Eemeli Merisalo

Sensoriverkot

Metropolia Ammattikorkeakoulu

Insinööri (AMK)

Tietotekniikka

Insinöörityö

16.4.2015

Metropolia

Tekijä(t) Otsikko Sivumäärä Aika	Eemeli Merisalo Sensoriverkot 38 sivua 16.4.2015
Tutkinto	Insinööri (AMK)
Koulutusohjelma	Tietotekniikka
Suuntautumisvaihtoehto	Tietoverkot
Ohjaaja(t)	Director of Service Operations Matti Pärssinen, Cygate Oy Lehtori Jukka Louhelainen

Työn tavoitteena on tutustua sensoriverkkoihin, niiden toimintaan ja niiden käyttämiin siirtoyhteyksiin. Tässä insinöörityössä käydään läpi, minkälaista osaamista sensoriverkkojen hallinta ja valvonta vaativa palveluntuottajalta.

Työ on tehty kirjallisena tutkimuksena ilman käytännön osuutta. Se pitää sisällään useista lähteistä kerättyä ja analysoitua tietoa.

Sensoriverkkojen tietoturva, niiden käyttämät teknologiat ja siirtoyhteydet, mukaan lukien teollinen internet ovat tämän työn pääkohdat. Pääkohdat käydään läpi yksityiskohtaisesti esimerkkien ja kuvien avulla. Työssä käydään läpi myös sensoriverkkojen hyötyjä ja riskejä.

Sensoriverkot ovat yleistymässä ja ne tuovat mukanaan haasteita, kuten tietoturvan kehityksen ja jatkuvasti kehittyvät teknologiat.

Haasteista huolimatta voidaan todeta sensoriverkkojen ja teollisen internetin hyödyn olevan kiistaton.

Avainsanat	teollinen, internet, sensoriverkot, sensori, solmu

Author(s) Title Number of Pages Date	Eemeli Merisalo Sensor Networks 38 pages 16 April 2015
Degree	Bachelor of Engineering
Degree Programme	Information and Communications Technology
Specialisation option	Data Networks
Instructor(s)	Matti Pärssinen, Director of Service Operations, Cygate Oy Jukka Louhelainen, Senior Lecturer

The main goal of this bachelor's thesis was to research sensor networks and to study their transfer connections. The question this thesis answers is what kind of understanding the service provider needs to monitor and manage sensor networks.

This thesis is a research without a practical part. It contains information gathered from several different sources.

The security of sensor networks, their technologies and transfer connections are the main points of this thesis. Industrial Internet is also briefly covered. The main points are covered in detail with figures and examples. The benefits and disadvantages of the sensor networks are also included in the study.

Sensor networks are becoming more and more common creating challenges such as security and developing technologies. Even if there are some challenges it is safe to say that sensor networks and Industrial Internet are and will be extremely useful.

Keywords	Industrial, Internet, node, sensor, network

Sisällys

Lyhenteet

IoT	Internet of Things eli asioiden internet. Asiat, jotka ovat liittyneet Internetiin yksilöllisillä tunnisteilla.
M2M	Machine to Machine. Laitteesta suoraan toiselle laitteelle toimiva yhteys.
WPAN	Wireless Personal Area Network. Suomeksi likiverkko.
ETSI	European Telecommunications Standards Institute. Eurooppalainen tele-kommunikointialan standardointijärjestö.
GSM	Global System for Mobile Communications. Maailmanlaajuisesti käytetty matkapuhelinjärjestelmä.
GPRS	General Packet Radio Service. GSM-verkoissa toimiva pakettikytkentäinen tiedonsiirtopalvelu.
EDGE	Enhanced Data rates for Global Evolution. Matkapuhelinten pakettikytkentäiseen tiedonsiirtoon suunniteltu tekniikka.
ITU	International Telecommunication Union. Kansainvälinen telekommunikaatioliitto.
IMT-2000	International Mobile Telecommunications-2000. ITU:n määrittelemä standardiperhe 3G-teknologioille.
LTE	Long Term Evolution. 4G-standardi.
WiMAX	Worldwide Interoperability for Microwave Access. 4G-standardi.
W-CDMA	Wideband Code Division Multiple Access. 3G-protokolla.
6LoWPAN	IPv6 over Low power Wireless Personal Area Networks. Vähän virtaa kuluttava langaton likiverkko.

CSMA/CD Ethernetin kaistanvarausmenetelmä on CSMA/CD (Carrier Sense Multiple Access With Collision Detection.

1 Johdanto

Sensoriverkot on yksi suurimmista teollisen internetin alueista. Sensoriverkkoja käytetään mm. erilaisissa tehtaissa ja valtateillä valvomaan ja hallitsemaan esimerkiksi lämpötiloja tai muuta toiminnallisuutta.

Suuret määrät toisiinsa liitettyjä sensoreita muodustavat verkkoja, jotka keräävät dataa ja lähettävät sen analysoitavaksi. Sensoriverkkoja voi datan keräämisen lisäksi käyttää ohjaamaan erilaisia laitteita. ”Puhtaat” sensoriverkot pyritään rakentamaan vähän virtaa kuluttaviksi. Tällaisia verkkoja varten onkin luotu omia protokolliaan kuten ZigBee ja 6LoWPAN. Nämä protokollat mahdollistavat sensorien välisen vähän virtaa kuluttavan kommunikoinnin.

Tässä työssä pyritään vastaamaan kysymykseen, minkälaista osaamista sensoriverkkojen valvonta ja hallinta vaativat palveluntuottajalta. Työssä käsitellään sensoriverkkoja itsessään, sensorien välillä käytettäviä protokollia ja siirtoyhteyksiä, joilla data liikkuu itse verkkojen ja palvelimien välillä.

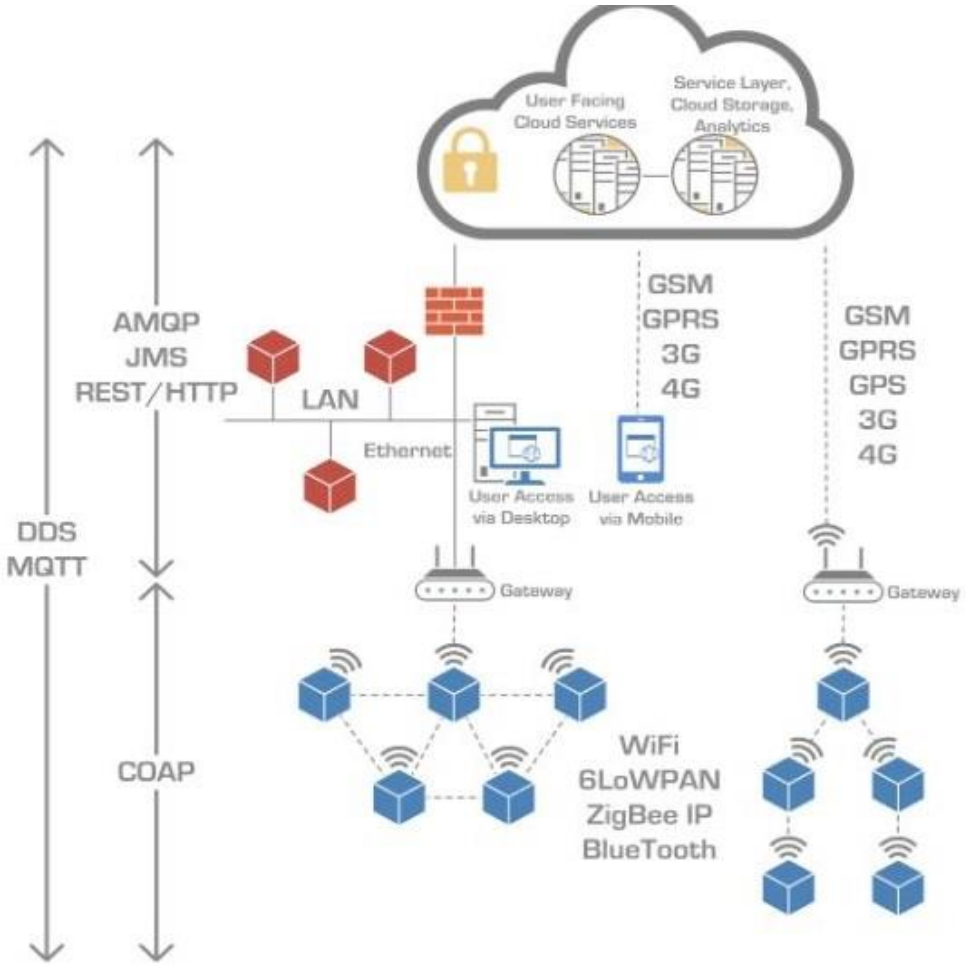
Teollinen internet on Genereal Electricin lanseeraama termi, joka sitoo toisiinsa fyysiset laitteet, ohjelmistot ja niihin liitetyt sensoriverkot [1]. Internet of Things eli asioiden internet käsitteellä tarkoitetaan usein samaa kuin termillä teollinen internet, vaikka eroja on. Teollisen internetin tavoitteena on toiminnan tehostaminen ja teollinen tuottavuus, kun IoT tarkoittaa ”kaikkien esineiden” verkottumista.

2 Teollinen internet

Kun teollisuudessa laitteiden toimintaa pyritään automatisoimaan ja niiden valvontaa halutaan kehittää, voidaan niihin liittää sensoreita. Sensoreilla voidaan valvoa suuriakin tehtaita ja niiden laitteiden toimintaa erittäin tarkasti. Sensoriverkot mahdollistavat nykyään myös laitteiden hallinnan internetin yli. Eli jos tehdas sijaitsee Joensuussa ja halutaan nopeuttaa yhden linjaston tahtia, voidaan se ohjelmoida Helsingistä. Näin helppoa se nykyään on. Sensoriverkot muodostavat teollisen internetin ytimen yhdessä

Big Datan kanssa. Big Data tarkoittaa hyvin suuren tietomäärän keräämistä, käsittelemistä, analysointia ja säilömistä.

Käsitteinä Teollinen internet ja Internet of Things sekoitetaan hyvinkin usein ja niillä tarkoitetaankin lähes samaa asiaa. Erona on, että teollinen internet tarkoittaa hyötykäyttöön valjastettua laitteiden verkkoa ja Internet of Things kattaa myös huvikäyttöön tarkoitetut sovellutukset. Molemmissa luodaan yhteyksiä laitteiden välille niin, että yhteydet kulkevat myös Internetin yli. [2.]



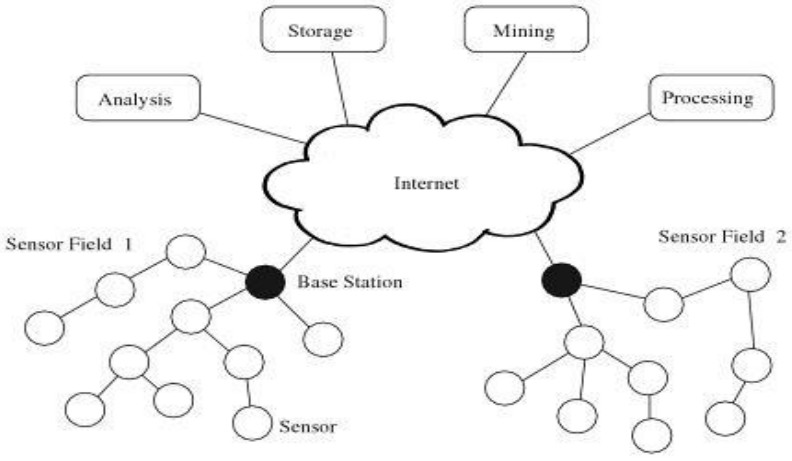
Kuva 1. Teollinen internet – yhteyskaavio [3]

3 Sensoriverkot

Sensoriverkot ovat langattomaan teknologiaan perustuvia verkkoja, jotka ovat olennainen osa teollista internetiä. Sensoreihin perustuvia verkkoja voidaan käyttää mm. ilman saasteiden monitorointiin, veden laadun monitorointiin tai esimerkiksi tehtaissa laitteiden toimivuuden varmistamiseen. Esimerkiksi suureen tunneliin voi olla asennettuna satoja, tai jopa tuhansia sensoreita, jotka kommunikoivat keskenään. Kun sensorit havaitsevat esimerkiksi hiilimonoksidipitoisuuden liian korkeaksi, ne reagoivat ja lähettävät signaalin palvelimelle, joka reagoi saastepitoisuuden nousuun ja tekee tarvittavat toimenpiteet. Tai ihminen, joka seuraa palvelimen tapahtumia reagoi CO-pitoisuuden nousuun ja esimerkiksi sulkee tunnelin. [4.]

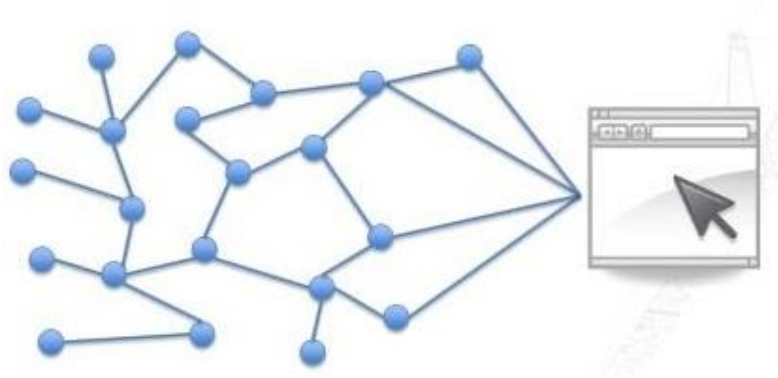
Waltenegus Dargie ja Christian Poellabauer kuvaavat hyvin sensoriverkkojen hyötyjä kirjassaan [5, s. 3]:

> Sensors link the physical world with the digital world by capturing and revealing real-world phenomena and converting these into a form that can be processed, stored, and acted upon. Integrated into numerous devices, machines, and environments, sensors provide a tremendous social benefit. They can help to avoid catastrophic infrastructure failures, conserve precious natural resources, increase productivity, enhance security, and enable new applications such as context-aware systems and smart home technologies.

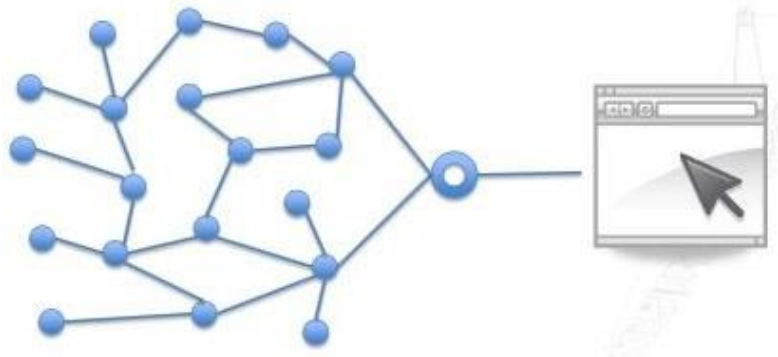


Kuva 2. Sensoriverkon toiminnan pääpiirteet. [6]

Suuri määrä sensoreita muodostaa verkon, joka kerää dataa ja lähettää sen analysoitavaksi. Nykyiset sensoriverkot ovat ns. kaksisuuntaisia eli niiden avulla voidaan datan keräämisen lisäksi myös ohjata joko yhtä tai useampaa laitetta. Sensoriverkot ovat pääsääntöisesti joko ”puhtaita” mesh-verkkoja (kuva 3) tai yhdyskäytävämallin mukaisia verkkoja, jossa sensorit muodostavat kuitenkin keskenään mesh-verkon (kuva 4). Myös muunlaisia verkkoja voidaan käyttää, mutta se ei ole sensoriverkoille ideaalista.



Kuva 3. Mesh-verkko



Kuva 4. Yhdyskäytävämalli

Mesh-verkoissa useat solmukohdat ovat yhteydessä toisiinsa kuvien osoittamalla tavalla. Solmukohdat ovat laitteita tai tässä tapauksessa sensoreita. Sensori voi viestiä tietoa toiselle sensorille, joka on lähempänä verkon yhteistä yhdyskäytävää, tai sensorit voivat olla yhteydessä suoraan internetiin lähettäen kerättyä dataa. Tai vastaavasti Internetistä käsin voidaan ohjata verkkoja tai niiden laitteita. Jos yksittäinen sensori on

suoraan yhteydessä interntiin, tarvitaan IPv6-protokollaa käyttävä standardi, kuten 6LoWPAN.

Sensoriverkot eivät itsessään ole minkään arvoisia ilman palvelimia, joihin sensoriverkko on yhteydessä. Palvelimet tekevät sen tärkeän työn, kuten datan tallennuksen, prosessoinnin ja analysoinnin. Datan määrä, jota sensoriverkot tuottaa, on erittäin suurta ja sille onkin oma käsitteensä, Big Data. Kun palvelimien ja sensoriverkkojen välinen yhteys toimii toivotulla tavalla, voidaan sensoriverkkoja hyödyntää erittäin laajoihin tarkoituksiin. Tämän kokonaisuuden toimintaan vaikuttavat itse sensoreiden väliset yhteydet sekä datan siirtoyhteydet.

3.1 Sensoriverkkojen teknologiat

Sensorit voivat olla yhteydessä toisiinsa erilaisten protokollien avulla, kuten Wifi, 6LoWPAN, Bluetooth tai ZigBee. Kun käytetään suuria määriä pelkkiä sensoreita tietoverkon rakentamiseen, on huomioitava virrankulutus; sensoreilla ei ole ulkoisia virtalähteitä, joten vähävirtaiset protokollat ovat optimaalisia tällaisiin verkkoihin. Protokollan valinnassa on myös otettava huomioon kantama, datan siirtonopeus ja se, tarvitaanko suora yhteys jokaiselta sensorilta internetin yli. Näiden ominaisuuksien perusteella on valikoitunut kaksi suurinta protokollaa sensoriverkkoihin, eli ZigBee ja 6LoWPAN. Alla ei ole läpikäytynä kaikkia sensoriverkkojen teknologioita vaan suhteellisen kattava läpileikkaus suurimmista.

3.1.1 ZigBee

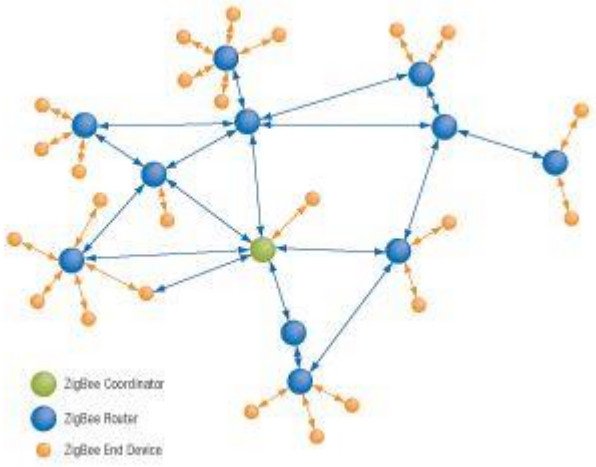
IEEE 802.15.4 -standardiin perustuva lyhyen kantaman tietoliikenneverkko eli ZigBee on vähävirtainen langaton verkko, joka määritellään OSI-mallin fyysisellä ja siirtoyhteyskerroksella. ZigBee on vähävirtainen langaton verkko, joka on määritelty avoimessa IEEE 802.15.4 -standardissa [7]. IEEE 802.15 -standardit määrittelevät langattomat WPAN-yhteydet.

ZigBee soveltuu erityisen hyvin M2M-sensoriverkkoihin pienen virrankulutuksen takia ja akun kesto sitä käyttävillä laitteilla saattaa olla useita vuosia. Se toimii lisensoimattomilla 2.4 GHz, 900 (915) MHz ja/tai 868 MHz –taajuuksilla.

Maksimaalinen datansiirtonopeus vaihtelee taajuuden mukaan välillä 20 – 250 kbps [8]. ZigBee käyttää IEEE 802.15.4 -standardin määrittelemää AES128-salausta.

Dataa siirretään maksimissaan 128 tavun paketteina, jolloin yhden paketin tietosisältö on 104 tavua. IEEE 802.15.4 -standardi tukee 64-bittisiä IEEE-osoitteita, jolloin täyteen verkkoon voidaan liittää jopa 65 000 solmua. Kun solmujen välimatka voi olla jopa 70 metriä, voidaan todeta että ZigBee mahdollistaa erittäin suurien, vähävirtaisten verkkojen rakentamisen [8; 9]. Jos solmukohtia on yli 2^16, voidaan verkko jakaa omikse aliverkoikseen, eli ZigBee-verkkojen solmukohtien määrää voidaan lisätä lähes loputtomasti [10].

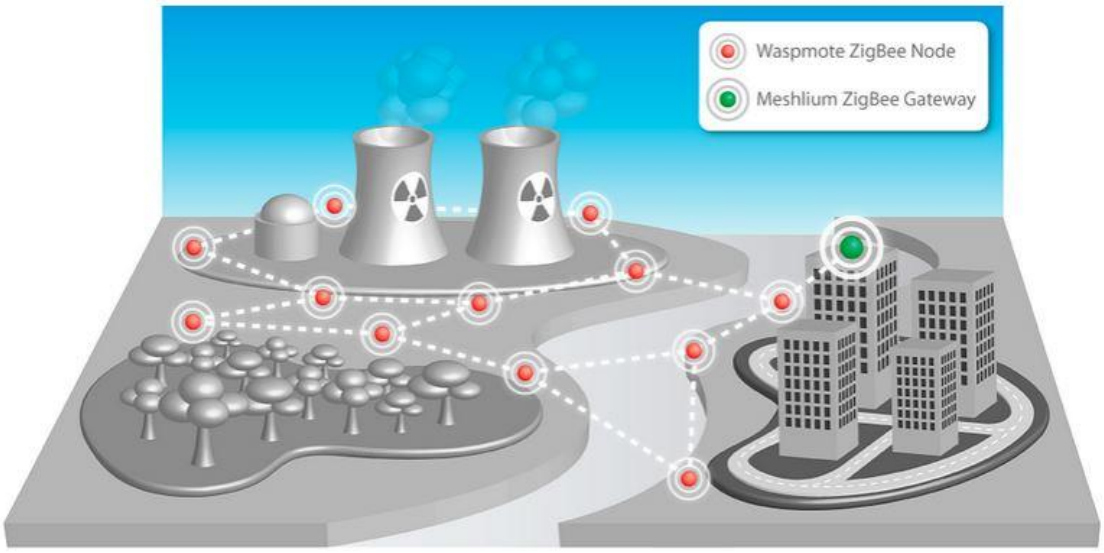
IEEE 802.15.4 -standardi määrittelee ZigBee-verkkoon kaksi fyysistä ja kolme loogista tyyppiä. Fyysiset tyypit ovat Full Function Device (FFD) ja Reduced Function Device (RFD). Näiden tyyppien ero on siinä, että vain FFD-laitteet voivat toimia verkossa reitittiminä, kun molemmat muuten voivat toimia itse sensorina. Kolme loogista tyyppiä ovat päätelaite eli sensori, reititin ja koordinaattori, joka on vastuussa verkon muodostamisesta ja verkon tietojen säilyttämisestä. Koordinaattori on FFD-laite. [10.]



Kuva 5. ZigBee-tietoverkko. Oranssit toimivat vain sensoreina, siniset sensoreina ja reitittiminä. Vihreä verkon koordinaattori, josta liikenne lähtee verkon yhdyskäytävän kautta eteenpäin. [10]

ZigBee-verkko tarvitsee oman yhdyskäytävän datan kuljettamiseen verkosta. Data kulkee kohti yhdyskäytävää reitittimien määräämää reittiä sensorilta toiselle. Reitityksen täytyy olla jollain tapaa ns. järkevää eli se ei yksinkertaisesti käytä lyhintä

mahdollista fyysistä reittiä, vaan reitti riippuu muilta sensoreilta saadusta informaatiosta. [10.]



Kuva 6. ZigBee-verkko ydinvoimalan säteilyn monitorointiin. Kuva havainnollistaa käytännönläheisemmin minkälaisiin sovellutukseen ZigBee-verkkoja voidaan käyttää. [11]

ZigBee IP on perinteisen ZigBeen laajennus, joka tuo sensoreille IPv6-osoitteet ja tiukemman tietoturvan. ZigBee IP:n avulla yksittäiset sensorit voivat olla suoraan yhteydessä Internetiin ja sen yli. [11.]

ZigBee Alliancen tiedotteessa 27.3.2013 todettiin seuraavaa koskien ZigBee IP:tä [11].

> The ZigBee® Alliance, a global ecosystem of companies creating wireless solutions for use in energy management, commercial and consumer applications, today announced the completion and public availability of its third specification, ZigBee IP. ZigBee IP is the first open standard for an IPv6-based full wireless mesh networking solution and provides seamless Internet connections to control low-power, low-cost devices.

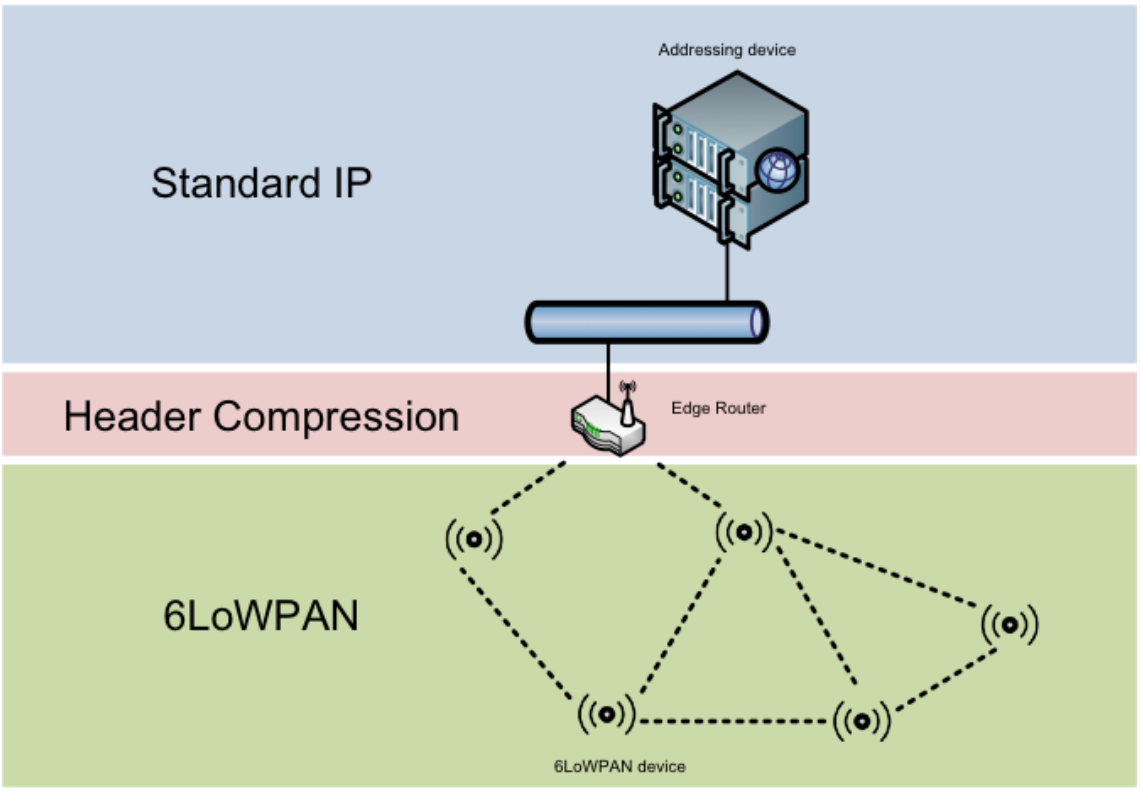
Kuten yllä todettu, ZigBee IP mahdollistaa IPv6-pohjaisen full mesh -verkon toteuttamisen, jonka avulla voidaan saumattomasti kontrolloida vähävirtaisia sensoreita Internetin yli. IPv6-osoitteiden avulla voidaan ZigBee IP:tä käyttävät sensorit kytkeä myös muihin IPv6-osoitteita käyttäviin verkkoihin, kuten WLAN-verkkoihin.

3.1.2 6LoWPAN

6LoWPAN tarkoittaa vapaasti suomennettuna IPv6-osoitteita käyttävää vähävirtaista likiverkkoa. Näissä verkoissa jokaiselle sensorille määritellään oma typistetty 64-bittinen IPv6-osoite, jonka avulla ne kommunikoivat toisilleen, sekä Internetin yli palvelimille. Tällaisen sensoriverkon yhdyskäytävä muokkaa osoitteita sekä paketteja niin sanotun sisäverkon ja ulkoverkon välillä. [12.]

Yhdyskäytävä pakkaa ja purkaa IPv6-paketteja tavallisten IPv6- ja 6LoWPAN-verkkojen välillä. Kun IPv6-paketti paketti tulee ulkoisesta verkosta 6LoWPAN-verkkoon, irrottaa yhdyskäytävä siitä 64-bittisen kohdeosoitteen prefixin. Sama toisin päin, eli kun paketti lähtee 6LowPAN-verkosta, liittää yhdyskäytävä siihen 64-bittisen osoite-prefixin. Prefixin poistamisen jälkeen osoitteet ovat 64-bittisiä IPv6-osoitteita. Joissain tapauksissa yhdyskäytävä voi pakata pakettia vielä lisää, jolloin 6LoWPAN-verkon osoitteet jäävät vain 16 bitin pituisiksi, omassa verkossaan persoonallisiksi osoitteiksi. [12.]

Itse sensoriverkko toimii IEEE 802.15 -standardissa määritellyllä tavalla eli verkon laitteet, sensorit, toimivat langattomassa ympäristössä toisilleen kommunikoiden. Sensorit keräävät dataa tai vaihtoehtoisesti niillä voidaan ohjata erilaisia laitteita. [13.]

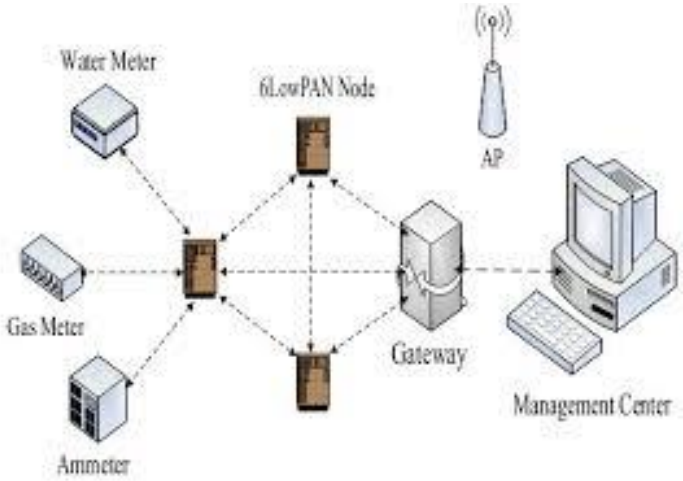


Kuva 7. 6LoWPAN-verkon ja ulkoisen IPv6-verkon riippuvuus. [14]

6LoWPAN on tavallinen internetprotokolla, joka tarvitsee vain reunareitittimen sisäverkon ja IPv6-ulkoverkon välillä. Se ei myöskään tarvitse erillisiä ohjelmistoja toimiakseen, vaan 6LoWPAN-verkon laitteita voi hallita tavallisella tietokoneella mistä päin maailmaa tahansa, kunhan verkko on oikein konfiguroitu. [14.]

Sensorit 6LoWPAN-verkossa operoivat 2,4 GHz:n taajuudella datan siirtonopeuden ollessa 250 kbps. Vaikka verkko reitittyy suoraan IPv6-osoitteiden kanssa, ei yhteen verkkoon voida liittää kuin 100 sensoria. Sensorit voivat kuitenkin olla jopa 200 metrin etäisyydellä toisistaan, mikä mahdollistaa kohtuullisen laajojen verkkojen rakentamisen. [15.]

Vähävirtaisuus ja verkon sensorien suhteellisen pieni määrä tekevät 6LoWPAN:sta optimaalisen kodin tai teollisuuden automatisointiin.



Kuva 8. Esimerkki kodin automatisaatiosta 6LoWPAN-verkolla. [16]

3.1.3 MyriaNed

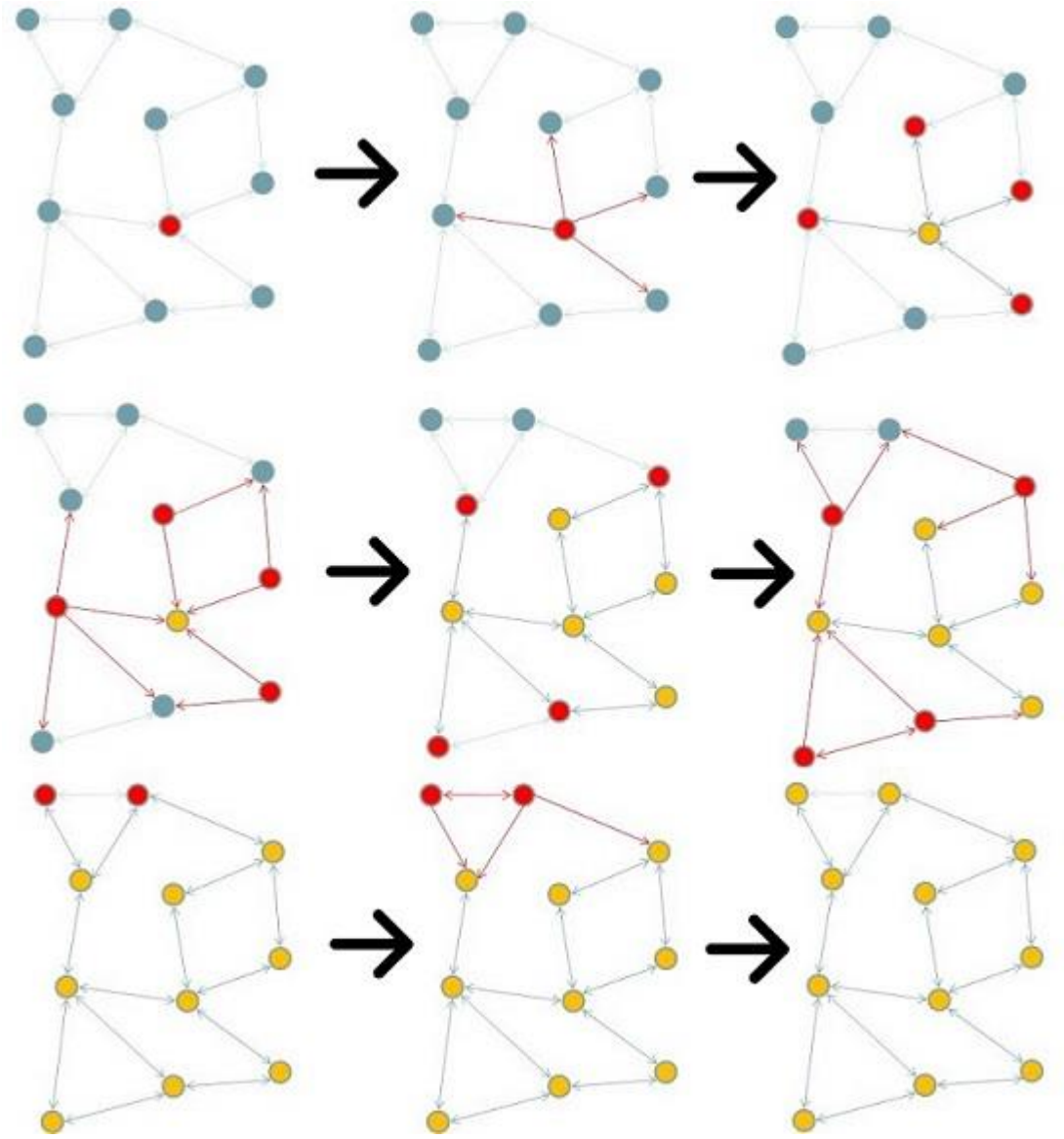
MyriaNed on DevLab:n kehittämä teknologia sensoriverkoille. Siinä verkon laitteet kommunikoivat radiolähetyksellä. Sensoreille ei tarvitse määritellä omaa verkkoaan, vaan ne voivat vapaasti hyppiä verkosta toiseen. Tämä ominaisuus tekee verkoista skaalautuvia joko pieniin, suuriin tai keskisuuriin verkkoihin. Myös sensorien liikuteltavuus tai vaihto onnistuu erittäin hyvin tässä teknologiassa. [17.]

DevLab:n virallisilla MyriaNed –sivuilla kuvaillaan teknologiaa seuraavalla tavalla [18]:

> DevLab's approach is called MyriaNed, which is inspired by biological processes where many nodes (birds, ants, cells) operate in large distributed systems (resp. flocks, organized colonies, organisms). It is a bottom up approach, where the behavior of a single element (node) will result in emerging behavior of the system (application).

Teknologialla on kaksi suurta etua; koska teknologia käyttää broadcast-lähetystä kommunikoimiseen, sen ei tarvitse tuntea naapureitaan ennen viestin lähettämistä. Toinen etu on verkon luotettavuus; lähetetty viesti voi kulkea useita eri reittejä määränpäähänsä. [17.]

MyriaNed-teknologia on itsekonfiguroituva eli jos siitä poistetaan tai siihen lisätään sensori, ei tämä muutos tarvitse konfigurointia vaan verkko toimii saman tien. Verkot ovat puhtaita mesh-verkkoja, joissa sensorit kommunikoivat kaikille lähellä olevaille sensoreille. Kuvassa 9 nähdään, että viesti leviää verkossa kuten virus. [17.]

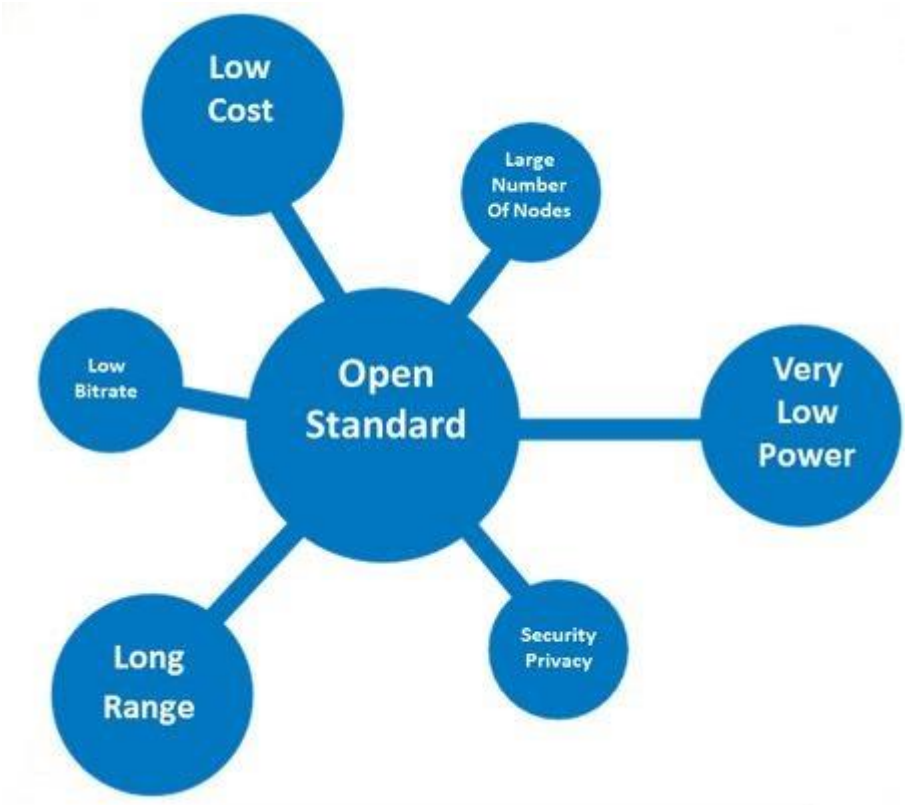


Kuva 9. Viestin ”leviäminen” MyriaNed-verkossa. [19]

3.1.4 DASH7

DASH7 on avoimen lähdekoodin langaton teknologia, joka toimii 433 MHz:n taajuudella. Se on suunniteltu käytettäväksi juuri sensoriverkoissa pienen virrankulutuksensa vuoksi. Tätä teknologiaa käyttävien sensoreiden akku kestää jopa vuosia. Fyysisesti suuriin sensoriverkkoihin DASH7 sopii mitä parhaitan, sillä sen kantama ulkona on jopa muutamia kilometrejä. Teknologian on kehittänyt ja sen standardeja ylläpitää voittoa tavoittelematon DASH7 Alliance. [20.]

DASH7-verkot ovat erittäin kevyitä, sillä useimpien sovellusten pakettien koko on rajattu 256 tavuun sekunnissa ja esimerkiksi ääntä tai videota ei lähetetä verkoissa. Myös useiden peräkkäisten pakettien lähetystä vältetään mutta kyseistä käyttäytymistä voi tarvittaessa esiintyä. Verkoissa ei käytetä beaconeita, vaan solmut vastaavat vain hyväksytyille laitteille. Tämä teknologia on suunniteltu pääasiassa tiedon keräämiseen ja sen eteenpäin lähettämiseen esimerkiksi palvelimille. [20.]



Kuva 10. DASH7-teknologian havainnekuva. [20]

3.1.5 Z-Wave

Z-Wave on erityisesti kodin automaatioon kehitetty langaton teknologia, josta vastaa Z-Wave Alliance. Z-Wave protokollaa käyttävää verkoa voidaan kontrolloida ja monitoroida etäältä päätelaitteella, joka voi olla esimerkiksi älypuhelin. Verkossa ei tarvita niin sanottua koordinoivaa solmua, vaan solmut ovat saman arvoisia. Solmukohdat muodastavat keskenään full mesh -verkon, jossa solmut kommunikoivat useille muille solmuille. [21.]

Z-Wave-sensoriverkot operoivat alle 1 GHz:n taajuuksilla, joten se sopii kodin automaation erittäin hyvin. Se ei aiheuta häiriötä WLAN-teknologioiden tai muiden 2,4GHz:n taajuutta käyttävien teknologioiden kanssa. Tämä taajuuksien käyttöero on kodin automaatiossa hyvinkin tärkeä, sillä erityisesti WLAN-teknologia on yleistynyt. [21.]

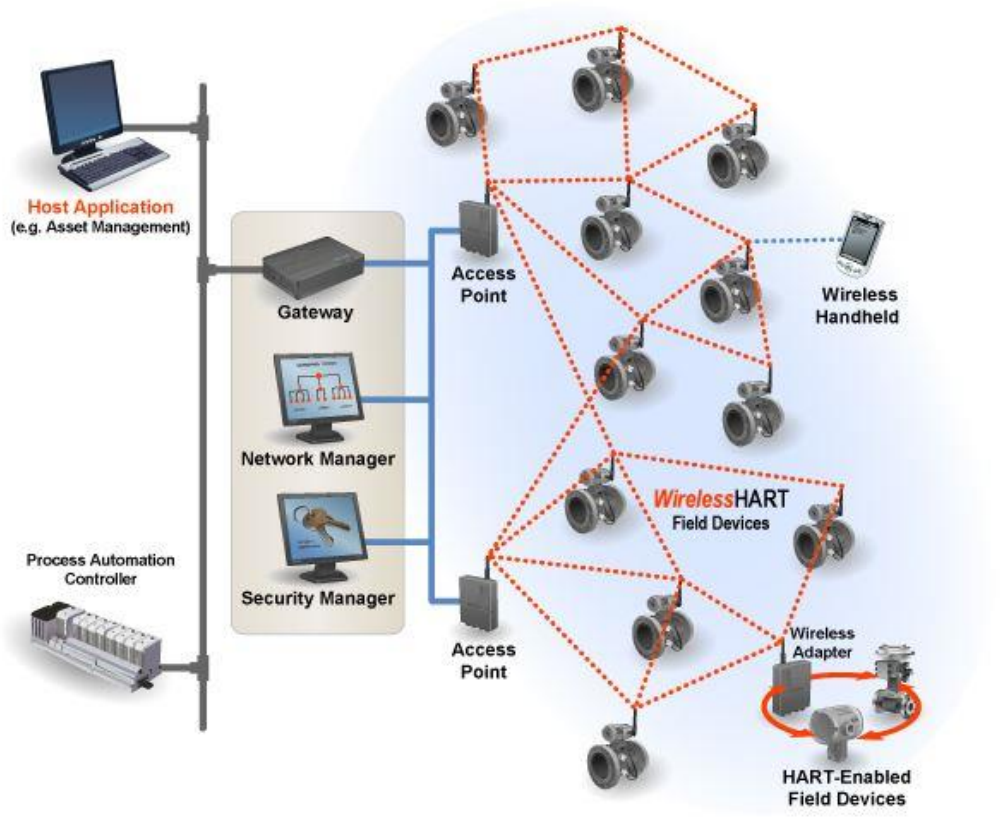
Kuva 11. Esimerkkinä erilaisia kodin laitteita, joita Z-Wavella voidaan valvoa ja ohjata. [22]

3.1.6 WirelessHART

Kuten ZigBeekin, perustuu WirelessHART IEEE 802.15.4 -standardiin ja toimii 2,4 GHz:n taajuusalueella. Tämä teknologia on kehitetty erityisesti teollisuuteen, kuten esimerkiksi suuriin tehtaisiin. WirelessHART-teknologiaa käyttävät verkot ovat itsestään huolehtivia mesh-verkkoja. Verkko tarkkailee datapolkuja ja löytää datan siirrolle vaihtoehtoisen polun, jos esimerkiksi joku verkon solmukohta hajoaa. [23.]

Jokainen WirelessHART-verkko sisältää vähintään yhden tukiaseman, yhdyskäytävän, laitteen, joka hallinnoi verkkoa ja laitteita, joissa on kiinni teknologiaa tukeva adapteri. Itse verkon laitteet, joista kerätään tietoa tai joita ohjataan, ovat mesh-verkkona yhteydessä tukiasemaan. Tukiasemat puolestaan ovat yhteydessä sekä yhdyskäytävään että laitteeseen joka hallinnoi verkkoa. Yhdyskäytävän kautta verkko on yhteydessä päätteeseen, johon tieto kerätään. Hallinnoiva laite on vastuussa verkon konfiguroinnista, verkonlaitteiden kommunikaation ajastuksesta, viestireittien

hallinnoinnista ja verkon tilan monitoroinnista. Jokainen laite voi toimia reitittimenä verkossa, eli ne välittävät viestiä eteenpäin. Näin jokaisen solmun ei tarvitse olla yhteydessä suoraan tukiaseman kautta yhdyskäytävään. [24.]



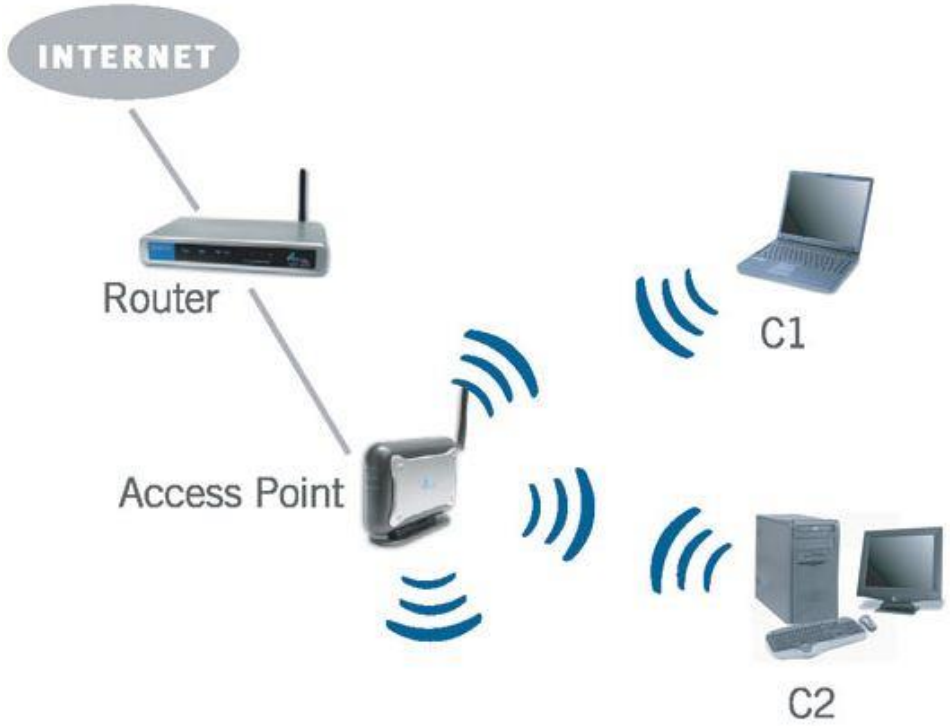
Kuva 12. WirelessHART-verkko käytännössä. [24]

3.1.7 Wi-Fi

Wi-Fi on langaton lähiverkkoteknologia, joka sallii laitteiden kommunikoinnin 2,4 GHz:n ja 5 GHz: taajuuksilla. Jokainen IEEE 802.11 -standardien mukainen WLAN-laite luetaan kuuluvan Wi-Fi:in [25].

IEEE 802.11 -standardien verkot toimivat tukiasemaperiaattella, jossa laitteet yhdistyvät tukiasemiin, ja tukiasemat ovat yhteydessä toisiinsa, joko langattomasti tai kiinteällä yhteydellä. Laitteet voivat olla yhteydessä myös toisiinsa suoraan ad hoc-yhteydellä, joka mahdollistaa kommunikoinnin ilman tukiasemia.

Wi-Fi-laitteet kuluttavat kohtuullisen paljon energiaa, joten ne eivät sovellu sinänsä pelkkiin sensoriverkkoihin. Jos sensori on kiinnitetty laitteeseen, jolla on oma virransyöttö, on Wi-Fi laitteiden käyttö mahdollista myös teolliseen internetiin soveltuvien mesh-verkkojen rakentamiseen.



Kuva 13. WLAN-verkon toimintaperiaate. Tukiasema, johon päätelaitteet ovat yhdistyneet. Reititin, jossa tukiasema on kiinni. Reitittimestä lähtö Internetiin. [26]

3.1.8 Bluetooth

Bluetooth on toinen IEEE 802.15 -standardin WPAN-yhteys, joka mahdollistaa langattoman kommunikoinnin laitteiden välillä (IEEE 802.15.1). Bluetooth on lyhyen kantaman langaton teknologia, ja se käyttää taajuusväliä 2.4 - 2.485 GHz [27]. Kohtuullisen virrankäytön takia (2.5 mW) myöskään Bluetooth ei ole optimaalisin vaihtoehto sensoriverkkoihin [28].

Kuva 14. Erilaisia mahdollisia bluetooth-yhteyksiä

4 Sensoriverkkojen tietoturva

Sensoriverkot, kuten muutkin tietoliikenneverkot, ovat alttiita hyökkäyksille, ja verkkojen turvaaminen onkin tärkeää. Vähäinen teho ja datan tallennustila sekä valvomattomat operaatiot tekevät sensoriverkoista vaikean suojata keinoilla, joita käytetään perinteisissä verkkolaitteissa. Tietoturvan toteuttamista häiritsee myös se, että sensoreiden prosessointiteho on lähes vuosikymmeniä jäljessä niin sanotusti tavallisia verkkolaitteita. Vaikka sensoriverkkojen suojaus onkin haaste, niin täytyy muistaa, että sensoriverkot eivät ainakaan vielä ole yhtä iso maalitaulu hyökkäyksille kuin muut tietoliikenneverkot. [29; 30.]

Sensoriverkkojen tietoturvan kannalta täytyy ottaa huomioon haasteet, joita sensoriverkot luovat, hyökkääjän tavoitteet ja kuinka tietoturvaa voidaan kehittää ja parantaa.

4.1 Tietoturvan haasteet sensoriverkoissa

Tietoturva on kehittynyt harppauksin tietokoneiden ja tietoliikenneverkkojen yleistyessä. Nykyistä lähestymistapaa tietoturvaan on kuitenkin vaikea toteuttaa sellaisenaan sensoriverkoissa, koska sensoriverkot eroavat paljon perinteisistä tietoliikenneverkoista. Nykyiset tietoturvamekanismit antavat kuitenkin hyvät lähtökohdat sensoriverkkojen turvaamiselle ja niistä voidaankin poimia hyviä ideoita. [29; 30.]

4.1.1 Rajalliset resurssit

Pienten sensoreiden tehon ja muistin käyttö sekä tallennustila on hyvin rajoitettua. Tämä tuo isoja haasteita tietoturvan toteuttamiseen sensoriverkoissa. [29.]

Sensorit ovat pieniä laitteita, joilla on vain pieni määrä muistia ja tallennustilaa. Pienen tallennustilan takia sensoreiden tietoturva-algoritmin kokoa täytyy rajoittaa. Myös muut tietoturvaan liittyvät koodit on rajoitettu hyvinkin pieneksi. [29.]

Tehon käyttö on suurin sensoreiden ominaisuuksia rajoittava tekijä. Oletuksena on, että kun sensori on asennettu ja liitetty verkkoon, sen korvaaminen on hankalaa tai sen akkua on vaikea ladata. Akun varaus täytyy siis säilyä koko sensorin ja verkon käyttöiän ajan. Tämä täytyy ottaa huomioon, kun lisätään sensoriin joko salausfunktio tai -protokolla, sillä se vaikuttaa myös sensorin virran kulutukseen. Näin ollen, kun lisätään tietoturvaa, sensorin käyttöikä lyhenee. [29.]

4.1.2 Epäluotettava kommunikaatio

Verkon tietoturva riippuu vahvasti käytetystä protokollasta, joka on taas riippuvainen kommunikaatiosta. Pakettien reitittäminen sensoriverkoissa on yleensä yhteydetöntä ja luonnostaan epäluotettavaa. Paketit voivat esimerkiksi vaurioitua matkalla kanavien virheilystä johtuen, tai ne voivat tippua ruuhkautuneilla solmuilla. Vaurioituneita paketteja voivat aiheuttaa myös epäluotettavat langattoman kommunikoinnin kanavat. [29.]

Vaikka kanava olisi luotettava, voi kommunikaatio olla silti epäluotettavaa, johtuen sensoriverkkojen tavasta lähettää broadcast-liikennettä. Jos paketit kohtaavat siirron keskellä, tapahtuu konflikti ja siirto itsessään kariutuu. Suuritiheyksisissä verkoissa tämä voi olla suurikin ongelma. [29.]

Verkon ruuhkautuminen, solmujen prosessointi ja multi-hop-reititys voivat aiheuttaa suurta viivettä verkossa, joka taas voi johtaa ongelmiin sensoreiden synkronoinnissa. Ongelmat synkronoinnissa voivat olla erittäinkin kriittisiä, jos esimerkiksi verkon tietoturvamekanismit ovat riippuvaisia ajantasaisista raporteista tai salausavaimen jakamisesta. [29.]

4.1.3 Vartioimaton toiminta

Riippuen siitä, mihin tarkoitukseen sensoriverkko on tarkoitettu, voi verkko olla kokonaan tai osittain valvomatta pitkiäkin aikoja kerrallaan. Valvomattomia verkkoja uhkaa kolme isoa riski. [29.]

Jos verkko on täysin valvomatta, kohdistuu siihen automaattisesta fyysisten hyökkäysten uhka. Tai jos verkkoa operoidaan etänä, on lähes mahdoton havaita onko verkkoon kajottu fyysisesti. Sensoriverkot rakennetaan ilman keskeistä hallinnointipaikkaa tuoden verkkoon eloisuutta. Jos verkko on kuitenkin suunniteltu virheellisesti, tulee verkosta tehoton ja hauras. [29.]

4.2 Hyökkääjän tavoitteet

Sensoriverkot ovat haavoittuvaisia tietyn tyyppisille hyökkäyksille, joita voidaan toteuttaa usealla eri tavalla. Erityisesti palvelunestohyökkäykset, yksityisyyden loukkaaminen, liikenteen analysointi ja fyysiset hyökkäykset ovat isoja riskejä sensoriverkoissa. Esimerkiksi suojautuminen hyvin organisoidulta palvelunestohyökkäykseltä on lähes mahdotonta verkon solmujen asymmetrisyyden takia. Solmut voivat käyttää eri tehoa tai niiden rajoitukset voivat muuten olla erilaiset. Tehokkaampi solmu voikin tukkia koko sensoriverkon ja estää toiminnan, johon se on alunperin tarkoitettu. [29.]

4.2.1 Palvelunestohyökkäykset

Tavoitteena sensoriverkoissa on yksinkertaisesti jumittaa yksi tai useampi verkon solmukohta. Tämä voidaan tehdä lähettämällä dataa taajudella, joka häiritsee sensoriverkon käyttämiä taajuuksia. Jumittaminen voidaan tehdä kahdella tapaa, joista toinen on ajoittainen ja toinen jatkuva jumittaminen. Näistä jatkuvalla tavalla saadaan aikaan koko verkon jumittuminen, jolloin viestejä ei pystytä lähettämään eikä vastaanottamaan. Ajoittainen tapa päästää viestit läpi aika ajoin, joka sekin aiheuttaa suuren vaikutuksen verkkoon. [29.]

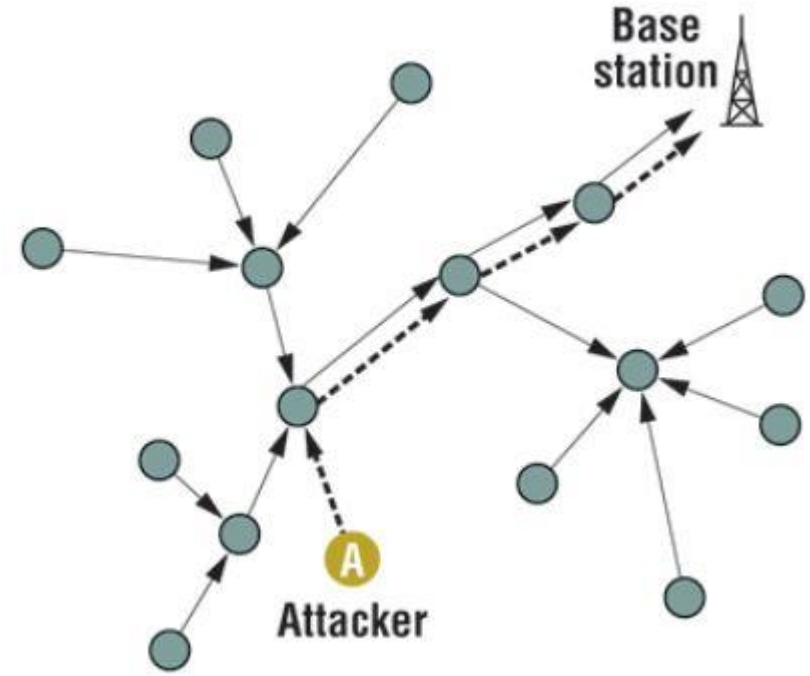
Hyökkäyksiä voidaan toteuttaa myös häiritsemällä kommunikaatioprotokollaa eli lähettämällä jatkuvasti viestejä. Näin saadaan verkossa aikaan törmäyksiä ja siten verkon jumiutumista. Jos ja kun törmäyksiä tapahtuu, täytyy paketti lähettää uudestaan. Jos verkon solmukohta eli sensori joutuu lähettämään paketteja useasti uudelleen, voidaan lopputuloksena saada sen virtalähde kulumaan loppuun ennen aikojaan. [29.]

Reititystasolla voidaan verkko saada jumiin estämällä reititys tietyn solmukohdan kautta. Sensoriverkot ovat usein multihop-verkkoja, jotka reitittävät pakettia viereiselle solmukohdalle ja jos estetään reititys tietyn solmun läpi, viestit eivät kulje sen viereisiltä sensoreilta. Verkon niin sanottu tulviminen kuljetuskerroksessa voi mahdollisesti myös jumiuttaa verkon. Tämä saadaan aikaan lähettämällä niin paljon viestejä, ettei solmun teho riitä käsittelemään niitä. [29.]

4.2.2 Liikenteen analysointi hyökkäykset

Sensoriverkot on usein suunniteltu useista vähävirtaisista solmukohdista ja muutamasta vahvasta tukiasemasta. Yksittäiset sensorit keräävät dataa ja reitittävät sen lopulta tukiasemalle. Hyökkääjä voi saada verkon hyödyttömäksi vain lamauttamalla tukiaseman. [29.]

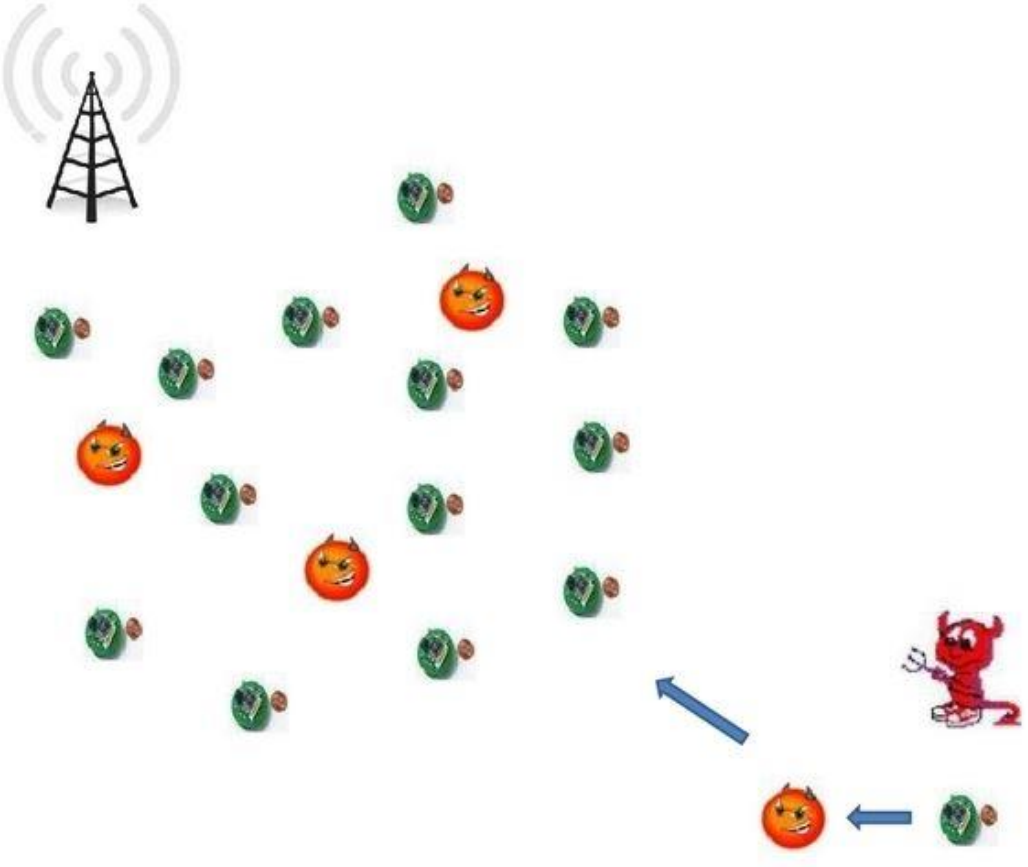
Voidaan olettaa, että solmu, joka on lähellä tukiasemaa, lähettää ja vastaanottaa enemmän paketteja kuin solmu, joka on kauempana. Näin hyökkääjä voi monitoroida pakettien lähetyksen määrää ja seurata sitä tukiasemalle asti (kuva 15). Vihollinen voi myös itse generoida tapahtumia ja monitoroida, mihin solmu viestin lähettää. [29.]



Kuva 15. Hyökkääjä seuraa viestiä tukiasemalle. [31]

4.2.3 Solmujen replikaatio -hyökkäykset

Replikaatio-hyökkäys on hyvinkin yksinkertainen. Hyökkääjän tarvitsee vain etsiä sensori ja kopioida sen ID-sensoriin, jonka itse aikoo lisätä verkkoon. Kopioitu solmu voi häiritä verkon toimintaa hyvinkin paljon. Se voi aiheuttaa pakettien korruptoitumista ja niiden väärää reitittymistä. Tämä voi johtaa hajanaiseen verkkoon, sensoreiden lukeman tiedon vääritymiseen ja niin edelleen. Jos hyökkääjällä on fyysisesti pääsy verkon laitteisiin, hän voi jopa kopioida verkon salausavaimen replikoituun sensoriin. Fyysinen pääsy laitteisiin mahdollistaa myös replikoidun solmun lisäämisen strategisesti tärkeään kohtaan. [29.]



Kuva 16. Hyökkääjä on onnistunut lisäämään verkkoon replikoituja sensoreita. [32]

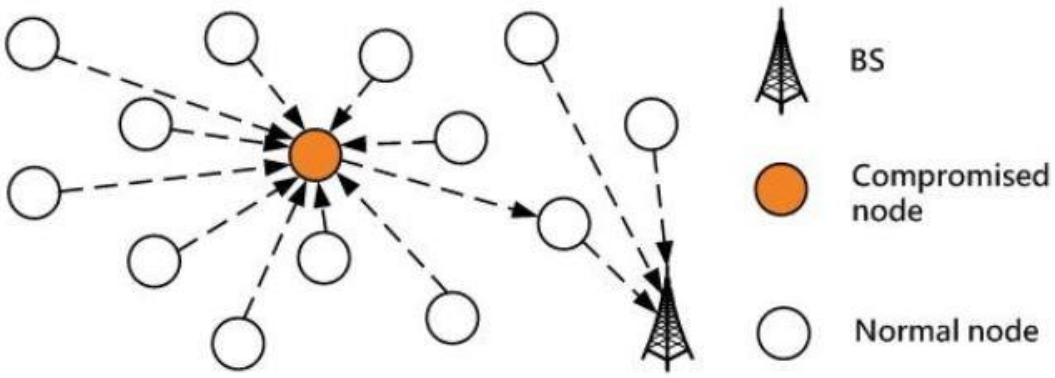
4.2.4 Hyökkäykset yksityisyyttä vatsaan

Automaattinen datan keräys kasvaa sensoriverkkojen tehokkaan käyttöönoton mukana. Vaikka tämä tuo suurta hyötyä, niin se on mahdollisesti myös suuri väärinkäytön kohde. Erityisesti yksityisyyden turva on yksi suuri huolenaihe, sillä sensoriverkot lisäävät datan keräämisen kapasiteettia huomattavasti. [29.]

Suurin huolenaihe ei kuitenkaan ole kasvanut kapasiteetti, vaan suuriin tietomääriin käsiksi pääseminen etäyhteydellä. Hyökkääjän ei siis tarvitse olla fyysisesti läsnä, vaan tiedon keräys onnistuu anonyymisti ja lähes riskeittä. Etäyhteys mahdollistaa myös sen, että yksittäinen hyökkääjä voi monitoroida useita kohteita samanaikaisesti. [29.]

Monitorointi ja salakuuntelu on hyvin ilmeinen hyökkäys. Siinä hyökkääjä seuraa liikennettä ja voi helpostikin saada selville arkaluonteista tietoa, kuten informaatiota

verkon konfiguraatiosta. Joissain tapauksissa ja useastikin tarvitaan liikenteen analysointia tiedon keräämisen jälkeen. Näin voidaan saada selville esimerkiksi tietyn solmukohdan rooli verkossa. [29.]



Kuva 17. Hyökkääjä on saanut haltuunsa keskeisen sensorin, jonka läpi paketit kulkee. [33]

Naamioituminen tarkoittaa sitä, että hyökkääjä lisää verkkoon pahantahtoisen sensorin, jonka kautta saadaan paketit kulkemaan. Kun hyökkääjä hallitsee tätä sensoria, on sen läpi kulkemien pakettien analysointi hyvinkin helppoa. [29.]

4.2.5 Fyysiset hyökkäykset

Sensoriverkot ovat usein ulkona ja valvomatta fyysisiä uhkia kohtaan. Fyysiset hyökkäykset, toisin kuin jotkut edellisistä, ovat usein peruuttamattomia. Esimerkiksi jos sensori rikotaan tai varastetaan, ei sitä enää saada toimintaan ilman ylimääräisiä kustannuksia. Verkon toiminta voi heikentyä näin pitkäksikin aikaa. Jos hyökkääjä pääsee käsiksi sensoriin, voi hän mahdollisesti muuttaa solmun sisäistä koodia. [29.]

5 Siirtoyhteydet

Datan siirtämiseen käytetään pidemmälle kantavia kiinteitä tai langattomia yhteyksiä. Data ei yleensä olen kooltaan isoa, joten siirtoyhteyksiin ei välttämättä tarvita suuria datansiirtonopeuksia. Näiden yhteyksien kautta voidaan joko hallita sensoriverkkoja tai kerätä dataa niistä. Nämä siirtoyhteydet lähtevät niin sanotusta verkon yhdyskäytävästä.

5.1 GSM (2G)

GSM on ETSI:n kehittämä toisen sukupolven standardi matkapuhelinverkoille [34]. GSM käyttää langattomaan liikenteeseensä 900 MHz:n ja 1800 MHz:n taajuuksia tai 800 MHz:n ja 1900 MHz:n taajuuksia Pohjois-Amerikassa. Vaikka GSM kehitettiin matkapuhelinten puheliikenteeseen, sitä voidaan käyttää myös datapakettien liikuttamiseen eli käytännössä Internetin käyttöön. GSM:n siirtonopeus ei ole kovinkaan suuri, vain teoreettisessa maksimissaan 9600 bittiä/s. Sitä voidaan hyvin silti käyttää sensoriverkkojen siirtoyhteyksissä, sillä data mitä verkot kerää, ei ole kovinkaan suurta. [35.]

Operaattorit ovat sitoutuneet tukemaan 2G:tä eri maissa eri vuosiin asti. Esimerkiksi AT&T on sitoutunut tukemaan 2G-verkkoa vuoteen 2017 asti [36]. Sen jälkeen joudutaan miettimään vaihtoehtoisia ratkaisuja datan siirrolle. Kun osa jo asennetuista sensoreista tukevat vain 2G:tä, on niiden vaihtaminen työläs prosessi. 2G-verkot kattavat kuitenkin suurimman osan maapallon alueista, joten kuuluvuuden kannalta se on käyttökelpoisin siirtoyhteystekniikka sensoriverkoille.

GSM:ää kuten useita muitakin standardeja on kehitelty vuosien mittaan paremmiksi. Kaksi tärkeää tiedonsiirtoon liittyvää laajennusta ovat GPRS- ja EDGE-standardit. [35.]

Kuva 18. GSM kuuluvuuskartta maapallolta. Voidaan todeta että GSM-verkot kattavat kaikki suurimmat asuinalueet ja niiden lähistöt. Langttomaksi tiedonsiirtotekniikaksi GSM on kattava mutta siirtonopeudet ovat pieniä. [37]

GPRS tuo pakettikytkentä-ominaisuuden alkuperäisesti piirikytkentäiseen GSM-standardiin. Se mahdollistaa jatkuvan datayhteyden käytettäväksi esimerkiksi internetin selailuun. GPRS tarjoaa perinteistä GSM:ää nopeamman yhteyden, joka teoreettisessa maksimissaan on 171 kbit/s. Useimmat operaattorit eivät kuitenkaan tarjoa tätä maksiminopeutta. Maksinopeudeksi mielletään 115 kbit/s. GPRS on hyvinkin käyttökelpoinen standardi tämän hetken sensoriverkkoihin, sillä kuten aiemminkin todettu, ei kerätty liikkuva data ole kovinkaan suurta. [38.]

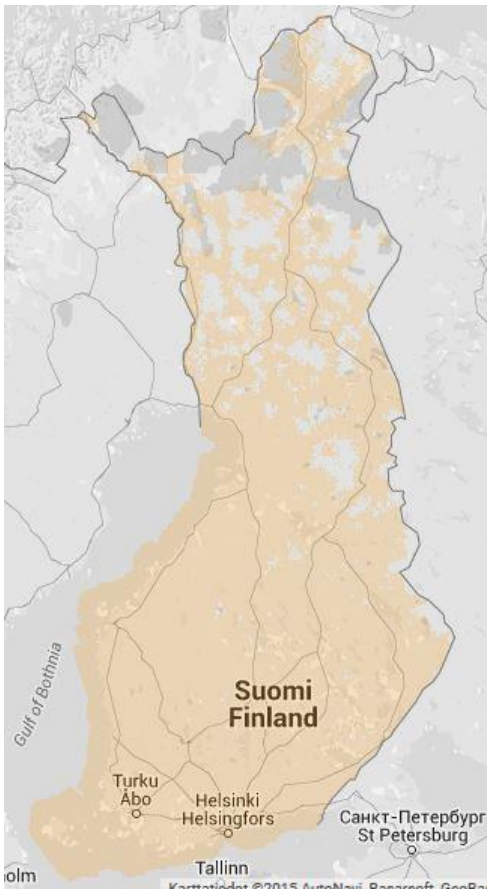
EDGE on suora parannus GSM-teknologiaan. Se tarjoaa nopeammat siirtoyhteydet sekä pakettikytkentäisille että piirikytkentäisille sovelluksille. EDGE-standardi nostaa maksimi datansiirtonopeuden 384 kilobittiin sekunnissa. EDGE:ä pidetään yleisesti 2.5G-standardina. [39.]

5.2 3G

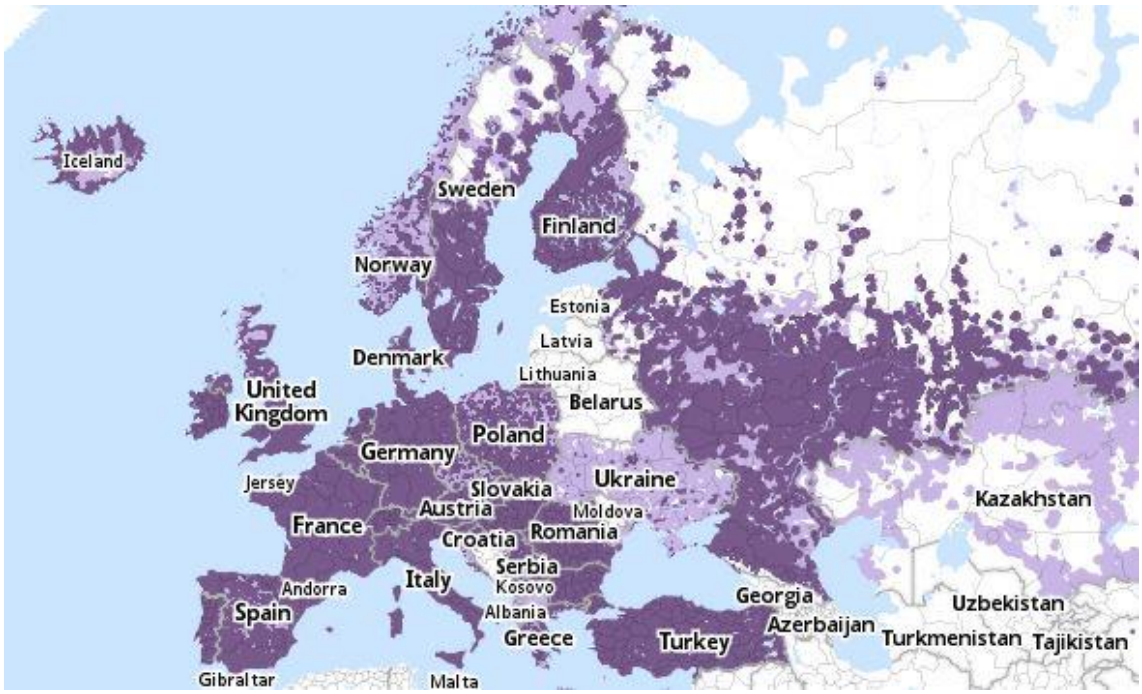
3G eli kolmannen sukupolven teknologiat nostavat datansiirtonopeuksia entisestään ja yleisesti kaikkia teknologioita, joiden datansiirtonopeus ylittää 384 kilobittiä sekunnissa, pidetään vähintään 3G:nä. 3G kattaa useita teknologioita, kuten W-CDMA:n ja HSPA:n, joka kuitenkin usein mielletään 3.5G-teknologiaksi. [40; 41.]

3G on tietoverkkoprotokolla, jonka standardit on määrittänyt ITU eli kansainvälinen telekommunikaatioliitto. Nämä IMT-2000 -standardit määrittelevät, mitkä teknologiat luetaan kuuluviksi 3G:hen. [41.]

Kolmannen sukupolven verkot kattavat jo suuren osan asutusalueista, joten 3G-teknologioiden käyttö onkin mahdollista useimmissa paikoissa. 3G:n suuremmät nopeudet ja laajentuneet kuuluvuusalueet tekevät 3G-teknologioista erittäin käyttökelpoisen sensoriverkkojen siirtoyhteyksissä.



Kuva 19. Elisan 3G-kuuluvuuskartta Suomesta. [42]



Kuva 20. Suuntaa antava kartta 3G:n kuuluvuuksista Euroopassa [43]. Operaattoreille on omat kuuluvuuskarttansa, joten yleistä karttaa kuuluvuuksista on erittäin vaikea saada.

W-CDMA on 3G-verkoissa käytetty rajapinta, joka tarjoaa teoreettisessa maksimissaan 21Mbits/s nopeuden. Käytännössä nopeudet rajoittuvat 10 megabittiin sekunnissa.

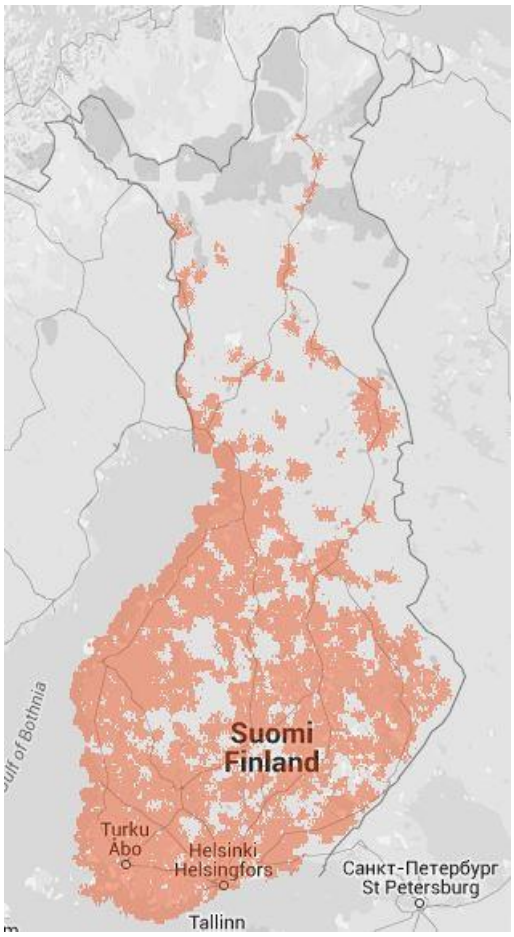
HSPA on edellistä kehittyneempi ja sitä pidetäänkin yleensä 3.5G-protokollana. Se nostaa datan siirtonopeuksia entisestään, teoreettisen maksimilatausnopeuden ollessa 42Mbit/s:ssa. [44.]

5.3 4G

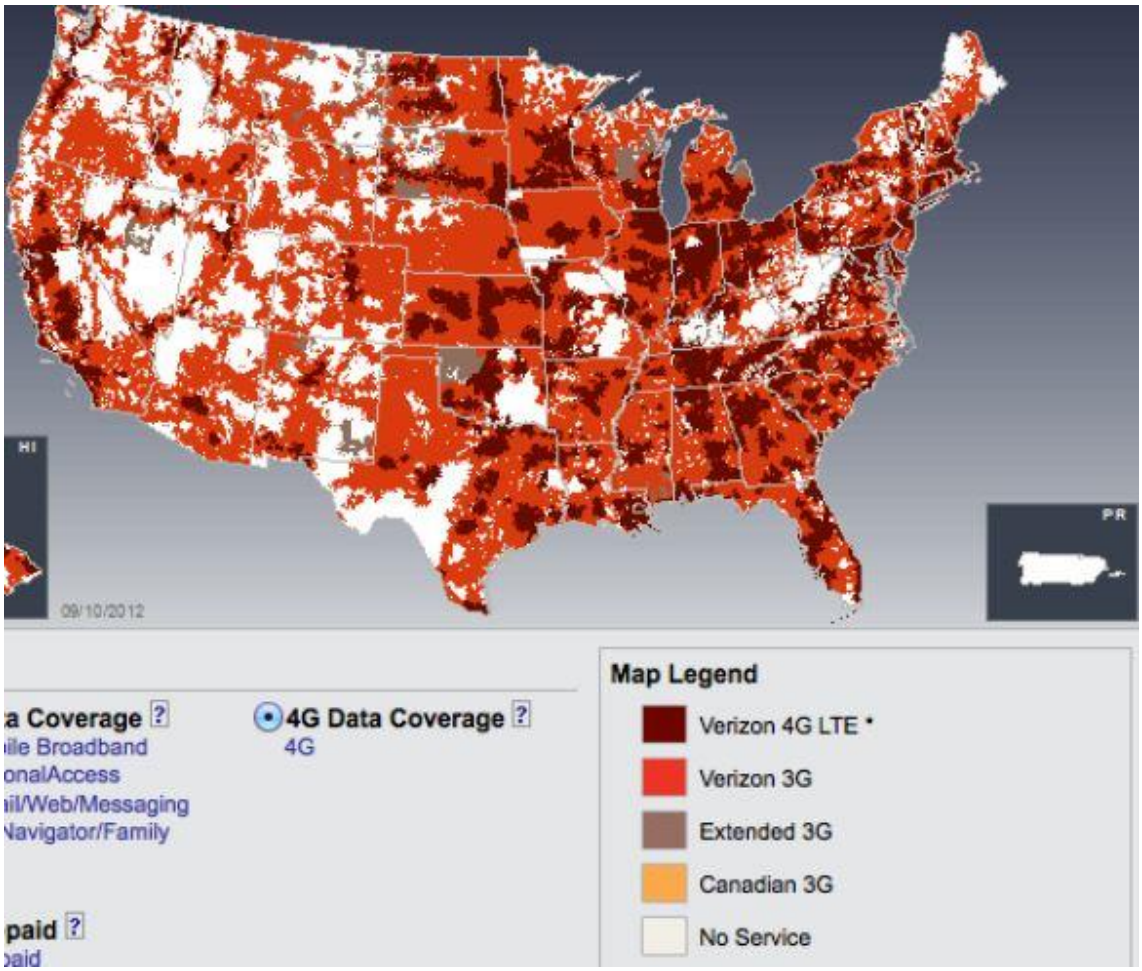
ITU määrittelee neljännen sukupolven tietoverkot siten, että ne ovat ovat täysin pakettikytkentäisiä. Kannettavan laitteen täytyy 4G-verkoissa yltää vähintään 100Mbit/s datansiirtonopeuteen, kun 3G:n vähimmäisnopeus on 384 kbit/s. Suurin ero 3G:hen onkin tämä moninkertainen siirtonopeus. [45; 46.]

Operaattorit eivät ole vielä päässeet täysin yhteisymmärrykseen siitä, pitäisikö 4G-tietoverkot rakentaa käyttäen LTE:tä vai WiMAX:ia. [45] Molempia standardeja kuitenkin käytetään yleisesti tällä hetkellä.

4G-verkkojen ongelma on tällä hetkellä kuuluvuus. Teknologia ei ole vielä laajalle levinnyt, joten varsinkin matkustaessa tulee usein vastaan alueita, joihin 4G-verkko ei kuulu. Tämä aiheuttaa ongelmia varsinkin taajama-alueiden ulkopuolella. Vähäinen peittoalue ei tee 4G-teknologioista vielä tällä hetkellä optimaalisia sensoriverkkojen tiedonsiirtoon. 3G- ja 2G-verkkojen kuuluvuus on huomattavasti parempi kuin 4G-verkkojen. Myös aiempien sukupolvien, ja varsinkin 3G:n siirtonopeudet ovat varsin riittäviä sensoriverkkojen siirtoyhteyksiin.



Kuva 21. Elisan LTE kuuluvuuskartta Suomesta. [42]



Kuva 22. Verizonin LTE-kuuluvuuskartta Yhdysvalloista. Kuvassa myös mukana 3G-verkot, joiden avulla voidaan helposti todeta, kuinka pieni 4G-teknologioiden levinneisyys on verrattuna kolmannen sukupolven teknologioihin. [47]

5.3.1 LTE

Tämä neljännen sukupolven tekniikka perustuu EDGE- ja HSPA-teknologioihin tarjoten maksimilatausnopeudeksi 100Mbit/s ja maksimilähetysnopeudeksi 30Mbit/s. Se myös lyhentää latenssiaikoja verrattuna aiempiin teknologioihin ja on myös yhteensopiva niiden kanssa. [48; 49.]

Vaikka LTE:tä mainostetaan 4G-teknologiana, se ei täytä ITU:n asettamia vaatimuksia neljännen sukupolven teknologioille. Eli LTE on pikemminkin ns. 3.9G-teknologia. LTE kuitenkin luo pohjan kehitteillä oleville teknologioille, joten voidaan myös tässä yhteydessä lukea se neljännen sukupolven teknologiaksi. [48; 49.]

5.3.2 WiMAX

WiMAX on hyvin samankaltainen teknologia kuin Wi-Fi mutta hyvin paljon suuremmalla kantamalla, joka voi olla jopa 50 kilometriä tukiasemasta. WiMAX perustuu langattomaan IEEE 802.16 -standardiin, joka on yhteensopiva langattomiin lähiverkkoihin käytettävän IEEE 802.11 -standardin kanssa. WiMAX-verkoissa kuten Wi-Fi-verkoissa, kaista jaetaan käyttäjien kesken, joten verkon luvatut maksiminopeudet eivät käytännössä koskaan toteudu. [50.]

WiMAX on jäänyt vähemmälle huomiolle kuin useiden operaattorien tukema LTE-teknologia. Silti WiMAX on potentiaalinen vaihtoehto sensoriverkkojen siirtoyhteyksiin, etenkin jos siirtomatka ei ole erityisen pitkä. WiMAX tarjoaa tarvittavan nopeuden ja luotettavuuden sensitiivisen datan siirtämiseen.

5.3.3 HSPA+

HSPA+ nostaa tiedonsiirtonopeutta edelleen verrattuna HSPA:han. Sitä ei pidetä varsinaisesti 4G-verkkona vaan 3,5G-verkkona. Tämä johtuu siitä, että HSPA+ ei ole erityisen uusi teknologia, ja se on hyvin lähellä 3G:tä. Kategorisoidaan tämä kuitenkin 4G:n alle, sillä nopeudet vastaa neljännen sukupolven verkkojen tasoa. [51.]

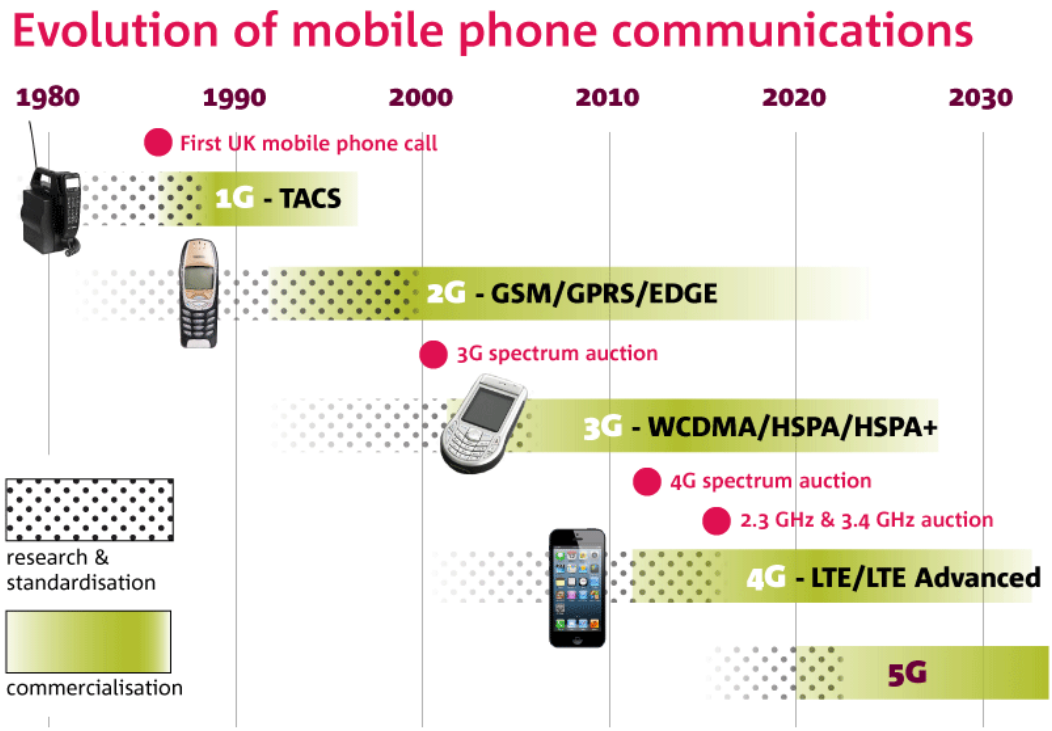
2G	2.5G		3G		4G	
Name	Name	Download	Name	Download	Name	Download
TDMA	GPRS	115 Kbit/s	WCDMA (UMTS)	384 Kbp/s	LTE	100 Mbp/s
	EDGE	236 Kbp/s	HSPA (UMTS)	14 Mbit/s	WIMAX	50 Mbp/s
					HSPA+	56 Mbit/s
CDMA2000			EVDO (CDMA2000)	3.1 Mbit/s		

Kuva 23. Langattoman tiedonsiirron kehittyminen. [52]

5.4 5G

Vielä kehitteille olevat viidennen sukupolven matkapuhelinverkkojen teknologiat tuovat tulevaisuudessa huomattavasti suuremmat datan siirtonopeudet ja huomattavasti pienemmät viiveet. Kun älylaitteiden määrä kasvaa ja niiden halutaan olevan yhteydessä toisiinsa, tarvitaan myös suurempaa kaistanleveyttä kattamaan lisääntynyt datansiirron tarve. Tästä hyvänä esimerkkinä kodin automaatio, jossa suurikin määrä laitteita on yhteydessä toisiinsa ja niitä voidaan hallita juurikin matkapuhelimella tai muulla mobiiliverkkoa käyttävällä laitteella. [53.]

5G:n suurimpia haasteita on standardisointi. Useat eri ryhmät kehittävät jo nyt tulevaisuuden teknologioita, jotka ovat yhteensopivia myös nykyisten 4G:n ja 3G:n kanssa, kun taas monet yritykset uskovat että tarvitaan globaali standardi, jolla voidaan määritellä 5G. Toinen suuri haaste on radiomastojen eli antennien rakentaminen ja sijoittelu. 5G käyttää suurempia taajuuksia kuin aiempien sukupolvien teknologiat, joka tarkoittaa sitä, että radioaallot eivät kuulu yhtä pitkälle. Näissä taajuuksissa on vähemmän häirintää mutta suurena miinuksena on se, etteivät radioaallot kanna läheskään yhtä pitkälle kuin esimerkiksi neljännen sukupolvien teknologioissa. Optimistisimmat arviot povaavat ensimmäisiä viidennen sukupolven kuluttajaverkkoja tulevan käyttöön vuonna 2020. [53.]

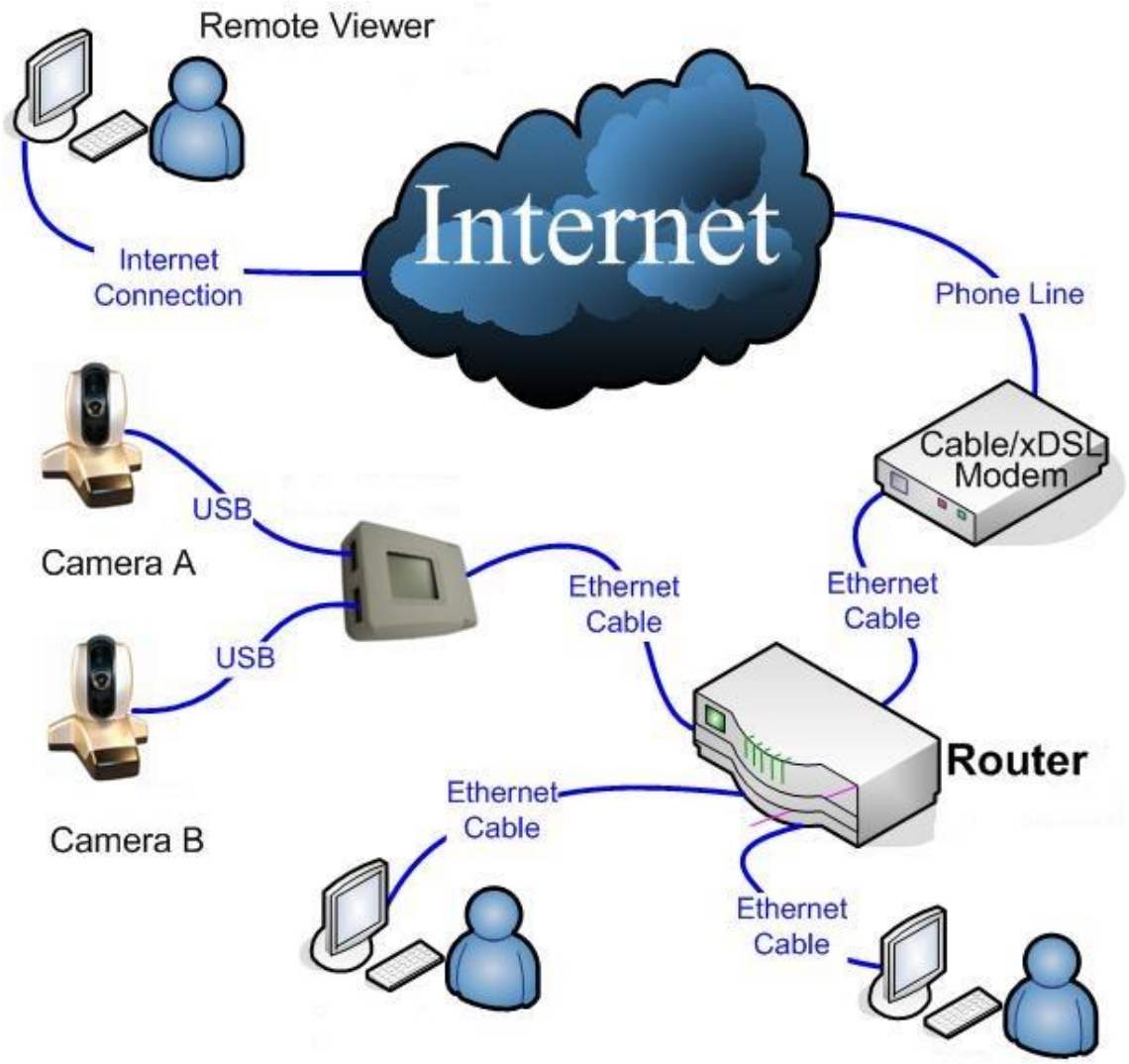


Kuva 24. Ennustettu 5G:n saapuminen kuluttajakäyttöön verrattuna aikaisempiin teknologioihin. [54]

5.5 Ethernet

Ethernet on IEEE 802.3 -standardin pakettipohjainen lähiverkkotekniikka, joka käyttää kiinteitä verkon komponentteja. Se käyttää CSMA/CD-kaistanvarausmenetelmää, jossa millä tahansa muulla verkon laitteella on oikeus aloittaa lähetys, jos mikään muu laite ei lähetä paketteja. Jos enemmän kuin yksi laite lähettää paketin kerralla, tapahtuu törmäys ja lähettäjät lopettavat lähetyksen. Törmäyksen tapahduttua laitteet odottavat tietyn ajan ennen seuraavaa lähetysyritystä.

Sensoriverkkojen kiinteissä siirtoyhteyksissä voidaan käyttää joko pelkästään Ethnernetiä tai lähiverkosta liikenne voidaan ohjata muualle, vaikka valokuitua käyttäen internetin lävitse. Tällöin käytetään tietenkin esimerkiksi IPSec-tunnelia, jotta data pysyy matkalla koskemattomana. Ethernet pystyy nykyään jopa 10 Gb:n siirtonopeuksiin.



Kuva 25. Ethernetiä käyttävä LAN-verkko, jonka liikenne ohjattu Internetiin. [55]

6 Haasteet / mahdollisuudet

Sensoriverkot ja teollinen internet itsessään avaavat suuren määrän mahdollisuuksia, joista hyötyvät erityisesti yritykset ja miksi eivät aivan tavalliset ihmisetkin. Aikaisempaa suuremman datamäärän kerääminen ja analysointi tuovat hyötyjä useissa sovellutuksissa riippumatta alasta tai elämän osa-alueesta. Internetiin kytkeytyneet laitteet ovat jatkuvassa kasvussa ja niitä ennustetaankin olevan noin 75 miljardia vuoteen 2020 mennessä [56]. Näin suuri kasvu tuo mukanaan tietenkin haasteita ja

riskejä, jotka täytyy ottaa huomioon. Erilaiset vakoilupaljastukset ovat saaneet ihmiset valveutuneimmiksi omasta yksityisyyden suojastaan ja sensoriverkkojen yleistyessä tämä tulee olemaan varmasti yksi huolenaihe. Näin suuren datamäärän kerääminen voi tuntua jopa pelottavalta. Tämän takia tietoturvan kehittäminen onkin erityisen tärkeää.

Yksi suurimmista haasteista on siis tietoturva, joka on samalla myös mahdollisuus. Kuten aiemmin tässä työssä todettu, on internetiin kytkettyjän laitteiden tietoturva vielä heikkoa, ja se vaatiikin suuren määrän kehitystä. Sensoriverkoille täytyy kehittää erilaisia ratkaisuja kuin tavallisten tietoverkkojen turvaamiseen jo on. Tämä tuo mahdollisuuden ja uudenlaisen haasteen tietoturvan ammattilaisille teollisen internetin kehittämiseen.

Toinen haaste tulevaisuudessa tulee olemaan siirtoyhteyksien kehitys ja niiden uusiutuminen. Vaikka kerätty datamäärä on suurta, se ei tarvitse kerralla kovinkaan suuria nopeuksia. Nykyään 2G onkin yksi yleisesti käytetyistä siirtoyhteyksistä. Mitä tapahtuu, kun kehitys jatkaa kulkuaan ja 2G-verkot poistetaan käytöstä? Sitä siirtoyhteytenään käyttäviä sensoriverkkoja todennäköisesti täytyy kehittää tai jopa uusia kokonaan. Tämä voi olla hyvinkin kallista. Esimerkiksi Yhdysvaltalainen AT&T on ilmoittanut tavoitteekseen 2g-verkon alasajon vuonna 2017. Suomessa ei aikataulua ole vielä päätetty. [36.]

Teollinen internet ja sensoriverkot todennäköisesti tulevat tulevaisuudessa olemaan tavalla tai toisella osa jokapäiväistä elämäämme. Haasteista ja riskeistä huolimatta on teollisen internetin ja sensoriverkkojen hyöty niin suuri, että niiden kehitystä olisi jopa tyhmää jarruttaa.

Lähteet

1 General Electric Pitches an Industrial Internet. Verkkodokumentti. http://www.technologyreview.com/news/507831/general-electric-pitches-an-industrial-internet/. Luettu 14.1.2015.

2 Industrial Internet ja Internet of Things – mistä oikeastaan puhumme? Verkkodokumentti. http://www.alykassuomi.fi/2014/06/industrial-internet-ja-internet-things-mista-oikeastaan-puhumme/. Luettu 14.1.2015.

3 Messaging Technologies for the Industrial Internet and the Internet of Things Whitepaper. Verkkodokumentti. http://www.prismtech.com/sites/default/files/documents/Messaging-Comparison-Whitepaper-July2014.pdf. Luettu 14.1.2015.

4 An Introduction to Wireless Sensor Networks. Verkkodokumentti. http://ceng.usc.edu/~bkrishna/research/talks/WSN_Tutorial_Krishnamachari_ICISIP05.pdf. Luettu 14.1.2015.

5 Waltenegus Dargie, Christian Poellabauer. 2010. Fundamentals of Wireless Sensor Networks: Theory and Practice. United Kingdom: John Wiley & Sons Ltd

6 Message Authentication in Sensor Networks using En-route Filtering. Verkkodokumentti. http://enroutefiltering.blogspot.fi/. Luettu 16.1.2015.

7 IEEE 802.15 WPAN™ Task Group 4 (TG4). Verkkodokumentti. http://www.ieee802.org/15/pub/TG4.html. Luettu 16.1.2015.

8 ZigBee Technology Tutorial. Verkkodokumentti. http://www.radio-electronics.com/info/wireless/zigbee/zigbee.php. Luettu 16.1.2015.

9 ZigBee® Wireless Standard. Verkkodokumentti. http://www.digi.com/technology/rf-articles/wireless-zigbee. Luettu 28.1.2015.

10 Using ZigBee Wireless Networking to Develop Commercial Products. Verkkodokumentti. http://rtcmagazine.com/articles/view/100656. Luettu 28.1.2015.

11 Il Leaning Lab e la rete delle cose. Verkkodokumentti. http://www.sensor-networks.org/index.php?page=1111011026. Luettu 28.1.2015.

12 Interoperability of 6LoWPAN. Verkkodokumentti. http://tools.ietf.org/html/draft-daniel-6lowpan-interoperability-01. Luettu 28.1.2015.

13 Low Power Consumption Wireless Technologies for Smart Metering. Verkkodokumentti. http://zigbeevsmbus.blogspot.fi/2012/06/fossil-energy-crisis-havealways-lead-to.html. Luettu 3.2.2015.

14 How to set up a 6LoWPAN network. Verkkodokumentti. http://www.embedded.com/electronics-blogs/embedded-cloud-talkers/4236873/How-to-setup-a-6LoWPAN-network. Luettu 3.2.2015.

15 Home Automation with 6LoWPAN. Verkkodokumentti. http://www.academia.edu/5275604/Home_Automation_with_6LoWPAN. Luettu 3.2.2015.

16 Low Power Consumption Wireless Technologies for Smart Metering. Verkkodokumentti. http://zigbeevsmbus.blogspot.fi/2012/06/fossil-energy-crisis-havealways-lead-to.html. Luettu 3.2.2015.

17 MyriaNed. Verkkodokumentti. http://dbpedia.org/page/MyriaNed. Luettu 10.2.2015.

18 MyriaNed, a self organizing, gossiping Wireless Sensor Network. Verkkodokumentti. https://www.devlab.nl/myrianed. Luettu 10.2.2015.

19 Model-Based Testing applied to a Wireless Sensor Network Node. Verkkodokumentti. http://www.quasimodo.aau.dk/esweek/ESweekMBT.pdf. Luettu 10.2.2015.

20 Why DASH7? Verkkodokumentti. http://www.dash7-alliance.org/?page_id=18. Luettu 18.2.2015.

21 Z-Wave Alliance. Verkkodokumentti. http://z-wavealliance.org. Luettu 18.2.2015.

22 Z-Wave. Verkkodokumentti. http://www.wikid.eu/index.php/Z-wave. Luettu 18.2.2015.

23 WirelessHART Overview. Verkkodokumentti. http://en.hartcomm.org/hcp/tech/wihart/wireless_overview.html. Luettu 25.2.2015.

24 WirelessHART - How it works. Verkkodokumentti. http://en.hartcomm.org/hcp/tech/wihart/wireless_how_it_works.html. Luettu 25.2.2015.

25 Wi-Fi. Verkkodokumentti. http://www.webopedia.com/TERM/W/Wi_Fi.html. Luettu 25.2.2015.

26 AP421W Super G™ Multi-function Access Point Diagram. Verkkodokumentti. http://airlink101.com/products/ap421w_diagram.php. Luettu 25.2.2015.

27 A brief tutorial on Bluetooth wireless technology. Verkkodokumentti. http://www.bluetooth.com/Pages/Fast-Facts.aspx. Luettu 2.3.2015.

28 A Look at the Basics of Bluetooth Technology. Verkkodokumentti. http://www.bluetooth.com/Pages/Basics.aspx. Luettu 2.3.2015.

29 Wireless Sensor Network Security: A Survey. Verkkodokumentti. http://www.cs.wayne.edu/~weisong/papers/walters05-wsn-security-survey.pdf. Luettu 2.3.2015.

30 Sensor Network Security: More Interesting Than You Think. Verkkodokumentti. https://security.cs.georgetown.edu/~msherr/papers/sensor-interesting.pdf. Luettu 2.3.2015.

31 Denial-of-Service in Wireless Sensor Networks: Attacks and Defenses. Verkkodokumentti. http://www.computer.org/csdl/mags/pc/2008/01/mpc2008010074-abs.html. Luettu 2.3.2015.

32 A Security Mechanism for Clustered Wireless Sensor Networks Based on Elliptic Curve Cryptography. Verkkodokumentti. http://ieeesmc.org/newsletters/back/2010_12/main_article3.html. Luettu 12.3.2015.

33 Nodes replication. Kuva. http://www.hindawi.com/journals/ijdsn/2013/745069/fig1/. Luettu 12.3.2015.

34 ETSI World Class Standards. Verkkodokumentti. http://www.etsi.org/standards. Luettu 12.3.2015.

35 Mobile technologies GSM. Verkkodokumentti. http://www.etsi.org/technologies-clusters/technologies/mobile/gsm. Luettu 12.3.2015.

36 Milloin gsm-verkko kuolee? Näin vastaavat operaattorit. Verkkodokumentti. http://www.tivi.fi/Uutiset/2012-10-04/Milloin-gsm-verkko-kuolee-N%C3%A4in-vastaavat-operaattorit-3195116.html. Luettu 19.3.2015

37 Coverage Maps. Verkkodokumentti. http://www.worldtrackingsolutions.com/coverage-maps. Luettu 19.3.2015.

38 General Packet Radio Service, GPRS. Verkkodokumentti. http://www.etsi.org/index.php/technologies-clusters/technologies/mobile/gprs. Luettu 19.3.2015.

39 EDGE. Verkkodokumentti. http://www.etsi.org/index.php/technologies-clusters/technologies/mobile/edge. Luettu 19.3.2015.

40 What is "3G"? Verkkodokumentti. http://www.mobileburn.com/definition.jsp?term=3G. Luettu 25.3.2015.

41 3G Technology. Verkkodokumentti. http://www.engineersgarage.com/articles/what-is-3g-technology-specifications. Luettu 25.3.2015.

42 Elisa kuuluvuuskartta. Verkkodokumentti. http://elisa.fi/kuuluvuus/. Luettu 25.3.2015.

43 Kindle Experimental: Worldwide 3G Internet Browser. Verkkodokumentti. http://www.wonderoftech.com/kindle-experimental-worldwide-3g-internet-browser/. Luettu 25.3.2015.

44 What is 3G? Explained in simple terms. Verkkodokumentti. http://www.3g.co.uk/PR/Feb2012/3g-what-is-3g-explained-in-simple-terms.html. Luettu 25.3.2015.

45 4G (fourth-generation wireless). Verkkodokumentti. http://searchmobilecomputing.techtarget.com/definition/4G. Luettu 29.3.2015.

46 Understanding 4G Technology Standards. Verkkodokumentti. http://www.whatsag.com/G/Understanding_4G.php. Luettu 29.3.2015.

47 Apple Shows Off iOS 6 Maps with Turn by Turn and 3D. Verkkodokumentti. http://www.gottabemobile.com/2012/09/12/apple-ios-6-maps-with-turn-by-turn-and-3d/. Luettu 29.3.2015.

48 Long Term Evolution (LTE). Verkkodokumentti. http://searchmobilecomputing.techtarget.com/definition/Long-Term-Evolution-LTE. Luettu 29.3.2015.

49 Understanding LTE Technology Standards. Verkkodokumentti. http://www.whatsag.com/G/Understanding_LTE.php. Luettu 29.3.2015.

50 Understanding WiMAX Technology Standards. Verkkodokumentti. http://www.whatsag.com/G/Understanding_WiMAX.php. Luettu 5.4.2015.

51 HSPA+: A Definition. Verkkodokumentti. http://cellphones.about.com/od/phoneglossary/g/what-is-hspa-4g.htm. Luettu 5.4.2015.

52 Mobile Data Networks Understanding 2.5G vs 3G vs 4G. Verkkodokumentti. http://www.szelins.com/blog/tag/3g. Luettu 5.4.2015.

53 What Is 5G, and What Does It Mean for Consumers? Verkkodokumentti. http://recode.net/2015/03/13/what-is-5g-and-what-does-it-mean-for-consumers/. Luettu 9.4.2015.

54 Laying the foundations for 5G mobile. Verkkodokumentti. http://www.futuretimeline.net/blog/2015/01/22.htm#.VR2O8uFUvIU. Luettu 9.4.2015.

55 Basic Principles of Network Routing. Verkkodokumentti. http://homework.uoregon.edu/pub/class/155/router.html. Luettu 9.4.2015.

56 Kytömäki, Antti, Viestimies, numero 1, 2015.