Timo Peltonen

IoT ja M2M

Langattomat, lyhyen kantaman protokollat

Metropolia Ammattikorkeakoulu

Insinööri (AMK)

Automaatiotekniikan koulutusohjelma

Insinöörityö

22.4.2014

Metropolia

Tekijä(t) Otsikko Sivumäärä Aika	Timo Peltonen IoT ja M2M - Langattomat, lyhyen kantaman protokollat 31 sivua + 1 liitettä 22.4.2014
Tutkinto	Insinööri(AMK)
Koulutusohjelma	Automaatiotekniikka
Suuntautumisvaihtoehto	Kappaletavara-automaatio
Ohjaaja(t)	Lehtori Timo Tuominen

Internet-of-Thingsistä puhuttaessa puhutaan usein Internetin sovellusten ja palvelujen yhteen liittämistä fyysiseen maailman asioihin, jotta voisimme paremmin tuntea ja kontrolloida ympäristöämme.

Insinöörityön aiheena oli tutkia Internet-of-Thingsiä ja sen yhtä toimialaa Machine-to-Machine-kommunikointia, ja koska vuosien päästä käytetyin tekniikka tällä saralla on lyhyen kantaman teknologiat, niin tuli selvittää, kuinka eri lyhyen kantaman protokollat soveltuisivat tähän tarkoitukseen ja vertailla niitä keskenään. Valittiin vielä langattomat teknologiat, koska uskotaan, etteivät M2M-sovellukset langallisena versioina globalisoidu.

Aluksi perehdyttiin IoT:hen ja M2M:iin, jonka jälkeen tutkittiin protokollia ja vertailtiin niitä keskenään. Tuloksena huomattiin, että IoT on vasta alkutaipaleella, jonka takia ei löydy yhtenäistä määritelmää tai viitekehystä IoT:n arkkitehtuurille. Löytyy vain paljon hajanaisia ratkaisuja tietoliikenteen rakentamiselle. Huomattiin myös, että protokollat ovat kehittyneet paljon lähivuosina ja se vaikeutti tiedonhakua niistä.

Tuloksena päädyttiin lopulta siihen, että kun ei ole mitään tiettyä vallitsevaa pohjaa IoT:n M2M-kommunikoinnille, ja tätä myöten vaatimuksia protokollilta, on vaikea sanoa sen suuremmin protokollien soveltuvuudesta kyseiseen tietoliikenteeseen. IEEE 802.11x-protokollat tuntuvat kuitenkin olevan eniten valmiita IoT- ja M2M-kommunikointiin muun muassa niiden korkeamman tiedonsiirtonopeuden ja valmiiksi suuremman markkinaosuuden takia, joka ulottuu usealle alalle.

Pääpiirteittäin voidaan sanoa, että tarvittaisiin laajempi tutkimus, jotta saataisiin protokollien soveltuvuudet paremmin esiin koskien IoT:ta ja M2M:a. Tämä insinöörityö kuitenkin ottaa ensiaskeleet kyseiseen aiheeseen ja antaa pohjan uutta tutkimusta varten.

Avainsanat	Internet of Thing, Machine to Machine, protokolla, langaton verkko, PAN, LAN

Author(s) Title Number of Pages Date	Timo Peltonen IoT and M2M - Wireless, short-range protocols 31 pages + 1 appendices 22 Apr 2014
Degree	Bachelor of Engineering
Degree Programme	Automation technology
Specialisation option	Manufacturing Automation
Instructor(s)	Timo Tuominen, Senior Lecturer

When talking about the Internet-of-Things, we often talk about interconnecting applications and services of the Internet with the physical world of things, allowing us to get better sense and control of our environment.

The topic of this thesis was to study the Internet-of-Things and one of its domains Machine-to-Machine-communication, and because years later the most used technology in this field is short-range technologies, therefore it was important to investigate how different kind of short-range protocols would be suitable for this kind of purpose and compare them with each other. Wireless technologies were chosen because it is believed that M2M-applications will not spread globally in wired versions.

At first I familiarized myself with IoT and M2M and after that protocols were studied and compared. As a result it was concluded that IoT is in the early stage and that is why there is no coherent definition or framework for the architecture of IoT. There are only scattered solutions for the construction of communications. It was also found that protocols have evolved much in the past few years and it complicated the search of information.

As a result it was concluded that when there is no certain dominant basis for the M2M-communications of IoT, and therefore requirements for the protocols, it is difficult to judge the suitability of protocols for this communication. However IEEE 802.11x-protocols seem to be the most ready for IoT- and M2M-communication because of higher data transfer rate and already larger market share which extend to several fields.

In summary we can say that there is need for wider research in order to get better information about the aptitude of protocols in IoT and M2M. This thesis, however, takes the first steps in this topic and provides base for new research.

Keywords	Internet of Thing, Machine to Machine, protocol, wireless network, PAN, LAN

Sisällys

Lyhenteet

Protokolla	Yhteiskäytäntö tai standardi, joka määrittelee tai mahdollistaa laitteiden tai ohjelmien väliset yhteydet.
ICT	*Information and Communications Technology*, tietotekniikka, informaatioteknologia
IoT	*Internet of Things*, esineiden Internet
M2M	*Machine to Machine*, koneiden välinen älykäs kommunikointi
RFID	*Radio Frequency IDentification*, radiotaajuinen etätunnistus, menetelmä tiedon etälukuun ja tallentamiseen käyttäen tageja eli RFID-tunnisteita
EPC	*Electronic Product Code*, sähköinen tuotekoodi
IP	*Internet Protocol*, TCP/IP mallin Internet-kerroksen protokolla, joka huolehtii IP-tietoliikennepakettien toimittamisesta perille pakettikytkentäisessä Internet-verkossa.
TCP	*Transmission Control Protocol*, tietoliikenneprotokolla, jolla luodaan yhteyksiä tietokoneiden välille, jolla on pääsy Internetiin.
TCP/IP	Yhteisnimitys Internetissä käytettäville tietoliikenneprotokollille
WSAN	*Wireless Sensor Actuator Network*, langattomien antureiden ja toimilaitteiden verkko
(W)HAN	*(Wireless) Home Area Network*,yksi lähiverkon tyyppi, kodin tai sen välittömään läheisyyden tietoliikenteeseen tarkoitettu verkko, (W) langaton

(W)PAN	*(Wireless) Personal Area Network*, likiverkko, tiedonsiirtoverkko, jossa henkilökohtaiset elektroniset laitteet voivat kommunikoida keskenään, (W) langaton
(W)LAN	*(Wireless) Local Area Network*, lähiverkko, on rajoitetulla maantieteellisellä alueella toimiva tietoliikenneverkko, (W) langaton
WAN	*Wide Area Network*, laajaverkko, tiedonsiirtoverkko, joka peittää laajoja maantieteellisiä alueita, yhdistää lähiverkkoja ja kaupunkiverkkoja yhdeksi suureksi verkoksi
OSI-malli	*Open Systems Interconnection Reference Model*, malli, jonka puitteissa tietoliikennejärjestelmät voi suunnitella
MAC	*Media Access Control*, IEEE 802-verkoissa verkon varaamisen ja itse liikennöin hoitava osajärjestelmä
GRIP	*Gateway Remote Interface Protocol,* binääriprotokolla, joka vaihtaa ZigBee-pinon rakenteet TCP-yhteyksissä
UDP	*User Datagram Protocol*, yhteydetön protokolla, joka ei vaadi yhteyttä laitteiden välille, mutta mahdollistaa tiedostojen siirron
CAP	*Compact Application Protocol,* avoin kehys, joka yhdistää IP-maailman ja ZigBee-teknologian
RF	*Radio Frequency*, radiotaajuus
P2P	*Peer-to-Peer*, vertaisverkko
PPP	*Point-to-Point Protocol*, tiedonsiirtoprotokolla, jossa suora yhteys verkkolaitteiden välillä
BLE	*Bluetooth Low Energy*, vähävirtainen versio Bluetoothista

WSN	*Wireless Sensor Network*, langattomien antureiden verkko
UART	*Universal Asynchronous Receiver Transmitter*, sarjaliikennepiiri, tyypillisesti mikropiiri, joka muuntaa rinnakkaismuotoista tietoa sarjamuotoiseksi ja päinvastoin
SPI	*SCSI*, *Small Computer System Interface*, väyläohjain, standardi tiedon välittämiseksi keskuslaitteen ja oheislaitteiden välillä
USB	*Universal Serial Bus*, sarjaväyläarkkitehtuuri oheislaitteiden liitämiseksi keskuslaitteeseen
FSK	*Frequency Shift Keying,* kantoaallon taajuuden muuttamiseen perustuva taajuusmodulointimenetelmä, jolla lähetetään digitaalista tietoa
HVAC	*Heating, Ventilation, and Air Conditioning*, lämmitys, ilmanvaihto ja ilmastointi
DSSS	*Direct Sequence Spread Spectrum*, suorasekventointi, lähetettävä sanoma jaetaan pieniin osiin ja lähetetään koko taajuusalueelle yhtenä signaalina
FHSS	*Frequency Hopping Spread Spectrum*, taajuushyppely, lähettäjä vaihtaa lähetystaajuutta tietyn algoritmin mukaan
PTP	*Precision Time Protocol,* protokolla, jonka avulla synkronoidaan kellot verkon sisällä
ISM-taajuusalue	*Industrial, Scientific, and Medical*, maailmanlaajuinen radiotaajuuskaista, jonka käyttö ei vaadi eriilistä lupaa ja on alun perin tarkoitettu teolliseen, tieteelliseen ja lääketieteellieen käyttöön
SMS	*Short Message Service*, tekstiviesti

GPRS	*General Packet Radio Service*, GSM-verkossa toimiva pakettikytkentäinen tiedonsiirtopalvelu
de facto	Formaatti, kieli tai protokolla, josta on tullut standardi, koska se on laajalti käytössä ja tunnustettu teollisuudessa, ei standarditoimien takia

1 Johdanto

Vuosikymmenien tutkimusten ja teollisen vaivannäön ansiosta tietotekniikan, ICT:n parissa olemme siinä tilanteessa, että ihmisillä on annettu mahdollisuus nopeaan, melkein missä ja milloin vain tapahtuvaan sosialisoitumiseen toistensa kanssa, sekä vuorovaikutukseen Internet-sovellusten ja palvelujen kautta. Kehitys ei ole kuitenkaan pysähtynyt, vaan seuraava askel on jo aloitettu. Sen tavoitteena on helpottaa Internetin sovellusten ja palvelujen yhteen liittämistä fyysiseen maailman asioihin, jotta voisimme paremmin tuntea ja kontrolloida ympäristöämme. Tähän viitataan usein puhuttaessa Internet-of-Things:stä (IoT).

Internet-of-Thingsin käyttöä tutkitaan ahkerasti useiden yritysten ja organisaatioiden toimesta todella suurillakin budjeteilla. Yksi tutkituimmista toimialoista on koneiden välinen kommunikointi (M2M). Tulevaisuudessa M2M-kommunikoinnin oletetaan olevan IoT:n suurin toimiala yhdistetyissä laiteissa ja lyhyen kantamien teknologioiden hoitavan siitä tietoliikenteestä suurimman osan. [7] Koska vielä uskotaan, että langattomuus on yksi vaatimus markkinoiden kasvamiselle, niin tässä insinöörityössä perehdytään siihen, minkälaisia vaihtoehtoja langattomat, lyhyen kantaman protokollat tälle tietoliikenteelle tarjoavat. Käydään läpi 12 potentiaalista protokollaa juuri IoT:lle ja M2M:lle ja vertaillaan niitä keskenään. Pyritään antamaan kuva protokollien tämän hetkisestä soveltuvuudesta ja mahdollisista ongelmakohdista. Samalla pyritään antamaan selkeä kuva käsitellyistä tiedonsiirtotekniikoista myös yleisesti.

2 Internet-of-Things

2.1 Määritelmät

Kirjallisuudesta löytyy useita eri määritelmiä Internet-of-Thingsille, joista seuraavat kolme ovat yleisesti hyväksytyimmät. Vaikka ne tuntuvatkin täydentävän toisiaan ja ovat osittain päällekkäisiä, ne ovat erotettavissa ja osaltaan kaikki oikeassa. [1, s. 9; 2].

Asioihin suuntautuneessa näkemyksessä keskitytään asioiden identiteettiin ja toiminnallisuuteen. Tämä näkemys on lähtöisin MIT Auto-ID Labs:n ideasta käyttää RFID

tunnisteita yksilölliseen tunnistamiseen. Tästä on vain jätetty pois pelkkä RFID ja EPC sidonnaisuus ja tunnistettavaan esineeseen on lisätty myös virtuaalimaailma. Tästä näkökulmasta nähden IoT on määritelty seuraavanlaisesti:

> “Asiat, joilla on identiteettejä ja virtuaalipersoonallisuuksia, toimivat älykäissä tiloissa käyttäen älykästä rajapintaa kytkeytyäkseen ja kommunikoidakseen sosiaalisessa ympäristössä ja käyttäjäyhteyksissä.”
>
> tai
>
> “Yksilöllisesti osoitteellisten yhteen liitettyjen asioiden maailmanlaajuinen verkko, joka perustuu standardoituihin kommunikointiprotokolliin.
> [1, s. 9; 3].

Internetiin suuntautunut näkemys painottaa verkon infrastruktuuria ja se on huolissaan nykyisen ja tulevan Internetin infrastruktuurin, IP protokollapinon ja Web standardien soveltuvuudesta, kun liitetään älykkäitä esineitä verkkoon. Sen mukaan IoT tulisi rakentaa Internetin rakenne huomioonottaen, ja kun on tarpeellista, niin yksinkertaistaa nykyisiä protokollia ja standardia. Tästä näkökulmasta IoT määritellään kyseisellä tavalla:

> ”Globaali verkkoinfrastruktuuri, joka yhdistää fyysiset ja virtuaaliset asiat tiedonkeruuta ja kommunikointivalmiuksia hyväksikäyttäen. Infrastruktuuri sisältää jo olemassa olevaa sekä kehittyvää Internetiä ja verkon kehityksiä. Se tulee tarjoamaan erityistä kohteentunnistusta sekä anturi ja liitäntävalmiuksia perustana palvelujen ja sovellusten itsenäiselle yhteistyölle.
> Nämä palvelut ja sovellukset tulevat olemaan tunnettuja korkean asteen itsenäisestä tiedonkeruusta, tapahtumien siirrosta, verkon liitettävyydestä ja yhteen toimivuudesta.” [1, s. 9].

Semanttisessa näkemyksessä keskitytään systemaattiseen lähestymistapaan tiedon ilmaisemisessa, organisoimisessa ja tallentamisessa. Käytetään semanttista teknologiaa IoT:n lähestymistapana:

> “Semanttisten teknologioiden sovellus edistää yhteen toimivuutta IoT:n resurssien, tietomallien, datatarjoajien ja kuluttajien välillä. Se helpottaa tehokasta tietojen saatavuutta ja integraatiota, resurssien löytämistä, semanttista päättelyä ja tietä-

myksen koostamista tehokkaiden menetelmien kautta, jotka voivat jäsentää, kommentoida, jakaa ja tehdä ymmärrettäväksi IoT:n datan ja helpottaa sen muuttamista toiminnalliseksi tietämykseksi ja älykkyydeksi erilaisilla sovellusaloilla.” [1, s. 10; 4].

2.2 IoT ja M2M

M2M:llä tarkoitetaan automaattista älykästä tiedonsiirtoa laitteiden, koneiden ja järjestelmien välillä, mutta se ei sulje pois ihmistä sovelluksen käyttäjänä ja järjestelmän osana. M2M on ratkaisu langattomiin ja langallisiin sovelluksiin, jossa käyttäjän läsnäolo ei ole välttämätöntä koneen tai laitteen äärellä. IoT:n ja Machine-to-Machinen (M2M) suhde onkin hyvin ristiriitainen. Osa ihmisistä olettaa niiden olevan sama asia. Ne ovatkin hyvin samanlaisia, mutta täytyy muistaa, ettei koneiden välinen kommunikointi (M2M) välttämättä käytä Internetiä, kun taas IoT:ssä tämä on oletus. IoT ja M2M ovatkin hyvin samanlaisia tavoitteiltaan, mutta hieman erilaisilla sovelluksilla ja toteutuksilla.[5].

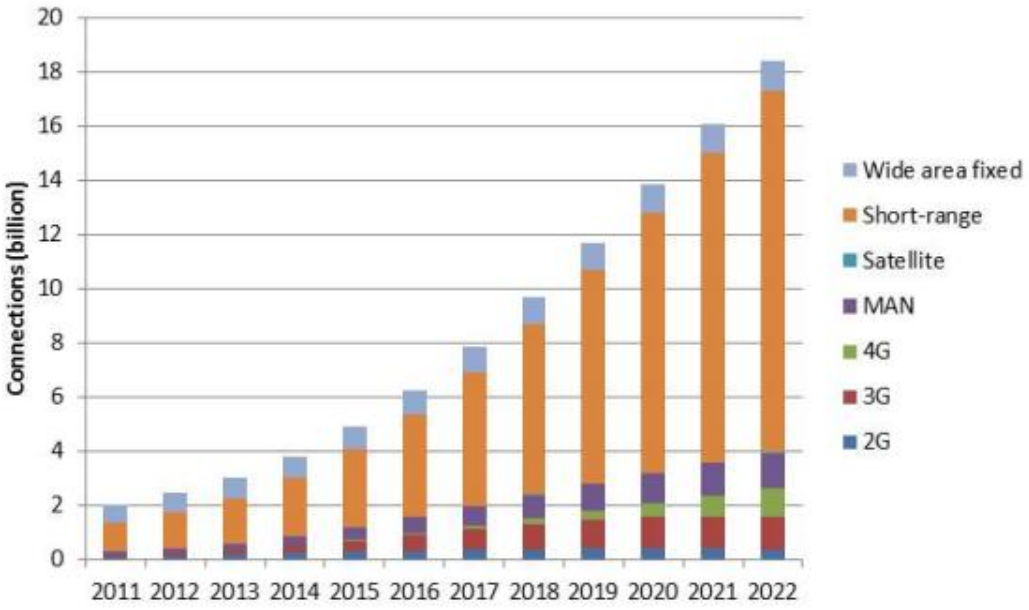
M2M onkin yksi IoT:n toimialoista, jossa IoT:n lisäkäyttöä tutkitaan ahkerasti koko ajan. Muita toimialoja ovat muun muassa Radio Frequency IDentification (RFID), Machine Type Communication (MTC), langattomien antureiden ja toimilaitteiden verkot (WSAN), jokapaikan tietotekniikka ja Web-of-Things (WoT). Näitä teknologioita käytetään hyvin laajalla sovellusalueella, minkä takia se, mikä tänään tunnetaan IoT:na, edustaakin useiden toimialojen lähentymistä ja voidaan nähdä yläkäsitteenä yhdistämään nämä näkemykset ja teknologiat. [1].

2.3 Markkinakapasiteetti

Markkinoita ja yritysten liiketoimintaa ajatellen IoT tarjoaa suuren mahdollisuuden monenlaisille yrityksille muun muassa IoT sovellus- ja palvelutarjoajille, IoT:n alustan tarjoajille ja integroijille kuten myös teleoperaattoreille ja ohjelmiston myyjille. Tällä hetkellä IoT:n markkinat ovat vasta alkutekijöissä, mikä näkyy hajanaisina ratkaisuina kohdistuen vain tiettyyn alaan ja/tai sovellukseen. Nykyisille ratkaisuille on myös ominaista suuri valikoima patentoituja alustoja, protokollia ja käyttöliittymiä, minkä takia niiden komponentit eri toimittajilta ovat harvoin yhteensopivat, mikä taas pitää komponenttien hinnat korkealla. Ei ole myöskään hallitsevia, markkinoita määrääviä standardoituja protokollia, käyttöliittymiä eikä alustoja vielä. Lisäksi ei ole viitekehystä IoT:n arkkiteh-

tuurin rakentamiselle, eikä tietoa, kuinka valita ratkaisujen ja komponenttien välillä. Nämä asiat yhdessä estävät tällä hetkellä IoT suurempaa leviämistä. [1]

Kuitenkin useiden IoT-teknologioiden odotetaan kasvavan nopeasti markkinoilla tulevina vuosina, mikä heijastuu kasvavana määränä IoT-tuotteita ja suurempina liikevaihtoina. Vuoteen 2020 mennessä IoT:ssa yhdistettyjen laitteiden määrän odotetaan kasvavan 25,7 miljardiin nykyisestä 11.3 miljardista. [6]. Suurimman nousun odotettaan olevan M2M-kommunikoinnissa, jossa vuoteen 2022 mennessä 2 miljardista yhdistetystä laitteesta noustaan 18 miljardiin laitteeseen. [7]. Kuvassa 1 nähdään, miten näiden M2M-yhdistettyjen laitteiden odotetaan jakaantuvan teknologioiden kesken. Liikevaihdon odotetaan nousevan 4,5 biljoonaan vuodessa 2020 mennessä IoT-yhdistetyissä laitteissa [6]. ja M2M-kommunikoinnissa vuoteen 2022 mennessä 1,2 biljoonaan nykyisestä 200 miljardista.[7].



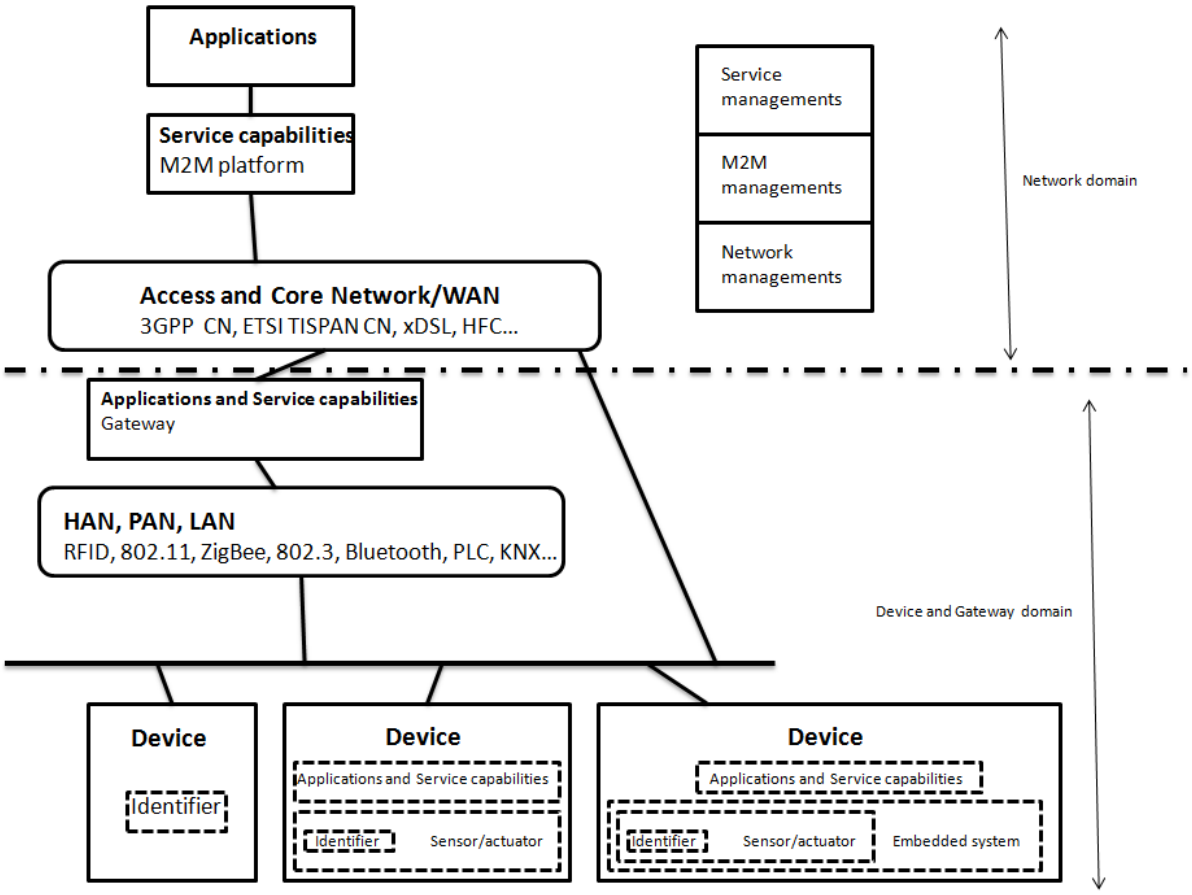
Kuva 1. M2M-kommunikointi, yhdistetyt laitteet ja hajonta teknologioiden kesken [7].

M2M-kommunikoinnin odotetaan siis olevan suurin tekijä IoT:n markkinoilla, ja kuten kuva 1 osoittaa, niin lyhyen kantaman teknologiat dominoisivat markkinoilla tulevaisuudessa, vallaten jopa 73 % osuuden M2M-yhdistetyistä laitteista vuonna 2022. Suurimman sektorin näissä odotetaan olevan rakennus- ja kiinteistöautomaatio 37 % osuudella. Tätä seuraavat älylaitteet 32 %, hyödykkeet 10 % ja autoteollisuus 8 % osuudella. Loput 13 % jakaantuu muiden sektorien kesken. Liitteessä 1 nähdään, minkälaisia pal-

veluja ja sovelluksia eri sektoreilla voidaan toteuttaa M2M kommunikoinnin ja IoT:n avulla.[7; 8].

3 Tekninen toteutus

Julkisten tutkimusprojektien, kaupallisten aloitteiden ja standardointitoimien tuloksena on syntynyt useita eri ratkaisuja IoT:n arkkitehtuurin rakentamiselle. Niistä suurin osa keskittyy erityisesti IoT:n aliverkkoon. Esimerkiksi SENSEI:n ratkaisu keskittyy langattoman antureiden verkkoon ja EPCglobal:n RFID teknologiaan. ETSI TC M2M tekee tässä poikkeuksen. Sen tarjoama ratkaisu sisältää kokonaisvaltaisen arkkitehtuurin IoT:lle, sisältäen sovellustason käyttöliittymät, palvelin ominaisuudet ja sovellustason yhdyskäytävät helpottamaan eri verkkojen yhdessä toimimista (Kuva 2). [9; 10].



Kuva 2. ETSI TC M2M:ään perustuva Internet-of-Things arkkitehtuuri. [10].

Vaikka yllä oleva ratkaisu onkin vain yksi monista vaihtoehtoista, niin sen avulla voidaan hahmottaa hieman IoT:ta ja sitä mitä tässä työssä käsitellään. Kuten edellisessä

luvussa kerrottiin, niin IoT:n markkinallisesti suurimman toimialan ennustetaan olevan M2M. M2M kommunikoinnissa odotetaan taas lyhyen kantaman teknologioiden hoitavan 73 % kaikista yhteyksistä vuoteen 2022 mennessä. Tästä syystä tässä työssä keskitytään HAN (Home Area Network), PAN (Personal Area Network), LAN (Local Area Network) alueen langattomien verkkojen protokolliin. Langalliset vaihtoehdot jätetään syvemmin käsittelemättä, koska uskotaan, etteivät M2M-sovellukset globalisoidu ja leviä kunnolla kaikkialle, jos ei tukeuduta langattomiin teknologioihin. Langattomat WAN (Wide Area Network)-verkot käsitellään lyhyesti luvussa 4.4.

3.1 Langattomat, lyhyen kantaman protokollat

Vaikka IoT on alkanut vasta viime vuosina kerätä suurta kiinnostusta, niin sitä mahdollistavia protokollia on kehitetty jo vuosikymmeniä. Tässä luvussa esitellään lyhyen kantaman langattomia protokollia, joita on jo kaupallisessa käytössä. Luvussa 3.2 esitellään myös muutama potentiaalinen teknologia, joka keskittyy pääosin langalliseen kommunikointiin, mutta jolla on myös vaihtoehtoja langattomaan, lyhyen kantaman kommunikointiin. Kerrotaan yksittäin, lyhyesti eri protokollista. Kerrotaan taustoista, ominaisuuksista, käyttökohteista ja protokollien mahdollisesta soveltuvuudesta IoT:lle ja M2M-kommunikointiin.

3.1.1 ZigBee

Motorola aloitti vuonna 1998 ZigBee-teknologian kehittämisen. Tuolloin Motorola oli kehittelemässä teknologiaa pienitehoiselle Mesh-verkolle. Tästä tuli myöhemmin perusta IEEE 802.15.4 standardille, joka julkaistiin 2003. IEEE 802.15.4 määrittelee vähävirtaisen WPAN:n. Se määrittelee verkon OSI-mallin fyysisen ja siirtoyhteyskerroksen. ZigBee-standardi määrittelee OSI-mallin verkkoyhteys- sekä kuljetuskerrokset. ZigBee-allianssi vastaa ZigBee-standardin kehittämisestä. Allianssin perustivat Motorola, Philips, Invensys, Honeywell ja Mitsubishi. Nykyään Allianssin jäsenmäärä on yli 400 ja siihen kuuluu useita suuryrityksiä, kuten Schneider Electric, Texas Instruments ja Carrier. Standardi on täysin avoin vain jäsenille. Yhden version standardista saa käyttöön ilmaiseksi ei-kaupallisiin tarkoituksiin. Vuosittaisella 4 000 dollarin jäsenmaksulla standardia saa käyttää kaupallisiin tarkoituksiin, mutta kokojäsenyys maksaa joko 9 900 tai 55 000 dollaria vuodessa. [9; 11].

ZigBee protokolla kehitettiin alun perin kiinteistöautomaatioon, mutta nykyään se soveltuu hyvin laajalle alalle. Suurin osa tuotteista kohdistuu kuitenkin kolmeen sektoriin, rakennusautomaatioon, telepalveluihin ja energian käyttöön. Sovelluksiin, jotka vaativat alhaisen tiedonsiirtonopeuden, todella pitkän akunkeston ja hyvän tietoturvan. ZigBee on myös hyvin halpa vaihtoehto. Zigbee on yksi maailman johtavista protokollista, jota käytetään tuotteissa, jotka valvovat, ohjaavat, informoivat ja automatisoivat energian ja veden siirtoa ja käyttöä. Rakennusautomaatiossa Zigbee:tä käytetään kotien laitteiden, valaistuksen, lämmityksen ja ilmastoinnin automatisointiin kustannustehokkaasti, turvallisesti ja luontoystävällisesti. ZigBee:n telepalvelut tarjoavat muun muassa turvallissia mobiilimaksupalveluja, mobiilipelaamista, mobiilimainostusta ja tiedonsiirtopalveluja. [9].

ZigBee perustuu pitkälti IEEE 802.15.4 standardiin, mutta uusin versio ZigBee Smart Energy ei ole enää sidottu kyseisen standardin fyysisiin eikä MAC(Media Access Control) ominaisuuksiin. ZigBee kehykset voidaan siirtää TCP:n päällä käyttäen GRIP (Gateway remote Interface Protocol):ä ja UDP:n päällä käyttäen CAP(Compact Application Protocol):ä. [11].

ZigBee-verkossa on kolme erilaista laitetta: ZigBee Coordinator(ZC), ZigBee Router(ZR) ja ZigBee End Device(ZED). ZC on vastuussa verkon muodostamisesta sekä verkon tietojen säilyttämisestä. ZC-laitteita on yksi jokaista ZigBee-verkkoa kohden. ZR-laite huolehtii datan reitittämisestä muille laitteille. ZED-laite on yksinkertainen laite, joka ei pysty kommunikoimaan suoraan toisen ZED-laitteen kanssa. Verkko voi olla topologialtaan Tree, Star, Mesh tai P2P. [11].

Mitään osuuksia markkinoista tai asennettujen ZigBee-pohjaisten laitteiden määrää on vaikea arvioida. Vaikka protokollan yksi ongelmista on IP yhteensopivuus, niin se on silti yksi vahvimmista ehdokkaista IoT:n parissa. ZigBee on yksi harvoista protokollista, joka soveltuu eri aloille ja ZigBee-allianssi tekee koko ajan töitä lisätäkseen protokollan yhteentoimivuutta natiivien Internet protokollien kanssa saadakseen joustavuutta nykyisiin teknologioihinsa.

3.1.2 Z-Wave

Z-Wave on lyhyen kantaman langaton teknologiaratkaisu, jota pidetään usein ZigBee suurena kilpailijana kiinteistöautomaation saralla. Z-Wave:n kehitys aloitettiin vuonna

1999 tanskalaisen pikkuyrityksen Zen-Sys:n toimesta. Myöhemmin Sigma Designs osti Zen-Sys:n ja Z-Wave:n, jota Z-Wave Allianssi nykyisin hallinnoi ja kehittää. Standardin saa käyttöön 350 dollarilla vuodessa ja jäsenyys maksaa 3 500 dollaria vuodessa. Isoista yrityksistä NEC, NTT Docomo, Verizon and Zyxel ovat jäseniä Z-Wave Allianssissa. [12].

Z-Wave-protokollaa käytetään pääosin kiinteistöautomaatiossa, erityisesti kaukoohjattavissa sovelluksissa asunnoissa ja pienissä kaupallisissa rakennuksissa. Z-Wave käyttää pienitehoista RF-radiota sulautettuna tai jälkiasennettuna kodin elektroniikka laitteisiin ja systeemeihin, kuten valaisuun, turvalaitteisiin, kotiteatteriin ja kodinkoneisiin. Z-Wave määrittelee Internet-yhdyskäytävän asetukset, mutta ei tomi yhteen muitten protokollien kanssa. [13].

3.1.3 Insteon

Insteon on SmartLabs:n kehittämä patentoitu teknologia kiinteistöautomaatioon. Insteon on suunniteltu mahdollistamaan kotilaitteiden yhteenliittymisen. Yhteenliittyminen tapahtuu sähköverkon tai radiotaajuuden (RF) tai molempien avulla. Insteon toimii P2P (Peer-to-Peer)-verkkona, jokainen kytketty laite pystyy lähettämään, vastaanottamaan ja toistamaan Insteon-protokollan mukaisia viestejä ilman että tarvittaisiin erillistä reititinohjelmistoa tai isäntälaitetta. Erona muihin Mesh-topologialla toimiviin standardeihin on, että kaikki Insteon-yhteensopivat laitteet toistavat kaikki saapuvat viestit eivätkä vain tietyt solmukohdat. Insteon tukee Internetiin liittymistä ja useita gateway-laitteita on saatavilla. Insteon-tuotteet sähköverkkoon kytkettynä voidaan valmistaa X10-yhteensopivaksi. Näin laitteet, jotka tukevat sekä X10:tä ja Insteonia ovat osittain yhteentoimivia. [14; 15].

Insteonia käytetään kodin ilmastoinnin, kodinkoneiden, valaisun ja turvalaitteiden hallintaan. Se soveltuu myös kotiteatterijärjestelmän hallinnoimiseen, energian käytön valvontaan, kodin langattomaan valvontaan Internetin kautta. Lisäksi se on yhteen toimiva äänentunnistusohjelmistojen kanssa. [16].

3.1.4 Bluetooth

Bluetooth on avoin standardi, jonka kehittäminen alkoi 1994 Ericssonin toimesta. Ericssonin aloitteesta vuonna 1998 perustettiin Bluetooth SIG, jonka perustajiin kuului myös Nokia, Toshiba, IBM ja Intel. Tavoitteena oli luoda de facto -standardi. Nykyään SIG:iin hallitukseen kuuluu melkein kaikki suuret tietoliikennealan yritykset. [17].

Bluetooth koostuu kolmesta osasta, jotka ovat radio-osa, radiolinkin hallintaosa ja yhteydenhallinta, ja ne mahdollistavat informaation siirron laitteiden välillä. Tavallinen Bluetooth perustuu PPP (Point-To-Point)-yhteyteen, jossa kaksi laitetta kommunikoivat keskenään. Toinen laitteista on isäntä ja toinen orja. Isäntä voi olla yhteydessä yhdessä verkossa seitsemään orjaan (Piconet). Hajaverkoissa, jokin laitteista on yhteydessä toiseen verkkoon (Scatternet). Laite voi olla isäntä tai orja, mutta laite voi kuitenkin keskustella vain yhden laitteen kanssa kerrallaan. Bluetoothin laajennukset, BLE (Bluetooth Low Energy)-versiot, sen sijaan perustuvat Star-Bus-topologiaan. Siinä isännät voivat olla yhteyksissä toisiinsa väylän kautta, mutta rengit ovat yhteyksissä vain omaan isäntäänsä. [17; 18].

Bluetooth on sisäänrakennettu moniin eri tuotteisiin laajalla skaalalla, matkapuhelimista ja tietokoneista, lääketieteellisiin laitteisiin, autoihin ja kaikennäköiseen pienelektroniikkaan. Bluetoothin suurimmat vahvuudet ovat globaalisuus, turvallisuus, halpa hinta ja energiatehokkuus. Bluetoothin ongelma IoT:ssa on kuitenkin se, että sen käyttöalue IoT:ssa on hyvin rajallinen, koska Bluetooth ei itsessään ole IP-pohjainen protokollapino. IP-protokolla pinoja voidaan silti siirtää Bluetoothin kautta esimerkiksi kännykän avulla, mutta tässä suositaan paljon enemmän muita vaihtoehtoja, kuten WLAN:a. [9; 17; 18].

3.1.5 ANT

ANT on patentoitu verkkoprotokolla ja RF-ratkaisu, joka on suunniteltu erittäin alhaista virrankulutusta vaativiin likiverkko (Personal Area Network, PAN) ja langattomien verkkojen (Wireless Sensor Network, WSN) sovelluksiin. ANT:n on kehittänyt Dynastream Innovations, jonka nykyään omistaa Garmin International. [19; 21].

ANT mahdollistaa pii-pohjaiset RF-lähetinradioratkaisut 2.4GHz:n ISM-taajusalueella noudattaen standardeja rinnakkaisuudesta, tiedon esityksestä, signaloinnista, toden-

nuksesta ja virheiden havaitsemisesta. ANT protokollalähettimet sisältävät valmiiksi ANT-protokollan ohjelmiston, mutta vaativat mikrosäätimen UART:n, SPI:n tai USB:n rajapinnan kautta ohjaukseen. ANT on teknologia, jota käytetään tiedon keräykseen, lähettämiseen ja seurantaan urheilu-, hyvinvointi- ja terveyssovelluksissa. Tyypillisiä ANT sovelluksia ovat sykemittarit, nopeus ja etäisyysmonitorit, pyörän eri anturit, painoindeksin mittaus, lämpöanturit ja kuntolaitteiden anturit. [20; 21].

Puhuttaessa ANT:stä puhutaan usein myös ANT+:sta. ANT+ voidaan liittää ANT-protokollaan, jolloin ANT-tuotteet valmistajasta riippuen pystyvät kommunikoimaan keskenään saumattomasti. ANT+ tarjoaa ennaltamäärätyt verkon parametrit ja rakenteet tietoliikenteelle tähän tarkoitukseen.

ANT:n suurimmat vahvuudet ovat erittäin alhainen virrankulutus, alhaiset kehitys ja ylläpito kustannukset ja verkon joustavuus ja laajennettavuus. Heikkoudeksi voidaan laskea, ettei protokolla suoraan tue yhteen toimivuutta toisten WSN (Wireless Sensor Network) teknologioiden kanssa eikä sisällä Internet yhdyskäytävän spesifikaatioita.

3.1.6 ONE-NET

ONE-NET on avoimen lähdekoodin protokolla, jonka kehittämisen kiinteistöautomaatioon aloitti Threshold yritys vuonna 2004, koska heidän mielestään mikään sen aikaisista protokollista ei ratkaissut kotien verkko-ongelmia. ONE-NET käyttää UHF-radiolähetintä ja hyödyntää Wideband FSK:ta (Frequence-shift keying) datalähetyksen koodaamiseen. [22].

ONE-NET on optimoitu alhaiseen virrankulutukseen ja alhaisiin kustannuksiin, mutta sen etu muihin protokolliin verrattuna on korkea turvallisuustaso ja pitkä kantama. Lisäksi se on ainut langattomien verkkojen protokolla, jossa on kaikille täysin avoin lähdekoodi. Heikkoutena voidaan pitää sitä, että protokollan yleinen kehittäminen on tällä hetkellä kysymysmerkki, kun protokollan viralliset sivutkin ovat poissa käytöstä. [22]

3.1.7 EnOcean

EnOcean on saman nimisen yrityksen kehittämä teknologia, joka on ratifioitu kansainväliseksi standardiksi vuonna 2012. Standardi kattaa OSI-mallin kolme alinta kerrosta,

fyysisen ja, siirto- ja verkkokerroksen. EnOcean teknologiaa hallinnoi EnOcean Alliance. Liitossa suurinta päätösvaltaa EnOcean:n kanssa jakaa muun muassa Honeywell ja Texas Instruments. Osallistujina on jo yli 150 yritystä, muun muassa ABB, Beckhoff ja Omron. Sen lisäksi on vielä alimman tason jäsenet. Kyseessä on siis maksullinen teknologia, jonka käyttöön saaminen maksaa jäsenyyden tasosta riippuen 250, 6 000 tai 35 000 dollaria vuodessa. [24].

EnOcean eroaa selvästi muista langattoman verkon teknologioista. EnOcean on paristoton radioteknologia. Sensorit ottavat energiansa ympäristöstään. Minimaaliset muutokset paineessa, liikkeessä, valossa, värinässä tai lämpötilassa mahdollistavat radiosignaalien välittämisen. EnOcean-teknologia mahdollistaa antureiden kommunikoinnin toimilaitteen, säätimen tai portin kanssa ja sen yhdyskäytävä spesifikaatiot tukevat langallisena yhteytenä useita muita automaattisysteemejä, kuten KNX, LONWorks ja ModBus sekä TCP/IP pinoa. [23; 25].

EnOcean teknologiaa käytetään pääasiassa kiinteistöautomaatiossa, valaisussa ja HVAC-sovelluksissa. Sovellusesimerkkeinä yleisimmät ovat paristoton langattomat valokatkaisimet, liiketunnistusvalot, avainkorttivalot, kosteus-, hiilidioksidi- ja lämpötila-anturit. EnOcean:n vahvuudet muihin nähden ovat paristottomuuden lisäksi ja sen takia, energiatehokkuus, matalat asennuskustannukset, huoltovapaus ja joustavuus. Heikkoutena voidaan pitää sovellusten pääasiallista keskittymistä vain yhteen osa-alueeseen. [23].

3.1.8 IEEE 802.11x

IEEE 802.11 on standardi langattomille WLAN-lähiverkoille. Markkinoinnissa tästä käytetään yleisesti nimeä WiFi. Ensimmäinen WLAN-standardi IEEE 802.11 julkaistiin 1997 ja standardin kehitys siitä on jaettu eri työryhmiin, jotka keskittyvät eri piirteisiin standardeissa. Työryhmän erottaa toisista kirjaimen tai kirjainyhdistelmän avulla standardin lopussa. [26].

IEEE 802.11 määrittelee OSI-mallin alimman kerroksen, fyysisen kerroksen sekä siirtokerroksen alemman MAC-kerroksen. Siirtotavoiksi määritellään 2,4GHz, 3,6GHz tai 5GHz radiotaajuus-alueilla toimivat radioaallot tai 850–950 nanometrin aallonpituusalueella toimiva infrapuna. Radiotaajuustekniikoista ovat käytössä suorasekvenssihajaspektri- (DSSS) ja taajuushyppelyhajaspektritekniikat (FHSS). Verkkotopologiaksi on

määritelty Ad Hoc –verkko, jossa verkon laitteet ovat suoraan yhteydessä toisiinsa sekä tukiasemiin pohjautuvan verkon (Star), jossa verkon laitteet suorittavat kommunikoinnin tukiasemien kautta. [28].

IEEE 802.11x standardiin perustuva WLAN on jo käytössä kaikkialla, kodeissa, toimistoilla, yleisillä paikoilla ja niin edelleen. Se onkin nähty hyvin potentiaaliseksi teknologiaksi IoT:lle ja M2M kommunikointiin. Ja vaikka se voi näyttää ylivoimaiselta muihin langattoman verkon protokolliin verrattuna (tiedonsiirtonopeus, nykyinen markkinaosuus), niin soveltuvuus IoT:lle ja kommunikoinnin toteuttaminen ei kuitenkaan ole itsestäänselvyys, ainakaan vielä. Yhtenä ongelmakohtana voidaan pitää IoT-laitteiden konfiguroimista suojattuun WLAN-verkkoon, koska monessa IoT-laitteessa ei ole näyttöä tai näppäimistöä. Tämä voidaan toki suorittaa toisen laitteen, esimerkiksi kännykän avulla, mutta tullaan siihen kysymykseen, kuinka helppoa käyttö olisi? Monimutkaisuus ja liika teknisyys olisi este IoT:n globalisoitumiselle. Lisäksi pieni kysymysmerkki on akun kesto nykyisellä tekniikalla. [27].

3.1.9 DASH7

DASH7 ei ole patentoitu teknologia ja se perustuu kansainväliseen standardiin ISO/IEC 18000-7, mikä kuvaa erilaisia RFID teknologioita, jotka kaikki käyttävät yksilöllistä taajuusaluetta. DASH7 noudattaa standardin parametreja aktiiviseen kommunikointiin ilma rajapintana 433MHz alueella. 433MHz on lisenssi-vapaa taajuus, jolla on sekä hyviä, että huonoja puolia. Se läpäisee betonia ja osittain vettäkin, ja sen kantama on paljon pidempi muihin langattomiin teknologioihin verrattuna, kuitenkin pienellä akun kulutuksella. Huonona puolena datanopeus jää muita alhaisemmaksi ja tehokkaat antennit kasvavat helposti suurikokoisiksi. Muita DASH7:n vahvuuksia ovat halpuus ja yhteen toimivuus muiden teknologioiden kuten IPv6:n kanssa. [29; 30].

Moniin muihin aktiivisiin RFID teknologioihin verrattuna DASH7 tukee Tag-to-Tag kommunikointia ja se toimii BLAST (Bursty, Light, Asynchronous, Stealth, Transitive) verkkoteknologialla. Data siirtyy siis äkillisesti, sisältää vain vähän, maksimissaan 256tavua, eikä vaadi laitteiden välistä synkronointia. Lisäksi vain ennalta hyväksytyille laitteille vastataan ja laitteet ovat luonnostaan transitiivisia. Tag-toTag kommunikoinnissa päätelaitteet voivat kommunikoida milloin vain ja suoraan toisen päätelaitteen kanssa. [29; 30].

Aseteollisuus ja Yhdysvaltojen puolustusministeriö oli ensimmäinen suuri DASH7 teknologiatuotteiden ostaja vuonna 2009. Muita jo läpilyöneitä sovelluskohteita ovat rengaspaineiden seuranta autoteollisuudessa, toimitusketjun hallinta yrityksissä, tehdas- ja varastorakennuksen optimointi ja energiatehokkuus rakennusautomaatiossa. [1].

3.1.10 RuBee

RuBee on kaksisuuntainen aktiivinen langaton protokolla, joka perustuu IEEE 1902.1 standardiin. RuBee hyödyntää alhaisia taajuuksia (131kHz) ja sillä on pitkä aallonpituus (2,289m), mikä erottaa sen muista teknologioista. Se on P2P protokolla, joka toimii samantapaisesti kuin IEEE 802.11x, mutta käyttää radioaaltojen sijaan magneettiaaltoja. Tästä johtuen RuBee toimii kovissa olosuhteissa muita langattomia teknologioita varmemmin. RuBeen antennien lähettämät 3D-volumetriset magneettiaallot läpäisevät metalleja kuten terästä sekä vettä. Alhaisen taajuuden takia akunkesto on muita pidempi ja toteutus voidaan tehdä pienellä akulla. RuBeessa myös korkea turvallisuuden ja yksityisyyden suoja (tietoturva) magneettisen signaalin takia. Se on ainut turvallinen langaton teknologia lähellä räjähteitä tai kiinni niissä. Suurimmat haittapuolet ovat hidas siirtonopeus ja pieneksi jäävä datansiirtomäärä. [31; 32].

Pääosin RuBee on teknologia asioiden tunnistettavuuteen, ”tagaukseen” vaativissa olosuhteissa. RuBeeta käytetään eniten erilaisissa kriittisissä sovelluksissa kuten ase-, räjähdevarastoissa, asekaapeissa ja kulun valvonnassa. [31].

3.1.11 NFC

NFC (Near Field Communication) on standardeihin ISO/EIC 14443 ja ISO/EIC 18092 perustuva langaton lyhyen kantaman teknologia, joka hyödyntää RFID (Radio Frequency Identification)-tekniikkaa. Vuonna 2004 perustettiin voittoa tavoittelematon NFC Forum edistämään teknologian kehitystä ja valvomaan sen käyttöä. Jäseniä on nykyään melkein 200 ja ylimmän tason jäseninä ovat mm. Nokia, Philips, Google, Visa, Sony ja Intel. Jäsenyys maksaa tasosta ja eduista riippuen 50 000, 25 000, 10 000, 5 000 tai 1 500 dollaria vuodessa. [33].

NFC ratkaisut koostuvat antennilla varustetusta NFC-lukijasta sekä NFC-tagista. NFC perustuu sähkömagneettiseen induktioon kahden laitteen välillä tyypillisten suorien

radiolähetysten sijaan ja se toimii 13,56MHz taajuudella. Toinen laite toimii lukijana tai kirjoittajana ja toinen tunnisteena. Laitteiden välille syntyy yhteys, kun ne tuodaan toistensa lähelle alle kymmenen senttimetrin läheisyyteen. Pieni taajuus ja tiedonsiirtonopeus soveltuvat pienten tietomäärien siirtoon. Suurempia määriä varten NFC-laitteisto voi muodostaa yhteyden Bluetooth tai WLAN yhteyden varsinaisen tiedon siirtämiseen. [33; 34].

Maksu ja tikettipalvelut ovat NFC:n syömähampaat, mutta muitakin samantyylisiä sovelluksia on. NFC toimii ”avainkorttina”, jolla voi tehdä hyvin paljon asioita kuten ostaa matkalipun, avata ovia, leimata työtunnit, kirjautua tietokoneelle, maksaa pysäköintimaksun tai ostoksia kaupassa. Nykyään NFC-maksaminen on käytössä lähes kaikissa maissa. Suomessakin tämä on yleistymässä ja koko ajan on enemmän paikkoja, joissa pienten ostosten (alle 25e) lähimaksaminen onnistuu eli ostaminen ilman PIN-koodia tai allekirjoitusta henkilöllisyystodistusta vastaan vain vilauttamalla maksupäätteellä NFC-tekniikalla perustuvaa maksu- tai luottokorttia, maksutarraa tai älypuhelinta, joka on varustettu NFC-ominaisuudella. [34].

NFC on yleistymässä oleva tekniikka, jonka vahvuuksia ovat vähäinen virrankulutus, nopea yhteydenmuodostus ja turvallisuus maksusovelluksiin, koska se perustuu sähkömagneettiseen induktioon ja toimii vain lähietäisyyksillä. Se toimii myös muiden langattomien yhteyksien kanssa. NFC teknologialla toimivilla sovelluksilla on kapasiteettiä levitä joka puolelle, mutta sovellusalue on hieman kapea vielä tällä hetkellä. Näyttää kuitenkin siltä, että NFC:lla voi olla rooli ainakin edistämässä IoT:n kasvua.

3.2 Muut potentiaaliset protokollat

3.2.1 KNX

KNX on standardoitu verkkoalusta ja seuraaja kolmelle aikaisemmalle standardille, European Home Systems Protocol (EHS), BatiBUS ja European Installation Bus (EIB). KNX:n on kehittänyt KNX Association, mihin kuuluu nykyään yli 300 jäsentä. [35].

Vaikka KNX onkin alun perin suunniteltu langalliseen kommunikointiin, niin nykyään se tarjoaa myös vaihtoehtoja langattomaan kommunikoimiseen. Tällöin puhutaan usein

KNX-RF:stä. Se mahdollistaa kommunikoimisen radiosignaalien kautta 868MHz:n taajuudella FSK-modulointimenetelmällä. Koodaukseen se käyttää Manchesteriä. [36].

KNX teknologia on käytössä rakennusautomaatiossa ja KNX-RF:ä voidaan käyttää muun muassa valaisun, ikkunoiden, HVAC-järjestelmien ja kodinelektroniikan hallintaan.

3.2.2 BACnet

BACnet on myös ratkaisu lähinnä rakennus- ja kiinteistöautomaatioon, jonka avulla kontrolloidaan tiedonsiirtoprosessia. BACnetin kehittäminen alkoi vuonna 1987. ANSI-standardiksi BACnet julkaistiin vuonna 1995 ja 2003 se ratifioitiin ISO-standardiksi. Protokollan valvonnasta ja siihen liittyvistä asioista vastaa BACnet International. [37].

BACnet määrittelee OSI-mallista vain ne kerrokset, joita edellytetään protokollan toimivuuteen. BACnet määrittelee, fyysisen-, siirto-, verkko-, ja sovelluskerroksen, mutta fyysinen- ja siirtokerros toteutetaan muilla teknologioilla. Ne voidaan toteuttaa muun muassa ARCNET:n, Ethernet:n, LonTalk:n tai PTP:n avulla. BACnet–protokolla ei myöskään määrittele kiinteää muotoa verkkotopologialle ja näin saadaan kasvatettua sovellusten joustavuutta. [9; 38].

BACnet:n sovelluskohteita ovat HVAC-, valaisu-, palo- ja turvallisuusjärjestelmät. BACnet on yhteentoimiva hyvin monien järjestelmien kanssa. BACnet on muun muassa yhteen toimiva KNX ja ZigBee protokollien kanssa. [38].

3.2.3 LonWorks

LonWorks:n kehittämisen aloitti amerikkalainen yritys Echelon Corporation, joka on vuonna 1989 perustettu juuri LonWorks:a varten. Tavoitteena oli luoda yleiskäyttöinen ja joustava kenttäväyläteknologia, mutta vuosien ja kehityksen saatossa käyttö on painottunut rakennusautomaation pariin. LonWorks onkin vapaa ja hajautettu järjestelmä eli sen käyttö ei ole valmistajasta riippuvainen ja jokainen LON–laite omaa itsenäisen älyn. LonWorksille on myönnetty standardit ISO/IEC 14908-1, -2, -3, -4 vuonna 2008. [39; 40].

Monesta muusta kenttäväylästandardista poiketen LonWorks tukee P2P (Peer-to-Peer)-tekniikka eli verkon solmut pystyvät kommunikoimaan keskenään ilman erillistä ohjausyksikköä. Master-slave -verkko ja keskitetty ohjaus ovat myös mahdollisia. LonWork-järjestelmä perustuu Echelonin kehittämään ja ylläpitämään LonTalk–protokollaan, joka määrittelee OSI-mallin kaikki seitsemän kerrosta. Protokolla mahdollistaa myös kommunikoinnin IP-verkon kautta. LonWorks on verkkotopologialtaan vapaa, ja myös siirtotie on vapaasti valittavissa. Siihen voi käyttää standardoitua kierrettyä parikaapelia tai sähköverkkoa kuten myös radiotaajuuksia, infrapunaa, koaksiaali- tai optista kaapelia. [9; 39; 40].

LonWorks-teknologian etuja ovat mahdollisuus integroitumiseen ja avoimuus kaikille. Myös vapaa verkkotopologisuus, muunneltavuus ja laajennettavuus ovat LonWorks:n hyviä puolia. LonWorks–verkon konfigurointi on kuitenkin usein hyvin monimutkaista. LonWorks teknologiaa käytetään rakennusautomaation lisäksi muun muassa prosessiautomaatiossa, kulkuneuvoissa, mittareiden etäluennassa. Sovelluskohteita ovat HVAC-, hissi-, valaisu-, turvallisuus-, bussi-, ja metrojärjestelmät sekä katuvalaisu. [39; 40].

3.2.4 ModBus

ModBus on nykyisen Schneider Electricin, silloisen Modiconin vuonna 1979 julkaisema avoin sarjaliikenneprotokolla. ModBus on täysin avoin ja lisenssimaksuton protokolla, jota hallinnoi ja kehittää ModBus Organization. Avoimuutensa ja yksinkertaisuutensa takia ModBus:sta on tullut de facto -standardi teollisuudessa. [42].

ModBus protokolla toimii master-slave -periaatteella, ja se määrittelee OSI-mallista fyysisen, siirto- ja sovelluskerroksen. ModBus on kuitenkin sovelluskerroksen viestintäprotokolla, koska fyysinen ja siirtokerros voidaan toteuttaa monella eri tavalla, langallisesti tai langattomasti. Langallisia vaihtoehtoja on muun muassa sarjaväylä tai Ethernet. Monet modeemit ja yhdyskäytävät tukevat ModBusia ja langattomasti yhteys voidaan toteuttaa ISM-taajuusalueen, SMS:n tai GPRS:n avulla. [41; 42].

ModBusin vahvuudet piilevät yksinkertaisuudessa ja datan siirron mahdollisuudessa eri valmistajien välillä yhdistettynä avoimuuteen ja lisenssimaksuttomuuteen. Huonoina puolina isäntä-orja -periaate aiheuttaa sen, ettei orjalaite pysty raportoimaan poikkeustilanteesta, josta johtuen isäntälaite joutuu kyselemään tietoja orjalaitteilta säännöllises-

ti, mikä taas vie paljon kapasiteettia. Lisäksi ModBusin on rajoitettu 254 laitteeseen väylää kohti eikä ModBusissa itsessään ole tietoturvaa.

ModBus kehitettiin teollisuuteen, jossa sitä käytetään paljon elektroniikkalaitteiden väliseen kommunikointiin, mutta nykyään se on yleisesti käytössä myös rakennusautomaatiossa ja energianmittaussovelluksissa. [42].

4 Protokollien vertailu

Jotta saataisiin laajempi kuva protokollista, niin tässä luvussa syvennytään protokolliin vertailun muodossa. Luku antaa myös uutta tietoa protokollista ja selittää teoriat teknisten tietojen taustalta.

4.1 Protokollien käyttökohteet

Edellisessä luvussa esitellyt langattomat, lyhyen kantaman protokollat voidaan jaotella sovelluskohteidensa perusteella. Tämä kartoitus nähdään seuraavalla sivulla taulukossa 1. Taulukossa on jätetty huomioimatta, jos protokollalla on vain pari sovellusta kyseisellä sovellusalueella. Merkinnän saaminen tarkoittaa siis, että kyseinen protokolla on onnistunut jo lyömään läpi kyseinen alan markkinoilla.

Älylaitteet tarkoittavat sovelluksia, missä antureita käytetään datan lähettämiseen vastaanottimelle, kuten sykemittari. Myös sovellukset, joissa käytetään tageja, joiden avulla käyttäjä voi esimerkiksi ostaa palveluja tai saada kulkuoikeuksia, kuuluvat tähän kategoriaan. Julkisen liikenteen matkakortit ovat hyvä esimerkki tästä. Rakennusautomaatiosta on eroteltu kiinteistöautomaatio parista syystä, vaikka sovelluskohteet ovat hyvin samanlaiset. Kiinteistöautomaatiolla tarkoitetaan asuntoja ja pieniä kaupallisia rakennuksia, joissa yhdistetään ja automatisoidaan erilaisten laitteiden toimintoja. Rakennusautomaatiolla taas tarkoitetaan suuria kaupallisia rakennuksia, toimistoja ja teollisuusrakennuksia. Rakennusten koko ja käyttötarkoituksen eroavaisuus kiinteistö- ja rakennusautomaation välillä johtaa erilaisiin vaatimuksiin samoiltakin sovelluksilta. Esimerkkeinä sovelluskohteista ovat HVAC-, turvallisuus-, ja valaisujärjestelmät. Protokollia käytetään autoteollisuudessa muun muassa rengaspaineiden seurantaan ja navigointiin. Aseteollisuudesta puhuttaessa puhutaan armeijoiden käyttötarpeista ja rä-

jähdysvaarallisista tiloista. Muu teollisuus kattaa kaiken muun, muun muassa prosessiteollisuuden ja liikennejärjestelmät. Yksityiskohtaisemmin protokollien käyttökohteista voit lukea edellisestä luvusta ja liitteestä 1 näkee suuremman variaation mahdollisista käyttökohteista.

Taulukko 1. Protokollien käyttökohteet

Protokolla	Älylaitteet	Kiinteistöautomaatio	Rakennusautomaatio	Autoteollisuus	Aseteollisuus	Muu teollisuus
ZigBee	√	√	√			√
Z-Wave		√				
Insteon		√				
Bluetooth	√			√		√
ANT	√					
ONE-NET		√				
EnOcean		√				
IEEE 802.11x	√	√	√	√		√
DASH7			√	√	√	
RuBee	√		√		√	
NFC	√					
KNX		√	√			
BACnet		√	√			
LonWorks		√	√			√
ModBus			√			√

Taulukkoa lukiessa tulee ottaa huomioon, että taulukon neljä viimeistä protokollaa (KNX, BACnet, LonWorks, ModBus) eivät ole langattoman verkon protokollia, vaan tarjoavat langallisten lisäksi langattomia vaihtoehtoja kommunikoimiseen. Taulukosta huomaa, että suurin osa protokollista on käytössä ainakin kiinteistöautomaatiossa ja/tai rakennusautomaatiossa. Tätä selittää se, että suurin osa näistä on kehitetty alun perin

juuri näille aloille, joista osa on laajentanut käytettävyyttä myös muihin aloihin. Osittain myös tästä syystä kiinteistö- ja rakennusautomaatiossa ollaan myös ”pidemmällä” M2M-kommunikoimisesssa. Näillä aloilla löytyy jo paljon enemmän valmiita kaupallisia sovelluksia.

IoT:lle ja M2M kommunikoinnille olisi parempi, jos jotain protokollaa pystyttäisiin käyttämään langattomaan kommunikoimiseen kaikkialla. Integraatio helpottuisi, ja komponentit halpenisivat, jos olisi hallitseva protokolla, koska tällöin tuotteita kehitettäisiin yhteentoimivammiksi. Tässä voidaan taulukon perusteella pitää ZigBeetä ja IEEE 802.11x:ä (WLAN) edelläkävijöinä, koska ne ovat käytössä jo laajalla saralla. Ne olisivat siis tältä kantilta katsottuna lähtökohtaisesti helpompi saada universaaliksi protokollaksi IoT:lle ja M2M:lle.

4.2 Tietoliikenne

Kansainvälinen standardointiorganisaatio ISO (International Organization for Standardization) kehitti 1980-luvun alussa seitsenkerroksisen pinomallin (Kuva3), jonka ideana on tarjota laitevalmistajille yhteinen rajapinta, jotta laitteistot kykenisivät kommunikoimaan lähiverkossa sujuvasti keskenään ja yhteensopivuus ongelmia eri verkoissa ei olisi. OSI-viitemalli (Kuva 3) on käsitteellisesti ehjä, mutta käytännön protokollapinoja sen mukaisesti kuitenkaan ei ole juuri kehitetty. OSI-malli muodostuu seitsemästä kerroksesta, joiden varaan tiedon välitys muodostuu. Kukin kerroksista käyttää yhtä alemman kerroksen palveluja ja tarjoaa palveluja seuraavalle kerrokselle. Jokainen kerros on myös yhteydessä vastaavaan kerrokseen mahdollisessa etäpäässä ja on itsenäinen kokonaisuutensa, jota voidaan kehitellä muista osista riippumatta. [43].

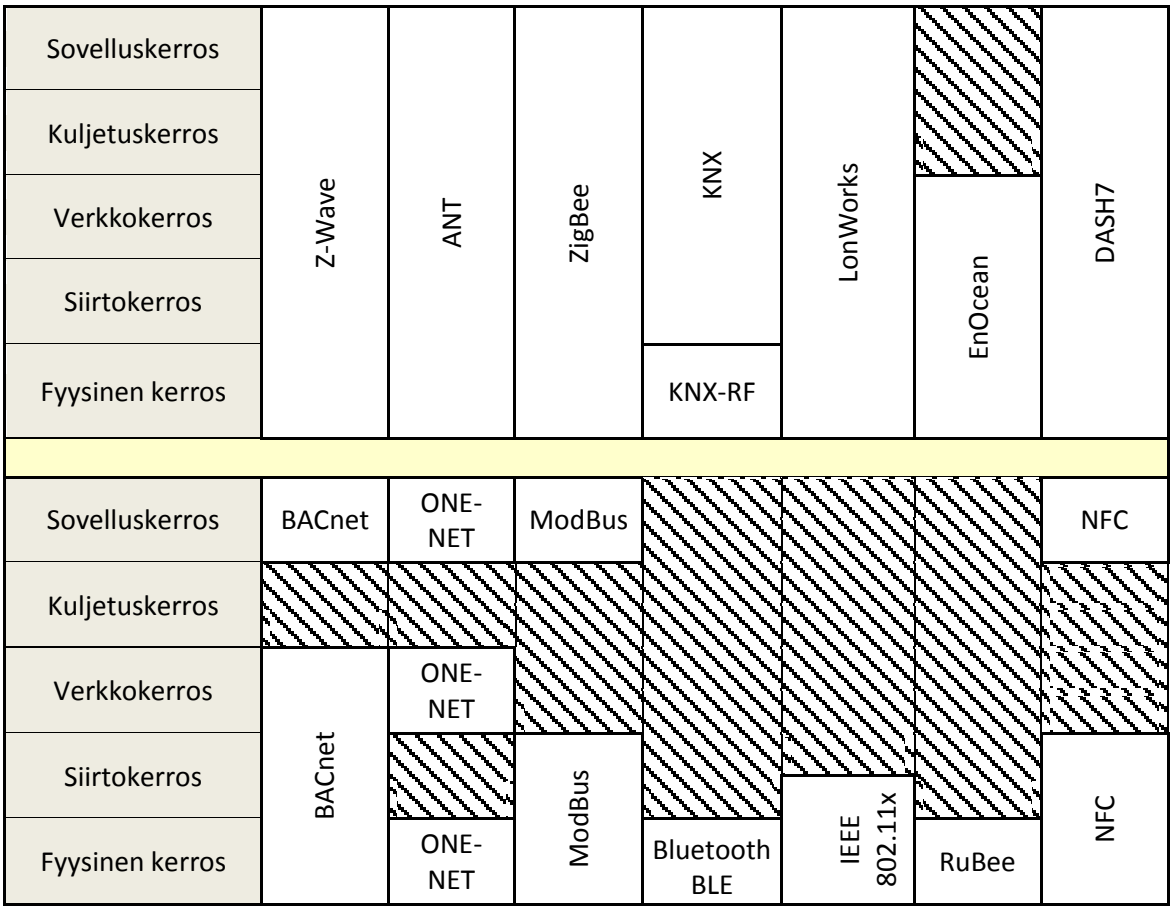
Kuva 3. OSI-malli [43].

Lyhyesti kerrosten tehtävät ovat:

- Fyysinen kerros määrittelee tiedonsiirron fyysisen liitynnän.
- Siirtokerros hoitaa yhteyden luomisen ja purkamisen.
- Verkkokerros välittää ylempien kerrosten tietoliikennettä verkon rakenteesta riippumatta.
- Kuljetuskerros takaa luotettavan päästä-päähän yhteyden verkkolaitteiden välillä.
- Istuntokerros huolehtii lähetyksen käynnistyksestä ja pysäyttämisestä.
- Esitystapakerros päättää, missä muodossa lähetettävä tieto esitetään.
- Sovelluskerros toimii linkkinä ohjelmaan, joka tarvitsee tiedonsiirtoa.

Taulukossa 2 nähdään muunneltu malli OSI-mallista työssä käsitellyistä protokollista. Taulukko on suuntaa-antava, koska kaikki patentoidut protokollat eivät paljasta tarkkaan, mitkä kerrokset protokolla toteuttaa. Taulukko ja malli on siis tehty parhaan käsityksen pohjalta. Sovellus-, esitystapa- ja istuntokerros on yhdistetty yhdeksi kerrokseksi. Tämä sen takia, että IoT-sovellus voi mahdollisesti itse pitää huolen istuntojen muodostamisesta ja purkamisesta samoin kuin tarvittavista tiedon esitystavan muutoksista. Erillisiä kerroksia ei välttämättä tarvita.

Taulukko 2. Langattomat, lyhyen kantaman protokollat



Taulukko 2 antaa kuvan siitä, kuinka pitkälle tietoliikenteen kulku on määritelty protokollassa. Käytännössä tämä tarkoittaa sitä, että pystyykö protokolla toteuttamaan tietoliikenteen fyysisestä liitännästä sovelluskerroksen ohjelmaan kokonaisuudessaan itse. Tämä ei kuitenkaan IoT:ta ja M2M kommunikointia ajatellessa välttämättä tuo etulyöntiasemaa, mikä nähdään IEEE 802.11x protokollien suosiossa, joka määrittelee itse vain fyysisen kerroksen ja siirtokerroksen alemman MAC-kerroksen. Ylempien kerrosten tietoliikenne jää muitten tehtäviksi.

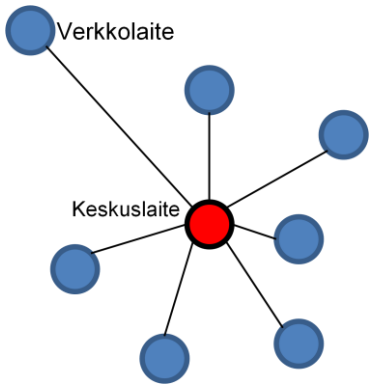
4.3 Tekniset ominaisuudet

Jotta langattomien protokollien eroavaisuudet tulisivat vielä konkreettisemmin näkyviin, niin taulukossa 3, 4 ja 5 on protokollien teknisiä ominaisuuksia. BACnet, LonWorks ja ModBus on jätetty taulukoista pois, koska ne eivät ole pelkästään lyhyen kantaman langattomia protokollia ja näin niiden tekniset tiedot eivät ole suoraan vertailukelpoisia muiden kanssa. KNX protokollan tekniset tiedot koskevat vain radiotaajuuksilla toimivaa KNX-RF:ä.

4.3.1 Verkkotopologiat ja maksimilaitemäärä

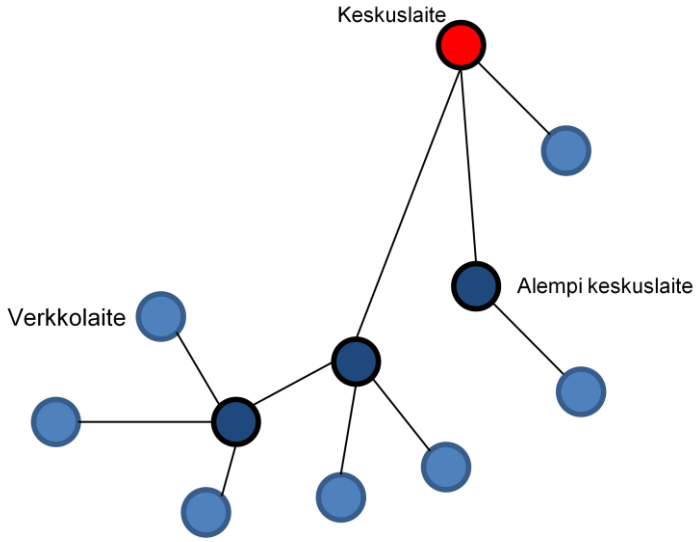
Taulukossa 3 käsitellään, mitä verkkotopologioita protokolla tukee ja kuinka monta laitetta voidaan kytkeä yhteen verkkoon. Neljä yleisintä topologiaa on selitetty alla, ja muiden topologioiden rakenteet on luettavissa edellisestä luvusta kyseisen protokollan kohdalla.

Star-topologiassa (Kuva 4) on keskuslaite, johon verkkolaitteet on kytketty. Verkon kaikki tietoliikenne kulkee keskuspisteen kautta. Yhden verkkolaitteen yhteyden katkeaminen vaikuttaa ainoastaan kyseiseen yhteyteen, mutta keskuslaitteen hajoaminen heijastuu koko verkkoon. Kytkettyjen laitteiden asennus ja ylläpito on helppoa. Hyvinä puolina voidaan pitää joustavuutta ja kaapeloinnin selkeyttä. Haittapuolina ovat kaapeloinnin kustannukset ja keskuslaiteen vioittuminen lamauttaa koko verkon. Keskuslaite on myös kovan tietoliikennekuormituksen kohteena, kun kaikki tietoliikenne kulkee sen kautta. [44].



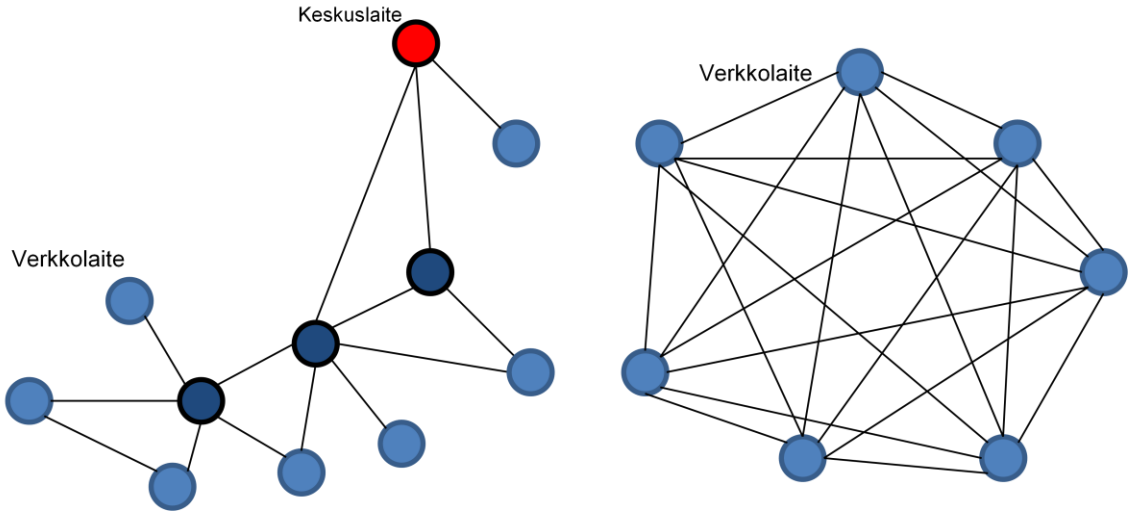
Kuva 4. Star-topologia

Tree-topologiassa (Kuva 5) on ylimpänä keskuslaite, johon on kytketty verkkolaitteita. Osa verkkolaitteista voi toimia keskuslaitteena alemmille verkkolaitteille muodostaen star-topologian tyylisen rakenteen, jossa verkkolaitteet voivat kommunikoida suoraan vain keskuslaitteensa kanssa. Alempi keskuslaite voi kommunikoida suoraan vain alapuolella olevien verkkolaitteidensa ja oman keskuslaitteensa kanssa. Jos siis esimerkiksi verkkolaite haluaa kommunikoida toisen verkkolaitteen kanssa, niin viesti kulkee ensimmäiseksi topologiassa ylöspäin niin kauan, että saapuu yhteiselle alemmalle keskuslaitteelle tai keskuslaitteelle, joka välittää viestin alaspäin halutulle verkkolaitteelle. Tree-topologiaa on helppo laajentaa ja yhden yhteyden katkeaminen ei lamauta koko verkkoa. Tosin keskuslaitteen vioittuminen taas voi lamauttaa koko verkon. Verkon hallinta on myös monimutkaista. [44].



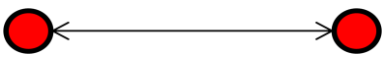
Kuva 5. Tree-topologia

Mesh-topologioissa (Kuva 6) tietoliikenne on paljon vapaampaa. Osittain kytketyssä Mesh-topologiassa osa verkkolaitteista voi olla suoraan yhteydessä muihin verkkolaitteisiin ilman viestin kulkua yhteisen keskuslaitteen tai alemman keskuslaitteen kautta. Mesh-topologinen verkko voi olla myös täydellisesti kytketty, jolloin kaikki ovat suorassa yhteydessä toisiinsa. Viestien eteneminen on Mesh-topologioissa nopeampaa ja varmempaa vaihtoehtoisten reittien takia. Multi-hop:t ovat hyvin samanlaisia osittain kytketyn Mesh-topologisen verkon kanssa. Mesh-verkot ovat hyvin vikasietoisia ja luotettavia. Yhden laitteen hajoaminen ei välttämättä vaikuta ollenkaan muun verkon toimintaa. Huonoina puolina ovat kallis hinta ja huono hallittavuus, koska Mesh-verkon hallinta on monimutkaista. [44].



Kuva 6. Osittain ja täydellisesti kytketty Mesh-topologinen verkko

P2P(Peer-to-Peer):ssa eli vertaisverkossa (Kuva 7) ei ole kiinteitä keskuslaitteita tai verkkolaitteita, vaan jokainen verkkoon kytketty laite toimii sekä isäntänä että orjana muille kytketyille laitteille. P2P-verkko on helppo asentaa ja toteuttaa. P2P-verkot ovat myös hyvin vikasietoisia, mutta verkon laitemäärän kasvaessa verkon hallinta muuttuu monimutkaiseksi. [45].



Kuva 7. P2P

Verkkotopologian valinta riippuu aina käyttötarkoituksesta, täydellisesti kytketty Mesh-verkko tai P2P ei ole aina paras valinta. Sen takia usean verkkotopologian tukeminen lisää joustavuutta ja käyttömahdollisuuksia.

Taulukko 3. Lyhyen kantaman, langattomien protokollien verkkotopologia ja maksimi laitemäärä

Protokolla	Verkkotopologia	Maksimi laitemäärä
ZigBee	Tree, Star, Mesh, P2P	63 536
Z-Wave	Mesh	232+sillat
Insteon	Mesh, P2P	2^24
Bluetooth	Star-Bus(BLE), PPP, Piconet, Scatternet	65 536
ANT	Tree, Star, Mesh, P2P	65 533
ONE-NET	Star, Mesh(multi-hop), P2P	4 096
EnOcean	Star, Mesh	>4000
IEEE 802.11x	Ad Hoc, Star, Mesh(11s)	2^32
DASH7	Multi-hop(2), Tag to Tag	2^32
NFC	P2P	-
RuBee	P2P	-
KNX-RF	Tree(Multi-hop)	64

Maksimilaitemäärä näkyy myös taulukossa 3 eli se kuinka monta laitetta voidaan liittää yhteen verkkoon. Tästä voimme päätellä, kuinka monimutkaisia järjestelmiä protokollalla voi tehdä ilman, että verkon suorituskyky kärsii. Näemme muun muassa sen, että KNX-RF on tarkoitettu yhdeksi osaksi suurempaa järjestelmää, ja että Z-Wave soveltuu hyvin vain pieniin järjestelmiin. Muissa sen sijaan jo yhteen verkkoon saa vähintään 4 000 laitetta. RuBee ja NFC verkon maksimilaitemäärää ei ole tiedossa. Ne ovat kuitenkin pääasiassa vain ”tagaukseen” käytettäviä protokollia, jolloin yhden verkon samanaikaisten laitteiden määrä ei välttämättä nouse kovin suureksi.

4.3.2 Taajuudet, tiedonsiirtonopeus ja kantama

Protokollien taajuudet Euroopassa on nähtävillä taulukossa 4. Taajuudella on merkitystä yhteyden ominaisuuksiin. Korkeammalla taajuudella on mahdollista saavuttaa suurempi tiedonsiirtonopeus pienemmillä antenneilla. Korkeat taajuudet kuitenkin läpäisevät esteitä huonommin. Vastaavasti matalien taajuuksien etuna on parempi esteenläpäisykyky, kuitenkin lähtökohtaisesti hitaammalla tiedonsiirrolla ja isokokoisilla antenneilla.

Työssä käsitellyt taajuudet käyttävät kolmea poikkeusta lukuun ottamatta UHF-radiotaajuuksia (Ultra High Frequency). IEEE802.11x protokolla toimii myös SHF-alueella (Super High Frequency), Rubee käyttää LF-aaltoja (Low Frequency) ja NFC

taas HF-aaltoja (High Frequency). UHF-aallot toimivat 0,3-3GHz alueella ja niiden aallonpituus on 10cm – 1m. UHF-alueella radioaallot etenevät suoran etenemisen mukaan ja yhteyden on oltava lähes näköyhteys antennista toiseen. UHF- ja SHF-alueella on myös ISM-taajusalue (Industrial, Scientific and Medical), joka on maailmanlaajuinen radiotaajuuskaista, jonka käyttö ei vaadi erillistä lupaa. 433MHz, 2,4GHz ja 2,46GHz kuuluvat näihin ISM-radiokaistoihin. SHF-alueella(3-30GHz) aallonpituus on 1-10cm. Radioaallot etenevät suoran etenemisen mukaan ja antennien välillä on oltava näköyhteys. LF-aaltojen(30-300kHz) aallonpituus on 1-10km ja ne etenevät pinta-aaltona. HF-aallot(3-30MHz) etenevät myös pinta-aaltona ja niiden aallonpituus on 10-100m. [46].

Taulukko 4. Protokollien taajuus, kantama ja tiedonsiirtonopeus

Protokolla	Taajuus Eurooppa	Tiedonsiirtonopeus	Kantama	
			sisätiloissa	ulkona
ZigBee	868MHz, 2,46GHz	≤250kbps	<100m	
Z-Wave	868MHz	≤100kbps	<100m	
Insteon	868MHz	≤13,165kbps	-	<45m
Bluetooth	2,4GHz	≤3Mbps	<10m	<100m, <50m(BLE)
ANT	2,4GHz	≤60kbps	<30m	
ONE-NET	868MHz	≤65,535kbps	<60m	<500m
EnOcean	868MHz	≤125kbps	<30m	<300m
IEEE 802.11x	2,4GHz, 3,6GHz, 5GHz	≤54Mbps(g)	<200m(2,4GHz)	
DASH7	433MHz	≤200kbps	<10m	<10 000m
RuBee	131kHz	≤1200baud(1,2kbps)	<15m(volumetrinen)	
NFC	13,56Mhz	≤424kbps	<0,1m	
KNX-RF	868MHz	≤32,768kbps	<150m	

Taulukossa 4 näkyvät tiedonsiirtonopeudet eli kuinka monta bittiä sekunnissa protokollat mahdollistavat maksimissaan siirtämään verkon laitteiden välillä. Taulukossa 4 esiintyvät kantamilla taas tarkoitetaan laitteiden välisen langattoman tiedonsiirron maksimietäisyyttä. Kantamaan vaikuttaa tiedonsiirrossa käytettävä lähetysteho, vastaanottimen herkkyys sekä antennin tyyppi. Kantamat eli kuuluvuusalueet on ilmoitettu näköyhteyksinä eli esteettöminä yhteyksinä antennien välillä pois lukien Rubee. Rubee:n kantama on volumetrinen, koska sen lähettämät 3D-volumetriset magneettiaallot läpäisevät metalleja kuten terästä sekä vettä. Osa protokollista on ilmoittanut kantamansa sisätiloissa ja ulkona erikseen, kun taas osasta on ilmoitettu vain yksi pituus.

4.3.3 Yhteentoimivuus

Yhteentoimivuus muitten protokollien kanssa lisää protokollan joustavuutta, ja helpottaa protokollan leviämistä kaikkialle. On suuri etu protokollalle, jos se pystyy integroitumaan muitten protokollien kanssa ilman suurempaa vaivaa. Tämä ja se, onko protokollassa määritelty valmiiksi Internetin yhdyskäytävän asetukset, ovat merkittäviä asioita IoT:ta ajatellen. Tällöin ollaan jo hieman lähempänä M2M-kommunikointia ja IoT:ta. Nämä tiedot näkyvät siis Taulukossa 5.

Taulukko 5. Protokollien yhteentoimivuus ja yhdyskäytävä spesifikaatiot

Protokolla	Yhteentoimivuus muitten protokollien kanssa	Internet gateway spesifikaatio
ZigBee	GRIP protokollan/CAP:n kautta	ON
Z-Wave	Ei	ON
Insteon	X10	ON
Bluetooth	useita protokollia päällä	-
ANT	Ei	EI
ONE-NET	avoin lähdekoodi	ON
EnOcean	EI	ON
IEEE 802.11x	useita protokollia päällä	-
DASH7	avoin lähdekoodi	ON
RuBee	useita protokollia päällä	-
NFC	useita protokollia	ON
KNX-RF	useita protokollia	ON

Taulukosta nähdään, että Z-Wave ja ANT ovat tästä näkökulmasta katsottuna kauimpana IoT:sta tällä hetkellä. EnOcean tukee yhteen toimivuutta muiden automaattijärjestelmien kanssa, mutta vain langallisena yhteytenä nykyisellään. Useilla protokollilla on siis jo vähintäänkin lähtökohdat IoT:lle ja M2M-kommunikoinnille.

4.4 Pitkän kantaman protokollat

Miksi edes käyttää lyhyen kantaman protokollia, kun pitkän kantaman protokollilla voitaisiin hoitaa koko kommunikointi? Siihen kysymykseen paneudutaan tässä kappaleessa. Monet pitkän kantaman M2M-sovellukset pohjautuvat neljä kerroksiseen TCP/IP-malliin, jossa OSI-mallin kolme ylintä kerrosta on yhdistetty pelkäksi sovelluskerrokseksi, joka hoitaa kolmen ylimmän kerroksen tehtävät. OSI-mallin kaksi alinta kerrosta on yhdistetty taas fyysiseksi kerrokseksi, joka johtuu siitä, ettei TCP/IP-malli määritä tark-

kaan, mitä tapahtuu verkkokerroksen alapuolella. Taulukossa 6 on nähtävillä, kuinka pitkän kantaman protokollat mallintuvat. [43].

Taulukko 6. Pitkän kantaman langattomat protokollat

Sovelluskerros	HTTP		
Kuljetuskerros	UDP		TCP
Verkkokerros	IPv6		IPv4
Fyysinen kerros	2G , 3G, 4G	LTE	White Space Technologies

IoT:n saralla huomataan muutamia haittoja pitkän kantaman teknologioissa verrattuna lyhyen kantaman teknologioihin (Taulukko 7). Suurin haitta on kova hinta, yli kaksinkertainen verrattuna lyhyen kantaman teknologioihin. Lisenssin alaiset taajuudet eivät myöskään ole suuri houkutin kuin isoille yrityksille. Tiedonsiirrossa pitkän kantaman teknologiat yleisesti pärjäävät paremmin, mutta eräät IEEE802.11x alaiset standardit pystyvät jopa peittoamaan pitkän kantaman teknologiat tiedonsiirtonopeudessa. Energiatehokkuus jätettiin pois taulukosta sen suuren vaihtelevuuden takia, mutta myös tässä lyhyen kantaman teknologiat suoriutuvat paljon paremmin. [47].

Taulukko 7. Lyhyen kantaman vs. Pitkän kantaman teknologiat [47].

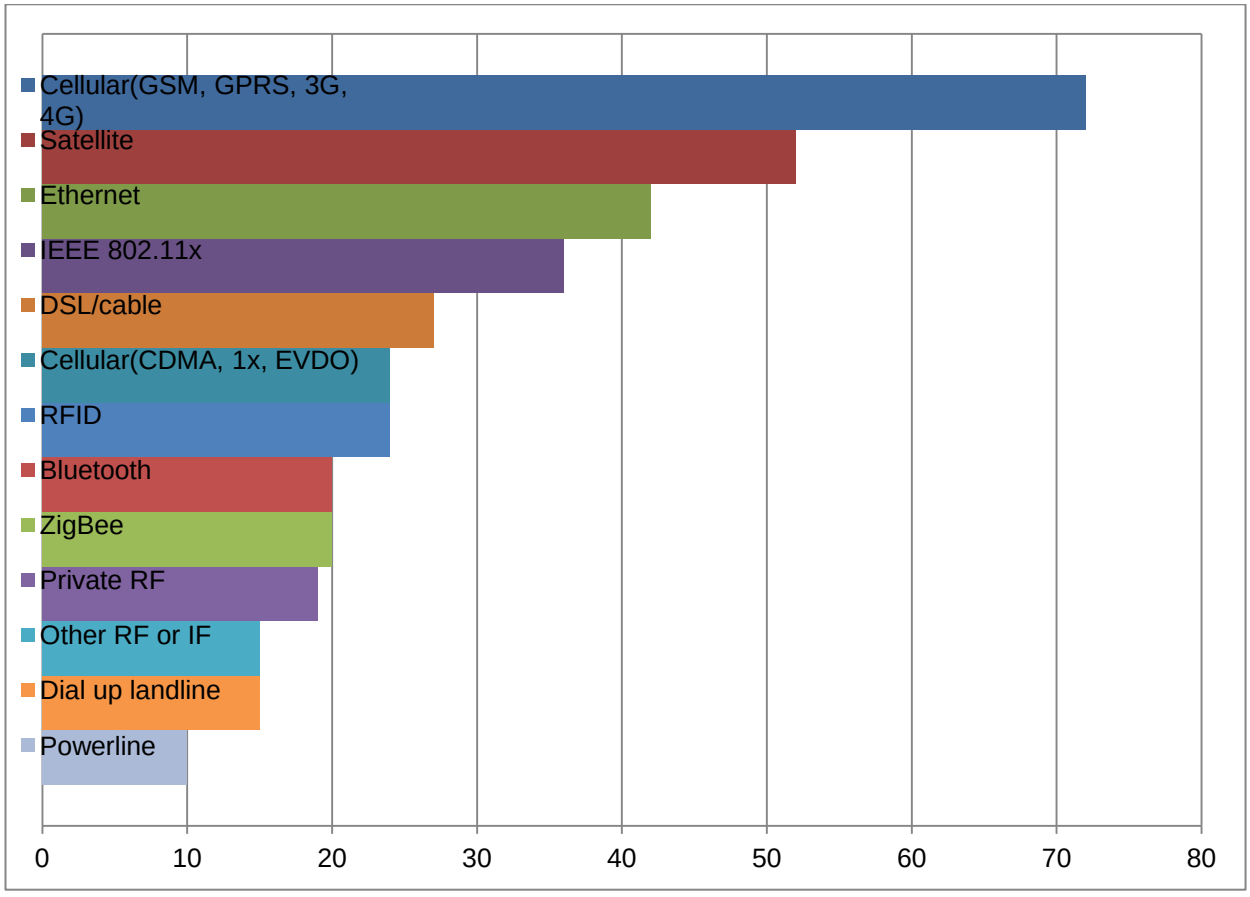
	PAN/LAN	WAN
Standardeja	IEEE 802.11X, ZigBee, Bluetooth	GPRS/GSM, WCDMA, LTE, WiMAX
Tiedonsiirtonopeus	ZigBee≤250kbps Bluetooth≤3Mbps IEEE802.11x≤54Mbps(b/g)	LTE≤100Mbps WDCMA 1-14Mbps, WiMAX≤75Mbps
Hinta	<5$	≥10$
Taajuudet	Ei lisensoitu	Lisenssin alla

Hinta on suurin haitta energiatehokkuuden kanssa pitkien kantamien teknologioiden käytössä M2M-sovelluksissa, ja sen takia suuryrityksiä tutkii koko ajan ratkaisua tälle ongelmalla. Hinnan reilu alentuminen nostaisi pitkän kantaman protokollat yleisesti kannattavammaksi valinnaksi IoT:lle sekakäytön tai pelkän lyhyen kantamien protokollien käytön sijaan. Tällä hetkellä uskotaan, että kummankin käyttö tulee yleistymään

M2M-sovelluksissa, mutta lyhyen kantaman teknologiat vievät kuitenkin suuremman osuuden.[7; 47].

4.5 Teknologioiden käyttö

Beecham Research:n teettämän tutkimuksen avulla saadaan karkea kuva, kuinka lyhyen kantaman ja pitkän kantaman teknologiat ovat käytössä IoT sovelluksissa tällä hetkellä. Tutkimuksessa kysyttiin M2M-kommunikointiteknologian käyttöönottajilta tiedonsiirtotekniikan valitsemista omiin M2M-ratkaisuihin. Tutkimuksen tuloksena nähdään kaaviossa 1, kuinka paljon eri teknologioita on käytetty M2M-ratkaisuihin. Yleisesti käytetyimpiä olivat matkapuhelinverkot, satelliittiyhteydet, Ethernet ja IEEE 802.11x standardit.



Kaavio 1. Kommunikointiteknologia M2M-ratkaisuihin[48]

Tutkimus on muutaman vuoden vanha, joten se on vain suuntaa-antava. Muutaman vuoden aikana muun muassa lyhyen kantaman ratkaisut ovat lisääntyneet ja satelliitti ja Ethernet yhteydet vähentyneet suhteessa muihin. Kaaviosta nähdään kuitenkin, että

tällä hetkellä käytetään sekä lyhyen että pitkän kantaman teknologioita M2M-ratkaisuissa, ja näin välillisesti myös IoT:ssa.

5 Päätelmät ja yhteenveto

Tässä insinöörityössä perehdyttiin Internet-of-Thingsiin ja pääasiallisesti sen yhteen toimialaan (M2M), jossa uusia ratkaisuja ja käyttömahdollisuuksia tutkitaan koko ajan lisää. Keskityttiin langattomiin, lyhyen kantaman protokolliin, koska näiden uskotaan yleistyvän vuosien saatossa. Tarkoituksena oli käydä läpi mahdollisesti IoT:lle ja M2M-kommunikointiin soveltuvia tietoliikenneverkkoja ja vertailla niitä keskenään. Työssä pyrittiin löytämään yksityiskohtia, jotka tukisivat protokollan soveltuvuutta IoT:lle tai päinvastoin tällä hetkellä hankaloittaisivat sitä. Lisäksi pyrittiin antamaan selkeä yleiskuva käsitellyistä protokollista.

IoT on vasta alkutaipaleellaan, ja tämä huomattiin työn alkuvaiheilla. IoT:lle ei löydy yhtenäistä määritelmää ja IoT:lle on olemassa vain hajanaisia ratkaisuja siellä täällä, eikä minkäänlaista viitekehystä arkkitehtuurin rakentamiselle. On vain useita ratkaisuja useilta eri tahoilta eikä kaikkia ole edes mahdollista saada käsiinsä. Huomattiin, että suuret yritykset tutkivat isolla budjetilla IoT:ta ja M2M:a, ja näin suuret osat niitä koskevista raporteistakin, niistä mitkä olisivat saatavilla, olisivat maksaneet useita tuhansia dollareita.

Protokollista löytyi hyvin tietoa, kunhan jaksoi etsiä hartaasti ja tarkkaan. Tässä täytyi kuitenkin olla tarkka, koska melkein kaikki käsitellyt protokollat ovat kehittyneet paljon lähivuosina, joten jo vuodenkin takainen tieto saattoi olla vanhentunutta. Monet protokollat kuten ZigBee tekevätkin koko ajan työtä pysyäkseen kehityksen mukana, ja että onnistuisivat valtaamaan lisää markkinoita itselleen.

Vertailun valmistuttua tultiin siihen lopputulokseen, mitä jo loppuvaiheella uumoiltiin. Kun ei ole mitään tiettyä pohjaa IoT:lle, ja tätä vasten tiettyjä vaatimuksia protokollilta, on hyvin vaikeaa sanoa sen suuremmin protokollien soveltuvuudesta. Tämän takia niiden soveltuvuutta käsiteltiin vain eri aspekteista. Lisäksi ainakaan tällä hetkellä ei ole mitään protokollaa, joka tuntuisi olevan hyvä vaihtoehto aina, vaan ympäristö, sovellus ja muut erilaiset vaatimukset määrittelevät mitä protokollaa kannattaa käyttää. Hallitseva protokolla tekisi hyvää IoT:lle ja M2M:lle.

Jos jotain soveltuvuudesta pystyy sanomaan, niin lyhyen kantaman langattomista protokollista IEEE 802.11x-protokollilla tuntui olevan parhaimmat edellytykset IoT- ja M2M-kommunikointiin. Niiden tiedonsiirtonopeus on korkea muihin verrattuna, markkinaosuus on suuri ja se ulottuu usealla alalla. Kysymysmerkkinä ovat kenties liika teknisyys ja akun kesto. Toinen ehkäpä muita valmiimpi on ZigBee, joka painii eniten Internet-yhteensopivuuksien kanssa, mutta tekee koko ajan tutkimustyötä tämän selvittämiseksi. Sitten on omalla osa-alueellaan hyvin menestyvät kuten NFC ja tagaussovellukset.

Pääpiirteittäin voidaan sanoa, että tarvittaisiin laajempi tutkimus, jotta saataisiin protokollien soveltuvuudet koskien IoT:ta ja M2M-kommunikointia paremmin esille. Tämä insinöörityö kuitenkin ottaa ensiaskeleet kyseiseen aiheeseen ja antaa pohjan uutta tutkimusta varten.

Lähteet

1 Mazhelis, Oleksiy & Warma, Henna. 2013. Internet-of-Things Market, Value Networks, and Business Models: State of Art Report. s. 9-12, 30-43.

2 Atzori, Luigi & Iera Antonio & Morabito Giacomo. 2010. Computer Networks 54, The Internet of Things: A Survey. s.2787-2805.

3 EPoSS. 2008. Internet of Things 2020: A Roadmap for the future.

4 Barnaghi, Payam & Wang, Wei & Taylor, Kerry. 2012. Semantics for the Internet of Things: early progress and back to future.

5 Frenzel, Lou. 2014. The Connected World Awaits. http://electronicdesign.com/communications/connected-world-awaits. Luettu 12.4.2014.

6 GSMA. 2014. The Mobile Economy 2014. http://www.gsmamobileeconomy.com/. Luettu 19.4.2014.

7 Machina Research. 2012. The Global M2M Market in 2013. http://www.telecomengine.com/sites/default/files/temp/CEBIT_M2M_WhitePaper_2012_01_11.pdf.

8 Beecham Research. 2009. M2M World of Connected Services, The Internet of Things. http://www.gsma.com/newsroom/wp-content/uploads/2012/04/internetofthingsm2mconnectedservicesbeechamresearch1.pdf.

9 Bui, Nicola. 2011. Internet of Things Architecture, IoT-A, Project deliverable D.1.1 – SOTA report on existing integration frameworks/architectures for WSN, RFID and other emerging IoT related Technologies.

10 ETSI. 2013. Machine-to-Machine communications (M2M); Functional architecture. http://www.etsi.org/deliver/etsi_ts/102600_102699/102690/02.01.01_60/ts_102690v020101p.pdf.

11 ZigBee Alliance. 2014. http://www.zigbee.org/Home.aspx. Luettu 3.1.2014.

12 Z-Wave Alliance. 2014. http://www.z-wavealliance.org/. Luettu 4.1.2014.

13 Z-Wave. 2014. http://www.z-wave.com/home. Luettu 4.1.2014.

14 Insteon. 2013. Whitepaper: Compared. http://www.insteon.com/pdf/insteoncompared.pdf.

15 Insteon. 2013. Whitepaper: The Details. http://www.insteon.com/pdf/insteondetails.pdf.

16 Insteon. 2014. https://www.insteon.com/. Luettu 17.1.2014.

17 Bluetooth SIG. 2014. http://www.bluetooth.com/Pages/Bluetooth-Home.aspx & https://www.bluetooth.org/en-us. Luettu 24.1.2014.

18 Tervakangas, Sallamaari. 2013. Bluetooth Low Energy–kehitysympäristö.

19 Dynastream Innovations Inc. 2014. http://www.thisisant.com/. Luettu 1.2.2014.

20 ANT. 2013. ANT Message Protocol and Usage.

21 Zaloker, Joseph & Arrow Electronics. 2014. ANT/ANT+.

22 ONE-NET. ONE-NET – wireless control for everyone.

23 EnOcean. 2014. http://www.enocean.com/en/home/. Luettu 8.2.2014.

24 EnOcean Alliance. 2014 http://www.enocean-alliance.org/en/home/. Luettu 8.2.2014.

25 EnOcean. 2011. EnOcean Technology – Energy Harvesting Wireless.

26 Bernardos, Carlos J & Soto, Ignacio & Banchs Albert. 2008. Medium Access Control in Wireless Networks: IEEE 802.11 Standards. s.235-253.

27 Berlind, David. 2013. Why WiFi Could Be Both a Blessing and Curse For The Internet of Things. http://blog.programmableweb.com/2013/08/30/why-wifi-could-be-both-a-blessing-and-a-curse-for-the-internet-of-things/#comments. Luettu 15.2.2014.

28 Rampanen, Jesse. 2010. Langaton lähiverkko ja IEEE-standardit.

29 DASH7. 2012. http://www.dash7.org/. Luettu 22.2.2014.

30 Hindawi. 2013. Research Article: Survey of the DASH7 Alliance Protocol for 433MHz Wireless Sensor Communication. https://dash7.memberclicks.net/assets/PDF/hindawi%20-%20oss.pdf.

31 Visible Assets. 2011. http://www.rubee.com/. Luettu 28.2.2014

32 Rubee. 2009. Rubee and RFID Differences. http://www.rubee.com/White-SEC/RuBee-SellingPoints-190208.pdf.

33 NFC Forum. 2014. http://nfc-forum.org/. Luettu 6.3.2014.

34 NFC lähiluku. 2014. http://nfc-tunniste.weebly.com/. Luettu 6.3.2014.

35 KNX Association. 2012. http://www.knx.org/knx-en/index.php. Luettu 12.3.2014.

36 Weinzierl, Thomas. 2006. KNX-RF, A new Standard for Wireless Networks within Buildings. http://www.weinzierl.de/download/references/KnxRf_WirelessConf_2006_10_18.pdf.

37 BACnet International. 2014. http://www.bacnetinternational.org/. Luettu 20.3.2014.

38 Kananen, Juha. 2010. BACnet-protokollan käyttö rakennusautomaatiossa.

39 Echelon Corporation. 2013. http://www.echelon.com/index.html. Luettu 22.3.2014.

40 Liminka, Jyri. 2011. Lonworks-kenttäväylän testauksen automatisointi.

41 Modbus Organization. 2014. http://www.modbus.org/. Luettu 29.3.2014.

42 Tikkanen, Jarkko. 2013. Modbus-integrointi rakennusautomaatiojärjestelmään.

43 krimaka.net. 2013. OSI ja TCP/IP -malli. http://www.krimaka.net/tietotekniikka/verkko-ja-ethernet/osi-ja-tcp-ip-mallit.html. Luettu 5.4.2013.

44 Wikipedia. 2014. Network Topology. http://en.wikipedia.org/wiki/Network_topology. Luettu 12.4.2013.

45 Wikipedia. 2014. Peer-to-Peer. http://en.wikipedia.org/wiki/Peer-to-peer. Luettu 12.4.2014.

46 Wikipedia. 2014. Radioaallot. http://fi.wikipedia.org/wiki/Radioaallot. Luettu 13.4.2014.

47 Morioka,Yuichi. 2012. Low Cost LTE for M2M Consumer Electronics, ETSI M2M Workshop 2012.

48 Duke-Woolley, Robin. 2012. Current State of the M2M Ecosystem, Beecham Research. http://www.telecomengine.com/sites/default/files/Welcome%20%26%20Keynote.pdf. Luettu 19.4.2014.

Liite 1. M2M ja IoT, käyttömahdollisuudet

[8]