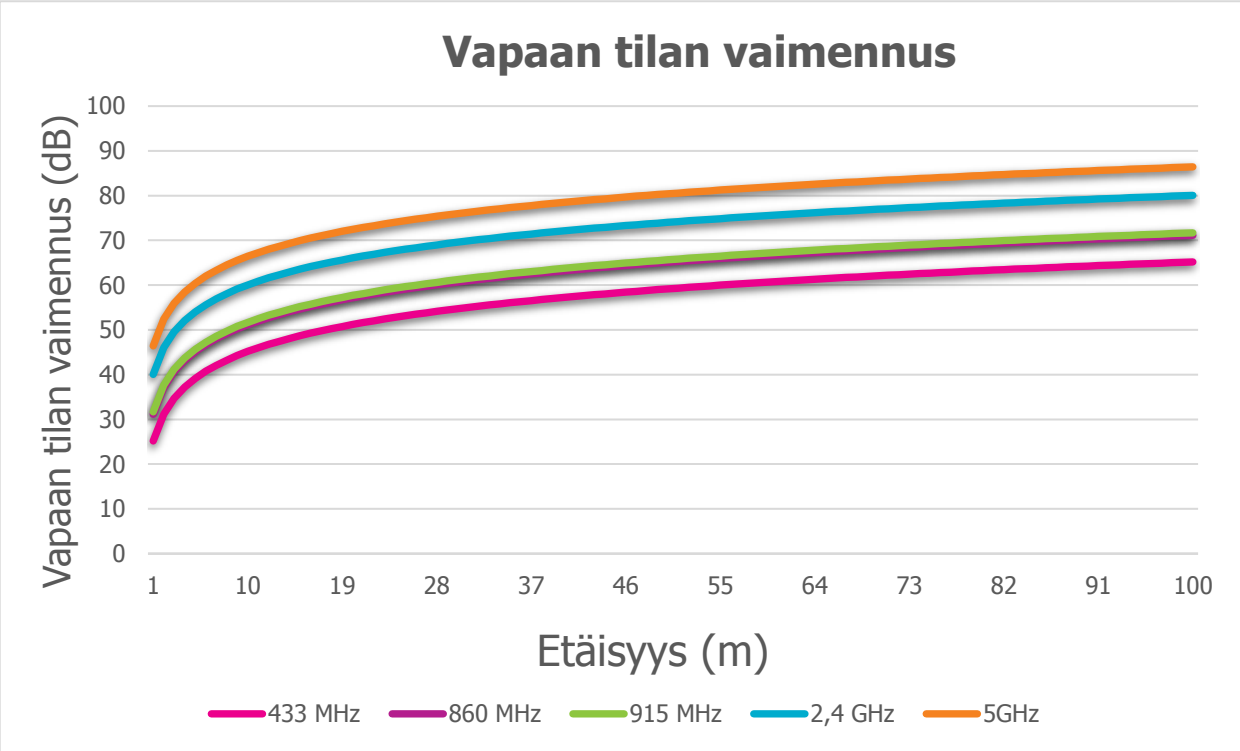
Heijastuminen tapahtuu, kun signaali osuu aallonpituutta suurempaan esteeseen, josta signaali ”kimpoaa” toisaalle. Tällöin osa signaalista absorboituu esteeseen ja signaalin suunta muuttuu, joka usein tarkoittaa pidempää kulkumatkaa ja mahdollisesti useampia heijastumisia.

Hajontaa tapahtuu signaalin osuessa esteeseen, joka on pienempi kuin signaalin aallonpituus tai jonka pinta on hyvin epätasainen. Tällöin signaali kimpoaa esteestä useaan eri suuntaan, jolloin alkuperäinen signaali ”hajoaa” useaan eri suuntaan, joka johtaa lähtevien signaalien pienempään amplitudiin. (Westcott, 2002)

Vaimentumisessa signaalin amplitudi pienenee, jota tapahtuu matkalla ilmassa sekä signaalin osuessa esteeseen, jolloin signaalintaso luonnollisesti laskee. Yksi keino arvioida ilmassa tapahtuvaa vaimentumista, on käyttää vapaan tilan vaimennus mallia, jonka kaava menee seuraavasti;

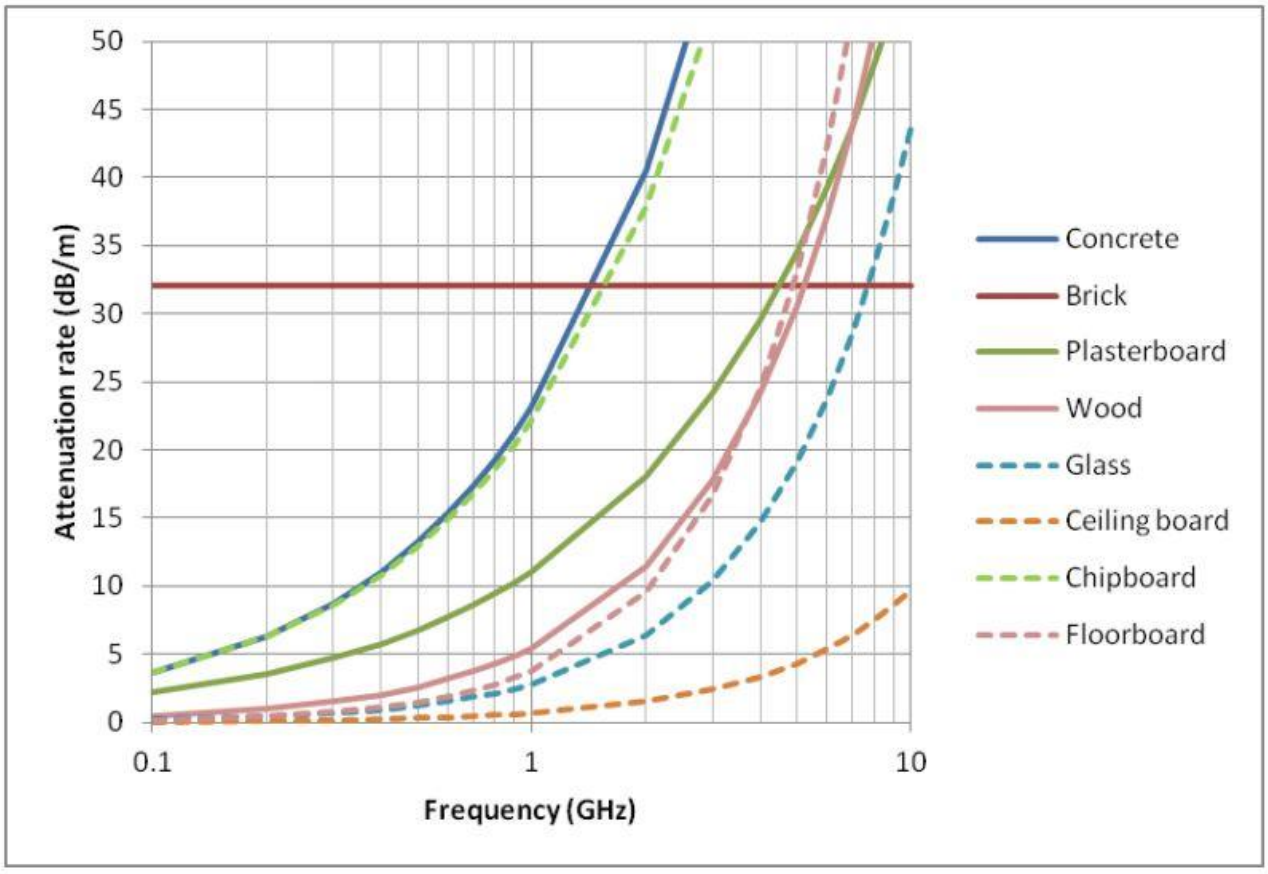
$$FSPL(dB) = 20\log_{10}(d) + 20\log_{10}(f) - 27.55 \quad (1)$$

Kaavassa lasketaan vapaan tilan vaimennus (Free-Space path loss) desibeleinä, jossa d on etäisyys metreinä ja f on taajuus megahertseinä.



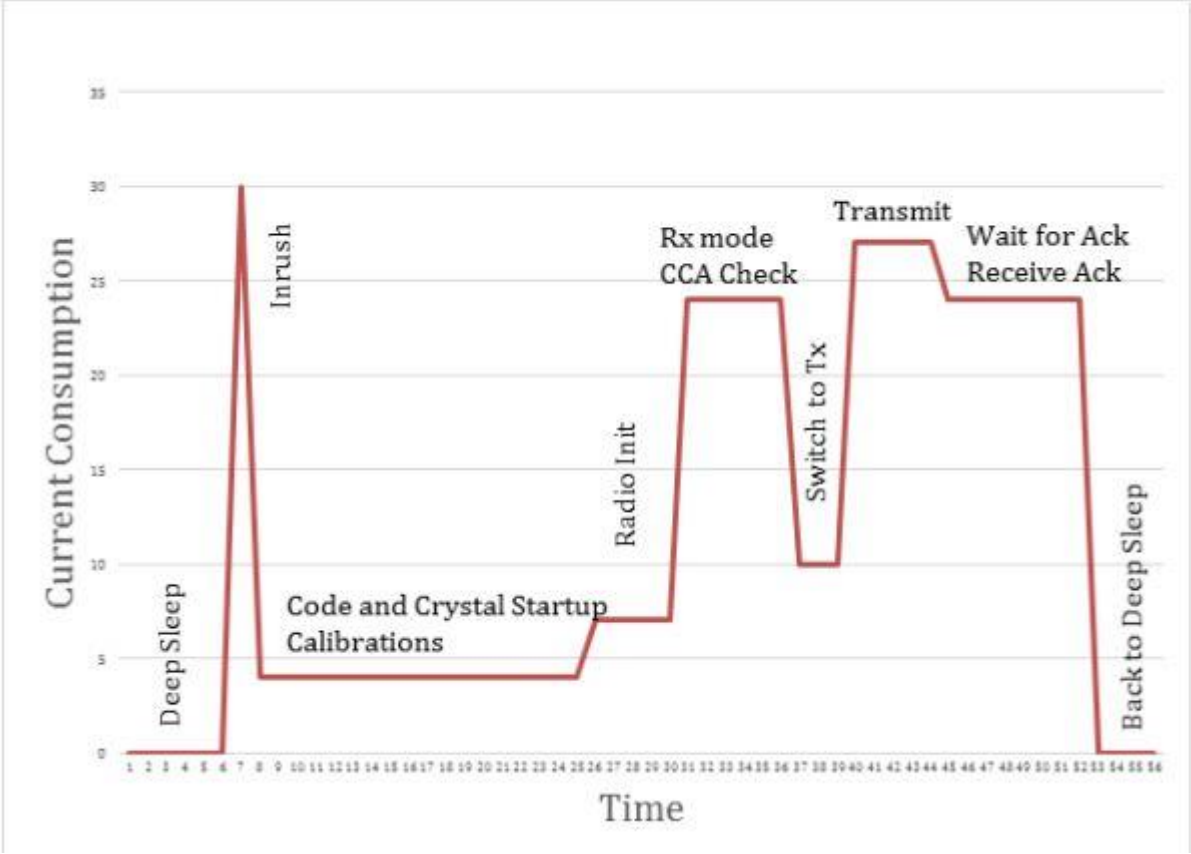
Kaavio 1, Vapaan tilan vaimennus eri taajuuksilla.

Kaaviosta 1 huomataan, miten pienemmillä taajuuksilla vaimennus on pienempää kuin suuremmilla taajuuksilla. Huomioitavaa on, että jokainen taajuusalue käyttäytyy samalla tavalla, eroa on vain vaimennuksen lähtötasossa. Ofcom:n teettämässä tutkimuksessa tutkittiin taajuuden vaikutusta signaalin kulkuun eri esteissä. Kaaviossa 2 nähdään miten taajuuden kasvaessa myös vaimennus kasvaa. (Dr Richard Rudd (Aegis), 2014)



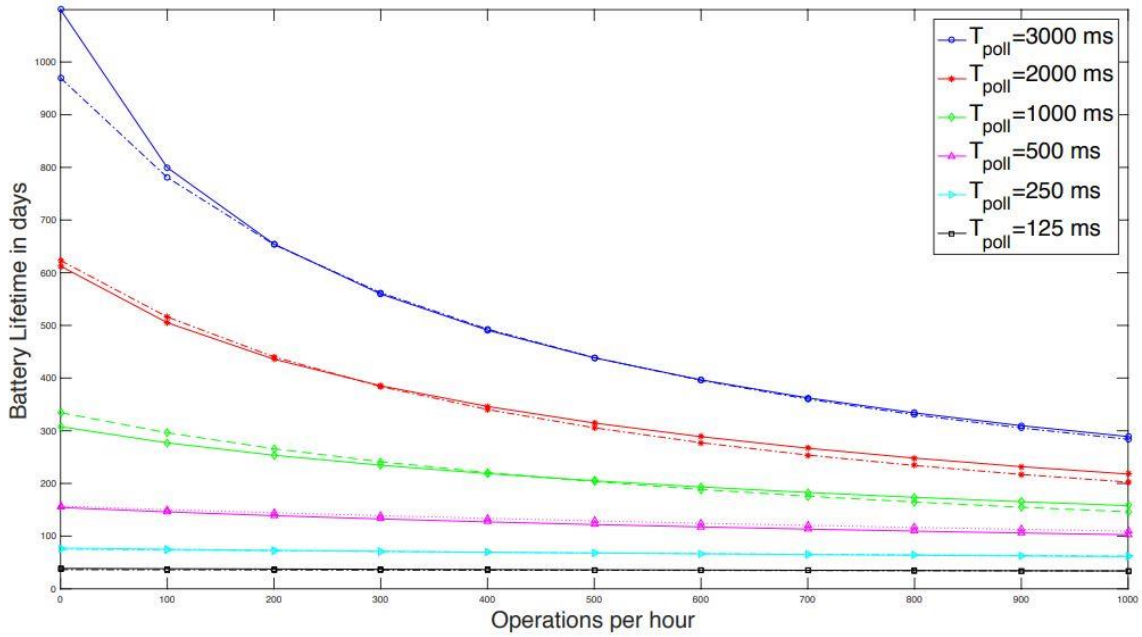
Kaavio 2, Taajuus ja vaimennus eri aineissa. (Dr Richard Rudd (Aegis), 2014)

Näiden perusteella alle gigahertsin verkkojen tulisi vaimentua vähemmän sekä ilmassa että esteissä. Sopivuudessa tulee myös pohtia eri standardien vaatimaa virran kulutusta. Suurin osa akullisten sensoreiden virrankulutuksesta aiheutuu tiedonsiirrosta. Kuvassa 3 nähdään akullisen Thread laitteen tyypillinen virrankulutus. Kuvasta huomaamme miten vähän itse laitteen mikropiiri käyttää virtaa päällä ollessaan (7 mA) ja nukkuessa (alle 1 mA). Sen sijaan suurin kulutus syntyy tiedonsiirrosta lähettäessä (27 mA) ja vastaanottaessa (24 mA).



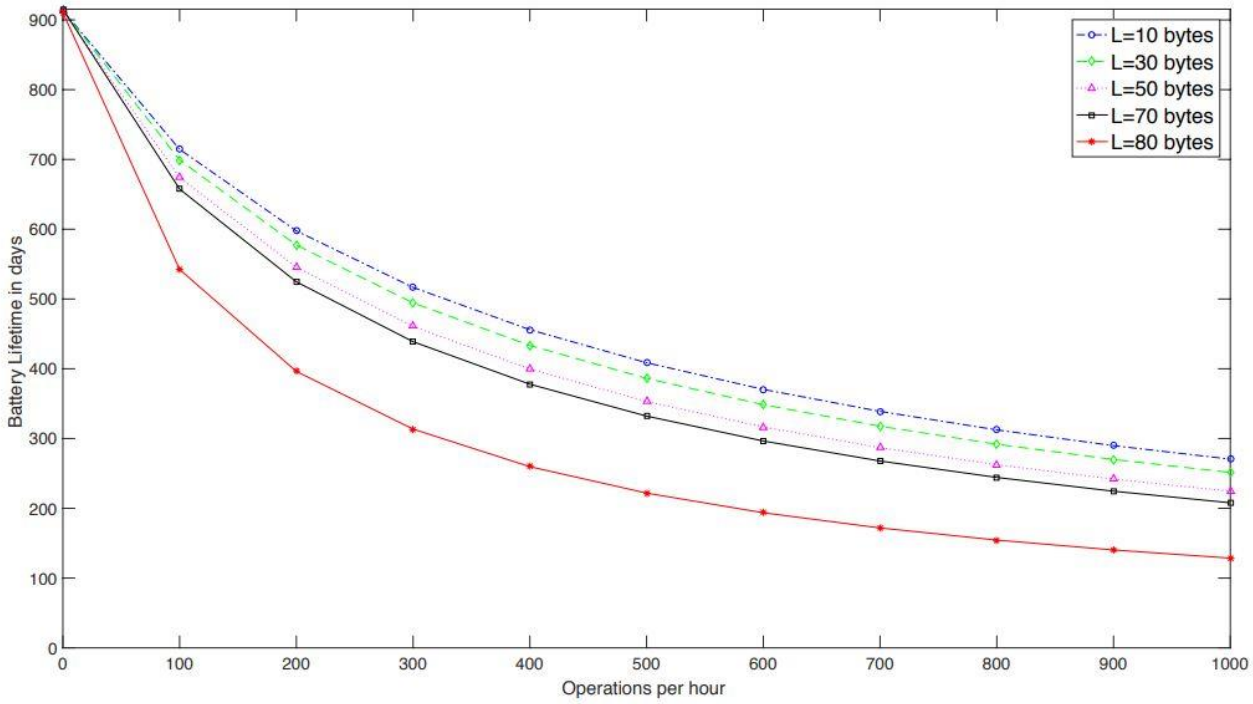
Kuva 3, Thread laitteen tyypillinen virrankulutus (Thread Group, 2015)

Tästä voimme päätellä, että suurin kulutus laitteella tulee sen tiedonsiirrosta, nukkuessaan kulutus on käytännössä vain muutama mikroampeeri. Tällöin akkukäyttöisten laitteiden akunkestoa voidaan vielä parantaa käyttämällä laitteita harkiten.



Kaavio 1, Akunkesto verrattuna herätysten määrään. (Azoidou, 2016)

Eva Azoidou opinnäytetyössään käsitteli Thread laitteiden akunkestoa eri skenaarioissa. Kaaviossa 3 Nähdään miten merkittävä ero arvoituun akunkestoon saadaan herätyksien väliä harventamalla. Kaaviossa herätyksessä laite ottaa yhteyden verkkoon ja lähettää mitatun arvon verkkoon. Alhaalla nähdään laitteen mittauskertojen määrä tunnissa. Kaaviosta huomataan miten alle 1000ms välein lähetettäessä mittauksessa viiva on lähes vaakatasossa. Se kertoo, ettei mittausten määrällä ole juurikaan merkitystä verrattuna verkkoon lähetettyjen arvojen suhteen. Tällöin suurin osa virrasta menee tiedonsiirtoon kommunikoidessa Thread verkon kanssa. (Azoidou, 2016)



Kaavio 2, Akunkesto verrattuna pakettien kokoon. (Azoidou, 2016)

Kaaviosta 4 huomataan, miten pakettien koon kasvaessa myös akunkesto heikkenee. Huomattava pudotus nähdään kuitenkin 70 ja 80 tavun välillä, joka johtuu IEEE 802.15.4 standardin maksimi tietosisällön koon ylittämisestä, joka on 127 tavua. Koska myös tiedonsiirto vaatii jonkin verran tilaa lähetetyssä sanomassa, täytyy 80 tavun paketti lähettää kahdessa osassa, joka luonnollisesti vaikuttaa akunkestoon. Akullisten IoT laitteiden virrankulutuksessa tulisikin pohtia, miten useasti sekä miten suuria määriä tietoa siirretään. Optimoimalla näitä voidaan parantaa huomattavasti laitteiden akunkestoa. (Azoidou, 2016)

Talotekniikan valinnassa tulisi myös pohtia laitteiden sekä järjestelmien pitkäikäisyyttä sekä maksullisuutta. Mikäli järjestelmän käytöstä joudutaan maksamaan kuukausihinnoiteltu maksu, voi se olla kiinteistön elinkaaren aikana maksaa suuren summan, kerralla ostettavaan järjestelmään nähden. Laitteiden käyttöiästä ei ole varmuutta, mutta akkukäyttöisissä laitteissa myös akkujenvaihtaminen luo kustannuksia, jotka tulisi ottaa huomioon järjestelmää hankkiessa. Mikäli toisen järjestelmän akku kestää vuoden ja toisen kymmenen vuotta tulee akun vaihto kustannuksissa todella suuri ero järjestelmän elinkaaren aikana. Huomioon kannattaa myös ottaa järjestelmien sekä laitteiden kehitys, jos akku kestää viisi vuotta niin tällöin kannattaa jo pohtia onko akun vaihtaminen todella halvempaa kuin päivittää laite uuteen, jotka ovat tuona aikana voineet kehittyä virrankulutuksen suhteen.

Työssä jätettiin perehtymättä syvällisesti NB-IoT, LTE-M sekä 5G verkkojen mahdollisuuksiin, sillä ne ovat puhtaasti maksullisia verkkoja, ja eivätkä välttämättä sovi idealtaan kiinteistöautomaation käyttöön, sillä tällöin kiinteistön sensorointi tiedot tulisivat kokonaan sisäverkon ulkopuolelta, jolloin myös kiinteistön reitittimen asetuksia täytyisi vähintäänkin muokata. Samalla se voisi aiheuttaa kiinteistön toiminnalle vakavia häiriöitä, mikäli kiinteistön oma internet yhteys tai IoT laitteen yhteys tukiasemaan katoaa. Oletettavasti näillä verkoilla tulee olemaan suuri suosio liikkuvien IoT laitteiden kanssa, joka voi ruuhkauttaa verkon IoT laitteiden määrän kasvaessa.

3.4.1 Wi-Fi

Wi-Fi on Wi-Fi-allianssin luoma langaton tiedonsiirto teknologia. Wi-Fi:ä on käytetty vuodesta 1999, muun muassa tietokoneissa ja älypuhelimissa. Allianssiin kuuluu jo yli 800 jäsenyritystä, ja allianssi on sertifioinut yli 45 000 laitetta. (Wi-fi Alliance)

Taajuus

Wi-fi perustuu IEEE:n 802.11 standardiin, jossa käytettävissä on 0.9 GHz, 2.4 GHz, 3.6 GHz, 4.9 GHz, 5 GHz, 5.9 GHz ja 60 GHz taajuudet. Käytännössä etenkin menneenä vuosikymmenellä Wi-Fi on käyttänyt vain 2.4GHz ja 5GHz taajuuksia. Uusimmassa käytössä olevassa 802.11ac tiedonsiirrossa on käytössä 80Mhz kaistanleveys, ja kantama on noin 50-100m (riippuen käytetystä taajuudesta). Teoreettinen maksimi nopeus on 1.3Gb/s, joka saadaan aikaiseksi käyttämällä sekä 2.4GHz, että 5GHz taajuutta. Wi-fi itsessään määrittelee vain OSI-kerroksista vain fyysisen- sekä linkkikerroksen, jolloin muiden kerroksien toiminta jää laitevalmistajien päätettäväksi, usein laitteista löytyy myös verkkokerros, jolloin IP pohjainen liikenne on mahdollista. (Wikipedia)

Wi-Fi allianssi on kuitenkin jo reagoinut IoT laitteiden tulemiseen ja lanseerasi standartin 802.11ah (HaLow) joka on kehitetty IoT silmällä pitäen, se käyttää alle 1GHZ taajuutta, jolloin sen kantama on perinteistä verkkoja suurempi, jopa kilometrin. Kaistanleveyksiä on useampia (1,2,4,6,16MHz) jolloin nopeus 1MHz kaistanleveydellä on noin 100kbit/s ja 16MHz kaistanleveydellä teoreettinen maksimi nopeus on 347 Mbit/s. 802.11ah standardi kuitenkin julkaistiin vasta vuonna 2017, jolloin parhaillaan ei ole yhtään IoT laitetta, joka sitä tukisi. Taajuuden muuttuminen alhaisemmaksi tarkoitta myös sitä, että perinteisellä tukiasemalla ei tue sitä suoraan. Mutta tulevaisuudessa voi tulla tukiasemia, jotka tukevat myös alhaisempaa taajuutta. (Wikipedia)

Wi-fi-verkot ovat aikaisemmin soveltuneet heikosti erittäin vähävirtaisten laitteiden käyttöön, sillä se on suunniteltu alun perin vain tietokoneiden väliseen tiedonsiirtoon, jossa tiedonsiirtonopeudella on ollut etusijalla. Vaikka Wi-Fi tukee myös mesh (IEEE 802.11s) verkkoja, vaativat ne useita noodeja toimiakseen, joka usein tekee järjestelmästä kalliita.

Uusin 802.11ax (Wi-Fi 6) mahdollistaa paremman tuen IoT laitteille, sisältäen OFDMA (Orthogonal frequency-division multiplexing) teknologian, joka mahdollistaa tiedonsiirron usealla tosiaan häiritsemättömillä kanavilla samanaikaisesti. Tämä mahdollistaa useiden laitteiden käyttävän samaa verkkoa samanaikaisesti, häiritsemättä toisiaan yhtä paljon mitä edellisillä Wi-fi-versioilla. Jolloin IoT-laitteita voidaan lisätä verkkoon huomattavasti suuremman määrän mitä aikaisemmin. ax-verkko mahdollistaa myös pienemmän latenssin sekä MU MIMO (multi-user multiple input, multiple output) antennin, jolloin sama laite voi käyttää useita antenneja samanaikaisesti, se myös mahdollistaa useamman laitteen palvelemisen samanaikaisesti. Uudessa standardissa on myös kehitetty TWT (Target Wake Time), joka mahdollistaa laitteiden ”nukkumisen”, kunnes laite tarvitsee tietoliikenneyhteyttä uudestaan. Tämä mahdollistaa huomattavan parannuksen laitteiden akun kestoon, sillä aikaisemmin niiden täytyi joko pysyä hereillä, tai liittyä verkkoon uudestaan nukkumisen jälkeen. Myös tietoturva päivittyi, aikaisempi WPA2 päivittyy WPA3 salaukseen, jonka myötä WPA2:sta löydetyt haavoittuvuudet jäävät historiaan. (Wi-Fi alliance)

Wi-Fi verkon etuna voidaan pitää niiden yleisyyttä, Wi-Fi tukiasemia löytyy jo useista kodeista, jolloin niiden hankinta kustannus on suhteessa pienempi, kuin kokonaan uuden langattoman standartin hankinta. Wi-Fin etuihin kuuluu myös todella nopeat yhteydet, jolloin paljon tietoliikennettä käyttävät laitteet voivat toimia. Tietyt laitteet vaativat suuria nopeuksia, jotta laitteisto voi siirtää kuvaa tai ääntä langattomien verkkojen yli, näihin toimintoihin Wi-Fi verkko on ihanteellinen. Myös Wi-Fi verkon mahdollistama suora IP-tuki, mahdollistaa Wi-Fi verkkoon kytkettyjen laitteiden ohjaamiseen ja tiedon välityksen usean eri sovelluskerroksen välillä, myös suoraan pilvipalveluiden välillä.
Heikkouksina voidaan pitää huomattavasti suurempaa virrankulutusta muihin langattomiin verkkoihin nähden, Wi-fi sirun fyysisesti suuri koko sekä tähtitopologia. Topologia voi vaikuttaa heikentävästi signaalin kantavuuteen, eikä yksi tukiasema välttämättä riitä yhdelle rakennukselle.

3.4.2 Zigbee

Zigbee on Zigbee-allianssin luoma avoin langaton standardi, joka perustuu IEEE 802.15.4 standardiin. Zigbeen kehitys aloitettiin 90-luvulla tarjoamaan ratkaisuja langattomaan tiedonsiirtoon, tuolloin langattomia standardeja olivat lähinnä Wi-Fi sekä Bluetooth. Nämä kaksi standardia eivät kuitenkaan tarjonneet tuolloin tarpeeksi alhaista virrankulutusta, eivätkä eri topologioita, joita Zigbeen luomisessa tavoiteltiin. Zigbee julkistettiin vuonna 2004 ja sen uusin versio 3.0 julkistettiin vuonna 2014.

Taajuus

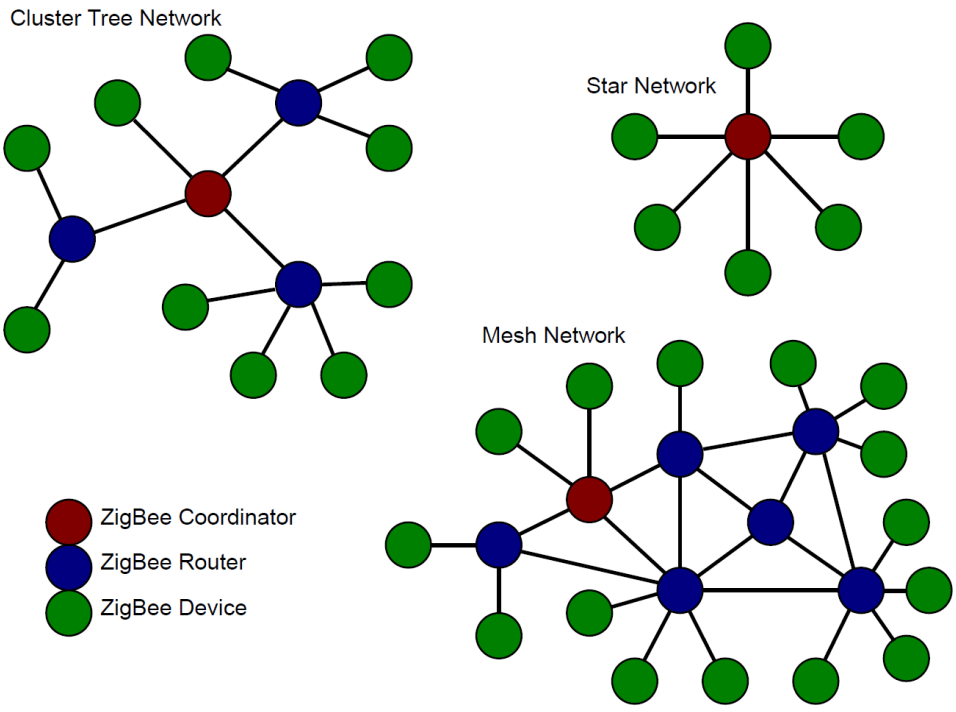
Zigbee toimii 2,4GHz taajuudella, vaikka standardi mahdollistaa myös 860-920MHz taajuudella toiminnan. Koska alle yhden gigahertsin taajuus alue ei ole joka maassa sama, käyttää iso osa Zigbee laitteista lähes kaikissa maissa vapaata 2,4GHz taajuus aluetta. Taajuuden etuja on, että se on vapaa käyttää suurimmassa osassa maailmaa, mutta heikkoutena on, että 2,4Gz taajuutta käyttää myös useat muut standartit, jolloin riskinä on, että laitteistot häiritsevät toistensa toimintaa ja myös siirtonopeudet voivat tippua. Zigbeeallianssi on pyrkinyt estämään tätä käyttämällä taajuuksia, joita suosittu Wi-fi verkko ei käytä. (Zigbee alliance)

Toiminta

Zigbee verkon laitteet voidaan jakaa neljään eri luokkaan, Zigbee Coordinator (ZC), Zigbee Router (ZR), Zigbee End Device (ZED) ja Zigbee Green Power (ZGP). Koordinaattori (Zigbee Coordinator) huolehtii verkon luomisesta sekä verkon tietojen ”säilymisessä”, näitä voi olla vain yksi jokaista Zigbee verkkoa kohti. Reititin (Zigbee Router) reitittää muilta laitteilta tulevaa dataa muille laitteille, joko toiselle ZR, ZC tai ZED laitteelle. Reititin vaatii myös jatkuvan virran, mutta laite voi myös itses-

tään toimia esimerkiksi Zigbee lamppuna ja reitittimenä saman aikaisesti. Viimeinen luokka on päätelaite (Zigbee End Device), joka on yksinkertaisempi, hyvin usein akulla toimiva laite, joka voi olla ”unessa” suuremman osan ajasta. Uusimpana tulokkaana löytyy myös ZGP laitteet, jotka toimivat energiaan keruu laitteiston varassa tai akuilla.

Zigbee tukee kolmea eri topologiaa Tähti, Puu sekä Mesh topologiaa. Tähti-topologiassa kaikki Zigbee päätelaitteet ovat suoraan yhteydessä Zigbee koordinaattoriin, eikä reitittimiä ole lainkaan. Puu-topologiassa Zigbee päätelaitteet ovat joko Zigbee reitittimen välityksellä tai suoraan yhteydessä Zigbee koordinaattoriin.
Puu-topologiassa myös Zigbee reitittimet ovat yhteydessä koordinaattoriin, mutta niiden täytyy olla suoraan yhteydessä koordinaattoriin laitteeseen, eikä esimerkiksi toisen Zigbee reitittimen välityksellä. Mesh-topologiassa Zigbee päätelaite voi olla yhteydessä suoraan, reitittimen välityksellä tai useamman kuin yhden reitittimen välityksellä Zigbee koordinaattoriin.
Zigbeen luoma Mesh-verkko soveltuu hyvin taloautomaatioon, sillä tällä tavoin on mahdollista saada yhtenäinen Zigbee-verkko toimimaan suurissakin rakennuksissa, säästäen tarvittavien tukiasemien määrässä. Zigbee standardiin on myös mahdollista liittää vahvistin, alueille joihin verkon kantama ei riitä, jolloin se toimii ainoastaan reitittimenä. Zigbeen Mesh verkko osaa myös ”korjata” itsensä, jos yksi reititin poistetaan tai se hajoaa, päätelaite ja koordinaattori ”etsivät” uuden korvaavan reitin tiedonsiirrolle. Zigbee vaatii kuitenkin ”keskuksen” mikäli Zigbee koordinaattori hajoaa, lakkaa koko verkko toimimasta. Jokainen Zigbee laite täytyy myös sertifioida riippumattomassa laboratoriossa, Zigbee laitteiden yhteensopivuuden takaamiseksi.

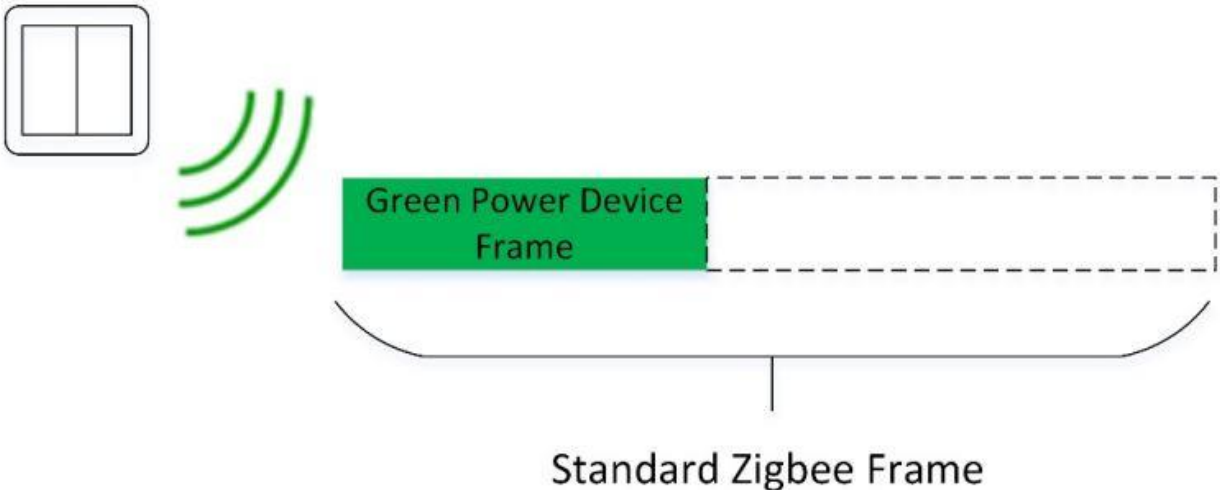


Kuva 4, Zigbee Topologia (pbworks)

Zigbee-verkon salaus on toteutettu 128 bittisellä AES-CCM (Advanced Encryption Standard) algoritmilla, ja uusin 3.0 standardi mahdollistaa verkon suojauksen lisäksi tietojen suojaamisen sovellus

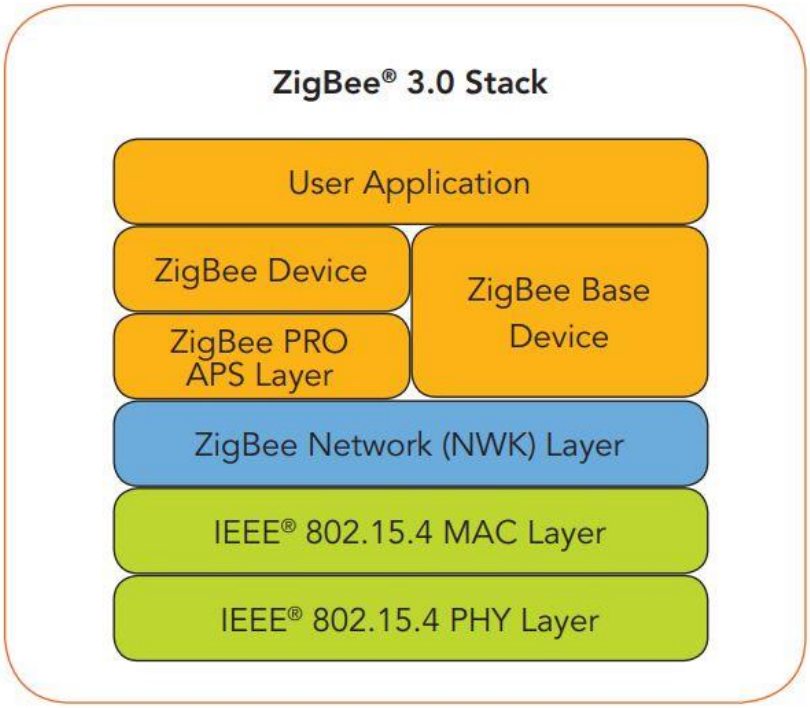
tasossa (AES 128 bittisellä suojauksella). Mutta sovellustasoinen suojaus ei ole pakollinen Zigbee laitteille.
Zigbee 3.0 toi mukanaan uusia turvallisuusmalleja, aikaisemmin jokainen Zigbee reititin kykeni luovuttamaan verkon salausavaimen, mikäli liittyminen oli mahdollistettu koordinaattorin toimesta. Uudessa mallissa, Zigbee verkkoon liittyvä laite tarvitsee koordinaattorilta (Zigbee Cordinator, Trust center) saadun avaimen, joka luovutetaan hyödyntämällä Zigbee laitteeseen tehtaalla ohjelmoitua salausavainta. Tällöin uudessa mallissa Zigbee-verkon avainta ei lähetetä missään vaiheessa salaamattomana, josta sitä voitaisiin kaapata. Uusi malli myös mahdollistaa salausavainten kierrättämisen, jolloin kerran saatua verkonsalausavainta ei voitaisi hyödyntää kuin lyhyen ajan. Uusi turvallisuusmalli toimii vain Zigbee 3.0 laitteilla, mikäli verkossa on vanhempia laitteita, ei uutta turvallisuusmallia voida käyttää. (Zigbee alliance)
Zigbee tukee 65 000 laitetta verkossaan, Zigbee reitittimen suurin tuettu määrä on kuitenkin vain 240 laitetta, jolloin yli 240 laitteiston verkon mahdollistamiseen tarvitaan myös useampia Zigbee reitittimiä. Käytännössä laitteiden tuetut määrät ovat kuitenkin vain teoreettisia. Zigbee kantavuus on 10-300m välillä riippuen laitteesta sekä laitteiden välisistä esteistä. Zigbee 3.0 verkoissa on mahdollisuus myös päivittää laitteita suoraan Zigbee-verkon kautta. IEEE 802.15.4 mahdollistama suurin paketti koko on 127 tavuinen, jolloin osa päivityksistä täytyy siirtää useassa osassa. IEE 802.15.4 myös määrittelee verkon nopeuden, joka on 250 kbps. Zigbee 3.0 myötä Zigbee päivittyi myös osittain IP pohjaiseksi. Zigbee IP kehitettiin yhdessä IEFT:n (Internet engineering task force) sekä IPSO:n (Internet Protocol for Smart Objects), tukemaan osittain IPv6 verkkoa. Toteutuksessa käytettiin hyvin paljon samoja ratkaisuja, kuin IEFT:n luomassa 6LoWPAN standardissa, mutta Zigbee IP ei kuitenkaan tue suoraa IPv6 osoitteellisuutta, vaan Zigbee Cordinator tarvitaan väliin muuntamaan IPv6 osoitteet Zigbee osoitteiksi. Zigbee 3.0 IP tuki on myös häilyvä, sillä se teoreettisesti tukee aikaisempaa Zigbee pro-version Zigbee IP:tä. Mutta koska se vaatii OSI-mallista osan ZCL (zigbee cluster library) käyttämästä tilasta, jolloin se ei ole täysin yhteensopiva kaikkien Zigbee laitteiden kanssa. Aikaisemmin myöskään ZCL ei tukenut toimintaa IP verkkojen ylitse, kunnes DotDot:n myötä se teoreettisesti tukisi sitä. Tällä hetkellä myös Zigbee Smart Energy 2.0 kuitenkin tukee IPv6 verkkoa.

Zigbee allianssi toi 3.0 päivityksessä myös ”Zigbee Green Power” osionsa, joka on tarkoitettu erittäin vähänvirtaisiin, akuttomille energiaa kerääville laitteille. Se mahdollistaa huomattavasti normaalia Zigbee-runkoa pienemmän rungon käyttämistä, joka puolestaan tarkoittaa huomattavasti pienempää virrankulutusta, jolloin Green Power laitteissa ei välttämättä tarvita lainkaan perinteisiä akkuja.
Myös sirun vaatimukset ovat pienempiä, normaalissa Zigbee laitteessa on vähintään 256 kilotavua muistia ohjelmalle ja 16 kilotavua tiedoille, tarvitsee tyypillinen Green Power laite vain 32kilotavua ohjelmalle ja 1 kilotavun tiedoille. Tämä tarkoittaa, että tyypillisestä Zigbee Mesh verkon laitteen lähetyksen vaatimasta 500uJ energia määrästä Green Power laitteet käyttävät viisikertaa vähemmän energiaa, parhaimmillaan vain 50uJ. (Silicon Labs) (Zigbee Alliance, 2017)



Kuva 5, Zigbee Green Power runko verrattuna normaaliin Zigbee runkoon.

Green Power laitteet voivat kuitenkin lähettää tietoa vain yhteen suuntaan, lukuun ottamatta laitteiden parittamista verkkoon. Joka tarkoittaa, ettei laitteita voida päivittää, eikä katsoa reaaliaikaista tietoa, vaan tiedonsaanti on riippuvainen laitteen omista asetuksista. Green Power laitteet eivät myöskään täytä Zigbee päätelaitteen (ZED) määritelmiä, vaan ovat alhaisemmassa kategoriassa (ZGB). Koska Green Power laitteet ovat erittäin vähävirtaisia, niiden lähettämät viestit tarvitsevat ”muunnoksen” Green Power Sink (GPS) laitteella, joka ainakin alkuvaiheessa löytynee Zigbee koordinaattorista, mutta tulevaisuudessa myös Zigbee reititin voi mahdollisesti muuntaa viestit puhtaiksi Zigbee viesteiksi. Jokainen Zigbee 3.0 reititin kuitenkin tukee Green Power-viestejä, jolloin reititin toimii välityspalvelimena Green Power-laitteen sekä Green Power Sink-laitteen välillä. Tämä tarkoittaa, ettei Green Power-laitteet ole yhteensopivia kaikkien aikaisempien Zigbee laitteiden kanssa



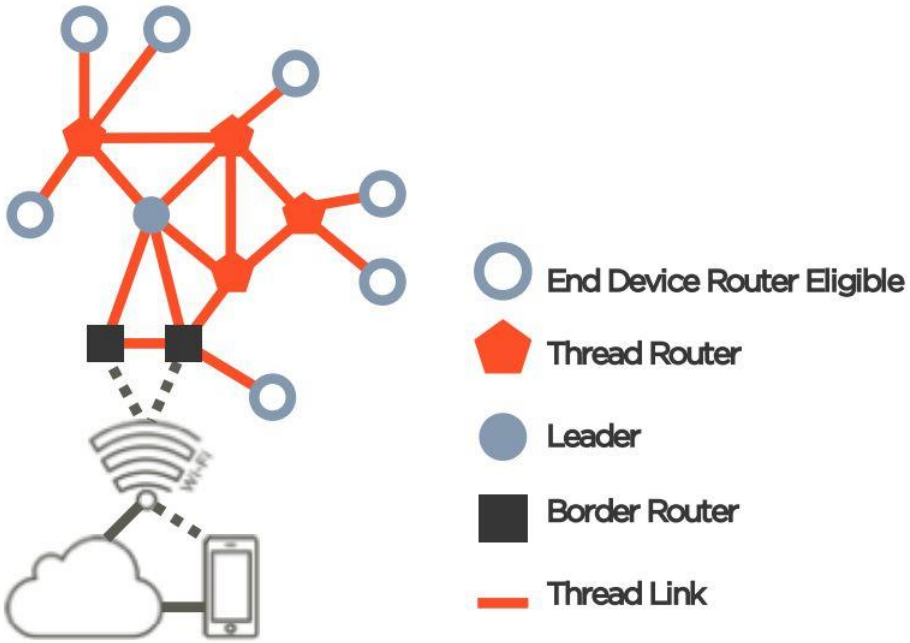
Kuva 6, Zigbee OSI-malli

3.4.3 Thread

Thread on Thread Groupin luoma avoin langaton standardi, joka perustuu Zigbeen tavoin IEEE 802.15.4 standardiin. Standardi on suhteellisen tuore, Thread Group julkaisi sen vuonna 2014, olemalla ensimmäisiä Mesh-pohjaisia standardeja, jotka tukevat IPv6 verkkoa. Thread toimii 2,4GHz taajuudella, ja kohtaa samoja haasteita mitä Zigbee, samoja taajuuksia käyttää useat eri standartit, jolloin eri standardien laitteistot voivat häiritä toistensa toimintaa.

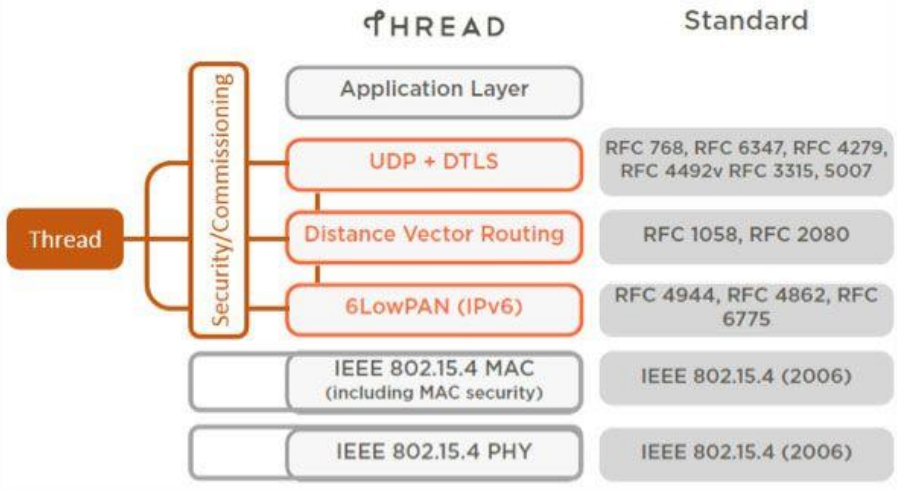
Toiminta

Thread verkon laitteet voidaan jakaa neljään eri luokkaan, Thread Leader (johtaja), Thread Router (reititin), Boarder Router (reuna reititin), End Device (päätelaite). Johtaja (Thread Leader) huolehtii verkon luomisesta ja koordinoi verkkoa Thread verkossa näitä voi olla vain yksi kerrallaan, mutta mikäli johtaja (Thread Leader) häviää verkosta voi jokin liitetty reititin (Thread Router) ottaa sen paikan. Reititin (Thread Router) reitittää muilta laitteilta tulevan tiedon toisille laitteille, näitä voi olla verkossa 32kpl ja ovat poikkeuksetta verkkovirralla toimivia. Reuna reititin (Thread Boarder Router) nimensä mukaisesti on yhteydessä joko kiinteällä tai langattomalla yhteydellä toisiin verkkoihin ja toimii reitittäjänä näiden verkkojen ja Thread verkon välillä. Näitä voi Thread verkossa olla useita kappaleita. Viimeisenä päätelaite (End Device), joka on usein akulla toimiva laite, ja joka voi olla ”unessa” suuremman osan ajasta. Mikäli päätelaite (End Device) toimii verkkovirralla voi se tarpeen vaatiessa toimia myös reitittimenä (Thread Router). Yksittäiseen reitittimen (Thread Router) voi olla yhteydessä korkeintaan 511 päätelaitetta (End Device).



Kuva 7, thread verkko.

Käytännössä Thread Group kuitenkin lupaa tukensa vain 250 laitteelle. Koska standardi ei määrittele, että jokaisen reitittimen (Thread Router) täytyy tukea 511 laitetta, alin lukema, jota standardissa määritellään tähän toimeen, on 10 laitetta. Tällöin 16 tuhannen laitteen tuki tippuu tukemaan noin 288 laitetta. Salaus on toteutettu 128 bittisellä AES suojauksella, jonka avulla radioliikenne pysyy salattuna (TI, 2017). Mesh verkko on myös itsestään korjautuva.
Thread ei ole määritellyt sovellustasoa, jolloin valmistajat voivat käyttää jo olemassa olevaa tai omaa sovellustason viestiliikennettä. Tämä onkin avannut Thread:lle uusia mahdollisuuksia, sillä se on alkanut tehdä yhteistyötä sekä Zigbeen (DotDot) sekä KNX kanssa, lopulta mahdollistaen DotDot tai KNX viestien käytön langattomissa Thread laitteissa. Kuitenkin tämä voi tarkoitta, että kuluttajat osatavat Thread laitteita, jotka eivät lopulta tue toisiaan, sovelluskerrosten ollessa yhteensopimattomia.



Kuva 8, Thread verkon OSI-malli.

Thread usein verrataan 6LowPAN standardiin, joka osittain pitää paikkaansa. Thread käyttää 6LowPan standardia omassa standartissaan, mutta Thread:lla on myös lisänä omia ratkaisujaan koskien verkon turvallisuutta sekä liikenteeseen verkon sisällä.
Thread etuina voidaan pitää suoraa IP osoitteellisuutta, itsestään korjautuvaa Mesh verkkoa sekä mahdollisuus käyttää useita reuna reitittimiä (Boarder Router) yhdessä verkossa.
Heikkouksena yhtenäisen sovelluskerroksen puuttumista.

3.4.4 Z-wave

Z-wave on vuonna 2003 perustettu ja alun perin tanskalaisen Zen-Sys yrityksen kehittämä langaton tiedonsiirto protokolla. Protokolla perustui silloisen Zen-Sys luomaan Z100 mikropiiriin, jonka lisenssiä Zen-Sys tarjosi muiden laitevalmistajien käyttöön. Vuonna 2005 Zen-Sys toi Z200 piirin markkinoilla ja perusti Z-wave allianssin, jonka tavoite on kehittää Z-wave standardia sekä hoitaa Z-waven markkinointia ja mainontaa. Allianssi myös varmistaa, että jokainen Z-wave laite noudattaa standardia ja on yhteensopiva muiden laitteiden kanssa. Ilman yhteensopivuutta, sertifiointia ja Z-wave allianssiin kuulumista ei laitevalmistaja voi käyttää Z-wave nimeä markkinoinnissa. Laitteita voidaan sertifioida useissa riippumattomissa laboratorioissa ympärimaailmaa.
Vuonna 2005 Z-wave oli suljettu standardi, jonka omisti Zen-Sys, myöhemmin Sigma Desingns osti Zen-Sys ja alkoi tuottamaan Z-Wavessa käytettyjä siruja yksinoikeudella. Vuonna 2015 julkaistiin ITU-T g.9959 standardi, joka kehitettiin pitkälti Z-waven pohjalta ja jota tulevien Z-wave laitteiden täytyy noudattaa. Standardi määrittelee OSI-mallissa fyysisen, sekä siirtokerroksen toiminnan, tämä myös mahdollisti muiden siruvalmistajien valmistaa Z-wave yhteensopivia siruja.
Vuonna 2016 Sigma Desingns julkisti Z-wavessa käytetyt tekniset erittelyt, jolloin standardi muuttui avoimemmaksi, tällöin myös OSI-mallin ylemmät kerrokset, joita ITU:n suositukset ei määritellyt, muuttui julkisiksi. Vuonna 2018 Silicon Labs osti Z-wave teknologiat Sigma Desingnilta, jatkaen standartin kehittämistä avoimempaan suuntaan. Vuonna 2018 Z-wave allianssiin kuului yli 700 yritystä ja markkinoilla oli yli 2400 Z-wave laitetta. (ITU, 2015)

Taajuus

Z-wave toimii alle gigahertsin taajuuksilla, joka tarkoittaa Euroopassa 868 MHz taajuus aluetta. Vuonna 2007 Z-wave lisäsi tuen 2,4 GHz taajuudelle, mutta valtaosa laitteista toimii edelleen alemmalla taajuudella. Z-wave lupaa jopa 100 metrin kantavuuden laitteiden välille, mutta sisätiloissa kantavuuden luvataan olevan noin 30m, johtuen seinistä sekä muista esteistä. Z-wave tukee 232 laitetta yhdessä verkossa, ja on topologialtaan mesh pohjainen, mutta tällä on rajoituksena, että laitteen ja ohjaimen välillä voi olla korkeintaan neljä laitetta, mikäli tämä määrä ylitetään, poistuu viesti verkosta. Tällöin teoriassa neljän laitteen välinen matka on maksimissaan noin 500 metriä Mesh-topologiaa käyttäen. Z-wave tukee maksimissaan 100 kbps nopeuksia, joskin aikaisemmat sirut mahdollistivat vain 9,6 ja 40 kpbs nopeudella toimimisen.

Toiminta

Z-wave laitteet jaetaan kolmeen luokkaan; ensimmäinen luokka on Ohjain (Controller, Hub, Gateway), toinen luokka reitittävä laite (Node) ja kolmas ei reitittävä päätelaite (Node).
Ohjain on vastuussa verkon luomisesta, yhteydestä internettiin ja kykenee ”linkittämään” laitteita keskenään. Ohjaimia voi olla verkossa useita, mutta yksi ohjain pitää osoittaa ”pääohjaimeksi”, joka on vastuussa verkon luomisessa ja sen ylläpitämisessä. Reitittävä laite on verkkovirta käyttöinen laite, joka muun laitteen toiminnan ohessa myös reitittää akkukäyttöisten laitteiden ja ohjaimen välisen tietoliikenteen. Päätelaite, on usein akkukäyttöinen ja hyvin vähävirtainen laite, joka on ”unessa” suurimman osan ajasta.
Z-wave kantama on noin 100 metriä avoimessa tilassa, mutta rakennuksissa luonnollisesti seinät ja muut materiaalit rajoittavat kantamaa, jolloin sisätiloissa Z wave allianssi suosittelee, että laitteiden

etäisyys toisistaan olisi korkeintaan noin 10 metriä. Salaus on Z-wave verkossa toteutettu 128 bittisellä AES salauksella, mutta aikaisemmat Z-wave laitteet eivät kykene tukemaan tätä, jolloin valintana on joko poistaa verkon suojaus, tai uusia vanhat laitteet tukemaan salausta. Myöskään uudet laitteet eivät välttämättä tue salausta, ellei sitä ole erikseen sertifioitu myös Z-wave Secure tuotteeksi. (Silicon Labs)

Z-waven etuja ovat yhteensopivat laitteet sekä sovelluskerros, kaikki laitteet toimivat toistensa kesken. Sekä koska standardi on vanha, löytyy sille jo paljon laitteita ja tukea.
Huonoja puolia ovat heikko mesh ratkaisu, joka mahdollistaa parhaimmillaan vain 4 laitteen hypyn laitteiden välillä. Z-wave ei myöskään tue suoraan IPv6 liikennettä Z-wave verkossa, vaikka standardi mahdollistaa Z-wave käskyjen liikkumisen normaalin IP verkon päällä, käyttäen yhteensopivaa yhdyskäytävää.

3.4.5 Bluetooth

Bluetooth SIG (Special Interest Group) on alun perin Ericsonin kehittämä langaton tiedonsiirto protokolla puhelinten ja tietokoneiden välille. Nykyisin Bluetooth tukee monia erilaisia yhteyksiä monien eri laitteiden välillä. Bluetooth SIG (Special Interest Group) perustettiin vuonna 1998 perustaja jäseninä olivat Intel, Nokia, Ericson ja Toshiba. Vuonna 2018 jäseniä oli jo yli 35 000. (Bluetooth SIG)

Bluetooth toimii 2,4GHz taajuudella, ja käyttää FHSS (Frequency Hopping Spread Spectrum) tekniikka radio taajuuksilla välttääkseen häiriöitä muilta verkoilta ja laitteilta.
Vuonna 2010 Bluetooth 4.0 julkaistiin ja Bluetooth jaettiin kolmeen eri kastiin, joista yksi on Bluetooth LE (toiselta nimeltä Bluetooth Smart) ja toinen Bluetooth high speed ja kolmas Classic Bluetooth. Bluetooth LE (Low Energy) on suunniteltu IoT:ta varten, se julkistettiin vuonna 2012 ja 2014 Bluetooth 4.2 antoi enemmän valmiuksia ja IPSP (Internet Protocol Support Profile) tuen. Jolloin Bluetooth laite voidaan liittää suoraan internettiin, Bluetooth gatewayn kautta.

Bluetooth LE tukee kahdenkeskeisessä (one to one) liikenteessä 128 bittistä AES salausta, 125 kb/s-2Mb/s ja maksimissaan 251 tavun tietosisällön. Kahdenkeskeinen liikenne sopii hyvin, esimerkiksi puhelimen ja älyrannekkeen väliseen tiedonsiirtoon, suuren tiedonsiirto kapasiteetin ja pienen virrankulutuksen suhteen, mutta ei taloautomaation suhteen, jossa on useita laitteita ja tarvittava tiedonsiirto kapasiteettia voidaan vieläkin laskea virrankulutuksen parantamiseksi. Tätä voidaan kuitenkin käyttää taloautomaatiossa sellaisissa laitteissa, jotka eivät suoraan toimi akulla, mutta tarvitsevat suurempaa tiedonsiirtokapasiteettiä.

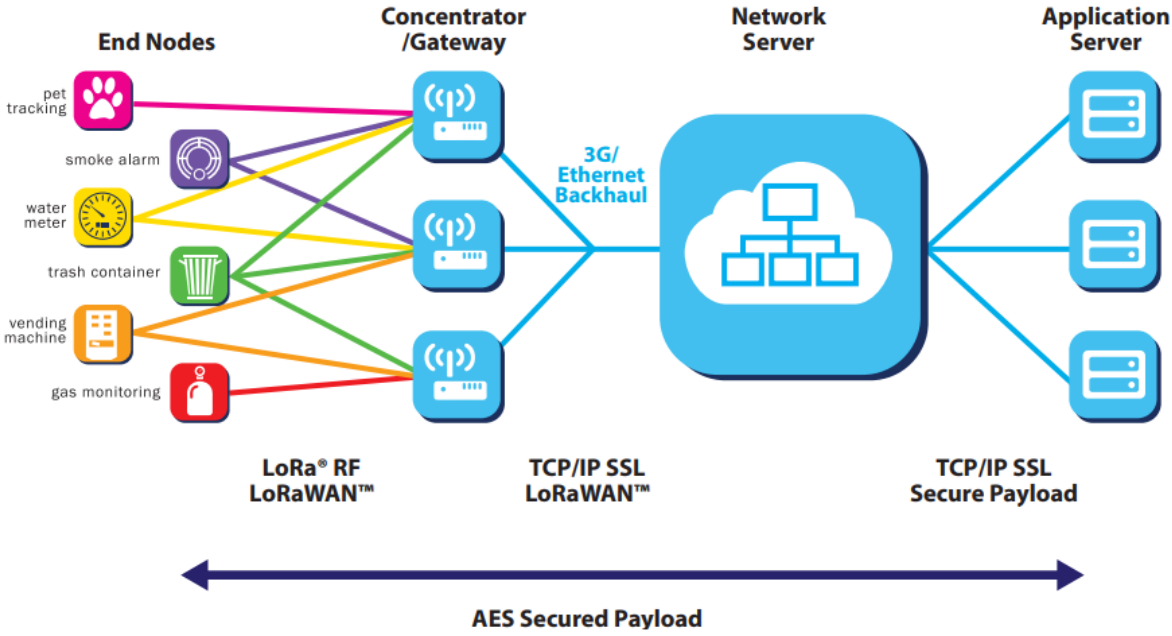
BLE tukee myös yhdeltä monelle (one to many) topologiaa, jolla voidaan mm. lähettää tietoa radiomajakan tapaan, jolloin tietoa voidaan lähettää usealle laitteella saman aikaisesti kertoen esimerkiksi jostain tuotteesta lisätietoa. BLE kolmas protokolla on monelta monelle (many to many) joka perustuu mesh topologiaan. Se tukee maksimissaan 32,757 laitetta, 128 bittistä AES salausta ja maksimissaan 29 tavun tietosisällön. Tämän lisäksi Bluetooth mahdollistaa myös sovellustason salauksen.

Bluetooth mesh-verkot käyttävät ns. ”hallittua tulvaa”, joka tarkoittaa, että lähetetyt viestit kulkevat verkon jokaiselle laitteelle, ja mikäli ne eivät ole tälle laitteelle, laite ei tee viestille mitään. Jos verkossa on nukkuvia laitteita, verkkovirtainen laite kerää tulevat viestit ja välittää ne nukkuvalle laitteelle, kun laite herää.
Viesteissä on myös toistoraja, joka tarkoittaa, että tietyn verran hyppyjä suorittanut viesti poistetaan automaattisesti. Tarkoituksena on estää verkon ruuhkautuminen vanhoilla viesteillä, tämä hyppyraja määritellään verkkoa luodessa. Koska mesh verkon tietosisältö on niin pieni, ei se tue suoraa IPV6 reititystä, vaan väliin tarvitaan aina, keskitin tai yhdyskäytävä. Bluetooth on myös alkanut myös kehitellä samalla tavoin jokaisen laitetyypeille ominaisia yhteneväisiä komentoja (GATT-profiileja), kuten Z-wave, Zigbee sekä KNX. (Bluetooth SIG, 2019)

Bluetoothin etuina voidaan pitää mesh verkkoa sekä suurta määrää tukevia laitevalmistajia. Heikkouksina ovat puutteellinen sovelluskerros, joka on johtanut muiden yhtiöiden halukkuuteen rakentaa omat sovellus- sekä kuljetuskerrokset bluetoothin päälle. Esimerkkinä suomalainen Wirepas on kehittänyt Bluetooth LE:n päälle oman sovelluskerroksen.

3.4.6 LoraWan

LoRaWAN on globaali sekä avoin standardi, joka toimii alle gigahertsin taajuuksilla. Se julkistettiin vuonna 2015, LoRa Alliancen toimesta. Allianceen kuuluu yli 500 jäsentä, Suomessa suurinta LoRaWAN verkkoa ylläpitää Digita Oy.
LoRaWAN toimii LoRa radioverkon päällä, usein star of stars-topologiaa käyttäen, jolloin yksittäinen LoRaWAN laite yhdistyy lähimpiin yhdyskäytäviin. Nämä yhdyskäytävät taas ovat internetin välityksellä yhteydessä LoRaWAN palvelimeen, josta sitten laitteiden tietoa voidaan käyttää. Tämä näkyy kuvassa 9.



Kuva 9, LoRAWAN topologia. (LoRA-Alliance, 2015)

LoRaWAN laitteet eivät itsessään tue IP verkkoja vaan vaativat aina yhdyskäytävän väliin. LoRaWAN verkon nopeus on 290bps- 50Kbps, viestin suurin tietosisältö 243 tavua sen kantama on 1-10km riippuen esteistä. Sillä ei ole sovellustasoista määrittelyä, joka tarkoittaa, että jokainen valmistaja voi tehdä oman rajapinnan tiedon välittämiseen. LoRaWAN verkot voivat myös olla osittain maksullisia, sillä vaikka omia verkkoja voidaan rakentaa, voi joku laite olla verkon kantaman ulkopuolella, jolloin laitteen viestin välittää ulkopuolinen verkko. Tällöin tämä verkko voi pyytää ”maksua” viestien välittämisestä, tai vaihtoehtoisesti olla välittämättä sille tulevia viestejä. Kaikki verkot eivät lähtökohtaisesti välitä viestejä toisille palvelimille, joka myös auttaa yksittäisten verkkojen ruuhkautumisessa. LoRaWAN parhaillaan kehittää mallia eri verkkojen ylläpitäjien kanssa, mahdollisista korvauksista verkkojen välillä.

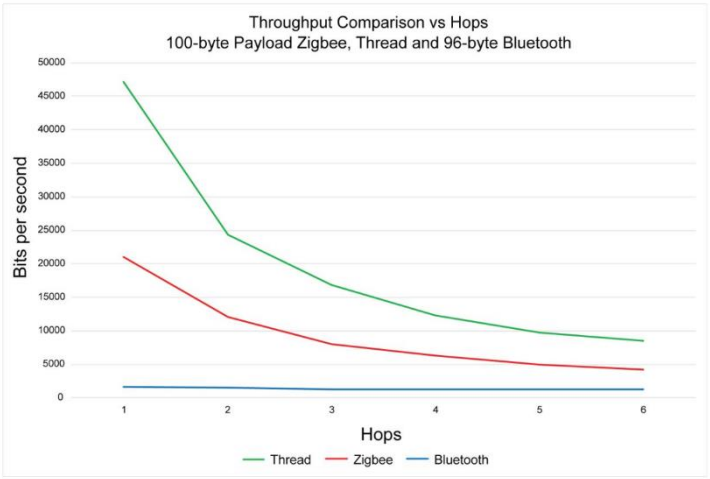
LoRaWAN lähettämät tiedot ovat suojattu käyttäen 128 bittistä AES suojausta, suojaamalla lähetetyn tiedon, koko matkan ajan laitteilta asiakkaan käyttöön. Yksi salausavain on käytössä laitteen ja LoRaWAN palvelimen välillä, ja toinen salausavain on laitteen ja asiakkaan palvelimen välillä. Tällöin

tiedot siirtyvät palvelimelle salattuna, jolloin sen lopullinen päämäärä pysyy salattuna palvelimelle asti, josta se lähtee asiakkaan palvelimelle. Tällöin vaikka laitteen lähettämä LoRa-radion lähetys saataisiin kaapattua, ei tietoja voida hyödyntää. Tällöin on myös sama, kenen omistaman yhdyskäytävän läpi liikenne kulkee, sillä yhdyskäytävä näkee vain, minne LoRaWAN palvelimelle paketti lähtee näkemättä laitteen lähettämää tietoa tai viestin lopullista osoitetta. Viesteissä on myös laskuri, jolla LoRaWAN palvelin voi tunnistaa duplikaatti lähetykset, mikäli sama viesti tulee useampaan kertaan palvelimelle. (LoRa Alliance, 2015)

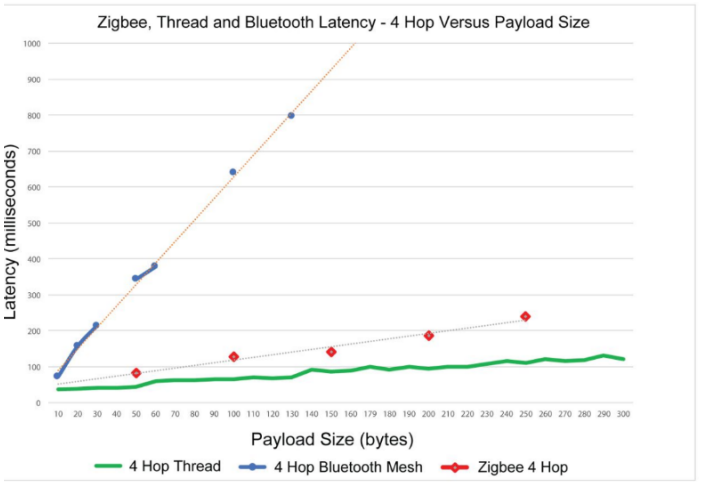
Etuina LoRaWAN verkoilla on todella pitkä kantama, jolloin teoriassa koko kiinteistö voitaisiin kattaa yhdellä yhdyskäytävällä. Heikkouksina on ns. ”avoin” sovelluskerros, joka mahdollistaa laitevalmistajien luoda omat ohjainmallit laitteillensa, LoRaWAN palvelin vaatimus, joka nostaa järjestelmän hintaa. Sekä LoRaWAN:n tuoreus, monikaan laitevalmistaja ei ole vielä lähtenyt tekemään LoRaWAN laitteita, jolloin niiden hinnat ovat tällä hetkellä suhteellisen korkea verrattuna muihin järjestelmiin. Mikäli LoRaWAN palvelin sekä asiakaspalvelin eivät fyysisesti sijaitse samassa rakennuksessa taloautomaation kanssa voi tietoliikenteen katkeaminen aiheuttaa suuria ongelmia.

3.5 Mesh verkkojen suorituskyky

Silicon labs testasi kolmen mesh standartin Zigbeen, Bluetooth LE:n sekä Thread:n suoritus kykyä, tiedonsiirron sekä latenssien suhteen, kun verkossa on useita laitteita. (Silicon Labs)

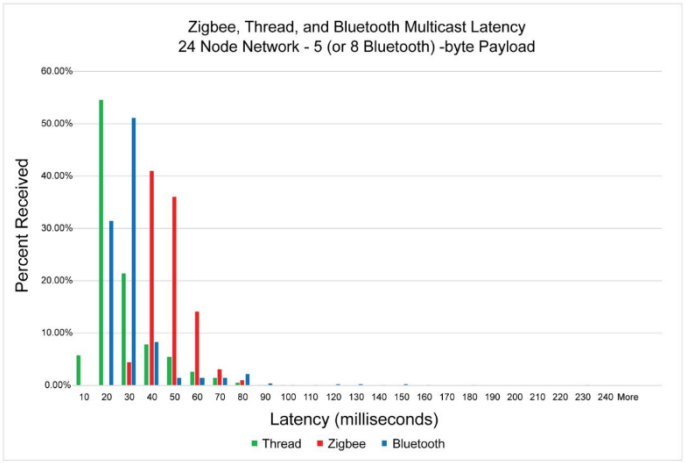


Kuva 10, Tiedonsiirto nopeus hyppyjen lukumäärän kasvaessa

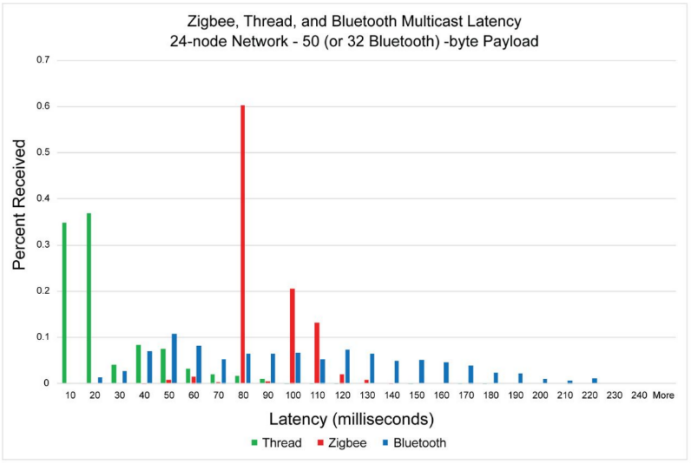


Kuva 11, Latenssin suhde pakettienkokoon.

Kuvissa 10 ja 11 nähdään, miten tiedonsiirtonopeus alkaa voimakkaasti laskea ja latenssi hiukan kasvaa sekä Thread, että Zigbee verkoilla, kun suuria tietopaketteja liikutellaan usean eri laitteen kautta. Bluetooth verkolla oli tässä testissä todella huono tiedonsiirtonopeus, kuvasta 11 nähdään miten myös latenssi kasvaa Bluetooth verkolla huomattavan paljon korkeammalle kuin kilpailevilla verkoilla.

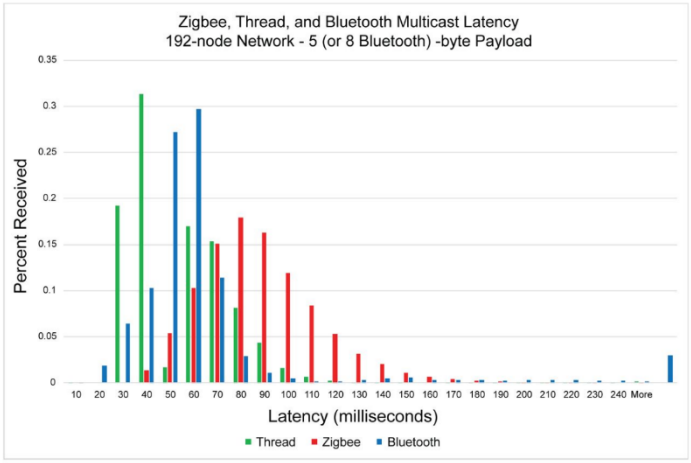


Kuva 12, Latenssi pienessä verkossa, pienellä pakettikoolla

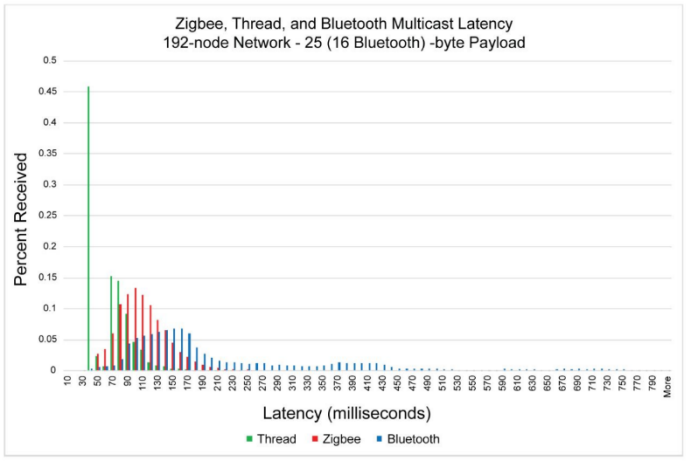


Kuva 13, Latenssi pienessä verkossa, suurella pakettikoolla.

Kuvassa 12 nähdään miten pienessä 24 laitteen verkossa, pienillä pakettikoilla Thread verkolla on pienin latenssi myös Bluetooth sekä Zigbee verkoilla latenssit ovat alle 100 ms. Kuvasta 13 kuitenkin nähdään, miten pakettikokojen kasvaessa Thread verkko kykenee ylläpitämään alle 100 ms latenssia. Zigbee verkostakin yli 60 % viesteistä saapuu alle 100 ms aikana, sen sijaan Bluetooth verkon latenssiajat ovat levittäytyneet hyvin laajalle, ja suurin latenssi aika on jopa 220 ms.



Kuva 14 Latenssi suuressa verkossa, pienellä pakettikoolla



Kuva 15, Latenssi suuressa verkossa, suurella pakettikoolla

Kuvassa 14 nähdään latenssiajat suuressa 192 laitteen verkossa pienellä pakettikoolla, Thread ja Bluetooth verkoilla latenssi on pääsääntöisesti alle 100 ms, kun taas Zigbee verkossa latenssi alkaa kasvaa verrattuna pienempään verkkoon. Kuvassa 15 nähdään latenssiajat suuressa 192 laitteen verkossa suurella pakettikoolla, Thread verkolla on edelleen paras latenssiaika, vaikka osalla paketeista aika valuukin jo yli 100 ms. Zigbee verkolla taas latenssiajat valuvat pahimmillaan lähemmäs 200 ms, vaikka iso osa paketeista saapuu 100 ms latenssilla. Bluetooth verkolla taas latenssiaika on pahimmillaan 750 ms ja se on pienenverkon tavoin levittäytynyt hyvin laajalle alueelle.

Näistä voidaan päätellä, että Thread verkolla on parhaat latenssiajat jokaisessa testin mallissa sekä nopein tiedonsiirto usean hypyn verkossa. Zigbee verkon sekä Bluetooth verkkojen suorituskyky sen sijaan on suhteellisen tasaista, Bluetooth verkko toimii hyvin pienemmillä latenssiajoilla pienillä pakettikoilla, mutta suuremmilla pakettikoilla taas asia kääntyy Zigbee verkon hyväksi. Myös usean laitteen hyppyjen välillä Zigbee verkossa on pienempi latenssi.

4 ZIGBEEN JA KNX:N YHDISTÄMINEN

Vaikka työssä löytyikin suoria yhdyskäytäviä yhdistämään KNX jo nyt yleisien IoT standardien välillä, päädyttiin kuitenkin rakentaa testiympäristö ”internet” pohjaisen IoT tiedonsiirtoon. Suurimmat syyt tähän olivat työn luonne, jossa tarkoitus oli etsiä keinoja erilaisten laitteistojen yhteensovittamiseen, sekä myös KNX omat suunnitelmat tulevaisuuteen, jossa myös jokainen KNX laite olisi ”IoT yhteensopiva”, tällöin yhdyskäytävä (gateway) ei toisi työn näkökulmasta uutta tietoa. Koska työtä aloitellessa ei ollut vielä tiedossa KNX suunnitelmia tulevaisuuteen, valittiin työhön lopulta Zigbee standardia käyttäviä automaatiolaitteita, niiden halvan hinnan sekä yleisyyden takia. Laitteita valittiin kiinteistöautomaation näkökulmasta, jolloin voitaisiin kokeilla, että laitteet sekä KNX toimivat yhteensopivasti. Zigbee laitteet itsestään eivät tukeneet suoraan IP verkkoja, sillä ne olivat vanhempaa Zigbee 1.0-2.0 standardia. Kiinteistöautomaatioon soveltuvia laitteita, jotka olisivat tukeneet Zigbee 3.0 ei tähän työhön löytynyt. Tämä luultavasti johtuu siitä, ettei Zigbee 3.0 ole ollut vielä kovinkaan pitkään olemassa.

Kuva 16, Xiaomi laitteet.

Kuvissa 16 ja 17 näkyy ostetut laitteet, Xiaomi:lta kaksiosainen kytkin, ovikytkin, lämpötilasensori (lämpötila, ilmanpaine, ilmankosteus), tärinäsensori (kosketus, tärinä, kallistuma), liiketunnistin (liiketunnistus, valoisuus), vesivuotosensori, sekä ”ohjaus kuutio” (tärinä, kallistus, siirtymä, pyöritys). Ikealta ohjattava pistorasia, väriä vaihtava himmennettävä lamppu sekä himmennin. Sekä luonnollisesti Raspberry Pi 3 sekä CC2531 Zigbee USB-Tikku.

Kuva 17, Ikean laitteet sekä Raspberry

4.1 Zigbee2mqtt asennus

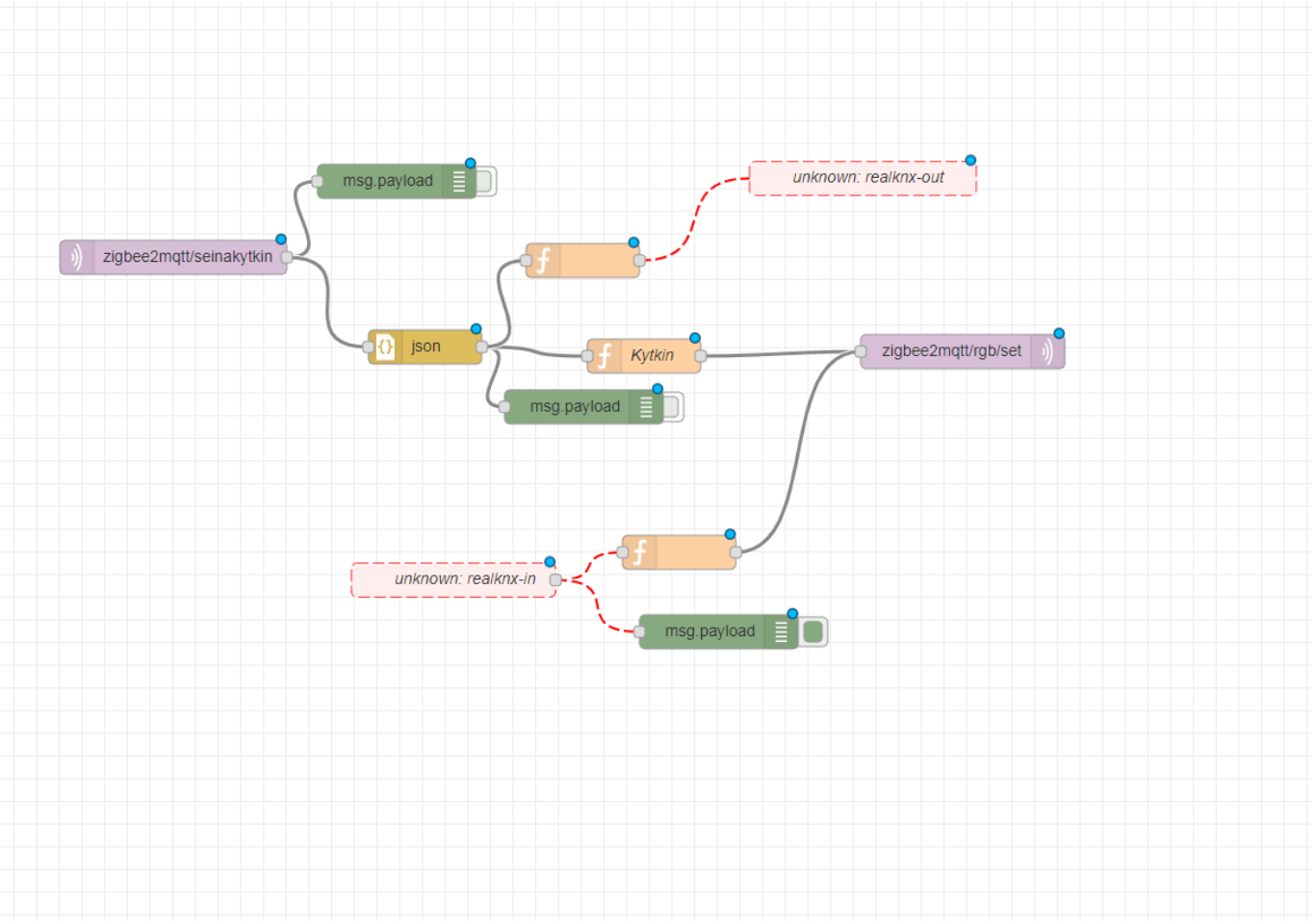
Lopulta ohjauksessa päädyttiin Raspberry Pi tietokoneeseen (Raspbian käyttöjärjestelmällä), ja siihen asennettavaan Zigbee-USB palikkaan. Raspberry Pi asennettiin USB adapterin lisäksi ”zigbee2mqtt” ohjelmisto, joka nimensä mukaisesti muuntaa Zigbee laitteilta tulevan tiedon MQTT formaattiin, jolloin Zigbee laitteita voidaan sekä lukea, että ohjata käyttäen MQTT rajapintaa. Zigbee verkossa Raspberry Pi toimii tällöin reitittimenä, joka myös muodostaa ja ylläpitää Zigbee verkkoa. Zigbee2mqtt ohjelmiston lisäksi asennettiin myös avoimeen lähdekoodiin perustuva MQTT ohjelmisto ”mosquitto”, jolloin Raspberry Pi toimii myös MQTT välittäjänä. Lopulta Raspberry:n asennettiin myös paikallinen tietokanta käyttäen mariaDB ohjelmistoa, tallentamaan laitteiden antamat arvot.

Zigbee2mqtt ohjelmisto vaatii Node.js JavaScript runtime-ympäristön, joka asennettiin komennolla *sudo apt-get install -y nodejs git make g++ gcc.* Ja seuraavaksi kopiotiin Zigbee2mqtt rasperry:lle komennoilla *sudo git clone https://github.com/Koenkk/zigbee2mqtt.git /opt/zigbee2mqtt* sekä *sudo chown -R pi:pi /opt/zigbee2mqtt .*
Jonka jälkeen asennus tapahtui komennoilla *cd /opt/zigbee2mqtt* sekä *npm install .*
Asennusten jälkeen täytyi uusi ohjelmisto konfiguroida, tämä tapahtui avaamalla configuration.yaml tiedosto, komennolla *nano /opt/zigbee2mqtt/data/configuration.yaml .* Jossa configuroitiin MQTT:n vaatimat kohdat topic, server, user, password, sekä Zigbee verkon vaatimat kohdat permit_join, network_key. Kyseisen tiedosto löytyy muokattuna liitteistä. Näillä toimilla varmistetaan, että MQTT on edes alustavasti suojattu salasanalla. Sekä Zigbee verkon turvallisuus vaihtamalla oletus suojaus avaimen, uuteen itse generoituun versioon. Tämä tapahtui käyttämällä komentoa *dd if=/dev/urandom bs=1 count=16 2>/dev/null | od -A n -t u1 | awk '{printf "["} {for(i = 1; i< NF; i++) {printf "%s, ", $i}} {printf "%s]\n", $NF}'.*
Tällä tavoin saadaan 16 satunnaista numeroa desimaali muodossa 0 ja 255 välillä. Samalla myös sallittiin Zigbee verkkoon liittyminen, jotta laiteet voidaan myöhemmin liittää verkkoon. Tämän jälkeen tehtiin ohjelmistosta ”palvelu” Raspberry palvelulistaan, jotta se käynnistyisi raspberryn käynnistyessä.

Laitteiden liittäminen tapahtui laitevalmistajien ohjeiden mukaan, usein painaen reset-nappia pohjassa raspberryn läheisyydessä, kunnes ohjelmisto tunnisti liittyvän laitteen ja lisäsi sen verkkoon. Laitteet myös ilmestyivät configuration.yaml tiedostoon muodossa *0x00158d0001dc126a*, mutta ne pystyttiin nimeämään helpommin muistettavaan muotoon. Kaikki laitteet eivät lopulta suostuneet liittymään verkkoon, vaikka ne olivat tuettuna ohjelmistossa ja niitä koitettiin parittaa laitevalmistajan ohjeiden mukaan. Yksi tällainen laite oli Xiaomi:n tärinäsensori, jota ei saatu liittymään verkkoon, myös Ikean himmentimen kanssa oli ongelmia, jotka ratkesivat laitteen patterin vaihdolla. Kun laitteet ovat liitetty verkkoon alkavat ne kommunikoida raspberry:n kanssa ja ohjelmisto hoitaa MQTT käskyt Zigbee komennoiksi.

MQTT viesteissä jokaisella laitteella on oma aihealue (topic), esimerkkinä lämpötilasensorilla aihealue on Zigbee2mqtt/lampotila. Aihealueita nimiä voidaan muuttaa configuration.yaml tiedostossa. MQTT viesti on JSON-formaatissa, esimerkkinä lämpötilasensori, {"temperature": 22.5, "linkquality": 110, "humidity": 39.21, "pressure": 1003, "battery": 91, "voltage": 2985}. Näiden viestien sisältö riippuu laitteista, mutta jokainen laite antaa jokaisessa viestissään usein vähintään kolme muuttujaa, jotka ovat yhteydenlaatu, akun taso sekä akun jännite. Viestien sisältö luonnollisesti muuttuu, mikä laiteella on muuttuvia parametrejä, kuten kytkimellä, myös viesti muuttuu, kertoen tapahtumista. Esimerkkinä kytkimen ollessa lepotilassa sen lähettämä viesti on seuraava *{"battery":100,"voltage":3035,"linkquality":118},* nappia painaessa viestiin lisätään muuttunut parametri *{"battery":100,"voltage":3035,"linkquality":136,"click":"left"}*. Puuttuvia osia ei voi ilman ohjelmiston valmistajan antamaa listaa päätellä, muutoin kuin kokeilemalla eri toiminnot läpi, jolloin ne näkyvät kyseisen laitteen aihealueella.
Mikäli laitetta halutaan ohjata, täytyy lähettää MQTT viesti aihealueelle zigbee2mqtt/XXXX/set, esimerkkinä lampun sytyttäminen tapahtuu lähettämällä viesti JSON-formaatissa *{"state":"on"}* aihealueelle zigbee2mqtt/rgb/set. Tällöin aihealueella zigbee2mqtt/rgb tulee viesti *{"state":"ON","linkquality":113,"brightness":253,"color_mode":2,"color":{"x":0.458,"y":0.41}}.* Koska kyseessä on väriä vaihtava himmennettävä lamppu, värin vaihto tapahtuisi komennolla *{"color":{"x":0.158,"y":0.25}}* tai himmennyksen taso *{"brightness":100"}.* Kaikki komennot voidaan antaa myös samalla kertaa, jolloin lamppu syttyisi suoraan haluttuun väriin halutulla kirkkaudella. Koska laitteet päivittävät omaa tilaansa aihealueellansa, myös laitteen säädetty väri sekä himmennys voidaan katsoa tai säätää jo etukäteen.

Kun laitteet oli lisätty sekä ohjelmisto toiminnassa, alkoi kokeilu saada olemassa oleva KNX järjestelmä toimimaan molempiin suuntiin. Tämä onnistui KNX järjestelmässä olevan KNX Proserv sekä RealKNX laitteiden avulla.
KNX Proserv toimi realKNX laitteen sekä KNX väylänvälisenä ”muuntimena”, johon on tallennettuna KNX asennuksen ETS tietokanta. RealKNX laite vastaavasti pystyy kommunikoimaan myös muiden IoT laitteiden sekä palveluntarjoajien kanssa mahdollistaen, sekä paikallisen, että pilven välisen ääniohjauksen. Laite sisältää Node-RED ohjelmointi työkalun, jolla KNX sekä Zigbee verkon kommunikointi lopulta muunnetaan toisiaan ymmärtävään muotoon. Node-RED vuo, jota käytettiin Zigbee:n sekä KNX järjestelmien välissä löytyy kuvasta 18 sekä liitteessä 5.



Kuva 18 Node-RED vuo, Zigbee sekä KNX järjestelmän väillä.

Node-RED vuossa käytettiin MQTT syöttöä raspberry:ltä, joka vaatii tunnukset, joilla syötteeseen päästään kiinni. Tämä olisi ollut mahdollista suojata lisäksi SSL tai TLS yhteydellä, jolla tietoliikenne olisi ollut salattua Raspberry:n sekä RealKNX laitteiden välillä, mutta se jätettiin pois käytöstä ajanpuutteen sekä Raspberry:n vaihtuvan fyysisen sijainnin kanssa, jolloin olisi täytynyt luoda useampia sertifikaatteja sekä tehdä tarvittavia muutoksia reitittimien asetuksiin.
MQTT syöte antaa syötteen JSON-muodossa, josta se muunnetaan JavaScript objektiksi. Tämän jälkeen käytettiin funktio ominaisuutta, jolla objekteista tarkastetaan saapunut arvo, tässä tapauksessa kytkimen vasenta painiketta, jolloin mikäli sitä painetaan, muunnetaan lähtevä arvon tietosisältö (payload) arvoon 0, muussa tapauksessa arvo on 1. Tietosisältö lähetetään tämän jälkeen Node-RED RealKNX sovellukseen, jossa se konfiguroitiin ohjaamaan KNX valaisinta. Tämä löytyy liitteestä 1.
Saman aikaisesti Zigbee kytkin ohjaa myös Zigbee lamppua, jolloin yksi kytkin saatiin ohjaamaan samanaikaisesti sekä Zigbee, että KNX laitetta. Koska syöte on muunnettu objekteiksi, tarvitaan funktio myös muuntamaan Zigbee valaisimelle menevän viesti takaisin JSON-muotoon. Tämä löytyy liitteestä 2.
Samalla vuolla ohjataan myös KNX kytkimellä Zigbee lamppua, joka tapahtuu Node-RED realKNX sovelluksella, jossa on valittuna KNX kytkimen ulostulo, tämäkin viesti täytyi muuntaa funktio sovellusta käyttämällä json muotoon. Tämä muunnos löytyy liitteestä 3. Lopulta KNX ja Zigbee laitteiden keskinäinen toiminta sujui hyvin. Molemman järjestelmän laitteilla kyettiin ohjamaan toista järjestelmää. Koko vuo löytyy liitteestä 5

4.2 Tietokannan asennus ja viestien siirto

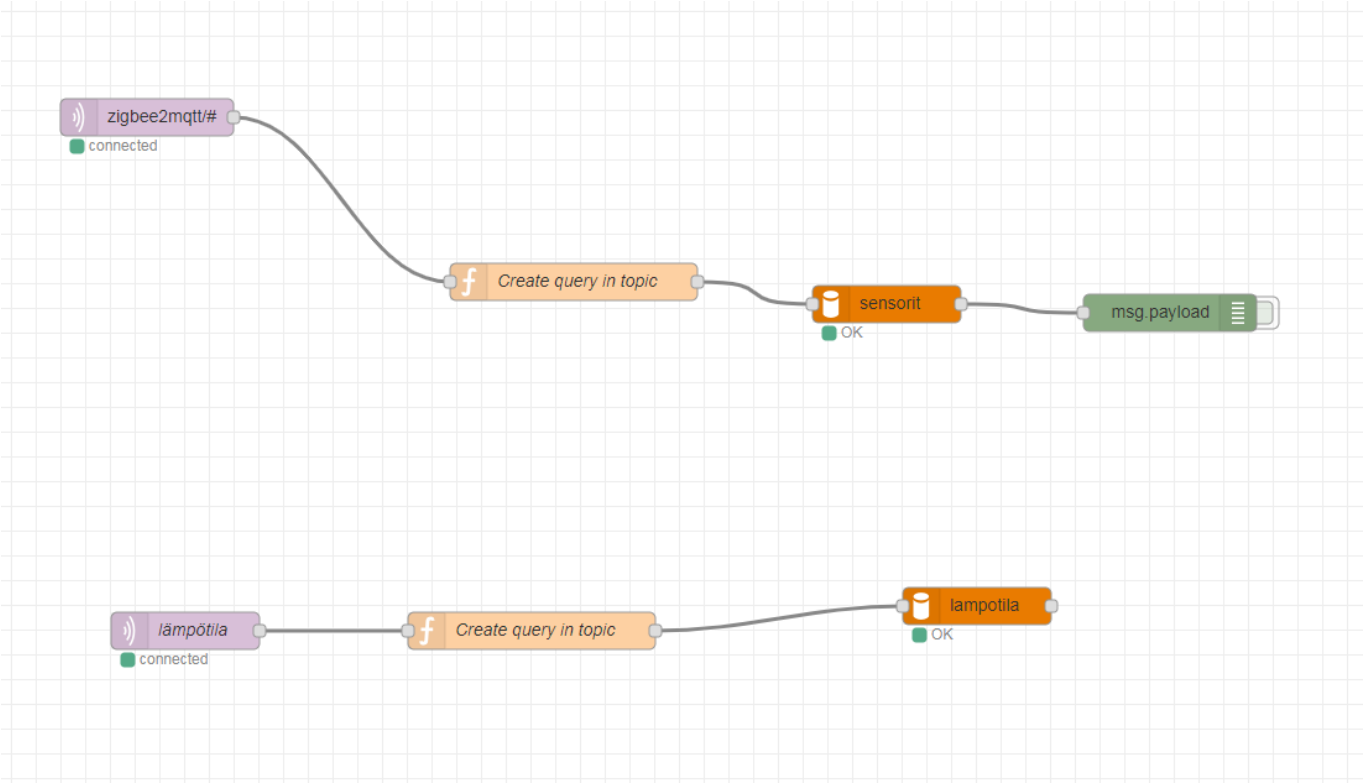
Seuraavana asennettiin MariaDB ohjelmisto, joka tapahtui käyttämällä komentoa *sudo apt-get install mariadb-server.* Asennuksen jälkeen ohjelmistolle asennettiin salasana, ja tämän jälkeen alettiin luoda tietokantaa, jonka nimettiin sensorit. Kokeilun vuoksi luotiin myös tietokanta muutamalle laitteelle. Joka tapahtui käyttämällä MariaDB ohjelmassa komento *create database sensorit;* jonka jälkeen tietokanta valitaan komennolla *use sensorit;.* Tämän jälkeen tietokannalle luotiin käyttäjä komennolla *create user ´XXXXXX´@´localhost´ identified by ´XXXXXXX´;* ja tälle käyttäjälle annettiin oikeudet käyttää tietokantaa komennolla *grant all privileges on sensorit * to ´XXXXXX´@´localhost´;* ja samalla päivitettiin käyttäjät komennolla *flush privileges;.*
Tämän jälkeen luotiin tietokantaan sarakkeita komennoilla *alter table sensorit add column id int(11) not null auto_increment primary key; alter table sensorit add column timestamp datetime not null; alter table sensorit add column topic text not null; alter table sensorit add column data text not null.* Tällöin saadaan tietokanta, jossa on sarakkeet, ID (järjestysnumero), timestamp (aikaleima), topic (aihealue) sekä data. Sarakkeita olisi voinut luoda myös lisää muutamalla laitteelta saadun tiedon MQTT JOSN-muodosta erikseen jokaiselle sarakkeelle. Tämä kuitenkin jäi tekemättä ajanpuutteen vuoksi sekä, koska tiedossa ei ollut suoraa käyttökohdetta näille tiedolle, jolloin sen olisi voinut tallentaa suoraan haluttuun muotoon. Tällöin tiedot päätettiin tallentaa kokonaisuudessaan json formaatissa, josta ne voidaan myös jälkeenpäin käsitellä.

Tämän jälkeen Node-RED ohjelmistosta luotiin uusi vuo, jossa MQTT viestit tallennetaan juuri luotuun tietokantaan käyttäen Node-RED MySQL sovellusta. Luotu vuo näkyy kuvassa 2, ja löytyy liitteenä. Vuossa jokaisen laitteen viesti tallennetaan käyttäen liitteen 4 mukaista skriptiä, siinä skripti luo aikaleiman, valitsee aihealueen (laitteen aihealueesta) sekä lopulta valitsee JSON tiedon data sarakkeeseen. Samalla kokeiltiin myös yhden laitteen lähettämän tiedon tallentamista omaan tietokantaan. Koko vuo löytyy liitteestä 6 sekä kuvasta 20.
Tällä saavutettiin paikallinen tietokanta, josta mahdolliset arkaluontoiset tiedot eivät päädy ulkopuolisille tai niitä ei tallenneta laisinkaan. Lopulta tietokantaan tallennetun tietojen muoto tarkastettiin komennoilla *use sensorit* ; sekä *select * from sensorit ORDER BY id DESC LIMIT 30;* joka löytyy kuvasta 19.

id	timestamp	topic	data
3030	2019-11-20 16:12:13	zigbee2mqtt/pistorasia	{"state":"ON","linkquality":110}
3029	2019-11-20 16:01:34	zigbee2mqtt/liiketunnistin	{"illuminance":0,"linkquality":115,"occupancy":false,"battery":100,"voltage":3025}
3028	2019-11-20 16:00:04	zigbee2mqtt/liiketunnistin	{"illuminance":0,"linkquality":115,"occupancy":true,"battery":100,"voltage":3025}
3027	2019-11-20 16:00:04	zigbee2mqtt/liiketunnistin	{"illuminance":0,"linkquality":113,"occupancy":true,"battery":100,"voltage":3025}
3026	2019-11-20 16:00:04	zigbee2mqtt/seinakytkin	{"battery":100,"voltage":3025,"linkquality":176}
3025	2019-11-20 15:58:43	zigbee2mqtt/lampotila	{"temperature":23.12,"linkquality":94,"humidity":42.85,"pressure":1008.9,"battery":91,"voltage":2985}
3024	2019-11-20 15:58:39	zigbee2mqtt/liiketunnistin	{"illuminance":0,"linkquality":110,"occupancy":true,"battery":100,"voltage":3025}
3023	2019-11-20 15:58:39	zigbee2mqtt/liiketunnistin	{"illuminance":0,"linkquality":110,"occupancy":false,"battery":100,"voltage":3025}
3022	2019-11-20 15:56:39	zigbee2mqtt/liiketunnistin	{"illuminance":0,"linkquality":115,"occupancy":false,"battery":100,"voltage":3025}
3021	2019-11-20 15:55:33	zigbee2mqtt/pistorasia	{"state":"ON","linkquality":110}
3020	2019-11-20 15:55:09	zigbee2mqtt/liiketunnistin	{"illuminance":0,"linkquality":115,"occupancy":true,"battery":100,"voltage":3025}
3019	2019-11-20 15:55:09	zigbee2mqtt/liiketunnistin	{"illuminance":0,"linkquality":115,"occupancy":true,"battery":100,"voltage":3025}
3018	2019-11-20 15:54:00	zigbee2mqtt/liiketunnistin	{"illuminance":0,"linkquality":110,"occupancy":true,"battery":100,"voltage":3025}
3017	2019-11-20 15:54:00	zigbee2mqtt/liiketunnistin	{"illuminance":0,"linkquality":110,"occupancy":false,"battery":100,"voltage":3025}
3016	2019-11-20 15:53:22	zigbee2mqtt/liiketunnistin	{"illuminance":0,"linkquality":99,"occupancy":false,"battery":100,"voltage":3025}
3015	2019-11-20 15:51:52	zigbee2mqtt/liiketunnistin	{"illuminance":0,"linkquality":99,"occupancy":true,"battery":100,"voltage":3025}
3014	2019-11-20 15:51:52	zigbee2mqtt/liiketunnistin	{"illuminance":0,"linkquality":99,"occupancy":true,"battery":100,"voltage":3025}
3013	2019-11-20 15:51:51	zigbee2mqtt/lampotila	{"temperature":23.06,"linkquality":107,"humidity":42.68,"pressure":1008,"battery":91,"voltage":2985}
3012	2019-11-20 15:51:51	zigbee2mqtt/lampotila	{"temperature":23.06,"linkquality":105,"humidity":42.68,"pressure":1008,"battery":91,"voltage":2985}
3011	2019-11-20 15:51:51	zigbee2mqtt/lampotila	{"temperature":23.06,"linkquality":105,"humidity":41.52,"pressure":1008,"battery":91,"voltage":2985}
3010	2019-11-20 15:50:39	zigbee2mqtt/liiketunnistin	{"illuminance":0,"linkquality":92,"occupancy":true,"battery":100,"voltage":3025}
3009	2019-11-20 15:50:38	zigbee2mqtt/liiketunnistin	{"illuminance":0,"linkquality":92,"occupancy":true,"battery":100,"voltage":3025}
3008	2019-11-20 15:50:02	zigbee2mqtt/ovikytkin	{"battery":100,"voltage":3035,"contact":false,"linkquality":97}
3007	2019-11-20 15:49:20	zigbee2mqtt/liiketunnistin	{"illuminance":0,"linkquality":94,"occupancy":true,"battery":100,"voltage":3025}
3006	2019-11-20 15:49:20	zigbee2mqtt/liiketunnistin	{"illuminance":0,"linkquality":94,"occupancy":true,"battery":100,"voltage":3025}
3005	2019-11-20 15:48:08	zigbee2mqtt/liiketunnistin	{"illuminance":0,"linkquality":97,"occupancy":true,"battery":100,"voltage":3025}
3004	2019-11-20 15:48:08	zigbee2mqtt/liiketunnistin	{"illuminance":0,"linkquality":99,"occupancy":false,"battery":100,"voltage":3025}
3003	2019-11-20 15:45:10	zigbee2mqtt/rgb	{"state":"OFF","linkquality":107,"brightness":253,"color_mode":1,"color":{"x":0.158,"y":0.25}}
3002	2019-11-20 15:45:09	zigbee2mqtt/rgb	{"state":"OFF","linkquality":110,"brightness":253,"color_mode":1,"color":{"x":0.158,"y":0.25}}
3001	2019-11-20 15:45:09	zigbee2mqtt/rgb/set	{"state":"off"}

30 rows in set (0.00 sec)

Kuva 19, mariaDB tietokannan muoto.



Kuva 20, MQTT muunnos tietokantaan vuo

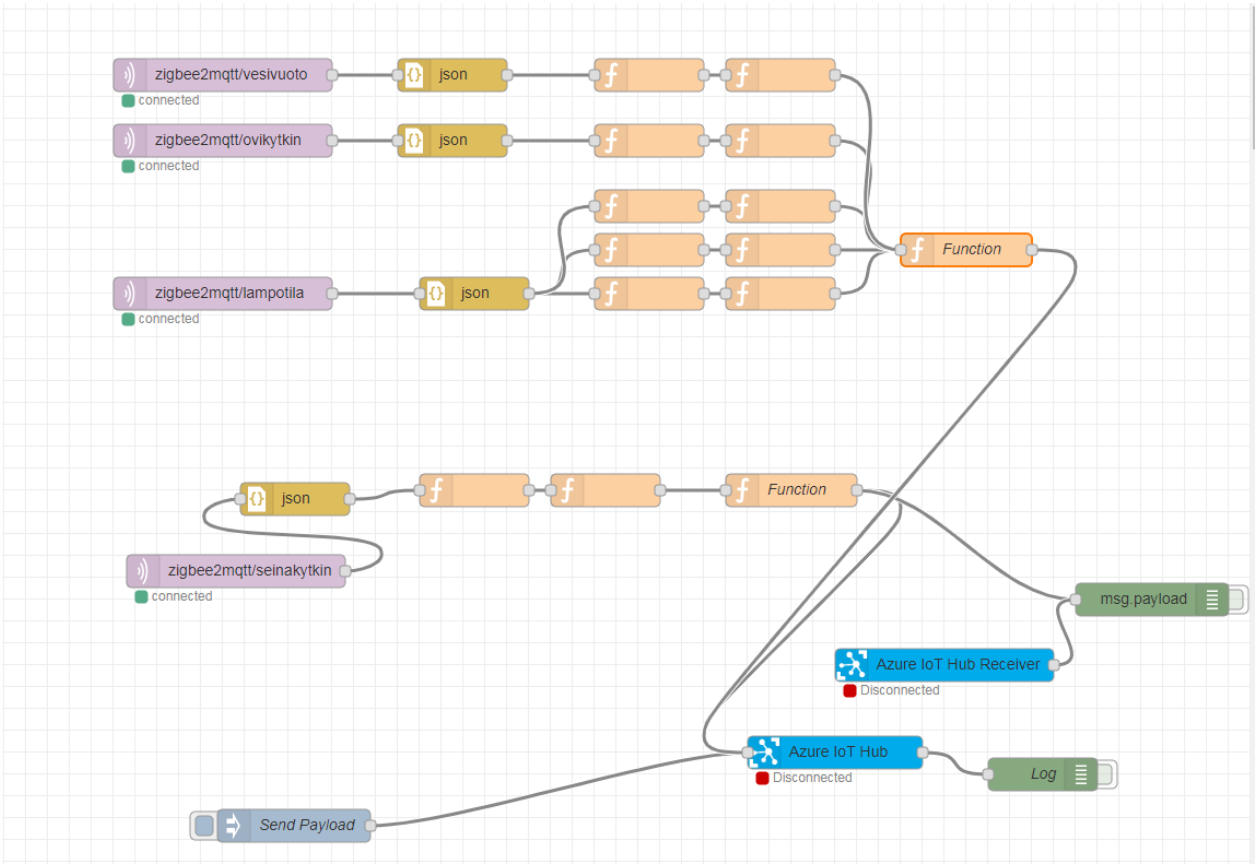
4.3 Pilvipalvelu

Viimeisenä kokeiltiin myös viestien siirtämistä Azuren IoT Hub-pilvipalveluun. Pohdinnassa oli myös koko paikallisen tietokannan kopiointi pilveen, mutta lopulta päädyttiin käyttämään Azuren palveluita siirtämällä sinne vain ne tiedot joita sinne halutaan.

Node-RED ohjelmistoon luotiin taas uusi vuo, jossa käytettiin Azure IoT Hub sovellusta, pienoisena ongelmana oli saada MQTT tiedot muunnettua Azuren vaatimaan muotoon. Jolloin normaalin json muodon vaihdon lisäksi tarvittiin kolme eri funktio skriptiä, jotta tiedot lopulta saatiin siirrettyä. Jostain syystä skriptien yhdistäminen siten, että Azure olisi hyväksynyt tiedot ei onnistunut. Ja mikäli laite antoi useampaa eri tietoa, täytyi niiden tiedot lähettää omilla funktioilla, esimerkiksi lämpötilasensorin lähettää lämpötila, kosteus sekä ilmanpaineen tiedon. Jolloin kaikille kolmelle täyty tehdä oma kolmen funktion sarja, ja näistäkin tiedoista huolimatta uupumaan jäivät akun tila, jännite sekä linkintaso. Teoriassa mikään ei olisi estänyt tehdä niille vielä täysin oma skripti, mutta koska käytössä oli Azuren ilmaisversio, niin ei siinä olisi ollut paljoa hyötyä. Sillä ilmaisversion viestimäärä täyttyy hyvin nopeasti ja käytössä on vain yksi laite, jolloin jokainen laite näkyi yhtenä laitteena Azuren palvelussa vain aihealueen erotellessa niitä.

Ensimmäisessä funktiossa otetaan MQTT viestistä haluttu tieto, seuraavassa vaihdetaan tämän aihealuetta, ja kolmannessa data muokataan lopulliseen muotoon, jossa on myös Azuren käyttö tunnukset sekä aikaisempi aihealue sekä itse tieto. Tämän jälkeen se lähetetään Azure sovellusta käyttäen Azuren palveluun. Azuren palvelussa ei pääse ilman maksua katsomaan mitä viestit sisältävät, mutta siellä näkyy vastaanotettujen viestien määrä, joka vastasi lähetettyjen viestien määrää.

Azuren palvelussa lähetyt tiedot saisi Azuren omaan tietokantaan, mutta ajanpuutteen takia Azuren palveluita ei tutkittu tätä enempää. Azuren pilvipalvelussa olisi myös mahdollista analysoida tietoja enemmän. Koko vuo löytyy liitteestä 7 sekä kuvasta 21.



Kuva 21, MQTT Azure muunnoksen vuo.

Lopputulemana Zigbee sekä KNX järjestelmä saatiin toimimaan molempiin suuntiin, samaan laitteeseen saatiin asennettu paikallinen tietokanta, sekä viestit saatiin välitettyä myös Azuren pilvipalveluun. Vaikka aivan kaikkia laitteita ei saatukaan toimimaan, onnistui kokeilu silti suhteellisen hyvin. Myyntiin tai käyttöön ei tallaista laitteita kannata ottaa, sillä laitteistossa voi piillä useita tietoturva-aukkoja, mutta tällä tavoin saatiin todistettua, että KNX järjestelmä voi käyttää myös muita internet pohjaisia automaatiolaitteita KNX ohjaukseen sekä ohjata muita järjestelmiä KNX laitteilla. Työllä saavutettiin ainakin pintaraapaisu eri järjestelmistä, jotka voivat olla myös tulevaisuudessa käytössä IoT laitteissa. Sekä yksi idea, jolla tulevaisuuden keskitin-ratkaisut voisivat toimia, paikallisella tietokannalla, paikallisessa verkossa jakamalla pilvipalveluihin vain ne tiedot mitä halutaan.

5 POHDINTA

IOT NYKYINEN TILA

Nykyisin jokaisella standardilla on oma gateway tai Hub laitteistonsa, ja eri standardit kommunikoivat lähinnä omien pilvipalveluiden kautta, jolloin laitteistoiden toimintaan voi tulla huomattava viivettä. Esimerkkinä voidaan käyttää yksinkertaista valokytkintä, joka sytyttää eri valmistajan valon. Painamisesta tieto välittyy ensin valokytkimen valmistajan yhdyskäytävään, yhdyskäytävästä tieto välittyy kytkimen valmistajan palvelimelle, koska valmistajan palvelin ei osaa käskeä muiden valmistajien lamppuja, tarvitaan väliin vielä erillinen palvelu (IFTT) joka yhdistää usean eri valmistajan palvelimilta saataviin tietoihin ja josta asiakas pääsee ohjelmoimaan mitä toimintoja mikäkin käsky tekee. Erillisestä palvelusta viesti kulkee lampun valmistajan palvelimille, joista taas tieto välittyy takaisin lampunvalmistajan yhdyskäytävään. Lopulta lamppu saa komennon syttyä.

Tuossa välissä käsky on matkannut ensin kytkimen valmistajan langattoman verkon lävitse, kiinteistön ulkopuolelle kolmen palvelimen kautta, ja lopulta takaisin kiinteistöön, lampun valmistajan langattoman verkon kautta lampulle. Jos oletettaisiin, että jokaisen laitteen välille tulee muutaman millisekunnin viive, on tämä viive kasvanut jo tässä vaiheessa kuusinkertaiseksi. Tähän lisäämällä vielä yhdyskäytävien sekä palvelimien omat viiveet, voi painikkeen painamisesta lampun syttymiseen syntyä jo huomattava viive. Jos yksikin ketjun yhteyksistä tai laitteista hajoaa, lamput eivät syty. Myös palvelimien sekä yhdyskäytävien päivitykset voivat rikkoa tämän ketjun. Yksikeino poistaa viiveet ovat ostaa samalla standardilla toimivat laitteet, mutta sekään ei välttämättä auta, mikäli tietyn valmistajan keskitin ei tue toisen valmistajien laitteita. Tällöin vaikka laitteet toimisivat täsmälleen samalla standardilla, ei ohjaukseen voida käyttää kuin pilvipalveluja. Tässä tapauksessa myös yksityisyys on koetuksella, mikäli yhdenkään välin tietoliikenne ei ole salattua, tai yhdenkään palvelimen tai yhdyskäytävän tietoturvasta löytyy aukko, on laitteiden käyttötiedot ulkopuolisten hallussa. Myös vaikkei tietoturva-aukkoja löydy, kiinteistön käyttötietoja on nyt kolmen eri valmistajien palvelimella, joista valmistajat voivat halutessaan (käyttöehtojen salliessa) myydä tiedot ulkopuolisille. IoT järjestelmien välillä kannattaakin huomioida myös se kuka kerätyn tiedon omistaa, ja millä ehdoin niitä voidaan hyödyntää.

KNX JA IOT TULEVAISUUS JA ONGELMAT

KNX tulevaisuuden IoT laitteet kuitenkaan eivät tule tukemaan suoraan muiden standardien käskyjä vaan tavoitteena on, että KNX sanomat välitettäisiin vain eri IP rajapintojen kautta. Ja muut standardit alkaisivat tukea KNX sanomaa. Tämä tarkoittaa, että KNX laitteet voivat siirtyä muiden standardien tiedonsiirto protokolliin. Lähes ainoana vaatimuksena on, että kyseinen standardi toimii suoraan IP-pohjaisena, jolloin se voi ottaa yhteyden IP verkon kautta muihin KNX laitteisiin. Tällöin KNX laitteen ei välttämättä tarvitse tukea yhtäkään ”perinteistä” väylämuotoa, vaan pelkkä IP-pohjaisuus riittää. Tällöin teoriassa KNX laitteet voisivat toimia Wi-Fi verkon tai Thread verkon päällä todella nopealla aikataululla. Koska Wi-Fi sekä Thread eivät määrittele OSI-mallin sovelluskerrosta on niille mahdollista saada sekä KNX, että Wi-Fi tai Thread sertifiointi.
Sen sijaan hyvin monille muille standarteille tämä ei välttämättä ole mahdollista, esimerkkeinä Zigbee, Bluetooth. Kumpikaan ei myöskään tue nativisti IP verkkoa tällä hetkellä, vaikka standarteilla on mahdollista käyttää IPv6 verkossa. Mikäli tämä joskus muuttuu ja myös nämä muuntuvat IPv6 pohjaisiksi, jäisi ongelmaksi valmiiksi määritelty sovelluskerros. Tällöin laitteen täytyisi ymmärtää sekä KNX komentoja, että Zigbee tai Bluetooth komentoja, joka voi aiheuttaa sertifioinnissa ongelmia.
Toinen vaihtoehto olisi sertifioida laite vain toiseen standardin käyttöön ja tukea epävirallisesti toista standardia, mutta mikä ei välttämättä ole minkään standartin tai laitevalmistajan haluama lopputulos. Myös muut kombinaatiot ovat mahdollisia, kykenisikö KNX laite ”puhumaan” myös muita kieliä? Jos tulevaisuudessa ilmestyy toinen hyvin yleinen kieli, onko laitevalmistajilla mahdollisuutta rakentaa laite, joka tukee myös muita IP-pohjaisia kieliä KNX sanoman lisäksi, jolloin esimerkiksi ilmanvaihtojärjestelmä voisi saada lämpötilatietoja muilta IP-pohjaisilta laitteilta näiden laitteiden käyttämällä ”kielellä”? KNX on ilmoittanut Thread Groupille, että Thread on valittu vähävirtaisen langattoman tiedonsiirto protokollaksi KNX IoT alustalle. Mikä oletettavasti tarkoittaa, että KNX laitteita alkaa ilmestyä ainakin Thread standartin verkkoihin. (Thread Group)

Tulevaisuudessa myös kiinteistöiden tietoliikenne infrastruktuuriin kohdistuu entistä enemmän paineita. Mikäli merkittävä osa KNX laitteista siirtyy tukemaan esimerkiksi langallisia IP yhteyksiä, alkaa se vaatia enemmän investointeja tietoliikenne kytkimiin tai vaihtoehtoisesti langattomilla ratkaisuilla laadukkaisiin reitittimiin. Mikäli Ethernet verkkoa käytetään ”perinteisessä” muodossa eli tähti topologialla, myös kytkinten määrä sekä kaapeleiden määrä kasvavat huomattavasti verrattuna KNX väylä-kaapeliin. Ellei siirrytä vanhaan Ethernet väylätopologiaan, jolloin näitä rajoituksia ei synny.
Kysymykseksi jää myös, halutaanko KNX verkko vielä ”eristää” muista kiinteistön laitteista joko omilla kytkimillä, langattomilla verkoilla tai VLAN verkoilla? Tämä luultavasti lisäisi järjestelmän hintaa joko lisälaitteiden tai kalliimpien laitteiden ostoilla. Mutta toisaalta pienentäisi riskiä, mikäli laitteistosta tulevaisuudessa löytyy haavoittuvuuksia. Tällöin myös olisi mahdollista eristää KNX verkko internetistä hyvin nopeasti, jolla pystyttäisiin hankkimaan lisää aikaa päivitysten tekoon laitevalmistajille. Tämä myös mahdollistaisi kiinteistön normaalin käytön ilman pelkoa KNX järjestelmän tai laitteen kaappauksesta. Mutta mikäli asian eteen ei tehdä mitään, parhaimmassa tapauksessa koko

kiinteistön yhteydet pitäisi katkaista, jotta saataisiin sama eristettävyys. Tällöin valinnaksi jäisi joko siirtyminen muilla laitteilla mobiiliverkkojen pariin tai elää pelossa hyökkäyksestä.

Kysymyksiä herää myös vastuurajoista, kuuluuko myös kiinteistön verkkoinfrastruktuuri urakoitsijan hoidettavaksi ja mikäli ei, kenelle jää vastuu, mikäli verkko on väärin mitoitettu tai toimii väärin? Ja kenellä on vastuu, mikäli tämä verkko kaatuu tai hajoaa, tällöin käytännössä koko KNX verkon voi kaatua yhden laitteen mukana. Vaikka tällöinkään itse KNX ei olisi riippuvainen internet-yhteydestä, se voisi silti kaatua, mikäli kytkin tai reititin hajoavat. Tämä taas tuo hajautettuun KNX järjestelmään SPOF kohteen (Single point of failure).
Myös laitteistoihin tuleva semantiikkatietomalli herättää kysymyksiä sen suhteen, että miten helposti se on ulkopuolisten saatavilla, sekä sisältääkö se myös arkaluontoisia tietoja. Sisältääkö semantiikka-tietomalli tai laite itsessään KNX verkon salausavaimia? Pääseekö niihin käsiksi käytetyissä laitteista? Tarvitseeko hajonneet KNX laitteet tuhota tietoturvallisesti?

TIETOTURVA JA YKSITYISYYS

Yksi suurimmista kysymyksistä IoT laitteissa on laitteiden tietoturva. Protokollat ja standardit ovat parhaillaan suhteellisen turvallisia, suoria hyökkäyksiä itse protokollaan, eli ilmateitse, on vaikeaa salauksen takia. Aikaisemmin löytyneet tietoturva-aukot, jotka hyökkäsivät itse langattomaan protokollaan, sekä Z-wave verkossa, että Zigbee verkossa johtuivat huonosti toteutetusta verkkoon liittymisestä. Aikaisemmin protokollat pitivät tärkeänä ominaisuutena helppoa asennusta, jolloin laitteiden lisääminen tapahtui lähettämällä salausavaimen langattomasti selkokielellä liitettävään laitteeseen. Jos hyökkäävä taho pääsi laitteiden lähelle ja pystyi myös vastaanottamaan tämän salausavaimen, oli myös hyökkääjällä mahdollisuus lukea salattua liikennettä. Nämä on kuitenkin ratkaistu uudemmissa malleissa laitteissa, joissa verkkoon liittymiseen vaaditaan laitteeseen esiasennettu salausavain, tai fyysistä nappia painamalla. Itse radioaalloilla olevaa liikennettä ei siis ole onnistuttu murtamaan, mutta eri tavoin verkkoon liittämisessä, jossa salausavainta jaetaan, on mahdollista saada salausavain haltuun ja tämän jälkeen, joko liittyä suoraan verkkoon, syöttää verkkoon komentoja sekä mahdollisesti muunnella laitteiden välistä tiedonsiirtoa.

Toisaalta myös laitevalmistajilla on oma vastuunsa laitteiden käyttäytymisessä verkoissa, jos tämä ei ole kunnossa hyökkääjä voi saada myös ihmisen itse päästämään hyökkääjän verkkoon tai aiheuttaa harmia talossa löytyvän laitteiston ohjauksessa. Esimerkiksi eräs Zigbee lamppuvalmistajan lampun pystyi radiotaajuuksia häiritsemällä ”kadottamaan” yhteyden muuhun verkkoon, jolloin laite nollasi itsensä ja vaati liittämistä verkkoon uudestaan. Jolloin laitetta uudelleen liitettäessä hyökkääjällä on mahdollista edellisten liittymiseen käytettävää tietoturva-aukkoa hyväksi saada salausavain haltuunsa. Samalla tavalla radiotaajuuksia häiritsemällä lampun pystyi myös lisäämään hyökkääjän luomaan ulkoiseen Zigbee verkkoon ja täten hallita laitetta haluamallansa tavalla. (The Verge, 2016)

Myös IoT laitteiden hävittäminen voi vaatia erillisiä toimia, kuin pelkästään hävittää ne SER-jätteiden kautta. IoT laitteet voivat säilöä tietoa ja jopa suoraan verkon salausavaimet suoraan salaamattomassa muodossa. LimitedResults omassa blogissaan kykeni lukemaan kolmen erivalmistajan WIFI LED-lampuista Wi-Fi:n SSID tunnuksen ja salasanan. (limitedresults, 2019)
Tulevaisuudessa myös laitteiden hävittämiseen täytyy kiinnittää huomiota, joko vakuuttumalla valmistajan antamiin tietoihin, ettei laitteisiin jää suojaamattomassa muodossa mitään tärkeää, tai ostamalla palveluita, joissa IoT laitteet tuhotaan tietoturvallisesti. Parhaillaan vain Z-wave tukee laitteiden ”poistamista” omasta verkosta, jolloin poistettua laitteisto ei voida käyttää ohjaaman Z-wave verkon toimintaa. IoT laitteiden salausavaimet eivät yleensä muutu verkon olemassaolon aikana, jolloin vanhojenkin laitteiden salausavaimet ovat voimassa. Tämä johtuu akkukäyttöisten laitteiden heikosta prosessointi tehosta, sekä akkukäyttöisten laitteiden ”nukkumistilasta”, jolloin laitteet voisivat ”nukkua” salausavaimen vaihdon yli, ja täten tippua verkosta.

Nyt IoT järjestelmien kehitys alkaa kulkea suoraan IP-pohjaiseen järjestelmään, missä laitteilla on oma IP-osoite ja se kykenee itse ottamaan suoraan yhteyden internettiin (yhdyskäytävän) kautta on sekä uhka, että mahdollisuus. Toisaalta se tarkoittaa, että internet on vihdoin saapumassa ”Internet of Things” maailmaan ja mahdollistaa älykkään kiinteistön ohjaamisen. Se mahdollistaa myös suorat ohjelmistopäivitykset laitteeseen, sekä mahdollisesti yhteensopivuuden muiden protokollien kanssa käyttäen IP-verkkoa tietojen välitykseen. Samat uhat ovat olemassa jo nykyisillä yhdyskäytävä pohjaisilla laitteistoilla, ja niistäkin on jo löydetty useita aukkoja. Suoran internet yhteyden uhka on kuitenkin, että niitä käytetään suoraan laitteissa mahdollisesti oleviin tietoturva haavoittuvuuksiin. Jolloin laiteet voidaan valjastaa palvelunestohyökkäyksiin, tai mahdollisesti estää järjestelmän toiminnan ulkopuolisella palvelunestohyökkäyksellä
Se mahdollistaa myös yksittäisten laitteiden tietojen valumista joko valmistajan tai kolmannen osapuolen haltuun, mikä ei aiheuta järjestelmän toimintaan häiriöitä, mutta onko se kiinteistön omistajan tai kiinteistön käyttäjien etujenmukaisia? Tulevaisuudessa tiedot voidaan myydä tai ne voivat päätyä esimerkiksi rikollisten hallintaan, jos valmistajan keräämät tiedot saadaan haltuun.
Äkkiseltään voisi tulla mieleen, ettei tietoja voida hyödyntää mihinkään vahingolliseen toimintaan, mutta tämä ei välttämättä pidä paikkaansa. Jo pelkästään nykyaikaisilla sensoreilla saadaan mahdottoman paljon tietoa työntekijöiden liikkeistä läsnäolo-sensoreiden avulla. Tätä tietoa voitaisiin käyttää esimerkiksi kiinteistön ryöstön yhteydessä, jos tiedetään työntekijöiden aikaisempi käyttäytyminen, voidaan ennakoida myös tulevaisuudessa sellainen aika, jolloin hälytykset eivät ole päällä, mutta työtekijät ovat jo lähteneet kotiin. Toinen keino on hyödyntää sitä työntekijöiden kotien ryöstöjä varten, jos tiedetään missä työhuoneessa työntekijä tekee töitä ja saadaan haltuun sen läsnäolosensorin tiedot, voidaan niiden avulla tehdä arvauksia, jolloin työntekijän talo on tyhjillään.
Tai jos kyseessä on henkilö, joka on esimerkiksi korkeassa asemassa yrityksessä tai valtiolla, voidaan näistä tiedoista tehdä nopeasti arvion, milloin ja missä henkilö olettavasti on minäkin päivänä.

Vielä tärkeämpi kysymys on mitä tietoja IoT järjestelmien tulisi kerätä? Jo nyt valmistajat ovat kehittäneet järjestelmiä, joissa puhelimen paikantamisella Bluetoothin avulla on mahdollista seurata ihmisten liikkumista kiinteistöjen sisällä. Onko esimerkiksi tämä niin tärkeä ominaisuus, että se tulisi sisällyttää automaatiojärjestelmään, usein pelkkä läsnäolosensorikin toimisi? Paras keino välttyä

henkilökohtaisten tietojen väärinkäytöltä on olla keräämättä niitä. Parhaimmillaan murtautujilla voisi olla reaaliaikainen tieto halutun henkilön sijainnista.
Internettiin kytkeminen myös mahdollistaa puhtaasti yritysvakoilun, jopa suurista yrityksistä google unohti mainita erään laitteen ostajille, että heidän laitteessaan on mikrofoni. Jos näitä ”unohdettuja” mikrofooneja löytyy muistakin laitteissa, ja vaikka sen valmistavalta yhtiöllä on hyvät aikeet, on silti olemassa mahdollisuus, että laite kaapataan, jolloin myös mikrofoonin tietoja voidaan käyttää hyödyksi. (Afterdawn, 2019)
Se miten näitä haavoittuvuuksia käytetään hyödyksi kannattaa pohtia, jos haavoittuvuutta käytetään näkyvästi hyödyksi esimerkiksi ohjaamalla laitteita aiheuttaen käyttäjille epämukavuuksia. Näkyvillä hyökkäyksillä saadaan ainakin kiinteistön omistaja tietoiseksi, että laitteisto on haavoittuvainen, jolloin se voidaan korjata. Jos sen sijaan haavoittuvuutta käytetään taloautomaation ohjaukseen, mutta vasta hyökkääjän haluamalla ajalla, se voi olla ”piilossa” usean viikon, kuukauden jopa usean vuoden, kunnes hyökkääjä päättää käyttää sitä. Tällöin hyökkääjällä on mahdollisuus valita mahdollisimman huono aika kiinteistön omistajille tai käyttäjille. Jos hyökkääjä on saanut useamman kiinteistön haltuun, voidaan näitä käyttää laajemmissa kohdistetuissa hyökkäyksissä. Myös haavoittuvuuksien käyttöä vakoiluun tai tietojen keräykseen on mahdollista tehdä ilman, että omistaja suoraan tätä huomaisi. Tietoturva yhtiö F-Securen mukaan 2019 Q1-Q2 aikana tietoturvahyökkäykset kasvoivat noin 300% vuoden 2018 tasosta, hyökkäyksiä oli yhteensä yli 2.9 miljardia (F-secure, 2019). Tulevaisuudessa hyökkäykset tulevat oletettavasti lisääntymään.
Osa laitteista ovat alkaneet tukemaan myös useita standardeja jo laitteissa itsessään, mikä mahdollistaa näiden kytkemisen usean eri standartin verkkoihin saumattomasti. Tämä voi myös aiheuttaa tietoturvan kautta ongelmia, mikäli laite tukee useampaa kuin yhtä standardia, tällöin laitteella on myös useamman kuin yhden standardin tietoturva-aukot. On hyvinkin mahdollista, jos laite tukee esimerkiksi neljää eri standardia, että tulevaisuudessa ainakin yhden tuki loppuu tai siitä paljastuu vakava tietoturva-aukko, jota ei kyetä enää paikkaamaan kyseisen sukupolven sirussa. Mikäli laitteen välityksellä on mahdollista päästä muiden standardien tietoliikenteeseen, aiheuttaa se todellisen riskin myös muiden laitteiden ja järjestelmän toimintaan. Jos standardit laitteissa ovat turvallisia, ettei niiden välillä liiku muuta tietoa kuin esimerkiksi kytkimen painaminen, rajoittaa se jo huomattavasti uhkaa, vaikka itse laitteen saisi toimimaan, miten ja milloin hyökkääjä haluaa.

Yleisesti pelkästään sensoripohjaisen IoT verkon yhdistäminen KNX:n on turvallisempi, kuin suoraan myös aktiivilaitteineen sekä kytkimineen yhdistetty IoT verkko. Tämäkään ei kuitenkaan poista riskiä, joka nämä hyökkäykset aiheuttavat. Esimerkkinä, jos taloautomaation ohjaus perustuisi ainoastaan IoT lämpötilasensoreiden varaan, on hyökkääjällä mahdollisuus syöttää virheellistä tietoa antureiden lukemista, ja sanoa vaikka keskellä pakkastalvea, että kiinteistön sisällä on 60 astetta lämmintä. Jolloin automaatio luonnollisesti ryhtyy viilentämään kiinteistöä jopa loputtomiin, johtaen lopulta kiinteistön jäätymiseen. Tämä olisi mahdollista ajoittaa esimerkiksi viikonlopulle, jolloin paikalla ei välttämättä olisi ketään, joka kykenisi asian huomaamaan ja ilmoittamaan siitä talohuollolle. Tämän takia mielestäni minkään automaatiojärjestelmän, joka kykenee ohjaamaan kiinteistöä ei tulisi perustua ainoastaan langattomiin IoT sensorijärjestelmään, vaan sillä tulisi olla omat luotettavat sensorit, joihin se voi verrata muualta saatuja arvoja, ja jos nämä tiedot poikkeavat merkittävästi,

tulisi laitteen antaa hälytys ja mikäli mahdollista käyttää ensisijaisesti omia sensoreitaan tai verrata arvoja jo kerättyihin historia tietoihin ja käyttää näitä arvoja.

Myös langattomien IoT laitteiden häirintä on mahdollista, ja kiinteistöautomaation näkökulmasta tulisi miettiä, miten rakennus toimii, jos IoT laitteiden välistä tiedonsiirtoa häiritään? Onko loppukäyttäjän suhteen kohtuullista, että valot ei syty, ilmanvaihto ei toimi, lämpötilaa ei voi säätää? Listaa voisi jatkaa loputtomiin, jo nyt alle 5 eurolla on mahdollista ostaa kämmenen kokoinen laite, joka kykenee häiritsemään Wi-Fi verkon toimintaa siten, ettei laitteet saa yhteyttä tukiasemaan (Nimbalkar). Tämmöisen laitteen voisi yhdistää laturiin, tai varavirtalähteeseen ja piilottaa sen kiinteistöön, jolloin IoT verkko- ja kiinteistöautomaatio voisi olla jumissa jopa useita päiviä. Muita esimerkkejä laitteiden häirinnästä on GPS signaalin häiritseminen, jolloin Yhdysvalloissa kokonainen lentokenttä jouduttiin sulkemaan useaan otteeseen (Tekniikka ja talous, 2011). Opettajien käyttämiä puhelimen häirintä laitteita, estämään oppilaiden puhelinten käytön. Suomessa viallinen langaton sääasema kykeni mykistämään ”älyavaimella” toimivan auton (Tiivi, 2019), samoin myös ”vikatilassa” toiminut kunnantalon sähköisestä äänestysjärjestelmästä esti useiden autojen keskuslukituksen toiminnan (Iltalehti, 2019). Myös murtovarkaat ovat jo alkaneet hyödyntämään langattomien murtohälyttimien häirintälaitteita (Yle, 2016). Jokaisessa tapauksessa on ollut omat syynsä signaalien häiritsemiseen, mutta silti myös ulkopuoliset ovat kärsineet näiden aiheuttamasta haitasta. Ei siis ole kohtuutonta olettaa, etteikö myös tulevaisuudessa langatonta tiedonsiirtoa tulla häiritsemään.

IOT TULEVAISUUS

Tällä hetkellä eri langattomat IoT ratkaisut ovat vieläkin hyvin kehittyvässä tilassa, jossa uusia ominaisuuksia tuodaan eri ratkaisuihin melkein kiihtyvään tahtiin. Huomattavaa kuitenkin on, että järjestelmät ovat alkaneet kehittymään hyvin samaan suuntaan, jolloin eroavaisuudet eri järjestelmien välillä ovat alkaneet kaveta merkittävästi. Suurin muutos viimevuosina, on ollut langattomien verkkojen IP-osoitteellisuus. Aikaisemmin vain Thread tuki IPV6 verkkoa, mutta Z-wave, Zigbee sekä Bluetooth ovat tuoneet viimeisten 5 vuoden aikana myös osittaisen IP-tuen standardeihin.
IP-tuen myötä kaikkien järjestelmien laitteet voivat teoriassa kommunikoida paikallisen lähiverkon kautta myös toistensa kanssa, jolloin standardien välillä ei välttämättä tarvitsisi tehdä valintaa vaan valinnan voisi tehdä laitteiden ominaisuuksien perusteella. Tähän kuitenkin on vielä matkaa, sillä vaikka IP-tuki on nyt olemassa, jokaisessa standardissa on vielä omatapansa mitä, ja missä muodossa tietoa välitetään. Tulevaisuudessa alkaakin seuraava ”kisa”, jossa jokainen laitevalmistaja luo omantapansa välittää näitä tietoja, jolloin eri standardien laitteiden välillä tarvittaisiin jokin laite, jotta ne voisivat kommunikoida keskenään. Zigbee on luonut oman kirjastonsa, johon muut laitevalmistajat pääsevät Dotdot:n kautta, Z-wave on julkaissut oman kirjastonsa myös muiden käytettäväksi, Bluetooth SIG on kehittämässä omaa kirjastoaan ja myös OCF (Open Connectivity Foundation) sekä AllSeen allianssi yhdistyivät OCF nimen alle ja alkoivat kehittää omaa kirjastoaan.

OCF:ssä on mukana tällöin suurista yrityksistä Intel, Microsoft, Qualcomm, Samsung sekä Cisco systems, kun taas Zigbeellä ja DotDot:lla on Amazon, Huawei, NXP, Schneider electric, Texas Instruments ja Silicon labs. Myös Google on kehittämässä omaa kirjastoaan (Waeve, Android things). Se, että mitkä tai mikä näistä ohjelmakirjastoista tulee olemaan suurin tulevaisuudessa, jää nähtäväksi.

Myös standardien omien laitteiden yhteen sopivuudessa tulee tulevaisuudessakin luultavasti olemaan ongelmia. Tällä hetkellä, useat standartit mainostavat ”yhteensopivuutta” vanhempien laitteiden kanssa, mikä on osittain totta, mutta vain niiltä ominaisuuksilta, joita vanhemmat laitteet tukevat. Esimerkiksi Z-wave on yhteensopiva vanhojen laitteiden kanssa, ongelmat tulevat siinä vaiheessa, kun uusia ominaisuuksia aletaan ottaa käyttöön. Jos Z-wave verkon halutaan käyttävän suojattua yhteyttä, täytyy laitteiden tukea Z-wave Securea, mikäli näin ei ole, ei laite voi toimia kyseisessä verkossa tai verkon muut laitteet eivät voi käyttää suojattua yhteyttä. Tästä voi tulla tulevaisuudessa ongelmia, mikäli vanhempien laitteiden tietoturvaa ei voida päivittää, vaan tarvitaan kokonaan uuden sukupolven siru, joka tukee uudempaa salausta. Tällöin laitteistoiden omistajien on tehtävä valinta joko päivittää kaikki laitteet tukemaan uudempaa salausta, tai jättää laitteistot päivittämättä ja toivoa, ettei vanhempaa salausta murreta tai käytetä hyödyksi. Mikäli laitteet päivitetään esimerkiksi 5, 10 tai 20 vuoden välein tuottaa myös suuren määrän elektroniikkaromua, mikä ei välttämättä ole eettisesti kestävää, vaikka laitteet itsestään eivät maksaisi rahallisesti suuria summia. Yhteensopivuus tulee olemaan yksi merkittävimmistä kysymyksistä tulevaisuudessa.

Zigbeen DotDot on kenties ensimmäinen standardi, joka pyrkii jakamaan omaa kirjastoaan muiden käytettäväksi, jolloin lopulta DotDot laitteet voisivat käyttää mitä tahansa langatonta tai langallista standardia, mutta standardista riippumatta laitteet kykenisivät kommunikoimaan keskenään. Täsmälleen sama idea siis mitä KNX yrittää luoda, DotDot oli ensimmäisiä kieliä, joka julkaistiin toiselle standardille, eli Thread:lle. Tällöin Thread laite voi saada sekä Thread että DotDot sertifioinnin, ja täten toimia Zigbee laitteiden kanssa. Myös KNX on valinnut Thread:n omaksi langattomaksi kumppanuus standardiksi, joten luultavasti muutaman vuoden päästä myös KNX laite voi myös toimia Thread standardin päällä. Tällä tavoin, myös langattomille KNX laitteille, jotka toimivat joko Thread tai Wi-Fi verkossa, olisi mahdollista tukea sekä KNX Data turvaa, että KNX IP turvaa. Tällöin KNX viestit siirtyisivät teoriassa täysin salattuina laitteiden välillä. Ongelmaksi voi lopulta muodostua hinnannousu, sillä useamman standardin tuki vaatii myös jokaisen standardin sertifioinnin. Yhteinen ohjelmointikieli mahdollistaisi laitteiden paremman yhteistoiminnan, sekä mahdollisesti paikallisen tietojen käsittelyn ja säilytyksen. Laitevalmistajat, keskitin-ratkaisut ja käyttäjien suosio lopulta ratkaisevat mihin suuntaan ala lähtee kehittymään.

6 YHTEENVETO

Opinnäytetyön tavoitteena oli selvittää KNX sekä tulevaisuuden IoT maailman yhteensovittamista. Työssä käytiin lävitse muutamia langattomia IoT standardeja sekä niiden haasteita, sekä KNX tulevaisuuden suunnitelmista IoT järjestelmien suhteen. Varsinaisena työnä rakennettiin myös demolaitteisto, joka mahdollistaa KNX ja yhden IoT laitteiston välisen yhteistoiminnan.

Työntuloksena saatiin toimiva demolaitteisto sekä tämänhetkiset tiedot KNX sekä IoT kehitys suunnista. Työnavulla voidaan myös seurata järjestelmien kehitystä, kunnes kenties lähitulevaisuudessa markkinoille ilmestyy toimivia ratkaisuja molempien järjestelmien suhteen.

Työssä eniten selvitystä aiheutti standardien jatkuva kehittyminen sekä myös KNX omat tulevaisuuden suunnitelmat. Tuoreiden tietojen löytäminen oli suhteellisen hankalaa, sillä standardit toivat jatkuvalla tahdilla uusia versioita sekä kilpailu langattomissa automaatiojärjestelmissä oli kova. Tämä tarkoitti, että monissa tietolähteissä oli jo vanhentunutta tietoa, vaikka se oli parhaimmillaan julkaistu vain vuosi takaperin. Kilpailu myös tarkoitti, että kaikki standardit ”kopioivat” toistensa ominaisuuksia, jolloin myös niiden vertailu hankaloitui. Myös standardien välinen sovellustason kilpailu, aiheutti hämmennystä, lähes jokainen langattoman standardeista, joilla on valmis sovelluskerros, on avannut lähdekoodinsa. Tällä ilmeisesti koitetaan houkutella kehittäjiä alustalle, sekä yritetään siirtää heidän sovelluskerroksensa toimimaan muiden standardien päällä. Taustalla pyörivät suuret teknologia yritykset myös tuntuvat muodostavan omat sisäpiirinsä lähes jokaisen standardin ympärille. Jolloin eri standardien laitteiden välinen viestien välittäminen ei välttämättä ole ollut heidän kärkihankkeitansa.
Koska ala kehittyy hyvin nopeaan tahtiin, jäi myös osa alkuperäisestä suunnitelmasta toteutumatta. Myös oma työtilanne hankaloitti työn aloittamista, jolloin työ lopullisesti valmistui vasta vuonna 2020

Työ itsessään oli hyvin mielenkiintoinen, etenkin kun työhön lähdettäessä ei oikeastaan ollut tiedossa millä tavoin KNX lähtee toteuttamaan KNX IoT ratkaisuaan. Työn edetessä saatiin myös KNX suhteen lisää tietoa heidän suunnitelmistaan, sekä muiden standardien suhteen. Toisaalta ajoitus työnaloittamiseen ei välttämättä ollut optimaalinen, sillä uskon, että aivan lähitulevaisuudessa KNX ja IoT laitteet voivat puhua suoraan keskenään. Tällä tavoin kuitenkin saatiin hyvät pohjatiedot uusista standardeista, jolloin tulevaisuudessa voidaan seurata tarkemmin näiden kehittymistä.

7 LIITTEET

LIITE1

Funktio muunnos JavaScript objektista RealKNX:n vaatimaan muotoon.

```
var msg0 = {payload: 0};
var msg1 = {payload: 1};
var click = msg.payload.click;

var clickMsg ={payload: click};

if (click =="left") {
    return msg0;
}
else {
    return msg1;
}
```

LIITE2

Funktio muunnos JavaScript objektista zigbee2mqtt:n vaatimaan json muotoon.

```
var msg0 = {payload: {"state":"off"}};
var msg1 = {payload: {"state":"on"}};
var click = msg.payload.click;

var clickMsg ={payload: click};

if (click =="left") {
    return msg0;
}
else {
    return msg1;
}
```

LIITE3

Funktio muunnos realknx laitteesta json muotoon.

```
var msg0 = {payload: {"state":"off"}};
var msg1 = {payload: {"state":"on"}};
var click = msg.payload;

var clickMsg ={payload: click};

if (click === 0) {
    return msg0;
}
else {
    return msg1;
}
```

LIITE4

Funktio muunnos MQTT:stä MySQL tietokantaan.

```
var out = "INSERT INTO sensorit (timestamp,topic,data)"
out = out + "Value ('" + new Date().toISOString() + "','"
out = out + msg.topic + "','" + msg.payload + "');"
msg.topic=out;
return msg;
```

LIITE5
Vuo KNX ja Zigbeen väliseen ohjaukseen


```
[
   {
      "id": "6c4c3fc.2467ac",
      "type": "mqtt in",
      "z": "8412925d.906ff8",
      "name": "",
      "topic": "zigbee2mqtt/seinakytkin",
      "qos": "2",
      "broker": "15898881.428d7f",
      "x": 194.49998474121094,
      "y": 233.40000915527344,
      "wires": [
         [
            "7df348c9.71d5e8",
            "85f4c9d4.66cdf"
         ]
      ]
   },
   {
      "id": "7df348c9.71d5e8",
      "type": "debug",
      "z": "8412925d.906ff8",
      "name": "",
      "active": false,
      "console": "false",
      "complete": "false",
      "x": 391.49998474121094,
      "y": 166.39999389648438,
      "wires": []
   },
   {
      "id": "85f4c9d4.66cdf",
      "type": "json",
      "z": "8412925d.906ff8",
      "name": "",
      "pretty": false,
      "x": 416.49998474121094,
      "y": 312.40000915527344,
      "wires": [
         [
```

```
            "3b1b8a48.e18b1e",
            "46dca799.b26f6",
            "581b61c3.7aa0e8"
        ]
    ]
},
{
    "id": "3b1b8a48.e18b1e",
    "type": "debug",
    "z": "8412925d.906ff8",
    "name": "",
    "active": false,
    "console": "false",
    "complete": "false",
    "x": 556.5,
    "y": 365.20001220703125,
    "wires": []
},
{
    "id": "46dca799.b26f6",
    "type": "function",
    "z": "8412925d.906ff8",
    "name": "Kytkin",
    "func": "var msg0 = {payload: {\"state\":\"off\"}};\nvar msg1 = {payload: {\"state\":\"on\"}};\nvar click = msg.payload.click; \n\nvar clickMsg ={payload: click};\n\nif (click ==\"left\") {\n    return msg0;\n}\nelse {\n return msg1;\n}\n",
    "outputs": 1,
    "noerr": 0,
    "x": 609.5,
    "y": 320.4000244140625,
    "wires": [
        [
            "4a5301a6.e6fdf"
        ]
    ]
},
{
    "id": "4a5301a6.e6fdf",
    "type": "mqtt out",
    "z": "8412925d.906ff8",
    "name": "",
    "topic": "zigbee2mqtt/rgb/set",
```

```
        "qos": "",
        "retain": "",
        "broker": "15898881.428d7f",
        "x": 890.5,
        "y": 316.4000244140625,
        "wires": []
    },
    {
        "id": "x00x0xxx.00000",
        "type": "realknx-in",
        "z": "8412925d.906ff8",
        "name": "",
        "controller": "x0x0xxx.x00000",
        "itemname": "Meeting room - Lights",
        "passthru": false,
        "booleanoutput": false,
        "outputatstartup": true,
        "x": 441.49998474121094,
        "y": 517.7999725341797,
        "wires": [
            [
                "b1d3030a.85e478",
                "cdfef410.fc3f68"
            ]
        ]
    },
    {
        "id": "b1d3030a.85e478",
        "type": "function",
        "z": "8412925d.906ff8",
        "name": "",
        "func": "var msg0 = {payload: {\"state\":\"off\"}};\nvar msg1 = {payload: {\"state\":\"on\"}};\nvar click =
msg.payload; \n\nvar clickMsg ={payload: click};\n\nif (click === 0) {\n    return msg0;\n}\nelse {\n    return
msg1;\n}\n",
        "outputs": 1,
        "noerr": 0,
        "x": 640.4999847412109,
        "y": 493.40000915527344,
        "wires": [
            [
                "4a5301a6.e6fdf"
            ]
```

```
        ]
    },
    {
        "id": "cdfef410.fc3f68",
        "type": "debug",
        "z": "8412925d.906ff8",
        "name": "",
        "active": true,
        "console": "false",
        "complete": "false",
        "x": 675.4999847412109,
        "y": 563.4000091552734,
        "wires": []
    },
    {
        "id": "x00x0xxx.00000",
        "type": "realknx-out",
        "z": "8412925d.906ff8",
        "name": "",
        "controller": "x0x0xxx.x00000",
        "itemname": "sihteeri - valot",
        "topic": "",
        "payload": "",
        "booleaninput": true,
        "skipfirst": true,
        "x": 802.4999847412109,
        "y": 163.8000030517578,
        "wires": []
    },
    {
        "id": "581b61c3.7aa0e8",
        "type": "function",
        "z": "8412925d.906ff8",
        "name": "",
        "func": "var msg0 = {payload: 0};\nvar msg1 = {payload: 1};\nvar click = msg.payload.click; \n\nvar
clickMsg ={payload: click};\n\nif (click ==\"left\") {\n    return msg0;\n}\nelse {\n    return msg1;\n}",
        "outputs": 1,
        "noerr": 0,
        "x": 555.4999847412109,
        "y": 236.1999969482422,
        "wires": [
            [
```

```
            "3833f558.8a9bc2"
          ]
        ]
    },
    {
        "id": "15898881.428d7f",
        "type": "mqtt-broker",
        "z": "",
        "broker": "00.00.00.00/00",
        "port": "1883",
        "clientid": "",
        "usetls": false,
        "compatmode": true,
        "keepalive": "60",
        "cleansession": true,
        "willTopic": "",
        "willQos": "0",
        "willPayload": "",
        "birthTopic": "",
        "birthQos": "0",
        "birthPayload": ""
    },
    {
        "id": "x00x0xxx.00000",
        "type": "realknx-controller",
        "z": "",
        "name": "realknx-ctrl",
        "host": "localhost",
        "port": "3000"
    }
]
```


LIITE6

Vuo MQTT viestien välitys tietokantaan

[{"id":"aa1c8d4a.183e3","type":"mqtt in","z":"50f782ae.dae37c","name":"","topic":"zigbee2mqtt/#","qos":"2","broker":"20b109b5.f71246","x":129,"y":165,"wires":[["68aa5cc9.8b9a04"]]},{"id":"68aa5cc9.8b9a04","type":"function","z":"50f782ae.dae37c","name":"Create query in topic","func":"var out = \"INSERT INTO sensorit (timestamp,topic,data)\"\nout = out + \"Value ('\" + new Date().toISOString() + \"','\" \nout = out + msg.topic + \"','\" + msg.payload + \"');\"\n \nmsg.topic=out;\n\nreturn msg;","outputs":1,"noerr":0,"x":474,"y":298,"wires":[["ef675d19.7c7e8"]]},{"id":"5b3f8017.96966","type":"debug","z":"50f782ae.dae37c","name":"","ac-

tive":true,"tosidebar":true,"console":false,"complete":"false","x":956,"y":323,"wires":[]},{"id":"ef675d19.7c7e8","type":"mysql","z":"50f782ae.dae37c","mydb":"d77e349d.e420f8","name":"","x":727,"y":316,"wires":[["5b3f8017.96966"]]},{"id":"88c5c7ed.f994f8","type":"mysql","z":"50f782ae.dae37c","mydb":"7ec20e54.ad8fe","name":"","x":800,"y":560,"wires":[[]]},{"id":"5247e393.38be8c","type":"mqtt in","z":"50f782ae.dae37c","name":"lämpötila","topic":"zigbee2mqtt/lampotila","qos":"2","broker":"20b109b5.f71246","x":160,"y":580,"wires":[["414016f1.9ec568"]]},{"id":"414016f1.9ec568","type":"function","z":"50f782ae.dae37c","name":"Create query in topic","func":"var out = \"INSERT INTO lampotila_anturi (timestamp,topic,data)\"\nout = out + \"Value ('\" + new Date().toISOString() + \"','\" \nout = out + msg.topic + \"','\" + msg.payload + \"');\"\n   \nmsg.topic=out;\n\nreturn msg;","outputs":1,"noerr":0,"x":440,"y":580,"wires":[["88c5c7ed.f994f8"]]},{"id":"20b109b5.f71246","type":"mqtt-broker","z":"","name":"Zigbee silta","broker":"localhost","port":"1883","clientid":"","usetls":false,"compatmode":true,"keepalive":"60","cleansession":true,"birthTopic":"","birthQos":"0","birthPayload":"","closeTopic":"","closeQos":"0","closePayload":"","willTopic":"","willQos":"0","willPayload":""},{"id":"d77e349d.e420f8","type":"MySQLdatabase","z":"","host":"127.0.0.1","port":"3306","db":"sensorit","tz":""},{"id":"7ec20e54.ad8fe","type":"MySQLdatabase","z":"","host":"127.0.0.1","port":"3306","db":"lampotila","tz":""}]

LIITE7

Vuo MQTT viestien välityksestä Azureen

[{"id":"d23c5e8.1202fa","type":"function","z":"8097a4bd.a995e8","name":"Function","func":"msg1 = '{\"deviceId\": \"laite1\", '\nmsg1 = msg1 + '\"key\": \"xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx=\", ' \nmsg1 = msg1 + '\"protocol\": \"http\", '\nmsg1 = msg1 + '\"data\": { \"' + msg.topic + '\": \"' + msg.payload + '\"}}'\n\nnewMsg = { payload: msg1 };\nreturn newMsg;\n","outputs":1,"noerr":0,"x":740,"y":460,"wires":[["e543efab.79a64","a67ecd91.ab41"]]},{"id":"fcb62a0a.a64b98","type":"mqtt in","z":"8097a4bd.a995e8","name":"","topic":"zigbee2mqtt/seinakytkin","qos":"2","broker":"20b109b5.f71246","x":232,"y":534,"wires":[["45d957f0.a283f8"]]},{"id":"45d957f0.a283f8","type":"json","z":"8097a4bd.a995e8","name":"","property":"payload","action":"","pretty":false,"x":286,"y":468,"wires":[["745946e6.248b38"]]},{"id":"a67ecd91.ab41","type":"debug","z":"8097a4bd.a995e8","name":"","active":false,"tosidebar":true,"console":false,"tostatus":false,"complete":"payload","x":1070,"y":560,"wires":[]},{"id":"41f7bde9.1d8b14","type":"debug","z":"8097a4bd.a995e8","name":"Log","active":false,"console":"false","complete":"true","x":970,"y":720,"wires":[]},{"id":"e543efab.79a64","type":"azureiothub","z":"8097a4bd.a995e8","name":"Azure IoT Hub","protocol":"http","x":780,"y":700,"wires":[["41f7bde9.1d8b14"]]},{"id":"d6683a9b.37ca98","type":"azureiothubreceiver","z":"8097a4bd.a995e8","name":"Azure IoT Hub Receiver","x":880,"y":620,"wires":[["a67ecd91.ab41"]]},{"id":"745946e6.248b38","type":"function","z":"8097a4bd.a995e8","name":"","func":"var click = msg.payload.click;\nvar clickMsg ={payload: click};\n\nmsg.topic = \"click\"\nmsg0 = click ;\nnewMsg = { payload: msg0};\nreturn newMsg \n\n","out-

puts":1,"noerr":0,"x":450,"y":460,"wires":[["ada1228e.88b54"]]},{"id":"ada1228e.88b54","type":"function","z":"8097a4bd.a995e8","name":"","func":"msg.topic = \"Lampotila\"\nreturn msg;\n","outputs":1,"noerr":0,"x":570,"y":460,"wires":[["d23c5e8.1202fa"]]},{"id":"eba71dc7.8c487","type":"mqtt in","z":"8097a4bd.a995e8","name":"","topic":"zigbee2mqtt/lampotila","qos":"2","broker":"20b109b5.f71246","x":220,"y":280,"wires":[["3ea83d01.1c7322"]]},{"id":"3ea83d01.1c7322","type":"json","z":"8097a4bd.a995e8","name":"","property":"payload","action":"","pretty":false,"x":450,"y":280,"wires":[["d2ba2bba.a77d38","9fc685.e9c57978","f41bbd3.9ae3b4"]]},{"id":"d2ba2bba.a77d38","type":"function","z":"8097a4bd.a995e8","name":"","func":"var temperature = msg.payload.temperature;\nvar temperatureMsg ={payload: temperature};\n\nmsg.topic = \"temperature\"\nmsg0 = temperature ;\nnewMsg = { payload: msg0};\nreturn newMsg \n\n","outputs":1,"noerr":0,"x":610,"y":280,"wires":[["e310521e.2154e"]]},{"id":"e310521e.2154e","type":"function","z":"8097a4bd.a995e8","name":"","func":"msg.topic = \"Lampotila\"\nreturn msg;\n","outputs":1,"noerr":0,"x":730,"y":280,"wires":[["5730b85f.daae48"]]},{"id":"9fc685.e9c57978","type":"function","z":"8097a4bd.a995e8","name":"","func":"var humidity = msg.payload.humidity;\nvar humidityMsg ={payload: humidity};\n\nmsg.topic = \"humidity\"\nmsg0 = humidity ;\nnewMsg = { payload: msg0};\nreturn newMsg \n\n","outputs":1,"noerr":0,"x":610,"y":240,"wires":[["e68b1cdb.7126"]]},{"id":"e68b1cdb.7126","type":"function","z":"8097a4bd.a995e8","name":"","func":"msg.topic = \"Lampotila/kosteus\"\nreturn msg;\n","outputs":1,"noerr":0,"x":730,"y":240,"wires":[["5730b85f.daae48"]]},{"id":"f41bbd3.9ae3b4","type":"function","z":"8097a4bd.a995e8","name":"","func":"var pressure = msg.payload.pressure;\nvar pressureMsg ={payload: pressure};\n\nmsg.topic = \"pressure\"\nmsg0 = pressure ;\nnewMsg = { payload: msg0};\nreturn newMsg \n\n","outputs":1,"noerr":0,"x":610,"y":200,"wires":[["5d0ad56a.23022c"]]},{"id":"5d0ad56a.23022c","type":"function","z":"8097a4bd.a995e8","name":"","func":"msg.topic = \"Lämpotila/Paine\"\nreturn msg;\n","outputs":1,"noerr":0,"x":730,"y":200,"wires":[["5730b85f.daae48"]]},{"id":"5730b85f.daae48","type":"function","z":"8097a4bd.a995e8","name":"Function","func":"msg1 = '{\"deviceId\": \"laite1\", '\nmsg1 = msg1 + '\"key\": \" xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx", ' \nmsg1 = msg1 + '\"protocol\": \"http\", '\nmsg1 = msg1 + '\"data\": { \"' + msg.topic + '\": \"' + msg.payload + '\"}}'\n\nnewMsg = { payload: msg1 };\nreturn newMsg;\n","outputs":1,"noerr":0,"x":900,"y":240,"wires":[["e543efab.79a64"]]},{"id":"dd73eddd.d80c4","type":"json","z":"8097a4bd.a995e8","name":"","property":"payload","action":"","pretty":false,"x":430,"y":140,"wires":[["33ad1ffe.b4dfa"]]},{"id":"33ad1ffe.b4dfa","type":"function","z":"8097a4bd.a995e8","name":"","func":"var contact = msg.payload.contact;\nvar contactMsg ={payload: contact};\n\nmsg.topic = \"contact\"\nmsg0 = contact ;\nnewMsg = { payload: msg0};\nreturn newMsg \n\n","outputs":1,"noerr":0,"x":610,"y":140,"wires":[["f200b039.ca6a4"]]},{"id":"f200b039.ca6a4","type":"function","z":"8097a4bd.a995e8","name":"","func":"msg.topic = \"Ovikytkin\"\nreturn msg;\n","outputs":1,"noerr":0,"x":730,"y":140,"wires":[["5730b85f.daae48"]]},{"id":"1dfe21b9.89defe","type":"mqtt in","z":"8097a4bd.a995e8","name":"","topic":"zigbee2mqtt/ovikytkin","qos":"2","broker":"20b109b5.f71246","x":220,"y":140,"wires":[["dd73eddd.d80c4"]]},{"id":"b90d3ef0.949cb","type":"json","z":"8097a4bd.a995e8","name":"","pro-

perty":"payload","action":"","pretty":false,"x":430,"y":80,"wi-
res":[["1d578f29.ffe361"]]},{"id":"1d578f29.ffe361","type":"func-
tion","z":"8097a4bd.a995e8","name":"","func":"var water_leak = msg.payload.water_leak;\nvar water_leakMsg
={payload: water_leak};\n\nmsg.topic = \"water_leak\"\nmsg0 = water_leak ;\nnewMsg = { payload:
msg0};\nreturn newMsg \n\n","outputs":1,"noerr":0,"x":610,"y":80,"wi-
res":[["e4274a.7ca548b8"]]},{"id":"e4274a.7ca548b8","type":"func-
tion","z":"8097a4bd.a995e8","name":"","func":"msg.topic = \"Vesivuoto\"\nreturn msg;\n","out-
puts":1,"noerr":0,"x":730,"y":80,"wires":[["5730b85f.daae48"]]},{"id":"d1e27bd2.5c3c08","type":"mqtt
in","z":"8097a4bd.a995e8","name":"","topic":"zigbee2mqtt/vesivuoto","qos":"2","bro-
ker":"20b109b5.f71246","x":220,"y":80,"wires":[["b90d3ef0.949cb"]]},{"id":"20b109b5.f71246","type":"mqtt-bro-
ker","z":"","name":"Zigbee silta","broker":"localhost","port":"1883","clientid":"","usetls":false,"compat-
mode":true,"keepalive":"60","cleansession":true,"birthTopic":"","birthQos":"0","birthPayload":"","closeTo-
pic":"","closeQos":"0","closePayload":"","willTopic":"","willQos":"0","willPayload":""}]

8 LÄHDELUETTELO

1sheeld. (ei pvm). *1sheeld.com*. Haettu 5. 3 2019 osoitteesta https://1sheeld.com/mqtt-protocol/

Afterdawn. (20. 2 2019). *Afterdawn.com*. Haettu 9. 4 2019 osoitteesta https://fin.afterdawn.com/uutiset/artikkeli.cfm/2019/02/20/google-asensi-piilotetun-mikrofonin-koteihin-myytavaan-laitteeseensa-vahingossa-sanoo-google

Azoidou, E. (2016). *Battery Lifetime Modelling and.* STOCKHOLM, SWEDEN 2016: KTH ROYAL INSTITUTE OF TECHNOLOGY.

Bluetooth SIG. (ei pvm). *Bluetooth.com*. Haettu 20. 10 2019 osoitteesta https://www.bluetooth.com/about-us/our-history/

Bluetooth SIG. (2019). *bluetooth.com.* Haettu 10. 11 2019 osoitteesta https://www.bluetooth.com/bluetooth-technology/topology-options/?_ga=2.11470006.38027037.1552301585-1568948671.1552301585

Brown, A. (2009). *Human resource management lessons.* Kuopio: Savonia-ammattikorkeakoulu. Liiketalouden yksikkö. Lokakuu 2009. Luento.

Dr Richard Rudd (Aegis), D. K. (2014). *Building Materials and.* Ofcom.

European Commission. (11. 10 2018). *European Commission*. Haettu 10. 10 2019 osoitteesta https://ec.europa.eu/digital-single-market/en/news/commission-harmonises-radio-spectrum-support-internet-things

F-secure. (9 2019). *F-secure.com.* Haettu 10. 10 2019 osoitteesta https://s3-eu-central-1.amazonaws.com/evermade-fsecure-assets/wp-content/uploads/2019/09/12093807/2019_attack_landscape_report.pdf

Härkönen, K. (2015). *KNX-järjestelmän perusteet.* Sähkötieto ry.

Hakala, J. T. (2004). *Opinnäyteopas ammattikorkeakouluille.* Helsinki: Gaudeamus.

Hintikka, K. A. (2009). *Twitter pikaviestii suuria uutisia*. Haettu 14. 9 2009 osoitteesta Helsingin Sanomat: http://www.hs.fi/arkisto/artikkeli/HS20090804SI1AT017cv

HiveMQ. (12. 1 2015). *Hivemq.com*. Noudettu osoitteesta https://www.hivemq.com/blog/mqtt-essentials-part-1-introducing-mqtt/

IETF. (2014). *ieft.org*. Haettu 10. 10 2019 osoitteesta https://tools.ietf.org/html/rfc7252

Iltalehti. (9. 8 2019). *iltalehti.fi*. Haettu 10. 10 2019 osoitteesta https://www.iltalehti.fi/kotimaa/a/e9c58ddc-1cdd-4ed3-8166-dad2806ceb7f

ITU. (ei pvm). *https://www.itu.int/net/ITU-R/terrestrial/faq/index.html*. Haettu 20. 4 2019 osoitteesta ITU (International Telecommunication Union).

ITU. (13. 1 2015). *itu.int*. Haettu 10. 2 2019 osoitteesta https://www.itu.int/rec/T-REC-G.9959-201501-I/en

ITU, International Telecommunication Union. (ei pvm). *ITU*. Haettu 15. 3 2019 osoitteesta https://www.itu.int/rec/T-REC-Y.2060-201206-I

Järvinen, P. (2007). *Ammattina esimies.* Haettu 23. 5 2008 osoitteesta http://www.wsoypro.fi/wsoypro.aspx?navi=Omat-sisallot&section=books

Jaatinen, P. (2004). *Miltä SAMKin opinnäytetyöt näyttävät toisin silmin? Satakunnan ammattikorkeakoulun vuoden 2002 opinnäytetöiden arvioinnista tehty tutkimus.* Pori: Satakunnan ammattikorkeakoulu.

Kananen, J. (2010). *Opinnäytetyön kirjoittamisen käytännön opas.* Jyväskylä: Jyväskylän ammattikorkeakoulu, liiketoiminta ja palvelut -yksikkö. Jyväskylän ammattikorkeakoulun julkaisuja 111.

KNX Association. (2013). *Knx uk*. Haettu 8. 3 2019 osoitteesta https://knxuk.org/images/pdf/A_History_of_KNX.pdf

KNX Association. (ei pvm). *KNX.fi.* Haettu 10. 10 2019 osoitteesta http://knx.fi/doc/esitteet/KNX_esineiden_internetissa.pdf

KNX Association. (1. 2 2016). *KNX.it KNX IoT Road map.* Haettu 10. 10 2019 osoitteesta http://www.knx.it/download/DOCUMENTAZIONE_KNX/04_M.Pandolfi_-_KNX-IoT.pdf

limitedresults. (23. 1 2019). *limitedresults.com*. Haettu 7. 3 2019 osoitteesta https://limitedresults.com/2019/01/pwn-the-lifx-mini-white/

LoRa Alliance. (2015). *lora-alliance.com.* Noudettu osoitteesta https://lora-alliance.org/sites/default/files/2019-05/lorawan_security_whitepaper.pdf

LoRA-Alliance. (2015). *lora-alliance.org.* Noudettu osoitteesta https://lora-alliance.org/sites/default/files/2018-04/what-is-lorawan.pdf

Mölsä, H. (2005). *Verkko-opetuksen käyttöönottoon vaikuttavia tekijöitä*. (Helsingin yliopisto. Viestinnän laitos. Pro gradu -tutkielma) Haettu 20. 11 2005 osoitteesta http://ethesis.helsinki.fi/julkaisut/val/viest/pg/molsa/verkkoop.pdf

Microsoft. (ei pvm). *Microsoft.com*. Haettu 10. 10 2019 osoitteesta https://docs.microsoft.com/en-us/azure/service-bus-messaging/service-bus-amqp-overview

Nimbalkar, K. (ei pvm). *instructables.com*. Haettu 18. 4 2019 osoitteesta https://www.instructables.com/id/DIY-Wifi-Jammer-With-ESP8266-and-Mobile-App/

OASIS. (2014). *oasis-open.org.* Haettu 2. 3 2019 osoitteesta https://www.oasis-open.org/news/announcements/mqtt-version-3-1-1-becomes-an-oasis-standard

Ojala, R. (2017). *MQTT IoT-protokolla.* JAMK.

pbworks. (ei pvm). *pbworks.com*. Haettu 27. 4 2019 osoitteesta http://zigbee.pbworks.com

Pylsy, A. (2010). *Tuotemallisto nostalgian inspiroimana.* Kuopio: Savonia-ammattikorkeakoulu.

Pynnä, S. (3. 8 2009). Satakunnan ammattikorkeakoulun henkilöstön kehittämispäivät 21.8.2009 klo 9.00-16.00 [sähköpostiviesti]. *Vastaanottaja Pirkko Tenkama*.

Silicon Labs. (ei pvm). *silabs.com.* Haettu 20. 6 2019 osoitteesta https://www.silabs.com/documents/public/user-guides/ug103-15-green-power-fundamentals.pdf

Silicon Labs. (ei pvm). *silabs.com*. Haettu 10. 2 2019 osoitteesta https://www.silabs.com/products/wireless/mesh-networking/z-wave/specification/faq#one

Silicon Labs. (ei pvm). *silabs.com.* Haettu 10. 10 2019 osoitteesta https://www.silabs.com/documents/public/application-notes/an1142-mesh-network-performance-comparison.pdf

Suhonen, P.;& Tenkama, P. (2010). *Raportointiohjeet.* Kuopio: Savonia-ammattikorkeakoulu.

Tekniikka ja talous. (3. 13 2011). *tekniikkatalous.fi*. Haettu 2. 5 2019 osoitteesta https://www.tekniikkatalous.fi/uutiset/varoitus-nettikaupan-gps-hairintalaite-voi-rampauttaa-kokonaisen-lentokentan/6f2b7598-3e9e-3ad9-b4cc-e75b2eab27e7

The Verge. (3. 10 2016). *theverge.com*. Haettu 19. 4 2019 osoitteesta https://www.theverge.com/2016/11/3/13507126/iot-drone-hack

Thread Group. (ei pvm). *Thread Group.* Haettu 20. 10 2019 osoitteesta https://www.threadgroup.org/What-is-Thread/Developers

Thread Group. (13. 6 2015). *Threadgroup.com.* Haettu 10. 10 2019 osoitteesta https://www.threadgroup.org/Portals/0/documents/support/BatteryOperatedDevicesWhitePaper_656_2.pdf

TI. (2017). *Ti.com.* Haettu 10. 10 2019 osoitteesta http://www.ti.com/lit/wp/swry010a/swry010a.pdf

Tiivi. (4. 2 2019). *Tiivi.fi*. Haettu 4. 5 2019 osoitteesta https://www.tivi.fi/uutiset/nain-selvisi-autojen-kaynnistysongelma-suomessa-isannoitsija-oli-kylla-mysteeri/e2b19b2a-470b-3c6f-a6e9-117783de4a2a

Ulrich, D. (2007). *Henkilöstöjohtamisella huipulle.* Helsinki: Talentum.

Westcott, C. &. (2002). *Certified Wireless Network Administrator Official Study Guide.* Planet3 Wireless, Inc.

Vidgren, M. (1. 3. 2012a). Ohjeet kypsysnäytteen tarkistamiseen. *Savonian radio*. Kuopio: Savonia-ammattikorkeakoulu.

Vidgren, M. (1. 3 2012b). OIS-ONT käytännössä. *Savonian uutiset.* Yle. Ykkönen, Kuopio.

Wi-fi Alliance. (ei pvm). *wi-fi.org*. Haettu 5. 4 2019 osoitteesta https://www.wi-fi.org/who-we-are/history

Wi-Fi alliance. (ei pvm). *wi-fi.org*. Haettu 10. 10 2019 osoitteesta https://www.wi-fi.org/file/wi-fi-certified-6-highlights

Wikipedia. (ei pvm). *wikipedia.org.* Haettu 10. 10 2019 osoitteesta https://en.wikipedia.org/wiki/Advanced_Message_Queuing_Protocol

Wikipedia. (ei pvm). *wikipedia.org*. Haettu 10. 4 2019 osoitteesta https://en.wikipedia.org/wiki/IEEE_802.11

Yle. (23. 9 2016). *yle.fi*. Haettu 20. 9 2019 osoitteesta https://yle.fi/uutiset/3-9185771

Zigbee alliance. (ei pvm). *zigbee.org.* Haettu 10. 10 2019 osoitteesta https://zigbee.org/zigbee-for-developers/zigbee-3-0/ Zigbee: Securing the Wireless IoT

Zigbee alliance. (ei pvm). *Zigbee.org*. Haettu 20. 6 2019 osoitteesta https://zigbee.org/zigbee-for-developers/zigbee-3-0/

Zigbee Alliance. (2017). *zigbee.org.* Haettu 10. 10 2019 osoitteesta https://zigbee.org/zigbee-for-developers/zigbee-3-0/# Zigbee Green Power White paper