TAMPEREEN TEKNILLINEN YLIOPISTO

Tero Vierimaa

Paikantaminen IoT:ssä

Kandidaatintyö

Tarkastaja: Yliopistonlehtori Erja Sipilä

TIIVISTELMÄ

TAMPEREEN TEKNILLINEN YLIOPISTO
Sähkötekniikan koulutusohjelma
Vierimaa, Tero: Paikantaminen IoT:ssä
Kandidaatintyö, 20 sivua
Heinäkuu 2018
Pääaine: Elektroniikka
Tarkastaja: Yliopistonlehtori Erja Sipilä
Avainsanat: iot, paikantaminen, gps, mobiiliverkot

Tämä työ käsittelee paikantamista esineiden internetissä. Työssä tarkastellaan esineiden internetiä itsessään, sekä sen vaikutusta muuhun yhteiskuntaan. Työssä esitellään muutamia paikannusmenetelmiä, jotka on jaettu sisä- ja ulkokäyttöön. Työn lopuksi vertaillaan erilaisia menetelmiä ja arvioidaan niiden soveltuvuutta erilaisiin olosuhteisiin. Tutkimus on tehty kirjallisuusselvityksenä.

Esineiden internet tarkoittaa kaikenlaisten laitteiden, anturien ja aktuaattorien, liittämistä internetiin ja niiden ohjaamista internetin yli. Paikantaminen on keskeinen osa esimerkiksi anturidatan hyödyntämisessä. Esineiden internetissä laitteet ohjaavat toisiaan joko suoraan tai palvelun välityksellä. Esineiden internet on erittäin laaja käsite ja sen alle lukeutuu paljon teknologioita ja konsepteja.

Paikannusdata voidaan sisällyttää metadatana periaatteessa minkä tahansa sensorin tai aktuaattorin dataan. Paikkatieto on usein myös tärkeä tieto fyysisiin laitteisiin liittyen. Monissa sovelluksissa paikannus voikin olla keskeinen osa itse tuotetta. Haasteina esineiden internetissä ovat esimerkiksi virrankulutus sekä langattomien verkkojen kaista ja monikäyttö.

ALKUSANAT

Haluan kiittää ohjaajaani Erja Sipilää työn ohjaamisesta sekä palautteesta, jota olen työstäni saanut. Haluan kiittää myös perhettäni ja ystäviäni, jotka ovat tukeneet paitsi työn kirjoittamisessa, myös koko opintojen ajan.

Tampereella, 31.7.2018
Tero Vierimaa

SISÄLLYS

LYHENTEET JA MERKINNÄT

A-GPS	Assisted Global Positioning System, Avustettu maailmanlaajuinen paikannusjärjestelmä
AOA	Angle of Arrival, Saapumiskulma
API	Application Programmin Interface, Ohjelmointirajapinta
AR	Augmented Reality, Lisätty todellisuus
B2B	Business to Business, Yritysmarkkinat
B2C	Business to Customer, Kuluttajamarkkinat
CDMA	Code Division Multiple Access, Koodijakoinen radiokanavan monikäyttö
COAP	Constrained Application Protocol, Rajoitettujen sovellusten protokolla
D2D	Device to Device, Laitteidenvälinen kommunikointi
GNSS	Global Navigation Satellite System, Maailmanlaajuinen naivointijärjestelmä
GPS	Global Positioning System, Maailmanlaajuinen paikannusjärjestelmä
HF	High Frequency, Korkeat taajuudet
HTTP	Hyper Text Transport Protocol, Hypermedian siirtoprotokolla
IoT	Internet of Things, Esineiden internet
IoV	Internet of Vehicles, Ajoneuvojen internet
LED	Light Emitting Diode, Valoa emittoiva diodi
LF	Low Frequency, Matalat taajuudet
LTE	Long-Term Evolution, 4G-mobiiliverkko
LPWAN	Low-Power Wide-Area Network,

	Pienikulutuksinen suuralueverkko
MAC	Medium Access Control, Kanavanpääsyhallinta
MIMO	Multiple Input Multiple Output, Radiokanavan kapasiteetin kasvattaminen hyödyntäen useita lähetin- ja vastaanotinantenneja sekä monitie-etenemistä
M2M	Machine to Machine, Koneidenvälinen kommunikointi
MQTT	Message Queying Telemetry Transport, Laitteiden välinen kommunikointiprotokolla
NB-IoT	Narrowband Internet of Things, 5G-verkkoihin suunniteltu kapeakaistainen verkkoliikenne
OFDM	Orthogonal Frequency Division Multiplexing, Ortogonaalinen taajuusjakoinen multipleksaus
PRS	Positioning Reference Signal, Paikannusreferenssisignaali
RFID	Radio Frequeny Identification, Radiotaajuuksinen identifiointi
RSS	Received Signal Strength, Signaalinvoimakkuus
SDMA	Space Division Multiple Access, Tilajakoinen radiokanavan monikäyttö
SSID	Service Set Identifier, Langattoman lähiverkon tunnus
TDOA	Time Difference of Arrival, Saapumisaikojen erotus
TOA	Time of Arrival, Saapumisaika
UHF	Ultra High Frequency, Erittäin korkeat taajuudet
VR	Virtual Reality, Virtuaalitodellisuus
WPAN	Wireless Personal Area Network, Langaton henkilökohtainen verkko
WLAN	Wireless Local Area Network, Langaton lähiverkko
WNAN	Wireless Neighborhood Area Network, Langaton alueverkko
WWAN	Wireless Wide-Area Network, Langaton suuralueverkko

1 JOHDANTO

Internet on muuttanut maailmaa paljon viimeisen 30 vuoden aikana. Nykyään puhutaankin paljon informaation keräämisestä, sen omistamisesta ja sen hyödyntämisestä. Yksi suurista mullistuksista tässä on esineiden internet (Internet of Things, IoT), jossa suuri määrä laitteita kerää erilaista dataa ja hyödyntää sitä jollain tavalla. Puhutaankin, että IoT:n ensimmäinen iteraatio on käynnissä juuri nyt. Myöhemmin todennäköisesti laitteiden lukumäärä kasvaa moninkertaisesti ja näin myös informaation määrä tulee kasvamaan. Tätä dataa voidaan myöhemmin hyödyntää erittäin moniin tarkoituksiin: dokumentointiin, analyyseihin sekä lopulta loppukäyttäjälle arvoa tuovaan palveluun. IoT mahdollistaa myös uudenlaisia ansaintalogiikoita uuden ja tarkemman tiedon myötä. Internet of Things on nimensä mukaisesti juuri laitteiden välistä kommunikointia, joka eroaa yleensä ihmisten välisestä kommunikaatiosta.

Tässä työssä keskitytään esineiden internetiin yleisesti ja lohkotasolla, paikantamiseen sekä sen toteutukseen IoT:ssä. Työhön on valittu muutamia yleisesti käytössä olevia paikantamisen menetelmiä sekä pari kehitteillä olevaa paikantamistekniikkaa. Työssä tarkasteltavat paikantamismenetelmät toimivat pääasiassa radioaaltojen avulla. Myös muihin antureihin perustuvia paikannusmenetelmiä on olemassa. Työssä pyritään vastaamaan kysymykseen millaisia paikantamisen menetelmiä on käytössä ja miksi.

Työn ensimmäisessä osassa tarkastellaan esineiden internetiä yleisesti, mistä se koostuu, mitä etuja sillä voidaan saavuttaa ja mikä sen merkitys on yhteiskunnalle. Työssä tarkastellaan myös liiketoiminta- ja ansaintamalleja IoT:n ympärillä. Toisessa osassa esitellään yleisimpiä käytössä olevia paikannusmenetelmiä sisä- ja ulkokäyttöön, sekä muutamia tutkittavana olevia paikannusmenetelmiä. Sisä- ja ulkotiloihin soveltuvat menetelmät on eroteltu toisistaan, sillä ne eroavat olosuhteiltaan toisistaan merkittävästi. Useat menetelmät toimivat molemmissa tilanteissa, mutta ovat silti vahvempia tai suunniteltuja jompaankumpaan.

2 IOT JA PAIKANTAMINEN

Esineiden internet on erittäin laaja konsepti, joka kattaa suuren määrän teknologioita ja pienempiä kokonaisuuksia. Tässä luvussa tarkastellaan IoT:tä yleisesti peruslohkoineen, paikannuksen merkitystä osana IoT:tä sekä IoT:n vaikutusta laajemmin yhteiskunnassa.

2.1 IoT yleisesti

Internetin tuoma hyöty on informaation lisääntyminen: tietojärjestelmien avulla monimutkaiset prosessit helpottuvat olennaisesti. Tietojärjestelmissä keskeistä on juuri eri tiedon kerääminen sekä kokoaminen yhteen paikkaan, josta sitä voi hakea ja muokata. Esineiden internet jatkaa tätä trendiä laajentaen sen fyysiseen maailmaan. Pyrkimyksenä on kerätä runsaasti ympäristöstä erilaista mittausdataaa, jota voidaan hyödyntää päätöksenteossa sekä automatisoida mekaanisia tehtäviä. Toistaiseksi IoT on esimerkiksi kotikäyttäjille ollut lähinnä mittausdatan esittämistä tai laitteiden manuaalista ohjaamista sähköisesti. Keskeinen termi IoT:ssä on kuitenkin laitteiden välinen kommunikaatio M2M (Machine to Machine), joka tarkoittaa juuri laitteiden ohjaamista automaattisesti esimerkiksi sensoridatan perusteella, jolloin ajantasaisen tiedon välittyminen erittäin pienillä viiveillä on kriittistä [1]. Tällöin IoT-palvelu, sensorit, aktuaattorit sekä ohjelmistopalvelut mukaanlukien, ohjaa automaattisesti järjestelmän toimintaa datan perusteella tai optimoi sen toimintaa. Esimerkiksi asunnossa voitaisiin seurata henkilöiden lukumäärää ja säätää ilmanvaihto automaattisesti kulutuksen mukaan ja vastaavasti työaikana asunnon tyhjentyessä vähentää ilmanvaihto minimiin.

Internetin myötä tekninen kehitys on ollut kiihtyvää ja tulevaisuuden vaatimuksia on vaikea ennustaa. Tämän takia IoT:lle keskeisinä vaatimuksina voidaan nähdä laajennettavuus, skaalattavuus, modulaarisuus sekä yhteensopivuus [2]. Nämä ovat tarpeellisia, sillä IoT on konseptina erittäin laaja ja monialainen ja sen sovelluskohteet ovat erittäin laajat. Tällöin erilaisia teknologioita tulee olemaan paljon ja niiden yhteensopivuus ja hyödynnettävyys tulee taata jollain tavalla.

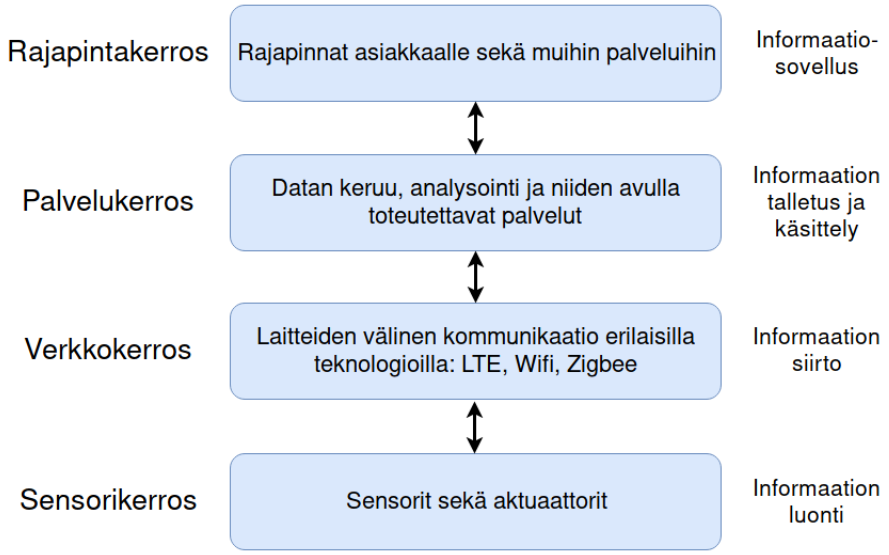
IoT:n sovellukset voidaan jakaa kahteen luokkaan: massiivijärjestelmiin sekä kriittisiin järjestelmiin. Ensimmäisessä laitteita tulee olemaan valtavia määriä ja jokainen näistä mittaa ympäristöä välittäen tiedon eteenpäin. Käyttökohteita massiivijärjestelmille ovat esimerkiksi maatalous, logistiikka, sekä älykkäät kaupungit. Toisaalta kriittisiä järjestelmiä ovat ne yksittäiset sovellukset, joiden toiminta perustuu kriittisen tiedon välittymiseen luotettavasti ja nopeasti. Tällaisia sovelluksia ovat esimerkiksi itseajavat autot sekä kriittisen infrastruktuurin ohjaus. [3]

Keskeisiä teknologisia hyötyjä ovat muun muassa tuotteiden identifiointi ja seuran-

ta, parannettu kommunikaatio, erilaiset verkostot laitteiden ja palveluiden välillä sekä palvelunhallinta. Identifiointi ja seuranta on keskeistä etenkin logistiikassa, mutta myös terveydenhuollossa sekä jälleenmyynnissä. Tähän asti identifiointi on perustunut pitkälti RFID:hen (Radio Frequency Identification), joka on myös IoT:ssä keskeinen teknologia. Palvelunhallinnalla tarkoitetaan esimerkiksi käyttäjän eristämistä verkkoteknologioista sekä -protokollista sekä itse päätelaitteista. Toistaiseksi esineiden internetissä käyttäjän on yleensä täytynyt tuntea melko tarkasti esimerkiksi sensoreiden toiminta ja eri sensorit ovat käyttäneet eri protokollia ja eri ohjelmistoja hallintaan. Tavoitteena on, että useimmat sensorit saisi kiinni samaan ohjelmistoon esimerkiksi välitysohjelmistojen (Middleware) avulla, jolloin käyttäjän ei tarvitse huolehtia heterogeenisestä laiteryhmästä. Näin ollen yksi keskeinen tavoite IoT:ssä on myös abstraktio: loppukäyttäjän ei tarvitse tuntea teknologioita tai fyysisiä laitteita, jotka dataa tuottavat tai joita ohjataan. [2]

2.2 IoT:n eri kerrokset

Esineiden internet voidaan hahmottaa jakamalla se eri kerroksiin kuvassa 1 näkyvällä tavalla. Kerrokset ovat sikäli hierarkiset, että alempi kerros tuottaa aina palvelun ylemmälle. Loppukäyttäjä on aina tekemisissä ainoastaan asiakasrajapinnan kanssa, mutta palvelun ja datan tuottavat alemmat kerrokset. Abstraktion myötä asiakkaan ei myöskään tarvitse tuntea alempia kerroksia välttämättä ollenkaan: standardoiduilla protokollilla laitteet voivat jopa itse liittyä palvelualustoihin ilman käyttäjän tarkempia konfigurointeja. Laitteiden määrä myös vähenee kerroksilla noustessa: sensoreita ja aktuaattoreita voi olla tuhansia tai jopa miljoonia kun taas palvelukerroksella laitteita on todennäköisesti enintään kymmeniä. Asiakkaita voi olla yksi tai useampia. [4, 2, 5]



Kuva 1. *IoT:n kerrokset [2, 5]*

Sensorikerroksella tapahtuu kaikki fyysisen maailman kanssa kosketuksissa oleva eli ympäristön mittaaminen ja laitteiden ohjaus. Täällä tapahtuu myös paikantaminen eri

menetelmineen. Verkkokerroksella siirretään kerätty tieto varsinaiselle palvelulle yleensä internetin yli. Palvelukerroksella tapahtuu varsinainen datan tallennus tietokantaan, käsittely, analysointi sekä mahdollisen palvelun tuottaminen. Tällä kerroksella tapahtuu myös datan abstraktio: relevantti data erotetaan laitteista, protokollista sekä esitystavasta. Viimeisenä kerroksena on rajapinnat. Niiden avulla asiakassovellus tai muut palvelut voivat pyytää dataa tai ohjata laitteita palvelukerroksen avulla. Asiakkaan ei tarvitse tuntea palvelun sisäisiä mekanismeja, verkkokerrosta tai fyysisiä laitteita. [4, 2] Usein IoT-alustana toimiva ohjelma tai palvelu vastaa kolmesta ylimmästä eli verkko- sovellus- sekä rajapintakerroksesta. Sovellus siis hyväksyy anturidataa ja ohjaa laitteita esimerkiksi MQTT- (Message Queying Telemtry Protocol), HTTP- (Hyper Text Transport Protocol) tai COAP- (Constrained Application Protocol) verkkoprotokollalla. Ohjelma tarjoaa antureille APIn (Application Programming Interface) jolla datan siirto tapahtuu. Sovelluskerroksella tieto käsitellään ja talletetaan, ja asiakasrajapinnalla toimii sitä varten kehitetty API. Tämä voi hyödyntää samoja protokollia kuin sensorit, mutta usein asiakas on yhteydessä sovellukseen selaimella tai mobiiliapplikaatiolla, jolloin tiedonsiirto esimerkiksi HTTP:llä. [6]

Eri kerroksiin liittyy paljon erilaisia teknologioita, jotka kaikki kehittyvät samanaikaisesti. Esimerkiksi rajapintakerroksella voi olla uudet selaimet ja niiden tukemat toiminnot, kuten HTML5 tai WebSocketit. Sovelluskerroksella taas puhutaan esimerkiksi Big Datasta, Cloud sekä Fog Computingista, mikä tarkoittaa laskennan hajauttamista internetiin eri palvelimille. Myös konteksti- tai tilannetietoisuus on sovelluksiin liittyvä aihe, joka tarkoittaa esimerkiksi relevantin datan erottelemista ja hallintaa ja että kaikkea mahdollista dataa ei ole välttämättä tarpeen analysoida. Verkkokerroksella taas kehitetään uusia verkkoprotokollia sekä -teknologioita, kuten esimerkiksi wlan- sekä mobiiliverkko. Myös sensori- ja aktuaattorilaitteiden suuri määrä on pitkälle verkkokerroksen ongelma, sillä suuri määrä laitteita voidaan verkottaa monella eri tavalla, esimerkiksi Mesh- sekä Ad-Hoc-verkkoina tai tavanomaisena verkkona. Sensorikerroksella taas puhutaan esimerkiksi erittäin pienikulutuksisista sensoreista sekä edullisista antureista tai toisaalta monipuolisista ja luotettavista päätelaitteista. [6]

2.3 IoT ja paikantaminen

IoT:ssä mitattavia datalähteitä voi olla useita. Datana voi olla esimerkiksi lämpötila, autojen lukumäärä tieosuudella tai osan läpäiseminen prosessivaiheessa. Usein varsinaista mittausdataa täydentää metatiedot, kuten sijainti. Kun anturien lukumäärä kasvaa, on sijaintitieto tärkeä datan analyysin kannalta. Näin paikkatieto toimii keskeisenä tekijänä IoT:ssä. Toisaalta sijaintieto on usein yksinään tarpeetonta: se ei välttämättä itsessään sisällä mitään hyötyinformaatiota, vaan se täytyy yhdistää muuhun dataan.

Paikkatiedon vaatimukset luotettavuuden, nopeuden sekä tarkkuuden suhteen riippuvat sovelluksesta. Esimerkiksi itseajavalle autolle on kriittistä tietää oma ja muiden autojen sijainti senttimetrien tarkkuudella erittäin pienillä viiveillä [7]. Toisaalta esimer-

kiksi kauppakeskuksessa navigoiva käyttäjä ei tarvitse vastaavaa tarkkuutta tilassa eikä ajassa. Muita vaatimuksia paikantamiselle ovat esimerkiksi virrankulutus, ajantasaisuus sekä toimivuus sisä- ja ulkotiloissa. Myös uusia paikannusmenetelmiä kehitetään ja esimerkiksi 5G-mobiiliverkko todennäköisesti mahdollistaa uusia paikannusmenetelmiä [7, 8]. Käytössä olevat paikannusmenetelmät ovatkin yleensä kompromisseja edellä mainittujen vaatimusten suhteen ja saattavat hyödyntää useita eri paikannustekniikoita.

Tärkeä seikka paikantamisessa on myös resurssit: erilaisten radioiden tai sensoreiden käyttö vaatii yleensä energiaa, mikä voi olla arvokas resurssi IoT-laitteelle. Vastaavasti lisälaitteisto, kuten radio, yleensä lisää hintaa ja monimutkaisuutta eli myös riskialttiutta laitteeseen. Tietoliikenneyhteydet saattavat myös olla maksullisia ja lukuisien laitteiden kohdalla tämä saattaa olla suuri kulu. Siksi on menetelmiä, jotka eivät edellytä suoraan minkään verkon osallisuutta, kuten GNSS-paikantaminen (Global Navigation Satellite System).

2.4 IoT osana yhteiskuntaa

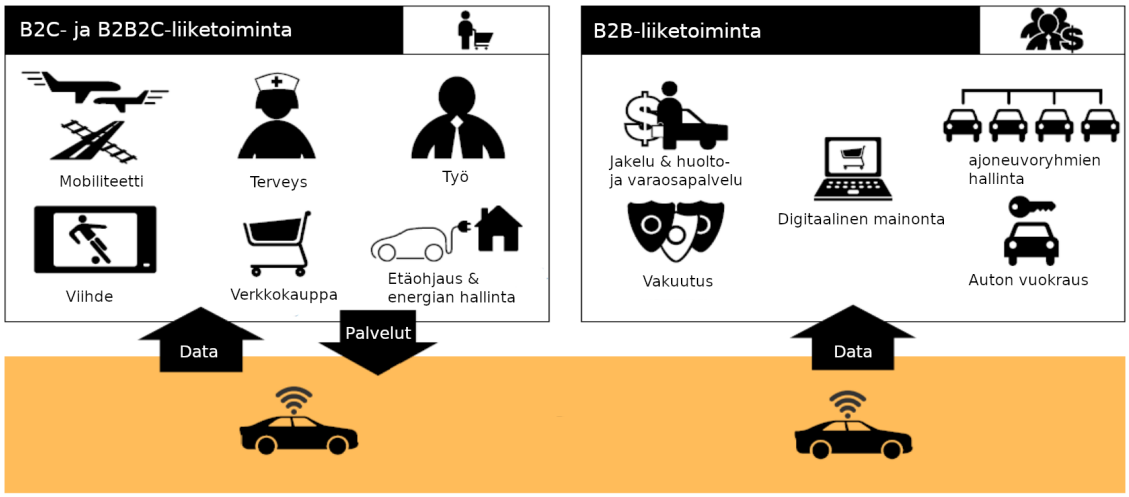
Tiedon määrän lisääntyessä keskeiseksi kysymykseksi nousee oikeudet ja omistaminen: kenellä on pääsy dataan ja mihin sitä saa hyödyntää. Monissa sovelluksissa tietoturva on tärkeä kriteeri palvelulle. Esimerkiksi terveysalalla potilasturva ei saisi vaarantua uudempien teknologioiden ja lisääntyneen informaation myötä [9]. EU:n tietosuoja-asetukset määrittelevät paikannustiedon henkilön yksilöiväksi dataksi [10]. Tietoturva täytyy tällöin huomioida myös teknisiä ratkaisuja toteutettaessa. Myös RFID-tunnisteissa tietoturva on keskeinen osa palvelua [11]. RFID-tunnisteet voivat sisältää itsessään harmitonta dataa, kuten tietoja itse tuotteesta. Kuitenkin, kun tieto yhdistetään kaikkeen muuhun dataan, kuten muihin käyttäjän ostamiin tuotteisiin kaupasta, voi tieto olla jo käyttäjän yksilöivää.

Esineiden internet todennäköisesti vaikuttaa ja hyödyttää sekä B2B- (Business to Business) että B2C-markkinoita (Business to Customer). B2B-markkinoilla hyöty on todennäköisesti logistista ja eri alueiden integrointia, esimerkiksi koko jakeluketjun läpi virtaavan tavaran seurantaa ja analysointia. Kuluttajapuolella taas hyödyt ovat todennäköiseseti uudenlaiset palvelut. Tällaisia voivat olla esimerkiksi uudenlaiset viihdepalvelut kuten VR- (Virtual Reality) sekä AR-lasien (Augmented Reality) tuomat informaatiopalvelut sekä älykoti erinäisine laitteineen ja automatisointeineen. [4]

Ruokaketjun hallinnassa yksittäisten tuotteiden tieto voi olla tärkeä osa pilaantumisen ehkäisyssä ja toisaalta järjestelmän optimoinnissa. Jokaiseen tuotteeseen voitaisiin lisätä RFID-tagi, jonka avulla kyseistä tuotetta voi seurata ketjun läpi ja loppukäyttäjä voi mahdollisesti todentaa sen avulla tuotteen alkuperän ja tuotantoajan. Terveydenhuollossa taas on jo laajasti saatavilla kuluttajille älyrannekkeita sekä muita sensoreita. Myös kattavampia mittaus- ja analyysipalveluita on kehitetty, esimerkiksi iHealth Lab on kehittänyt muun muassa langattomia glukoosimittareita, jotka käyttäjä voi kytkeä älypuhelimeensa [9].

Euroopan komission teettämän tutkimuksen mukaan IoT-pohjaiset liiketoimintamallit eroavat perinteisistä siinä, että ne pyrkivät tuottamaan laajoja, useita markkinoita lä-

pileikkaavia palveluita yksittäisten tuotteiden sijasta. Kuvassa 2 on esitelty älykkäisiin ajoneuvoihin liittyviä liiketoimintamalleja sekä B2B- että B2C-markkinoilla. Perinteiset liiketoimintamallit ovat kuvassa muiden lomassa ja niiden ympärille on kehittynyt tai kytkeytynyt muita palveluita. [12]



.

Kuva 2. *Liiketoimintamalleja älykkäiden autojen ympärillä. Muokattu lähteestä [12]*

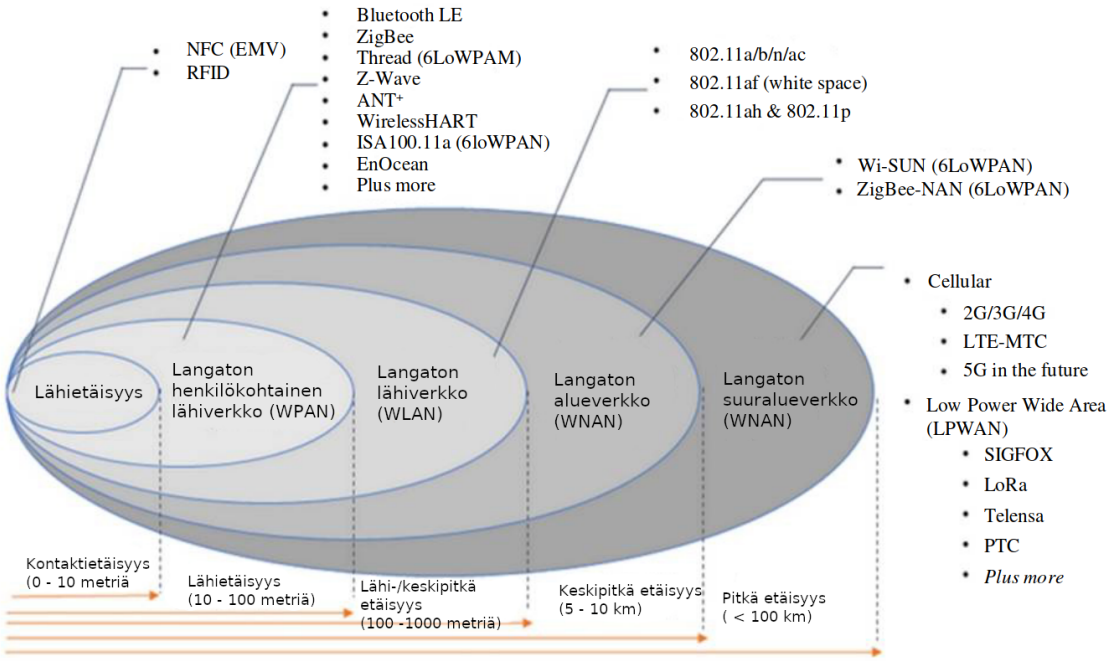
Usein palvelut ja data ovat saatavilla ohjelmointirajapintojen eli APIen kautta ja palvelusta maksetaan suoriteperusteisesti. Tämä mahdollistaa avoimen, joko ilmaisen tai maksullisen datan jakamisen muiden toimijoiden kesken, mikä mahdollistaa laajemmat markkinat sekä monipuolisemmat palvelut ja yhteistyöt eri toimijoiden välillä [12]. Tiedon lisääntymisen myötä on tärkeää oppia seulomaan ja yhdistelemään olennainen data, jotta siitä olisi käyttäjälle jotain hyötyä. Sen takia datan jakaminen eri tahojen kesken on tärkeää.

3 PAIKANTAMISMENETELMIÄ

Tässä kappaleessa tarkastellaan muutamia erilaisia paikannusmenetelmiä. Sisä- ja ulkotiloissa olosuhteet eroavat toisistaan merkittävästi: ulkona etäisyydet ovat suuremmat ja myös nopeudet ovat luultavasti suurempia. Rakennetulla alueella signaalit heikkenevät ja etenkin sisätiloissa vaimeneminen on merkittävää. Toisaalta myös nopeudet ovat usein pienempiä sisätiloissa. Varsinkin ulkoa tulevien signaalien voimakkuudet ovat varsin heikot sisätiloissa.

Myös vaatimukset sisä- ja ulkotiloissa ovat erilaiset: ulkona riittää usein kymmenien tai jopa satojen metrien tarkkuus. Toisaalta sisätiloissa usein tarvitaan parempia, metrien tai senttimetrien tarkkuuksia. Erilaisia paikannusmenetelmiä ja niiden soveltuvuutta esineiden internetiin tutkitaan paljon, ja erilaisia kokeellisia menetelmiä on kehitetty.

Keskeisiä parametreja on tarkkuuden lisäksi menetelmän monimutkaisuus: vaadittavan laitteiston ja ohjelmiston laajuus sekä käyttöönoton hankaluus vaikuttavat valittavaan menetelmään. Toinen seikka on hajautettu versus keskitetty laskenta: prosessoiko kukin laite itse sijaintinsa, vai lähettääkö sen toiselle yksikölle tai pilvipalvelulle laskettavaksi. Tämä vaikuttaa suorituskykyvaatimukseen ja esimerkiksi virrankulutukseen laitteessa, mutta ratkaisu on monimutkaisempi ja vaikuttaa moniin seikkoihin. Kolmantena on skaalautuvuus: voidaanko paikannusmenetelmä yksinkertaisesti toteuttaa suuremmalla maantieteellisellä alueella suuremmalla joukolla laitteita. Neljäntenä tekijänä on toimintavarmuus: kuinka hyvin menetelmä sietää erilaisia muutoksia ja haasteita ympäristössä. Myös hinta on tärkeä tekijä, riippuen laitteiden funktionaalisuudesta ja lukumäärästä voidaan haluta hyvinkin edullisia ja halvasti kopioitavia tuotteita. Myös muita rajoitteita voi olla: esimerkiksi GNSS ei sovellu sisätiloihin vaimentumien ja monitie-etenemisen takia. [13]



Kuva 3. *Erilaisia langattomia verkkoja. Muokattu lähteestä [14]*

Erilaisia radioverkkoja löytyy tänä päivänä paljon ja jokaisella on oma käyttökohteensa. Tunnetuimmat näistä lienevät WLAN- tai WiFi-verkot (Wireless Local Area Network), mobiili- sekä bluetooth-verkot. Kuvassa 3 on jaoteltu erilaisia verkkoja niiden maksimietäisyyden suhteen. Toistaiseksi WPAN- eli henkilökohtaiset verkot ovat vielä suhteellisen harvinaisia, mutta niitä voidaan hyödyntää IoT:ssä suurten laitemäärien hallintaan. WLAN-verkot taas ovat jo yleisessä käytössä ja laajasti saatavilla. Myös mobiiliverkot ovat melkein kaikkialla saatavilla.

Periaatteessa kaikkia verkkoja voidaan hyödyntää IoT:ssä ja niiden avulla voidaan myös paikantaa. Kuitenkin verkkojen erilaisen luonteenpiirteiden takia osa soveltuu paikantamiseen paremmin kuin toiset. Esimerkiksi WLAN-verkot ovat käytettyjä paikantamisessa juuri niiden laajan käyttäjäkannan takia. Kuvasta 3 näkee myös karkean jaottelun sisä- ja ulkotiloihin: monien radioverkkojen (Lähietäisyys, WPAN eli Wireless Personal Area Network, WLAN) maksimietäisyys ei yksinkertaisesti riitä ulkokäyttöön.

Pohjimmiltaan paikantamisen mittaus perustuu kolmeen mittaustapaan: Signaalin etenemisaikaan, signaalin saapumiskulmaan, signaalinvoimakkuuteen tai muuhun identiteettidataan, kuten solutunnisteeseen [15, 13]. Näitä menetelmiä on verrattu taulukossa 2. Etenemisaika (TOA, Time of Arrival) voidaan oikeastaan määritellä kolmella tavalla: signaalin etenemisaika, signaalin saapumisaika tai signaalien saapumisaikojen erotus (TDOA, Time Difference of Arrival) [15]. Ensimmäinen näistä edellyttää, että vastaanotin tietää tarkalleen, signaalin lähetysajan. Toisessa tapauksessa näin ei ole. Vastaanotetun kulman (AOA, Angle of Arrival) tapauksessa kerätään tieto useiden lähettimien signaalien suunnasta ja näistä määritetään geometrisesti sijainti. TDOA:ssa vastaanottimen tarvitsee vain

mitata kahden signaalin saapumisen erotus. Esimerkiksi GNSS perustuu aikaeron mittaamiseen kun taas WLAN-fingerprinting perustuu signaalinvoimakkuuteen (RSS Received Signal Strength) sekä wlan-tukiasemien tunnisteisiin. On olemassa myös hybrimenetelmiä, ja sisällä käytettävät menetelmät voivat toimia ulkona ja toisinpäin. Käytetyimmät paikannusmenetelmät tällä hetkellä ovat GNSS ja WLAN-pohjaiset menetelmät, sillä niiden edellyttämä infrastruktuuri on jo olemassa [10].

5G tulee tarjoamaan paljon mahdollisuuksia ja sitä pidetään yhtenä IoT:n mahdollistajista. Esimerkiksi massiivi-MIMO (Multiple Input Multiple Output) tarjoaa mahdollisuuden paikantaa käyttäjä solua pienemmissä keiloissa. Tarkkuutena tämä voi tarkoittaa jopa metrejä. [1]

Taulukko 2. *Eri mittaustapoja paikantamiseen [13]*

Menetelmä	Edut	Haasteet
TOA	Hyvä tarkkuus, luotettava	Edellyttää synkronointia lähettimen ja vastaanottimen välillä, kallis skaalata
TDOA	Hyvä tarkkuus, luotettava	Edellyttää synkronointia eri lähettimien kesken, kallis skaalata
AOA	Hyvä tarkkuus	Edellyttää lisäantenneja, voi olla hankala skaalata suuremmalle alueelle
RSS	Hyvä skaalautuvuus suurellekin alueelle, ei edellytä synkronointia	Heikko tarkkuus, monitieeteneminen heikentää tuloksia, etukäteen tehty kartoitus vie aikaa

3.1 Paikantaminen sisätiloissa

Moderneissa rakennuksissa eristemateriaalit ja paksut seinät tuovat haasteen radioaalloille. Etenkin passiivitaloissa käytetään rakenteissa paljon erilaisia metallikalvoja tai muita materiaaleja, jotka läpäisevät heikosti radioaaltoja. Käytännössä tämä johtaa siihen, että ulkoa tulevia signaaleja voidaan hyödyntää heikosti, jolloin täytyy hyödyntää sisätiloista löytyviä signaalilähteitä. Tällaisia ovat esimerkiksi WLAN:it tai esimerkiksi erilaiset RFID-järjestelmät. Myös toisia päätelaitteita voidaan hyödyntää paikantamisessa. Tällaisia signaaleja sisätiloissa ovat kaikki tietoliikenneväylät, esimerkiksi WLAN sekä Bluetooth. [15] Sisätiloissa taas haasteeksi muodostuu usein monitie-eteneminen, jossa signaali etenee useita reittejä vastaanottimelle ja summautuu yhdeksi signaaliksi. Signaalissa on tällöin eri komponentteja, joilla voi olla ajassa ja taajuudessa hajontaa, mikä hankaloittaa signaalin lukemista.

3.1.1 WLAN-fingerprinting

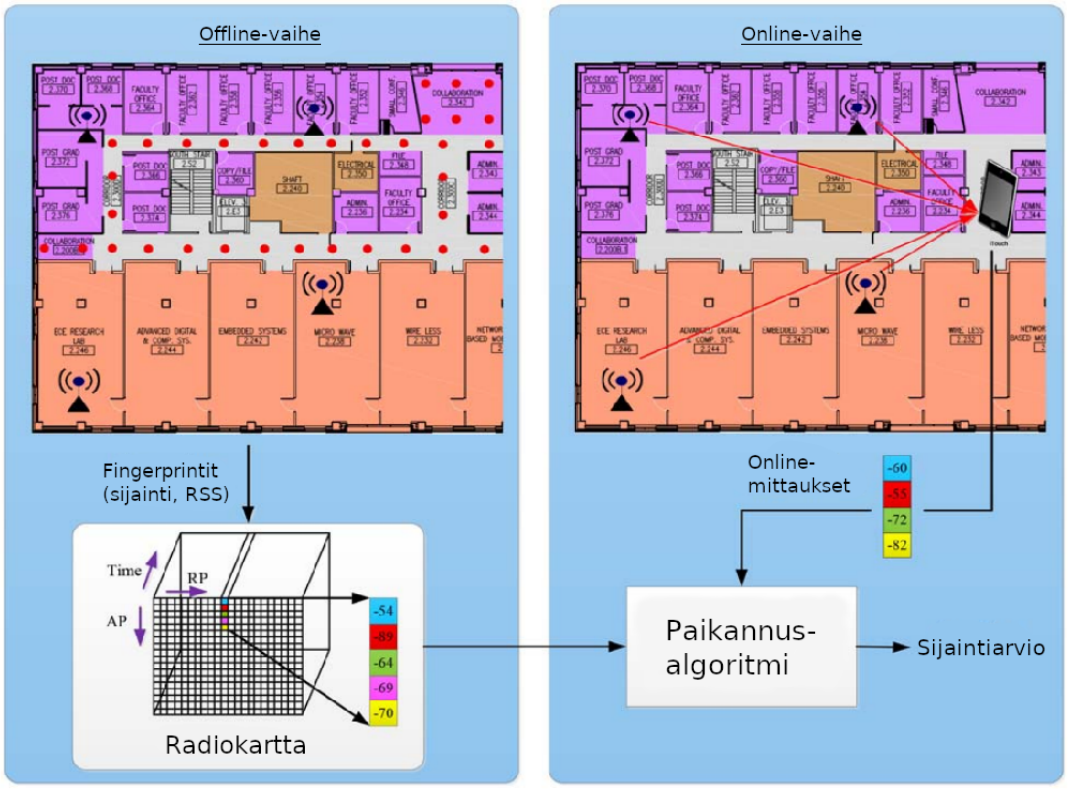
Yksi tapa paikantaa laite tai käyttäjä on hyödyntämällä kullonkin kuuluvia Wifi-tukiasemia. WLAN-fingerprinting -menetelmä perustuu signaalinvoimakkuuden mittaamiseen ja vertaamiseen tunnettuun arvoon. Wifi-verkoista siis kerätään erilaisia tunnistetietoja, esimerkiksi tukiaseman verkkotunnus eli SSID (Service Set Identifier), sekä signaalinvoimakkuus tunnetussa paikassa. Käytännössä esimerkiksi julkisessa tilassa kuuluu useita verkkoja, jolloin näistä karsitaan jollakin kriteerillä muutama verkko ja mitataan niiden voimakkuus ja tallennetaan tietokantaan [16]. Kun eri verkkojen voimakkuudet tunnettaan tarpeeksi monessa paikassa, esimerkiksi 5x5 metrin matriisissa, voidaan käyttäjän mittauksia verrata näihin referensseihin ja määrittää laitteen sijainti metrien tarkkuudella. Myös fyysisiä karttoja voidaan hyödyntää paikantamisessa, jolloin voidaan päästä parempiin tarkkuuksiin [13].

Sormenjälkiin eli RSS-tunnisteisiin liittyvää paikantamista voidaan tehdä periaattessa millä tahansa verkolla, esimerkiksi Bluetoothilla. Tällöin suorituskyky saattaa kuitenkin poiketa WLAN-pohjaisesta paikantamisesta. Esimerkiksi ZigBee-tunnisteiden avulla voidaan paikantaa vastaavalla tekniikalla kuin WLAN-fingerprinting:issä. Suurimpana erona tässä on erityisesti virrankulutus: ZigBee on pienivirtaisempi WLAN:iin nähden, esimerkiksi ZigBee-verkolla voidaan päästä jopa 60-75 % matalampaan virrankulutukseen. [13]

Yksi keskeisistä eduista WLAN-tunnisteiden käytössä on infrastruktuurin olemassaolo: tukiasemia löytyy laajsti toimistoista sekä julkisista tiloista ja nykyiset älypuhelimet hyödyntävät yleisesti WLAN-verkkoja. WLAN-fingerprinting hyödyntää verkon nimeä eli SSID:tä sekä verkon voimakkuutta ja modernit verkkokortit tuottavat nämä tiedot tarvittavalla tarkkuudella. [16]

WLAN-fingerprint:ien hyödyntäminen edellyttää siis ajantasaista radiokarttaa olemassa olevista langattomista verkoista ja niiden voimakkuuksista kuvan 4 mukaisesti. Aluksi

tämä täytyy luoda eli määrittää referenssipisteet tilasta ja mitata voimakkuudet näissä pisteissä. Tätä vaihetta kutsutaan myös offline-vaiheeksi, jossa luodaan tarvittava data paikannusta varten. Referenssidatasta muodostetaan radiokartta eli tietokanta eri verkkojen voimakkuuksista eri paikoissa. Referenssidatan muodostaminen voi olla työlästä, sillä referenssipisteet täytyy käydä usein käsin mittaamassa yksitellen ja suurissa rakennuksissa tämä voi olla aikaa vievää. Online-vaiheessa, eli varsinaisessa paikannustilanteessa, käyttäjä mittaa tukiasemien voimakkuudet ja valittu algoritmi vertaa kuuluvuuksia ennalta määritettyyn radiokarttaan. Algoritmista riippuen päästään metrien tai kymmenien senttimetrien tarkkuuteen. Eri algoritmit ovatkin kompromisseja laskentatehon ja virrankulutuksen, nopeuden, luotettavuuden sekä tarkkuuden suhteen. [16]



Kuva 4. *WLAN-fingerprinting. Muokattu lähteestä [16]*

Suurimpia haasteita WLAN-fingerprinting -menetelmässä ovat monitie-eteneminen, asiakaslaitteiden variaatio sekä referenssidatan ajantasaisuus. Monitie-etenemisessä signaalit etenevät tukiasemasta vastaanottimelle useita eri reittejä heijastellen ja siroutuen pintojen kautta. Eri signaalit summautuvat vastaanottimessa, jolloin summautuneen signaalin voimakkuus voi vaihdella paljon. [16, 13, 17]. Monitie-eteneminen aiheuttaa häipymää, joka tarkoittaa tukiasemien voimakkuuksien mahdollisesti suurtakin vaihtelua ajassa ja paikassa [17]. Käytännössä tämä lisää suoraan paikannuksen epätarkkuutta. Usein monitie-eteneminen eliminoidaan sijainninmääritysalgoritmissa, mutta toimenpide vaatii laskentaa, mikä kuluttaa virtaa ja tuo viivettä paikantamiseen. Asiakaslaitteiden fyysiset erot aiheuttavat epätarkkuutta mittaustuloksiin, mikä heikentää suoraan mittaustarkkuutta [16].

Myös referenssidatan ajantasaisuus on tärkeää tarkkuuden säilyttämiseksi. Käytännössä tämä tarkoittaa tukiasemien skannaamista tarpeeksi usein. Ratkaisuna tähän on esimerkiksi joukkoistaminen, jossa käyttäjät lähettävät mittausdataa. Haasteena joukkoistamisessa on lähinnä mittausdatan sekä todellisen sijainnin tarkkuus. [16]

3.1.2 RFID

RFID on jo verrattain vanha ja laajasti käytetty teknologia esimerkiksi fyysisessä pääsynhallinassa sekä logistiikan hallinnassa. Tuotteisiin tai esineisiin liitetään tunnisteita eli tageja, joita voidaan lukea erillisillä lukulaitteilla. RFID-tunnisteisiin voidaan kirjoittaa tietoa, kuten yksilöivä tunniste tai valmistuspäivämäärä ja -sarja. Moderneihin tunnisteisiin voidaan kirjoittaa monipuolisesti eri kenttiin ja kentät voivat olla kertakäyttöisiä tai uudelleenkirjoitettavia. Esimerkiksi jakeluketjussa tunnisteeseen voidaan päivittää aikaleima ja sijainti, jossa tuote on viimeksi ollut. RFID-tunnisteet voivat olla aktiivisia tai passiivisia. Aktiivisilla tunnisteilla on energialähde, kuten paristo, ja niillä saavutetaan pidempiä kantamia. Esimerkiksi lentokoneen transponderit ovat aktiivisia tunnisteita, ja niillä voidaan saavuttaa satojen kilometrien kantama. Passiiviset tunnisteet ovat usein pienempiä ja edullisempia. Ne saavat energiansa lukulaitteelta joko sähkömagneettisesti tai induktiivisesti. [18]

Tunnisteiden kantamaan vaikuttaa suuresti käytettävä taajuus, jonka aallonpituus taas rajoittaa tunnisteen pienintä mahdollista kokoa. Esimerkiksi LF-taajuusalueella (Low Frequency) tunnisteilla kantama on usein puoli metriä, HF-alueella (High Frequency) kantama on metrejä ja UHF-alueella (Ultra High Frequency) kantama voi olla jopa kymmeniä metrejä [11]. Tunnisteiden kantama kuitenkin kasvaa käytettävän teknologian kehittyessä. Myös tarvittava energiansaanti vaikuttaa kantamaan: sähkökentän energia putoaa nopeasti etäisyyden kasvaessa, jolloin tämä rajoittaa usein passiivisten tunnisteiden lukuetäisyyttä [18].

Passiiviset tunnisteet voidaan jakaa vielä kahteen osaan: lähikenttää sekä kaukokenttää käyttäviin tunnisteisiin. Termi liittyy sähkömagnetismin ja aaltojen muodostumiseen antennissa ja sen lähiympäristössä. Lähikenttä on taajuudesta riippuen yleensä alle 20 cm. Antennin lähikentässä energia voidaan siepata induktiivisesti, kun taas kaukokentässä energia täytyy siepata sähkömagneettisesta kentästä. Lähikentässä kommunikointi lukulaitteen kanssa tapahtuu kuormaa muuttamalla, mikä näkyy lähettimellä induktanssin muutoksena. Kaukokentässä taas voidaan puhua radioyhteydestä, jolloin paluuviesti täytyy lähettää radioteitse lähettimen avulla. [18]

RFID:tä käytetään paljon esimerkiksi tuotteiden seurantaan. Esimerkiksi jälleenmyynnissä tärkeää on RFID-tunnisteiden hinta, jotta niitä on järkevää laittaa jokaiseen myytävään tuotteeseen. Tällaisessa käytössä tuotteita voidaan seurata ja käsitellä suuria määriä nopeasti. Myös varastonhallinnassa voidaan varaston sisältö inventoida tehokkaasti RFID-tunnisteiden avulla. [18]

RFID-tunnisteeseen voidaan myös sisällyttää älyä tai sensoreita, jolloin tunnisteet

tarjoavatkin kanavan mitata tuotteiden olosuhteita, kuten lämpötilaa. Tunnisteeseen voidaan myös sisällyttää antureita, jotka mittaavat ympäristöä. Esimerkiksi kiihtyvyysanturi voi mitata tärähdyksiä ja ilmoittaa lukijalle jos tuote on pudotettu tai kokenut muutoin rasitusta kuljetuksen aikana. [18]

RFID-tunnisteista puhuttaessa keskeinen seikka on käyttäjien yksityisyys. Tunnisteet yksilöivät tuotteen, ja jos tämä tieto yhdistetään esimerkiksi asiakkaan pankkitiliin kassalla tuotetta ostettaessa, voidaan käyttäjää seurata tunnisteen avulla. Kun asiakas tulee seuraavan kerran myymälään, voidaan hänet yksilöidä sisääntullessa esimerkiksi paidassa olevan tunnisteen avulla. Tällaisen metadatan oikeanlainen kerääminen ja säilyttäminen täytyy huomioida tunnisteita hyödynnettäessä. [11, 18, 19]

3.1.3 Paikantaminen led-valaisinten avulla

Rakennuksissa on nykyisin jo melko laajasti käytössä led-valaisimia. Niiden edut ovat selkeät: pieni virrankulutus, pitkä käyttöikä sekä ympäristöystävällisyys. Kun ledien valoa moduloidaan, eli valoon sisällytetään esimerkiksi tunnistetietoja, voidaan valojen avulla paikantaa hyvinkin tarkasti. Sijainnin määrittäminen voi perustua joko signaalin saapumisaikaan eli TOA:han (Time Of Arrival), signaalinvoimakkuuteen eli RSS:ään (Received Signal Strength) tai signaalin saapumiskulmaan eli AOA:han (Angle Of Arrival). Paikannus ledien avulla voi perustua useaan eri tietoon. Kukin valaisin voi esimerkiksi lähettää yksinkertaisesti omaa yksilöllistä tunnistettaan. Asiakaslaite saa tämän tunnisteen, tai useita eri tunnisteita eri valaisimista, ja lähettää tämän tiedon langattomasti palvelimelle, joka kertoo laitteelle sen sijainnin tai tarjoaa suoraan jotain palvelua sijaintitiedon perusteella: esimerkiksi ruokahyllyjen valikoimia, museon tietoja tai sisätilaopastusta rakennuksessa. [20]

Kun samassa huoneessa on useita valaisimia, tarvitaan jonkinlainen pääsynhallinta (MAC, Medium Access Control) eli multipleksaus aika- tai taajuusjakoisesti eri valaisimien erottelemiseksi asiakas-laitteessa. Vastaanotto voidaan toteuttaa joko kameroilla, joita on älylaitteissa nykyisin kattavasti, tai erillisellä valodiodilla, joka lukee valaisinten lähettämää dataa. Valodiodilla paikantaessa signaalikanava on kuin radiokanava, signaalinvoimakkuus näkyy suoraan jännitteenä valodiodilla ja sitä voidaan lukea suurella taajuudella. Kameralla eli kuvasensorilla varustettu järjestelmä perustuu useiden kuvien ottamiseen peräkkäin. Tätä tietoa voidaan verrata joko kiihtyvyysdataan, toisen kuvasensorin tuottamaan dataan tai tietokantaan. [20]

Kaupallisista toimijoista esimerkiksi Philips toimittaa led-valaisimiin perustuvaa paikannuspalvelua esimerkiksi jälleenmyyntiin. Palvelussa luvataan 30 cm tarkkuus ja rajapinta, jonka avulla asiakas voi itse tehdä räätälöidyn palvelun sijaintiedon ympärille. Palvelu hyödyntää asiakkaan älypuhelinta ja oletettavasti sen kameraa paikantamiseen. [21]

Led-valaisimien avulla paikantaessa virheet ovat erittäin pieniä, jopa millimetriluokkaa, mutta usein senttimetrejä. Näihin tarkkuuksiin kuitenkin päästään vain laboratorio-olosuhteissa, jolloin valo etenee aina suoraan valaisimesta ilmaisimelle. Led-valaisimissa

ei ole vielä tarpeellista standardointia menetelmän käyttämiseksi laajemmin. [20]

3.2 Paikantaminen ulkona

Ulkotiloissa paikantamisen vaatimukset muuttuvat. Etäisyyksien kasvaessa aikaerot kasvavat, mutta myös virrankulutus saattaa kasvaa, mikäli laite joutuu lähettämään dataa paikantamisen takia eli paikantamaan aktiivisesti. Rakennetulla alueella esiintyy usein monitie-etenemistä korkeiden rakennusten takia, mutta ilmiö on kuitenkin heikompi kuin sisätiloissa. Monesti vaadittava tarkkuus on kymmeniä tai satoja metrejä eli heikompi tarkkuus riittää kuin sisällä.

3.2.1 GNSS

Satelliittipaikannusjärjestelmiä on kehitetty rinnakkain useissa maissa tai maanosissa noin 40 vuoden ajan. Tunnetuimmat näistä ovat USA:lainen GPS (Global Positioning System), eurooppalainen Galileo, venäläinen Glonass sekä kiinalainen Compass. Useissa näissä käytetyt tekniikat ja toimintaperiaatteet ovat toisiaan vastaavia ja ainoastaan satelliitit sekä tarkkuus eri maanosissa saattavata vaihdella. Paras palvelun taso saavutetaankin käyttämällä useampia yhdessä. Nykyaikaiset GNSS-vastaanottimet kykenevätkin erottelemaan useiden eri järjestelmien satelliitit toisistaan ja näin hyödyntämään eri järjestelmien paikannusdataa.

GNSS:n perusidea on, että avaruudessa olevat kymmenet satelliitit lähettävät sijaintitietoaan erittäin tarkan kellon avulla ja maassa oleva laite kuuntelee näitä lähetyksiä. Signaali viivästyy jonkin verran matkansa aikana, ja kun asiakaslaite vastaanottaa usean eri satelliitin signaalin, voidaan näistä viive-eroista päätellä geometrisesti asiakaslaitteen sijainti. [22]

GNSS-signaali hyödyntää hajaspektritekniikkaa ja satelliittien signaalit on jaettu CDMA-tasossa (Code Divison Multiple Access). Tällöin kaikki signaalit ovat samalla taajuuskaistalla. Varsinainen paikannusongelma sijainnin selvittämiseksi onkin erotella eri satelliittien lähetykset toisistaan. Tehtävää vaikeuttaa myös Doppler-siirtymä satelliittien suuren nopeuden takia. Tällöin etsittävä avaruus kasvaa suureksi, kun parametreja on useita. [22]

Koska GNSS perustuu juuri aikaerojen mittaamiseen, voivat pienetkin vääristymät ajassa heikentää tarkkuutta oleellisesti. Esimerkiksi monitie-eteneminen rakennetussa ympäristössä voi vääristää aikoja niin paljon, ettei tulos ole enää käyttökelpoinen [13]. Sisätiloihin mentäessä ilmiö voimistuu entisestään, mutta myös signaalintaso heikkenee oleellisesti, minkä takia GNSS ei sovellu sisätiloihin. Muita häiriölähteitä GNSS:ssä ovat ionosfäärin heijastumat sekä satelliittien kellon tai sijainnin epätarkkuus [22].

GNSS suurin hyöty on ehdottomasti sen saavutettavuus: GNSS on saatavilla kaikkialla maailmassa. Se on myös täysin maksuton ja se toimii tarvittaessa asiakkaan kannalta täysin passiivisesti. Huonona puolena tosin on mahdollinen epäluotettavuus kriittisissä sovelluksissa sekä verrattain suuri virrankulutus. GNSS:ssä haaste on juuri satelliittien seuranta CDMA-tasossa, mikä on suhteellisen raskas operaatio pienelle prosessorille. GNSS:ssä on

lisäksi paljon asioita, jotka täytyy huomioida sijaintia määritettäessä: esimerkiksi ionosphäärin vaikutus sekä dopplersiirtymä. Myös satelliitin löytyminen voi olla erittäin hidasta: sijainnin selvittäminen ensimmäisen kerran voi kestää useita minuutteja. Tähän on kehitetty ratkaisuksi A-GPS (Assisted Global Positioning System), joka hyödyntää mobiiliverkkoja ja niiden tukiasemia GNSS-signaalin löytämisessä. Tukiasemassa on GNSS-vastaanotin ja se tietää silloin tarkasti satelliittien sijainnin ja voi tällöin lähettää tämän tiedon asiakaslaitteelle, joka löytää samat satelliitit nopeasti. Avustettu GNSS toimii tosin vain jos laitteesta löytyy mobiiliverkkoyhteys. [23]

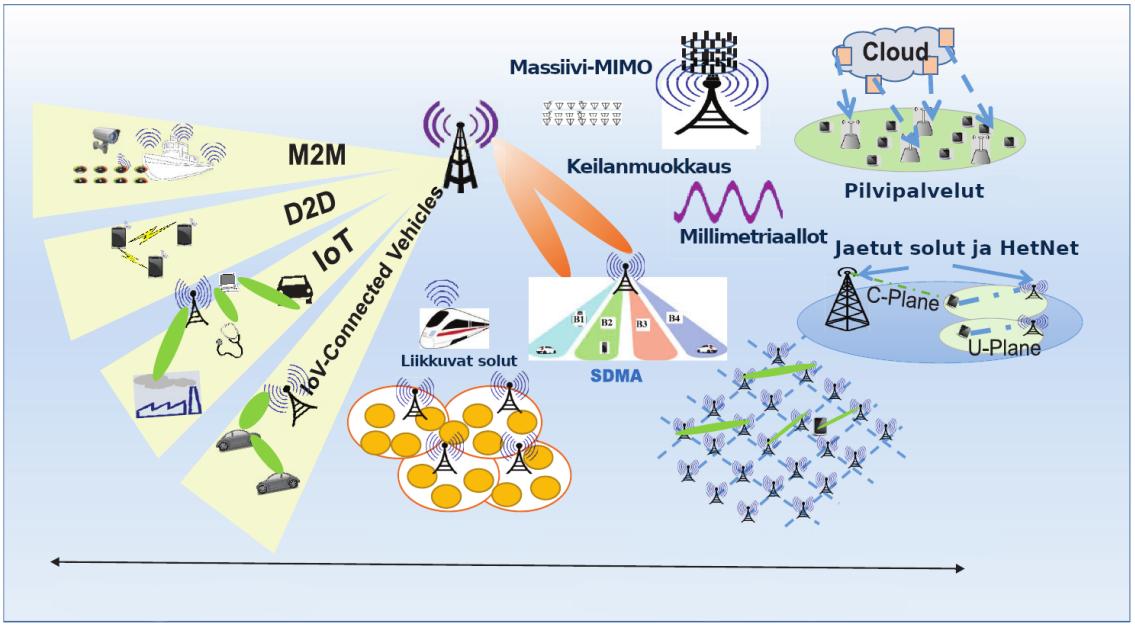
3.2.2 Paikannus mobiiliverkkojen avulla

Mobiiliverkot on jaettu paitsi operaattoreihin, myös tukiasemiin ja edelleen soluihin. Mobiiliverkkojen avulla saavutetaan paikkatieto solun perusteella, mikä tarkoittaa tarkkuutta 10 metreistä kilometreihin. Monissa sovelluksissa näinkin epätarkka sijaintitieto on kuitenkin riittävä, esimerkiksi sääennusteissa tai liikenneruuhkissa ei paremmasta tarkkuudesta ole hyötyä. Ajoneuvot ja varsinkin itseajavat autot tarvitsevat tarkkaa ja ajantasaista tietoa ennenkaikkea suhteessa toisiin ajoneuvoihin.

Mobiiliverkon täytyy tietää kaikkien laitteiden sijainti jollakin tarkkuudella, mikä tarkoittaa yleensä muutaman solun tarkkuutta. Tietoa käytetään muun muassa solunvaihtojen (Handover sekä Cell Reselection) toteuttamiseen. Tätä tietoa ei kuitenkaan tarvitse jakaa asiakaslaitteelle tai kolmansille osapuolille, joten tätä tietoa ei useinkaan ole saatavilla. Jokaisella tukiasemalla ja solulla on kuitenkin yksilöllinen tunniste, josta voidaan muodostaa tietokanta, jota hyödyntämällä voidaan paikantaa asiakaslaite solun tarkkuudella samalla periaatteella kuin WLAN-fingerprint:in käytössä. 4G-verkkojen myötä on ollut tarjolla pienempiä soluja eli makrosoluja, jotka voivat tarjota paljon pienempiä soluja ja siten tarkempaa sijaintietoa.

5G-verkoissa on huomioitu IoT:n tarpeet keskeisenä osana koko verkkoa. Tämä kiteytyy kolmeen selkeään tarpeeseen: äärimmäisiin nopeuksiin, laitteiden suureen lukumäärään sekä kriittisiin sovelluksiin, jossa viiveet ja luotettavuus ovat keskeisiä tekijöitä [24]. Erilaiset sovellukset hyödyntävät yhtä tai useaa näistä tarpeista, niin IoT:n osalta kuin muiltakin käyttäjäkunnilta.

Kuvassa 5 on esitelty vasemmalla 5G:n sovelluksia ja palveluita ja oikealla teknologioita, jotka mahdollistavat sovellukset. M2M tarkoittaa laitteiden keskinäistä keskustelua ilman käyttäjän interaktioa. D2D (Device to Device) puolestaan tarkoittaa kahden laitteen välistä suoraa yhteyttä ilman tukiasemaa tai reititintä. IoV (Internet of Vehicles) on osa IoT:tä, joka muodostuu ajoneuvoista. Ajoneuvot voivat esimerkiksi keskustella keskenään ja jakaa työtehtäviä. SDMA (Space Deviced Multiple Access) taas tarkoittaa tilajakoista radioresussien jakoa, jossa fyysisesti sektoroimalla tukiaseman alue useaan sektoriin saavutetaan lisää kapasiteettia. 5G-verkkojen tavoittena on hyvä paikantaminen ulkotiloissa ja erinomainen paikantaminen sisätiloissa. Tavoitteeksi on asetettu 10 metriä ulkona ja alle 1 metri sisällä [25].



Kuva 5. *5G-verkon keskeisiä trendejä. Muokattu lähteestä [1]*

5G-mobiiliverkot tuovat uusia mahdollisuuksia niin IoT:lle kuin paikantamiselle. Esimerkiksi solut tulevat pienenemään ja tihenemään, mikä tarjoaa itsessään jo tarkempaa sijaintitietoa. Soluja voi olla myös uusissa paikoissa, kuten julkisissa ajoneuvoissa. Myös adaptiivinen keilanmuokkaus ja massiivi-MIMO (Multiple Input Multiple Output) mahdollistavat dynaamisesti sektoroidut solut, jotka voivat olla erittäin pieniä, esimerkiksi muutamia neliömetrejä. Tällöin paikannustarkkuus voi olla erittäin hyvä. [1]

5G-verkoissa on muutoinkin huomioitu erityisesti IoT:n tarpeita. Esimerkiksi NB-IoT (Narrowband Internet of Things) on teknologia, joka mahdollistaa kapeakaistaiset lähetykset mobiiliverkoissa. Esimerkiksi 4G:ssä käytettävän OFDM-signaalin (Orthogonal Frequency Division Multiplexing) pienin kaistanleveys on 1,4 MHz, mikä mahdollistaa suurehkon datanopeuden, mutta kuluttaa paljon virtaa ja on monimutkaisempi toteuttaa. NB-IoT:ssä taas taajuuskaista on vain 180 KHz. Tämä sallii pienemmän nopeuden alhaisemmalla virrankulutuksella. Lisäksi samalle kaistalle mahtuu enemmän laitteita. NB-IoT tosin ei pysty tarjoamaan yhtä alhaisia viiveitä kriittisiin sovelluksiin kuin perinteinen laajakaistayhteys. [26, 8]

LTE-verkossa (Long-Term Evolution) on jo esitelty PRS-signaalit (Positioning Reference Signal) helpottamaan laitteen paikannusta. Kaikki tukiasemat siis lähettävät tällaisia referenssisignaaleja ja päätelaite voi paikantaa itsensä usean tukiaseman referenssisignaalien suhteen. Normaalisti referenssisignaalit kuitenkin vaihtavat taajuutta OFDM-signaalin sisällä, eli käyttävät taajuushyppelyä. NB-IoT:ssä asia on korjattu lisäämällä jokaiselle kantoaallolle oma referenssisignaali. Referenssisignaalissa ja saapumisajassa ongelmana on muun muassa kriittinen ajoitus, koska 1 nanosekunnissa valo etenee 30 metriä. Käytännössä tämä tarkoittaa, että alle kymmeneen metrin tarkkuus edellyttää erittäin suuria näytteenottotaajuuksia ja analysointia, eikä tällainen ole välttämättä mahdollista pienen

virrankulutuksen laitteissa. Yksi mahdollisuus olisikin käyttää ylälinkkiä paikantamiseen, eli käytännössä useat tukiasemat yrittäisivät paikantaa päätelaitteen sen lähettämän signaalin perusteella. LTE-verkossa PRS-signaalien avulla paikantamitarkkuudeksi saadaan 10-100 metriä. [8]

Millimetriaaltojen hyödyntäminen paikantamisessa on yksi keino saavuttaa hyvä tarkkuus. Esimerkiksi ajoneuvot voivat muodostaa Ad-Hoc -verkon eli verkon, jossa ei ole varsinaista reititintä eikä solmuja. Tällaisessa verkossa ajoneuvot voivat paikantaa itsensä suhteessa muihin, eli saada suhteeellisen paikkatiedon. Paikantaminen perustuu esimerkiksi signaalin etenemisaikaan. Millimetriaalloilla (30 GHz - 300 GHz) voidaan saavuttaa jopa alle 10 senttimetrin tarkkuus, mutta riippuen käytetystä menetelmästä sekä signaali-kohinasuhteesta tarkkuus jää alle metriin. [27]

4 YHTEENVETO

Esineiden internet on aiheena melko laajasti tunnettu ja siihen liittyy paljon erilaisia konteksteja. Tässä työssä tarkasteltiin paikantamista osana esineiden internetiä sekä erilaisia paikantamisen menetelmiä sisällä sekä ulkona. Sisätila eroaa ulkona paikantamisesta siinä, että ulkoa tulevat signaalit kuuluvat usein heikosti sisälle, ja sisällä monitie-eteneminen on voimakasta, mikä hankaloittaa paikantamista edelleen. Toisaalta sisätiloissa vaadittava tarkkuus on usein pienempi eli metriluokkaa tai alle, kun ulkona riittää usein kymmenet tai sadat metrit.

Esineiden internetissä tärkeitä kriteerejä paikantamiselle ovat sijainnin tarkkuus, paikantamisen viive sekä virrankulutus. Eri menetelmillä saavutetaankin erilainen suorituskyky edellä mainittujen vaatimusten suhteen. Monet laitteista tulevat olemaan pieniä ja kuluttavat vähän virtaa, jolloin nämä vaatimukset täytyy huomioida myös paikantamisessa. Ulkotiloissa suosituin paikantamisen menetelmä on edelleen GPS verrattain hyvän laadun sekä erittäin hyvän peiton vuoksi. Sisätiloissa taas WLAN-fingerprinting -menetelmä on suosittu olemassaolevan infrastruktuurin vuoksi. Myös RFID on erittäin käytetty menetelmä esimerkiksi tuotteiden seurantaan ja fyysisen pääsyn hallintaan. Kehitteillä on useita erilaisia paikantamisen menetelmiä monien antureiden avulla: magneettisesti, visuaalisesti sekä mobiiliverkkojen avulla.

Taulukossa 3 on vertailtu ja koostettu yhteen eri menetelmien ominaisuuksia ja soveltuvuuksia. Menetelmät ovat tarkemmin esiteltynä luvussa 3. Osa menetelmistä on jo laajasti käytössä, osa taas on joko tulevaisuudessa käytössä tai mahdollisesti ei tule käyttöön laajemmin. Esimerkiksi 5G tuo mukanaan paljon mahdollisuuksia paikantamiseen. Tärkeää on huomata menetelmien erilaiset luonteet ja etteivät menetelmät useinkaan ole toisensa poissulkevia, minkä takia monesti hyödynnetään eri menetelmiä samanaikaisesti parhaan lopputuloksen saamiseksi.

Taulukko 3. *Eri paikannusmenetelmien ominaisuuksia*

Menetelmä	Ominaisuudet
GNSS (GPS)	**Hyödyt:** Soveltuu hyvin ulkotiloihin, laajasti saatavilla ympäri maailman **Haasteet:** Suuri virrankulutus, sijainnin löytäminen aluksi voi olla hidasta, tarkkuus metriluokkaa, ei sovellu yksinään kriittisiin sovelluksiin **Sovellus:** Paikantaminen ulkona ja mahdollisesti syrjässä, esimerkiksi luonnossa tai maantiellä
WLAN-fingerprinting	**Hyödyt:** Soveltuu hyvin sisätiloihin, infastruktuuri pitkälti olemassa niin toimistoissa kuin kotonakin **Haasteet:** Datan kerääminen ja kartoitus aluksi voi olla aikaavievää ja kallista, datan ajantasaisuuden takaaminen tukiasemien tai rakennusten muuttuessa **Sovellus:** Käyttäjän likimääräinen paikantaminen toimistossa tai kauppakeskuksessa kerroksittain ja huoneittain, esimerkiksi lentokentät ja museot [13]
RFID	**Edut:** Edullinen tapa paikantaa tuotteita suhteessa lukulaitteeseen, voidaan paikantaa ja tunnistaa suuria määriä, esimerkiksi ostoskorillinen, tuotteita kerralla **Haasteet:** Jokainen tuote tarvitsee oman tunnisteen, eikä kaikista halvimpiin tuotteisiin ole vielä järkevää laittaa tunnisteita **Sovellus:** Tuotteiden seuranta logistiikassa tai jälleenmyynnissä sekä kirjastot [13]
Mobiiliverkot	**Edut:** Verrattain yleisesti saatavilla, 5G:n myötä erittäin hyvä suorituskyky niin sisällä kuin ulkona **Haasteet:** Infrastruktuurin pystyttäminen, ei toistaiseksi tue merkittävää paikannusta **Sovellus:** Itseajavat autot, navigointi
Led-valaisinten avulla paikannus	**Edut:** asiakaslaitteet kuten älypuhelimet laajasti saatavilla **Haasteet:** synkronointi valaisten välillä, mikäli käytetään TDOA-menetelmää **Sovellus:** navigointi sisätiloissa ja sijaintiperusteiset palvelut: esimerkiksi keskeisen tuotetiedon tai -esitteiden nopea löytyminen [20]

LÄHTEET

[1] M. Agiwal, A. Roy, and N. Saxena, "Next generation 5g wireless networks: A comprehensive survey," *IEEE Communications Surveys Tutorials*, vol. 18, pp. 1617–1655, thirdquarter 2016.

[2] L. D. Xu, W. He, and S. Li, "Internet of things in industries: A survey," *IEEE Transactions on Industrial Informatics*, vol. 10, no. 4, pp. 2233–2243, 2014.

[3] S. K. Goudos, P. I. Dallas, S. Chatziefthymiou, and S. Kyriazakos, "A survey of iot key enabling and future technologies: 5g, mobile iot, sematic web and applications," *Wireless Personal Communications*, vol. 97, pp. 1645–1675, Nov 2017.

[4] L. Atzori, A. Iera, and G. Morabito, "The internet of things: A survey," *Computer Networks*, vol. 54, no. 15, pp. 2787–2805, 2010.

[5] F. Hussain, "Internet of things : Building blocks and business models," pp. 2–4, Springer, 2017.

[6] Al-Fuqaha, Guizani, Mohammadi, Alehadri, and Ayyash, "Internet of things: A survey on enabling technologies, protocols, and applications," *IEEE Communications Surveys Tutorials*, vol. 17, no. 4, pp. 2347–2376, 2015.

[7] J. Li, X. Cui, Z. Li, and J. Liu, "Method to improve the positioning accuracy of vehicular nodes using ieee 802.11p protocol," *IEEE Access*, vol. 6, pp. 2834–2843, 2018.

[8] X. Lin, J. Bergman, F. Gunnarsson, O. Liberg, S. M. Razavi, H. S. Razaghi, H. Rydn, and Y. Sui, "Positioning for the internet of things: A 3gpp perspective," *IEEE Communications Magazine*, vol. 55, pp. 179–185, December 2017.

[9] S. M. Riazul Islam, D. Kwak, M. Humaun Kabir, M. Hossain, and K.-S. Kwak, "The internet of things for health care: A comprehensive survey," *IEEE Access*, vol. 3, pp. 678–708, 2015.

[10] L. Chen, S. Thombre, K. Jarvinen, E. S. Lohan, A. Alen-Savikko, H. Leppakoski, M. Z. H. Bhuiyan, S. Bu-Pasha, G. N. Ferrara, S. Honkala, J. Lindqvist, L. Ruotsalainen, P. Korpisaari, and H. Kuusniemi, "Robustness, security and privacy in location-based services for future iot: A survey," *IEEE Access*, vol. 5, pp. 8956–8977, 2017.

[11] A. Juels, "Rfid security and privacy: a research survey," *IEEE Journal on Selected Areas in Communications*, vol. 24, pp. 381–394, Feb 2006.

[12] PricewaterhouseCooper, "Cross-cutting business models for iot." https://publications.europa.eu/en/publication-detail/-/publication/da41ca52-113a-11e8-9253-01aa75ed71a1, 2017. viitattu: 10.5.2018.

[13] Z. B. Tariq, D. M. Cheema, M. Z. Kamran, and I. H. Naqvi, "Non-gps positioning systems: A survey," *ACM Comput. Surv.*, vol. 50, pp. 57:1–57:34, Aug. 2017.

[14] M. Mahmoud, "A study of efficient power consumption wireless communication techniques / modules for internet of things (iot) applications." http://dx.doi.org/10.4236/ait.2016.62002, 2016. viitattu: 17.4.2018.

[15] S. Goswami, *Indoor Location Technologies*, pp. 29–47. New York, NY: Springer, 2013.

[16] A. Khalajmehrabadi, N. Gatsis, and D. Akopian, "Modern wlan fingerprinting indoor positioning methods and deployment challenges," *IEEE Communications Surveys & Tutorials*, vol. 19, no. 3, pp. 1974–2002, 2017.

[17] S.-H. Fang, T.-N. Lin, and K.-C. Lee, "A novel algorithm for multipath fingerprinting in indoor wlan environments," *IEEE Transactions on Wireless Communications*, vol. 7, no. 9, 2008.

[18] R. Want, "An introduction to rfid technology," *IEEE Pervasive Computing*, vol. 5, no. 1, pp. 25–33, 2006.

[19] E. Welbourne, L. Battle, G. Cole, K. Gould, K. Rector, S. Raymer, M. Balazinska, and G. Borriello, "Building the internet of things using rfid: The rfid ecosystem experience," *IEEE Internet Computing*, vol. 13, no. 3, pp. 48–55, 2009.

[20] N. Hassan, A. Naeem, M. Pasha, T. Jadoon, and C. Yuen, "Indoor positioning using visible led lights: A survey," *ACM Computing Surveys (CSUR)*, vol. 48, no. 2, pp. 1–32, 2015;2016;.

[21] Philips, "Indoor positioning." http://www.lighting.philips.com/main/systems/lighting-systems/indoor-positioning#, 2018. viitattu: 10.5.2018.

[22] G. Xu, *GPS - Theory, Algorithms and Applications*. Springer, 2 ed., 2007.

[23] P. A. Zandbergen and S. J. Barbeau, "Positional accuracy of assisted gps data from high-sensitivity gps-enabled mobile phones," *The Journal of Navigation*, vol. 64, no. 3, pp. 381–399, 2011.

[24] E. Cero, J. B. Husi¿, and S. Barakovi¿, "Iot¿s tiny steps towards 5g: Telco¿s perspective," *Symmetry*, vol. 9, no. 10, p. 213, 2017.

[25] NGMN, "Ngmn 5g white paper." https://www.ngmn.org/fileadmin/ngmn/content/downloads/Technical/2015/NGMN_5G_White_Paper_V1_0.pdf, 2015. viitattu: 20.4.2018.

[26] A. Hoglund, X. Lin, O. Liberg, A. Behravan, E. A. Yavuz, M. V. D. Zee, Y. Sui, T. Tirronen, A. Ratilainen, and D. Eriksson, "Overview of 3gpp release 14 enhanced nb-iot," *IEEE Network*, vol. 31, pp. 16–22, November 2017.

[27] X. Cui, T. A. Gulliver, J. Li, and H. Zhang, "Vehicle positioning using 5g millimeter-wave systems," *IEEE Access*, vol. 4, pp. 6964–6973, 2016.