Tampereen ammattikorkeakoulu
Tietojenkäsittelyn koulutusohjelma
Tuukka Virtanen

Opinnäytetyö

Rakennustyömaan olosuhdevalvontajärjestelmän tietoverkkoratkaisut

Työn ohjaaja FM Ville Haapakangas
Työn tilaaja Salon Rakennuskonevuokraamo Oy
Tampere 12/2009

Tampereen ammattikorkeakoulu
Tietojenkäsittelyn koulutusohjelma

Tekijä Tuukka Virtanen
Työn nimi Rakennustyömaan olosuhdevalvontajärjestelmän tietoverkkoratkaisut
Sivumäärä 80
Valmistumisaika Joulukuu 2009
Työn ohjaaja Ville Haapakangas
Työn tilaaja Salon Rakennuskonevuokraamo Oy

TIIVISTELMÄ

Tämän opinnäytetyön tarkoituksena oli etsiä soveltuvimmat tietoverkkoratkaisut rakennustyömaakäyttöön suunniteltuun olosuhdevalvontajärjestelmään. Olosuhdevalvontajärjestelmä on tekninen ratkaisu, joka mahdollistaa mm. työmaan lämpötilan, sähköverkon toiminnan ja rikosilmoitusjärjestelmän tilan etäseurannan.

Parhaiden tekniikoiden kartoitus aloitettiin määrittelemällä kokonaisjärjestelmän ja käyttöympäristön asettamat vaatimukset. Vaatimusmäärittelyn pohjana käytettiin kokonaisjärjestelmän vaatimusmäärittelyä, suunnitelmia ja käyttöympäristöstä kerättyä tietoa.

Järjestelmän kolmeen tietoverkkoon etsittiin soveltuvimmat tekniikat vertaamalla tekniikoiden ominaisuuksia vaatimuksiin ja pisteyttämällä tekniikoiden vaatimustenmukaisuus. Pisteytyksen perusteella voitiin perustellusti osoittaa sopivimmat tekniikat järjestelmän käyttöön.

Soveltuvimmaksi tekniikaksi antureiden lukuun työmaalla osoittautui 868 MHz taajuudella toimiva ZigBee-verkko. Työmaan yhdistämiseen Internetiin soveltuivat parhaiten GSM-verkkoon pohjautuvat datasiirtotekniikat. Työmaan ja palvelinjärjestelmän välisen yhteyden tunnelointiin IPSec-tekniikka osoittautui parhaaksi.

Kaikenkaikkiaan työn tavoitteet saavutettiin käytössä olevien resurssien puitteissa hyvin. Tekniikoiden koekäyttö aidoissa kenttäolosuhteissa olisi parantanut valintaprosessin laatua ja luotettavuutta merkittävästi. Valitettavasti tälle työlle asetettujen taloudellisten ja ajallisten resurssien puitteissa tekniikoiden testaaminen ei ollut mahdollista.

Avainsanat vaatimusmäärittely, Ethernet, WiFi, IEEE 802.11s, ZigBee, 802.15.4, Flash-OFDM, GSM, IPSec, SSL-VPN

TAMK University of Applied Sciences
Business Information Systems

Writer	Tuukka Virtanen
Thesis	Network Solutions for Construction Site Environment Monitoring System
Pages	80
Graduation time	December 2009
Thesis supervisor	Ville Haapakangas
Co-operating company	Salon Rakennuskonevuokraamo Oy

ABSTRACT

The purpose of this thesis is to point out the best possible network technologies for a construction site environment monitoring system. Environment monitoring system is a solution for remote monitoring of temperature, electrical network and crime detection sensors.

The search for the best technologies started by mapping out the requirements mandated by the monitoring system and the operating environment. A requirement specification for the network technologies was based on the plans and specifications of the whole monitoring system and information were gathered from the operating environment.

The best technologies for the three separate networks of the system were found by comparing the requirements to the attributes of each technology. The correspondence to the specification was measured by scoring compliance to individual requirements. Numerical measurement of correspondence allowed for fair judgment and the selection of the best technology.

For reading the sensors at construction site, a ZigBee-network working at 868 MHz frequency range proved to be the most suitable solution. In order to connect the construction site to the Internet, the technologies based on GSM-network turned out to be the best. Finally, to secure and tunnel the connection between te construction site and the server system, IPSec was found to be the best for the job.

Given the resources available, the goals for the thesis were met well. The quality and reliability of the selection process would have been improved if technologies could have been tested out in a real life scenario. Unfortunately, the lack of financial resources and time made such testing impossible.

Keywords requirement specification, Ethernet, WiFi, IEEE 802.11s, ZigBee, 802.15.4, Flash-OFDM, GSM, IPSec, SSL-VPN

Sisällysluettelo

1 Johdanto

Rakennusalan laatuvaatimukset ovat viimeisen kymmenen vuoden aikana tiukentuneet merkittävästi samalla, kun työmaihin kohdistuva ilkivalta ja varkaudet ovat lisääntyneet huikealla vauhdilla. Toistaiseksi rakennusliikkeet ovat vastanneet uusiin ja vanhoihin laadunvalvontavaatimuksiin lisäämällä työmaan tarkkailua ja prosessien dokumentointia. Useimmiten tämä tarkoittaa sitä, että työmaan vastaava mestari vierailee työmaalla säännöllisesti myös iltaisin ja viikonloppuisin. Hän varmistaa, että lämmitysjärjestelmät toimivat, eikä vettä ole päässyt väärään paikkaan, betonivalujen kuivuminen etenee suunnitellusti ja työmaalla ei ole käynyt kutsumattomia vieraita. Rikosten torjuntaan yleisin menetelmä on vartiointiliikkeen palkkaaminen käymään työmaalla esim. kaksi kertaa illassa.

Työn toimeksiantaja Salon Rakennuskonevuokraamo Oy on vuodesta 1977 toiminut rakennuskonevuokraamo, joka päätoimintansa lisäksi myös myy rakennustarvikkeita ja suorittaa urakointina timanttileikkuuta ja huoneistojen otsonointia. Noin kymmenen henkeä työllistävän yrityksen toiminnan kulmakivenä on aina ollut asiantunteva ja suoraselkäinen palvelu Salon talousalueen rakentajille ja remontoijille. Rakennusala kuitenkin uudistuu. Onkin tullut aika tutkia myös uusia liiketoimintamahdollisuuksia, jotka vastaavat vasta noususssa oleviin rakentajien tarpeisiin.

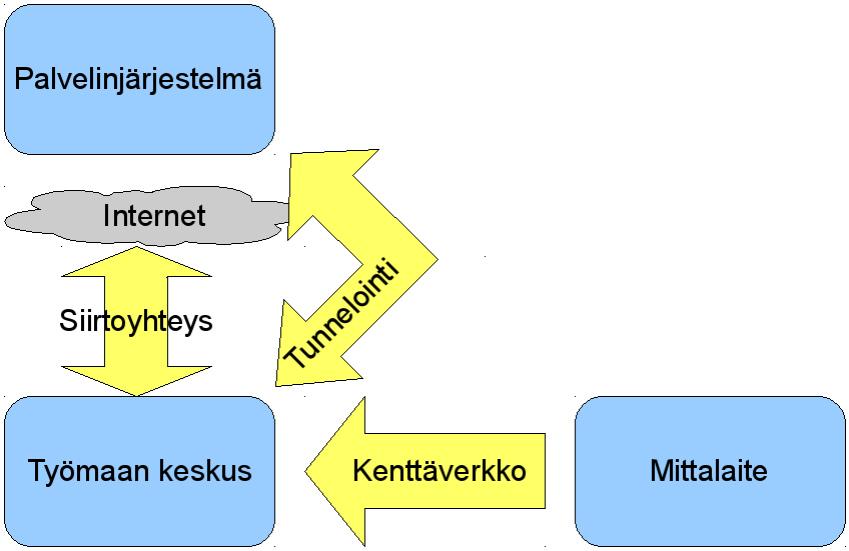
Jatkona nykyiselle liiketoiminnalle mutta täysin uutena aluevaltauksena syntyi ajatus olosuhdevalvontapalvelusta, jonka avulla työmaan olosuhteita, kuten lämpötilaa, sähköjen toimivuutta ja rikosilmoitusantureiden tilaa voidaan seurata käymättä työmaalla. Palvelun toteuttaminen edellyttää teknistä ratkaisua, joka mahdollistaa edullisten antureiden vapaan asentamisen työmaan erittäin vaihteleviin olosuhteisiin. Valvontajärjestelmä ei saa hankaloittaa työmaan arkea ja sen tulisi toimia mahdollisimman huoltovapaasti.

Tässä työssä käydään läpi tämän järjestelmän edellyttämien tietoverkkoratkaisujen valintaprosessi. Tavoitteena oli löytää aidosti paras tekninen ratkaisu järjestelmän tarpeisiin.

Aluksi luvussa tarve esitellään lähtötilanne, joka asettaa puitteet tietoverkkojen tarpeelle ja toteutukselle. Salassapitosyistä kokonaisjärjestelmän teknisiin yksityiskohtiin ei tämän työn puitteissa voida perehtyä. Vaatimukset luvussa määritellään kriteerit ja pisteytysjärjestelmä, jonka perusteella tekniikoiden soveltuvuutta arvioidaan. Lopuksi verrataan tekniikoiden vaatimustenmukaisuutta keskenään ja valitaan siten paras tekniikka kuhunkin järjestelmän verkkoon.

2 Tarve

Tämän työn taustalla oleva kokonaisprojekti suunniteltiin kuunnellen rakennusalan ammattilaisten tarpeita, tutkimalla nykyisen tekniikan suomia mahdollisuuksia ja selvittämällä rakentamisen laadun seurannan kannalta oleelliset laatua parantavat suureet. Tarpeiden ja mahdollisuuksien pohjalta laadittiin kokonaisprojektin vaatimusmäärittely ja sitä toteuttava arkkitehtuurisuunnitelma (*SRKV Oy 2009a, 2009b*). Se määritteli järjestelmän toiminnan mahdollistaman teknisen ratkaisun kiinnepisteet (Kuvio 1), kuten palvelinjärjestelmän, työmaan keskuksen ja mittalaitteen.



Kuvio 1: Kokonaisjärjetelmän kiinnepisteet

Kiinnepisteiden toiminnallisuuden ja tekniikan selvittyä laadittiin kokonaisprojektin vaatimusmäärittelyä ja kiinnepisteiden tietoja hyväksi käyttäen tämän dokumentin lähtökohtana toimiva tiedonsiirtojärjestelmän vaatimusmäärittely. Koska tietoverkkoratkaisujen valinta on kokonaisjärjestelmän kannalta erittäin kriittinen tehtävä, johon on sitouduttava koko järjestelmän elinkaaren ajaksi, päätettiin tekniikan valintaprosessista muodostaa aliprojekti. Sen tavoitteena oli tutkia potentiaaliset toteutusvaihtoehdot ja valita kokonaisjärjestelmän kannalta parhaat tekniikat järjestelmän tietoverkkoratkaisuihin. Aliprojektin tuotteena syntyi tämä dokumentti, joka vastaa kysymykseen: **Mitkä tiedonsiirtoratkaisut soveltuvat parhaiten työmaan olosuhdevalvontajärjestelmän tarpeisiin?**.

3 Vaatimukset

Projektin tietoverkkoratkaisujen vaatimusmäärittely perustuu kokonaisprojektin suunnitelmaan ja vaatimusmäärittelyyn, jotka asettavat tietoverkkojen toiminnalle rajat määritellen mm. järjestelmään luettavan tiedon ja sen määränpään. Vaatimusmäärittelyprosessissa kerätyistä kriteereistä käsitellään tässä työssä vain ne, jotka ovat tietoverkon perustekniikoiden valinnan kannalta oleellisia. Näitä ovat suorituskykyvaatimukset ja soveltuvuus työmaaolosuhteisiin. Tietoverkkoon välillisesti liittyviä vaatimuksia, kuten laitteiston mekaanista suojausta, ei tässä työssä käsitellä. (*SRKV Oy 2009a, 2009b.*)

Tietoverkkoratkaisujen vaatimusmäärittely pohjautuu vahvasti kokonaisprojektin suunnitelmissa tehtyihin ratkaisuihin koskien järjestelmän arkkitehtuuria, aktiivilaitteiden ominaisuuksia ja järjestelmän suorituskykyvaatimuksia. Verkkojärjestelmän vaatimusmäärittely toteutettiin omana kokonaisuutenaan mukaillen mm. Kaskelan suosittamaa ja hyväksi havaittua kolmiportaista vaatimusmäärittelyprosessia (*Kaskela 2005*).

Kokonaisprojektin arkkitehtuuri- ja toimintasuunnitelmia hyödyntäen määriteltiin tavoitteet tietoverkkoratkaisuille. Tavoitteet vastaavat kysymykseen, mitä tietoverkon pitää tehdä - sekaantumatta vielä sen enempää teknisiin kysymyksiin. Kenttäverkon kannalta oleellisin tavoite oli siis seuraavanlainen: **Kenttäverkon tulee mahdollistaa 300 mittapisteen tuottaman datan keskitetty keruu työmaaolosuhteissa.**

Tavoitteiden selvittyä voitiin siirtyä seuraavaan vaiheeseen eli tarpeiden tunnistukseen. Purkamalla osiin saadut tavoitteet päästiin käsiksi yksittäisiin tarpeisiin, joista järjestelmän on selviydyttävä. Esimerkiksi **tietoverkon on toimittava työmaaolosuhteissa**. Tarpeita tunnistettaessa on tärkeää hahmottaa kokonaisuus ja selvittää mahdolliset ristiriidat tarpeiden sekä esimerkiksi käyttöympäristön välillä.

Kolmantena ja viimeisenä vaiheena tarpeista jalostetaan varsinaiset vaatimukset. Esimerkiksi em. tarve toimia työmaaolosuhteissa pitää purkaa ja eritellä, **mitä vaatimuksia työmaaolosuhteet asettavat tietoverkolle**. Tässä vaiheessa pitää rakennettavan ver-

kon arkkitehtuurin hahmottua kokonaisuutena. Monet vaatimukset voivat toistua ja toisaalta osa saattaa kumota toisia.

Seuraavissa alaluvuissa esitellään tärkeimmät valintaperusteiksi sopivat vaatimukset. Ensimmäisissä alaluvuissa perehdytään kaikkiin tietoverkkoratkaisuihin vaikuttaviin vaatimuksiin ja niiden arviointitapoihin. Lopuksi eritellään suoraan kenttäverkkoon, siirtoyhteyteen ja tunnelointitekniikkaan vaikuttavat vaatimukset ja niiden arviointitavat.

Arviointi perustuu vaatimusten toteutumisen pisteyttämiseen aihepiireittäin. Useimpien aihepiirien asettamat vaatimukset on kiteytetty valinnan kannalta oleellisemmiksi väittämiksi, joista tekniikoita pisteytetään aihepiireissä määritellyllä tavalla. Osaa aiheista, kuten luotettavuutta ja kustannustehokkuutta, pisteytetään vaatimusten yhteydessä esitellyllä tavalla. Kunkin vertailtavan tekniikan osalta käydään läpi pisteyttäen kaikki sitä koskevat aihepiirit. Tekniikoiden lopullinen valinta tehdään vertailemalla pisteitä. Eniten pisteitä kerännyt tekniikka vastaa parhaiten asetettuja vaatimuksia. Eri tekniikoihin sovellettavat vaatimusaihepiirit käyvät ilmi oheisesta taulukosta 1.

Taulukko 1: Vaatimusaihepiirien soveltaminen verkonosiin

	Kenttäverkko	**Siirtoyhteys**	**Tunnelointi**
Luotettavuus	X	X	X
Kustannukset	X	X	
Yhteensopivuus	X	X	X
Turvallisuus	X	X	X
Mittapisteiden määrä ja maasto	X		
Mekaaniset ja sähköiset	X		
Mukautuminen	X		
Suorituskyky		X	
Saatavuus		X	

3.1 Luotettavuus

Ensimmäinen ja kenties tärkein kaikista järjestelmään kohdistuvista vaatimuksista on luotettavuus. Koska järjestelmän tärkein tehtävä on omaisuuden suojaaminen, ei virheille ole sijaa. Järjestelmän on toimittava ehdottoman luotettavasti ja mikäli järjestel-

män toiminta häiriintyy esimerkiksi sähkökatkoksen tai televerkko-ongelman takia, myös siitä on saatava tieto.

Luotettavuus on melko epämääräinen suure, jonka muodostavat mm. laitteiden, protokollien ja operaattoreiden toimintakyky. Tekniikoiden luotettavuuden absoluuttinen mittaaminen vaihtelevissa olosuhteissa on käytännössä mahdotonta. Jotta tekniikoita pystyttäisiin kuitenkin valintaprosessissa vertailemaan, tutkitaan luotettavuutta SWOT-taulukon (Strenghts, Weaknesses, Oppoturnities, Weaknesses) avulla. Se paljastaa verrattain hyvin tekniikoiden vahvuudet ja heikkoudet.

SWOT-taulukko ei itsessään vielä anna vertailukelpoista pisteytystä. Taulukot arvioidaan muodostamalla niille pistemäärä siten, että vahvuuksista ja mahdollisuuksista kertyy positiivisia ja heikkouksista sekä uhista negatiivisia pisteitä. Kertyneet pisteet summataan kokonaisluvuksi, jonka perusteella tekniikat voidaan asettaa paremmuusjärjestykseen. Parhaaksi arvioitu tekniikka saa 10 pistettä, toinen 8 ja kolmas 6.

3.2 Kustannukset

Koska järjestelmää kehitetään kaupalliseen käyttöön, kustannusten merkitykseltä ei voida välttyä. Järjestelmää kehitettäessä on varmistettava, että tuotteesta tulee taloudellisesti kannattava ja kustannuksiltaan kilpailukykyinen. Toisaalta myös pieni volyymi ja kehittävän yrityksen pieni koko sanelevat omat rajoitteensa kehitystyön budjettiin.

Käytännössä kustannuspaineet rajoittavat eniten siirtoyhteyden kustannuksia ja kenttäverkon päätelaitteiden yksikkökustannuksia. Absoluuttisia raja-arvoja näiden kustannuksille on mahdoton asettaa, mutta eri tekniikoiden kustannuksia voidaan verrata keskenään.

Vertailtaessa tekniikoita toisiinsa lasketaan niiden aiheuttamat investointi ja ylläpitokustannukset ennalta määritellyissä käyttötapauksissa. Käyttötapauksen kokonaiskustannuksissa pienimmät kustannukset aiheuttanut vaihtoehto on täten järkevin valinta. Kustannuslaskelmat tehdään verottomin vähittäismyyntihinnoin ja laskelmassa huomioi-

daan ainoastaan kyseisen tekniikan kiinteästi edellyttämät komponentit. Esimerkiksi akkuja ja kotelointeja ei sisällytetä laskelmaan. Kustannustehokkain ratkaisu saa 10 pistettä, toinen 8 ja kolmas 6.

3.3 Yhteensopivuus

Järjestelmää kehitetään hyvin pitkällä tähtäimellä pitäen avoimena tulevaisuuden mahdollisuudet. Merkittävä vaatimus on myös hyödynnettävien tekniikoiden avoimuus ja yleisyys, joka voidaan saavuttaa joko avoimen lähdekoodin ohjelmistoina tai muina standardoituina ja vakiintuneina tekniikoina. Verkkotekniikoiden standardointielimia ovat mm. IEEE (Institute of Electical and Electronics Engineers), ISO (International Organization for Standardization) ja IETF (Internet Engineering Task Force).

Yhteensopivuusvaatimus tulee parhaiten esille järjestelmän rajapinnoissa, joissa järjestelmän eri osat on sovitettava yhteen. Tällaisia rajapintoja on esimerkiksi kenttäverkon ja siirtoyhteyden sekä siirtoyhteyden ja palvelinjärjestelmän välissä. Niissä datan on liikuttava nopeasti ja luotettavasti riippumatta käytettävistä tekniikoista. Tekniikan avoimuus ja standardointi ovat parhaat tavat varmistaa tekniikoiden välisen rajapinnan toteutettavuus.

Standardien mukaisuudella pyritään myös varmistamaan järjestelmän komponenttien saatavuus. Mikäli esimerkiksi kenttäverkon päätelaitteiden valmistus loppuisi, standardoitu tai avoin arkkitehtuuri mahdollistaisi yhteensopivien laitteiden hankinnan toiselta valmistajalta.

Standardien mukaisuus edesauttaa järjestelmän CE-merkintää. Jotta järjestelmä ja sen komponentit voidaan merkata CE-tunnuksella eli vaatimustenmukaisuusvakuutuksella tulee sen täyttää kaikki kyseiseen tuoteryhmään kohdistuvat turvallisuutta, terveyttä, ympäristöä ja kuluttajansuojaa koskevat vaatimukset (*CE-merkintä: Tuote vastaa vaatimuksia 2008*). Tärkeimmät suunnitellun kaltaiseen järjestelmään vaikuttavat viranomaisvaatimukset ovat ns. EMC- ja RoHS-direktiivit (Electro Magnetic Compability ja Restriction of Hazardous Substances), jotka käsittelevät sähkölaitteen sähköisiä ominai-

suuksia, kuten häiriönsietoa ja -aiheutusta sekä laitteen rakenteessa käytettäviä vaarallisia aineita, kuten lyijyä. Tekniikan yhteensopivuutta arvioidaan pisteyttämällä toteutuneet kriteerit alla olevan taulukon 2 mukaisesti.

Taulukko 2: Yhteensopivuusvaatimusten pisteytys

Yhteensopivuus	**Max. pisteet**
Tekniikka noudattaa virallista standardia (ISO / IEEE / IETF)	2,5
Ohjelmistorajapintaan päästään kiinni avoimilla ohjelmistoilla	2,5
Tekniikan komponentteja saatavilla useilta toimittajilta	2,5
Tekniikkaan saatavilla CE-merkittyjä komponentteja	2,5
	10

3.4 Turvallisuus

Koska järjestelmää käytetään omaisuuden turvaamiseen, on järjestelmän turvallisuus ensiarvoisen tärkeää kaikissa vaiheissa. Tekniikoiden turvallisuuden arvioinnissa kiinnitetään huomiota tietoturvan kolmeen perustekijään: tunnistukseen, valtuutukseen ja tilastointiin, jotka tunnetaan termillä AAA (Authentication, Authorization, Accounting) (*Wendell 2005, 356*). Kaiken järjestelmän välittämän mittaustiedon tulee täyttää nämä kolme kriteeriä, ennen kuin mittaustulos voidaan tallentaa palvelimille ja niiden perusteella ryhdytään toimiin.

Tunnistuksella tarkoitetaan, että mittaustuloksen lukeva laite on tunnistettava. Samoin työmaan keskuslaitteen on tunnistauduttava palvelinjärjestelmälle luotettavasti. Tässä yhteydessä valtuutus tarkoittaa, että ennen mittaustuloksen tallentamista varmistetaan mittauspisteen datan todella kuuluuvan kyseiselle työmaalle. Kolmannella tekijällä, eli tilastoinnilla varmistetaan kaikkien suoritettujen toimenpiteiden tallentuminen lokitietoihin. Tilastointi ei käytännössä edellytä protokolla ja tekniikkatasolla toimenpiteitä, vaan tilastointi tehdään palvelinjärjestelmässä. Tekniikoiden turvallisuutta arvioidaan ja vertaillaan pisteyttämällä toteutuneet ehdot oheisen taulukon 3 mukaisesti.

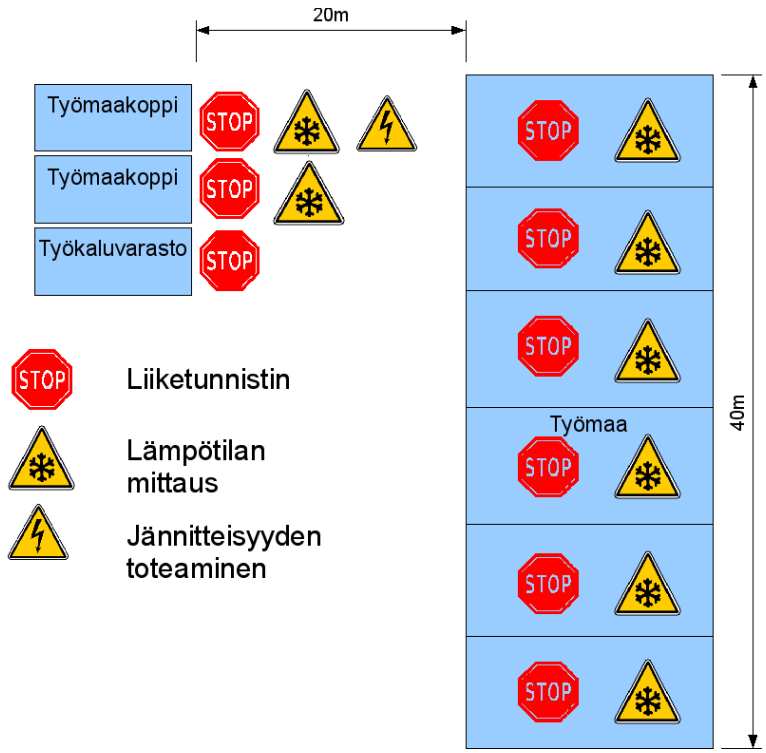
Taulukko 3: Turvallisuusvaatimukset

Turvallisuus	**Max. Pisteet**
Päätelaitteiden luotettava tunnistus	2
Datan eheydenvarmennus	2
Yhteyden salaus	2
Tekniikka yleisesti testattu	2
Ei vakavia haavoittuvuuksia	2
	10

3.5 Kenttäverkko

Kenttäverkolla tarkoitetaan tietoverkkoratkaisua, jonka avulla antureilta saatu data siirretään kohteen keskusyksikölle. Työmaaolosuhteet asettavat verkkoratkaisulle erittäin haastavan ympäristön, jossa perinteiset ja hyväksi havaitut tietoverkkoratkaisut eivät menestyisi.

Apuna kenttäverkon tekniikoiden arvioinnissa käytettiin kokonaisjärjestelmän suunnitelmien yhteydessä laadittua käyttötapausta (jatkossa UC2). Käyttötapaus on kuvitteellinen skenaario, jonka avulla simuloidaan työmaan etenemistä ja järjestelmän hyödyntämistä työmaan aikana. Kenttäverkon tekniikoiden arvioinnissa käytettiin vuoden kestävää rivitalotyömaata kuvaavaa käyttötapausta, jonka pohjalta laadittiin suunnitelmat kustannuslaskemia varten. (Kuvio 2)



Kuvio 2: Kenttäverkko käyttötapauksessa UC2 (SRKV Oy 2009c.)

Kenttäverkkoon kohdistuvat vaatimukset kerättiin tutkimalla rakennustyömaiden olosuhteita, olemassa olevia rinnastettavia järjestelmiä (esim. työmaasähköistys) ja haastattelemalla rakennusalan ja työmaasähköistyksen ammattilaisia. Lisäksi tekniikoiden soveltuvuutta arvioidaan sijoittamalla ne käyttötapauksiin ja tutkimalla muuta saatavilla olevan tekniikan käyttöönottoa ja käyttökokemuksia käsittelevää materiaalia.

3.5.1 Mittapisteiden määrä, etäisyydet ja maasto

Kokonaisjärjestelmän suunnitelmissa järjestelmän suurimmaksi mittauspistemääräksi määriteltiin 300 kpl, jotka hajautuvat jopa 50000 m² alueelle. Mittauspisteet sijaitsevat korkeintaan 50 m päässä toisistaan, mutta rakennustyömaan ympäristö on usein erittäin esteinen ja työmaa saattaa muuttua merkittävästi lähes päivittäin.

Yhden mittauspisteen data koostuu minimissään seuraavista tiedoista:
- Mittapisteen tunniste 16 b
- Mitattavan suureen tunniste 8 b
- Mittaustulos 8 b

Mittauspisteen nettodatamäärä on 32 b. Lisäksi on huomioitava siirtoprotokollan kehysten vaatima datamäärä. Esimerkiksi käytettäessä TCP/IP-protokollaa Ethernet-verkossa kasvaa mittapisteen bruttodatamäärä 512 bittiin (TCP/IP kehys 224 b + Ethernet-kehys 208 b = 424 b, mutta Ethernet-kehyksen minimikoko on 64 oktettia eli 512 bittiä). (*Cisco Networking Academy Program 2003, 262, 454.*)

Edellä mainittujen tietojen pohjalta laskettuna siirrettäväksi datamääräksi saadaan: 300 kpl x 512 b = 153600 b = 153,6 kb→ 19,2 kB

Järjestelmän on tarvittaessa pystyttävä reaaliaikaiseen valvontaan. Käytännössä mittauslukemien on voitava päivittyä kerran sekunnissa, jolloin järjestelmän minimisiirtokyvyksi saadaan 19 kB/s tai 1,2 kB/s nettodatana.

Tekniikan soveltuvuutta kenttäverkon suorituskykyvaatimuksiin vertaillaan pisteyttämällä toteutuneet ominaisuudet alla olevan taulukon 4 mukaisesti.

Taulukko 4: Mittapisteiden määrään, etäisyyteen ja maastoon liittyvät vaatimukset

Mittapisteiden määrä etäisyydet ja maasto	**Max. Pisteet**
300 päätelaitteen liittäminen mahdollista	5
Minimisuorituskyky saavutettavissa 300 päätelaitteen verkossa	2,5
Tekniikka soveltuu esteiseen maastoon	2,5
	10

3.5.2 Mekaaniset ja sähköiset vaatimukset

Ympäristö, jota järjestelmä rakennetaan valvomaan, on luonteeltaan erittäin vaativa komponenttien mekaanisen ja sähköisen keston kannalta. Havainnoitaessa vastaavissa

olosuhteissa käytettäviä laitteita havaitaan niiden rakenteen olevan järjestelmällisesti erittäin jämeriä ja tiiviitä. Komponenttien on kestettävä huomattavia fyysisiä rasitteita, kuten tärinää, iskuja ja murtovoimia, rikkoontumatta. Suurin osa mekaanisista vaatimuksista voidaan toteuttaa jälkeenpäin laitteiden koteloinnissa ja sähköistyksen toteutuksessa. Suoraan tietoverkkoratkaisun valintaan vaatimukset vaikuttavat esimerkiksi ratkaisun vaatiman kaapeloinnin, antennien ja häiriönsiedon osalta.

Yleisesti käytetyt tietoverkkoratkaisut on suunniteltu käytettäväksi verrattain helpoissa toimisto-olosuhteissa, joten työmaaolosuhteita varten vaaditaan merkittäviä muutoksia normaaleihin asennustarvikkeisiin, aktiivilaitteisiin ja asennustapoihin. Lähinnä työmaan olosuhteita ovat teollisuuden automaatiossa käytettävät ratkaisut, joiden kehitystyö on ollut erittäin aktiivista viime vuosina. Teollisuus ja työmaaympäristö asettaa yllättävän monia haasteita, joista päällimmäiset Marshall ja Rinaldi listaavat kirjassaan Industrial Ethernet (*Marshall & Rinaldi 2005, 1*). Seuraavassa rakennustyömaaolosuhteiden kannalta oleellisimmat haasteet Marshallia ja Rinaldia mukaillen:

- Tehtäväkriittisyys: käyttökatkoksilla saattaa olla merkittäviä taloudellisia seurauksia
- Ankarat olosuhteet: likaiset, tärisevät ja mekaanisesti koettelevat olosuhteet
- Sähköiset häiriöt: korkeajännitteet, suuret moottorit ja radio-ohjattavat laitteet
- Käyttöjännitteen syöttö: laitteille ei voida tuoda erillistä käyttöjännitekaapelia, vaan käyttöjännite tulee verkkokaapelista
- Turvallisuus: verkossa virukset yms. eivät uhkaa totutulla tavalla, vaan suurimmat uhat ovat inhimilliset erehdykset maallikoiden toimista

Työmaan olosuhteet ovat tietoverkolle varsin poikkeukselliset, sillä kaikki järjestelmän komponentit ovat käytännössä ulkotiloissa työmaan etenemisen mukaan. Sekä mekaanisten että sähköisten osien on toimittava -20C - + 30C lämpötiloissa ja siedettävä vähintään roiskevettä (IPX4). Käytännössä esimerkiksi kaapeleiden liitokset saattavat maata vesilätäkössä, joten luokitusvaatimukseksi asetettiin IP57. Se toteutetaan tarvittaessa lisäkoteloinnilla. (*STEK 2009.*)

Sähköteknisesti järjestelmän komponentteihin kohdistuu melkoisia haasteita, sillä järjestelmän mahdolliset kaapeloinnit saattavat kulkea samoja reittejä ajoittain hyvinkin suurivirtaisten kaapeleiden kanssa. Mittausjärjestelmän komponenttien lähellä saatetaan käyttää voimakkaita sähkömoottoreita, jotka saattavat häiritä elektronisten laitteiden toimintaa, ellei laitteita ole suojattu asianmukaisesti. Toisaalta tiedonsiirtoratkaisu ei saa häiritä muita järjestelmiä, kuten matkapuhelinverkkoa tai työmaan läheisyydessä sijaitsevia muita mittalaitteita (esim. sairaalat). Tämän vaatimuksen täyttöä edellyttää myös järjestelmälle tarvittavan CE-merkinnän kautta EMC-direktiivi.

Rakennustyömaaolosuhteissa tietoverkkoihin kohdistuu sähköisiä häiriöitä käytettiinpä tiedonsiirtoon kaapeleita tai radiotietä. Kaapeloituihin ratkaisuihin kohdistuvat ongelmat voivat olla joko häiriöluonteisia, kuten verkon liikennettä häiritsevä indusoituneiden jännitteiden aiheuttama kohina tai laiterikon, kaapelin rikkoutumisen tai salaman aiheuttama virtapiikki, joka saattaa tuhota verkon aktiivilaitteita. Kaapeloidun verkon ongelmilta suojaudutaan käyttämällä suojattua kaapelia, maadoittamalla kaapelit ja laitteet oikein ja suojaamalla aktiivilaitteet ylijännitesuojin.

Langattomien verkkojen ongelma piilee käytettävien taajuuksien valinnassa. Varsinkin yleisempien langattomien tekniikoiden kuten WiFi:n käyttämä 2,4GHz ISM-taajuusalue on paikoitellen erittäin ruuhkainen. Käytettävän tekniikan on kyettävä löytämään kohteessa parhaiten toimivat kanavat. Työmaaolosuhteissa radiotietä saattavat häiritä myös työmaalla käytettävät koneet, jotka saattavat tuottaa tilapäisiä mutta erittäin voimakkaita häiriöitä lähes mille tahansa taajuusalueelle. Radiotien toimivuutta voidaan varmistaa joko älykkäällä taajuuksien hallinnalla, jolloin laitteet esimerkiksi valitsevat itsenäisesti parhaiten toimivan kanavan tai silmukoidulla verkkoratkaisulla, jossa päätelaitteet voivat olla yhteydessä toisiinsa useampaa reittiä pitkin.

Mekaanisiin ja sähköisiin vaatimuksiin perustuva arviointi tehdään pisteyttämällä oheisen taulukon 5 mukaisesti.

Taulukko 5: Mekaaniset ja sähköiset vaatimukset

Mekaaniset ja sähköiset vaatimukset	**Max. Pisteet**
Tekniikassa huomioitu sähköiset häiriöt	3,33
CE-merkintä tai muu osoitus EMC vaatimustenmukaisuudesta	3,33
Tekniikkaa onnistuneesti sovellettu verrattavissa kohteissa	3,33
	10

3.5.3 Mukautuminen

Ehkä merkityksellisin perinteisistä lähiverkkojärjestelmistä poikkeava vaatimus tälle järjestelmälle on verkon sopeutumiskyky. Koska rakennustyömaan olosuhteet ja fyysinen ympäristö voi muuttua päivittäin, verkkoa on voitava muokata helposti ja nopeasti ilman tietoverkkotekniikan asiantuntemusta. Käytännössä tämä sulkee pois vaihtoehtoja esim. kaapeloinnin ja reititystekniikan osalta. Tietoverkon reitityksen on tapahduttava automaattisesti. Verkon tilaa ja liittyneitä päätelaitteita on pystyttävä seuraamaan keskitetysti toimintakyvyn varmistamista ja vikatilanteiden analysointia varten.

Jatkuvasti muuttuva rakenne vaikeuttaa myös aktiivilaitteiden sähkönsaantia, sillä oman sähköverkon rakentaminen järjestelmää varten ei ole mahdollista ja työmaan normaalista jakeluverkosta katkaistaan usein sähkö yöksi. Käytännössä tämä tarkoittaa, että järjestelmän päätelaitteiden on oltava akkukäyttöisiä.

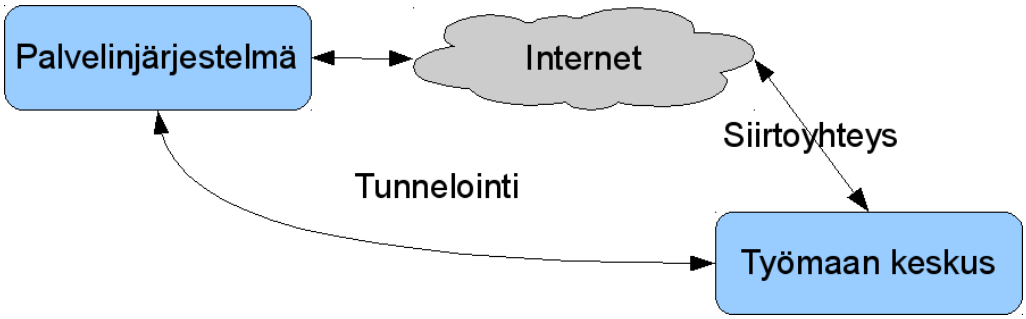
Tekniikan mukautumiskykyä arvioidaan pisteyttämällä sen ominaisuuksia alla olevan taulukon 6 mukaisesti.

Taulukko 6: Mukautumiskyvyn vaatimukset

Mukautuminen	**Max. Pisteet**
Langattomuus	2,5
Automaattinen reititys	2,5
Verkon tiladiagnostiikka	2,5
Komponentit optimoitu akkukäyttöön	2,5
	10

3.6 Siirtoyhteys

Siirtoyhteydellä tarkoitetaan työmaan keskuksen ja palvelimien välistä tietoverkkoratkaisua (Kuvio 3), jonka avulla työmaan kenttäverkon avulla kerätty data siirretään palvelinjärjestelmään tallennettavaksi jatkotoimenpiteitä varten.



Kuvio 3: Palvelinjärjestelmän ja työmaan keskuksen välinen yhteys

Eräs järjestelmän perustavan laatuisista suunnitteluperusteista on luoda teknisesti maanlaajuiseen toimintaan valmis ratkaisu. Tällöin siirtoyhteysverkon oma operointi on käytännössä mahdotonta. Luonteva ratkaisu siirtoyhteyden toteutukseen on siirtää data Internetin kautta palvelinjärjestelmälle. Ratkaistavaksi jää sopivan yhteystavan valinta, jolla työmaan järjestelmä yhdistetään Internetiin. Suomen markkinoilla toimii useita operaattoreita, jotka kykenevät toimittamaan Internet-yhteyden käytännössä kaikkiin Suomen kolkkiin. Vakioidut rajapinnat mahdollistavat käytettävän yhteystekniikan valinnan saatavuuden mukaan tarvittaessa.

3.6.1 Suorituskyky

Siirtoyhteyden suorituskykyvaatimusten lähtökohtana on mittapisteiden keräämä data, joka pitää siirtää välittömästi eteenpäin palvelinjärjestelmälle. Tämän lisäksi siirtoyhteyden kautta kulkee verkon hallintaan tarvittava data, jonka osuus siirrettävästä datamäärästä on hyvin pieni. Huomioitavaa siirtoyhteyden suorituskyvyn kannalta on, että liikenne suuntautuu ulospäin eikä sisään, kuten normaalissa koti- tai toimistokäytössä.

Kuten mittapisteiden määrä, etäisyydet ja maasto kappaleessa todettiin suurin osa kenttäverkon kautta saapuvasta datasta koostuu TCP/IP- ja Ethernet-protokollien kehyksistä. Vaikka Ethernet-kehykset eivät siirrykään eteenpäin, mittausdatan siirto erillisinä TCP/IP paketteina on tehotonta. Ratkaisuna kerätty data tallennetaan työmaan keskusyksikölle ja lähetetään edelleen yhtenä datavirtana, jolloin siirrettävä datamäärä tippuu 19 kB/s:ta 1,2 kB/s nettodatamäärään. Toki tämän lisäksi tunnelointi lisää kaistan tarvetta noin 8% pakettia kohden, mutta kokonaisuudessa mittausdatan siirto edellyttää n. 1,3 kB/s ulospäin suuntautuvaa kaistaa (*Network Stuff 2009*). Käytäntö on osoittanut, että verkko ei kuitenkaan toimi jatkuvasti maksiminopeudellaan. Yhteyksien nopeusvaatimukseen on aiheellista lisätä varmuuskerroin, joka tässä tapauksessa määriteltiin kahdeksi. Siirtoyhteydeltä edellytetään siis vähintään 2,6 kB/s ulospäin suuntautuvaa siirtonopeutta ja sama sisäänpäin.

Teknisesti useat tietoverkkoratkaisut mahdollistavat liikenteen priorisoinnin verkon operaattorin niin halutessa. Priorisoinnilla tarkoitetaan liikenteen luokittelua tärkeyden perusteella ja siten varmistaa, että tärkeämmäksi luokiteltu liikenne saa aina etuoikeuden muuhun liikenteeseen nähden, eikä siten kärsi verkon ruuhkaantumisesta.

Suorituskykyä arvioidaan pisteyttämällä tekniikan suorituskyky alla olevan taulukon 7 mukaisesti.

Taulukko 7: Suorituskykyyn kohdistuvat vaatimukset

Suorituskyky	**Max. Pisteet**
Tekniikka mahdollistaa liikenteen vähimmäissuorituskyvyllä	5
Tekniikka mahdollistaa dataliikenteen priorisoinnin	5
	10

3.6.2 Verkon saatavuus

Eräs kriittisimmistä siirtoyhteysmedian valintaan vaikuttavista tekijöistä on käytettävän verkon saatavuus, jonka koostuu verkon kattavuudesta, verkkoon kytkeytymisen helppoudesta ja yhteyden luotettavuudesta. Käytettävän yhteysmedian on toimittava määritellyllä miniminopeudella paitsi suurimpien kaupunkien keskustoissa, myös haja-asutus-

alueilla kautta Suomen. Rakennustyömaiden ja järjestelmän tilapäisen luonteen vuoksi siirtoyhteysmedia on oltava nopeasti kytkettävissä ja siirrettävissä esimerkiksi työmaa-koppiin.

Verkon maatieteellistä kattavuutta arvioidaan vertailemalla operaattoreiden julkaisemia tietoja. Tavoitteena on varmistaa, että operaattori kykenee toimittamaan yhteyden koko Suomen alueelle niin taajamiin kuin haja-asutusalueille. Poikkeuksena voidaan sallia pohjois-Suomen erämaa alueet ja ulkosaaristo, joissa voidaan tarvittaessa tukeutua vaihtoehtoisiin tekniikoihin.

Verkon kattavuuteen liittyy kiinteästi myös signaalin kuuluvuus, esimerkiksi kaupunki-olosuhteissa. Tavoitteena on että siirtoyhteys pystytään pääsääntöisesti toteuttamaan ilman erillisiä järjestelyjä, kuten ulkoista suunta-antennia. Siirtoyhteyden asennuksen pitää olla mahdollisimman yksinkertaista, oltiinpa missä päin Suomea tahansa. Kytkennän helppoutta tutkitaan vertailemalla operaattoreiden julkaisemia tietoja järjestelmästään ja saatavilla olevia käyttökokemuksia.

Verkon saatavuutta arvioidaan pisteyttämällä seuraavat ominaisuudet oheisen taulukon 8 mukaisesti.

Taulukko 8: Saatavuuden vaatimukset

Saatavuus	**Max. Pisteet**
Verkko kattaa koko Suomen	5
Verkon käyttö ei edellytä ulko- tai suunta-antennia	5
	10

3.7 Tunnelointi

Tunneloinnilla tarkoitetaan tekniikkaa, jonka avulla työmaan ja palvelinjärjestelmän välinen yhteys suojataan. Tunneloinnin pitää mahdollistaa yhteyden osapuolten vahva tunnistaminen, siirrettävän datan salaus tunnetulla ja testatulla algoritmilla sekä varmistaa siirretyn datan eheys ja oikeellisuus.

Tunnelointitekniikoiden arvioinnissa käytetään samoja kriteerejä kuin siirtoyhteystekniikoissa, mutta kustannuksia, suorituskykyä ja saatavuutta ei arvioida vähäisten erojen vuoksi.

4 Vaihtoehdot

Tässä työssä vertailtavat tekniikat karsiutuivat lukemattomien vaihtoehtojen joukosta lupaavimmiksi tekniikoiksi melko karkean, mutta tehokkaan valintaprosessin seurauksena. Kokonaisprojektin antamien raamien ja laaditun vaatimusmäärittelyn valossa etsittiin mahdollisimman monta tekniikkaa, jolla tarvittavan osan olisi voinut toteuttaa. Useimmat vaihtoehdot osoittautuivat käytännössä mahdottomiksi esimerkiksi kustannusten, saatavuuden tai yhteensopivuustekijöiden johdosta. Esimerkiksi siirtoyhteyden olisi teknisesti voinut toteuttaa satelliittiyhteydellä, mutta kustannusten kannalta se ei olisi ollut mitenkään mahdollista.

Arvioitavaksi päätyivät tekniikat, jotka selvisivät alkukarsinnasta lupaavimpina vaihtoehtoina ja joiden välisen paremmuuden arviointi edellytti tarkempaa tarkastelua ja tekniikoihin perehtymistä. Otokseksi päätyi kolme kenttäverkkotekniikkaa, kolme siirtoyhteystekniikkaa ja kaksi tunnelointitekniikkaa. Yhteensä otokseen kuuluu kahdeksantoista mahdollista kombinaatiota, joista mikä tahansa mahdollistaisi tavoitteen saavuttamisen.

4.1 Kenttäverkko

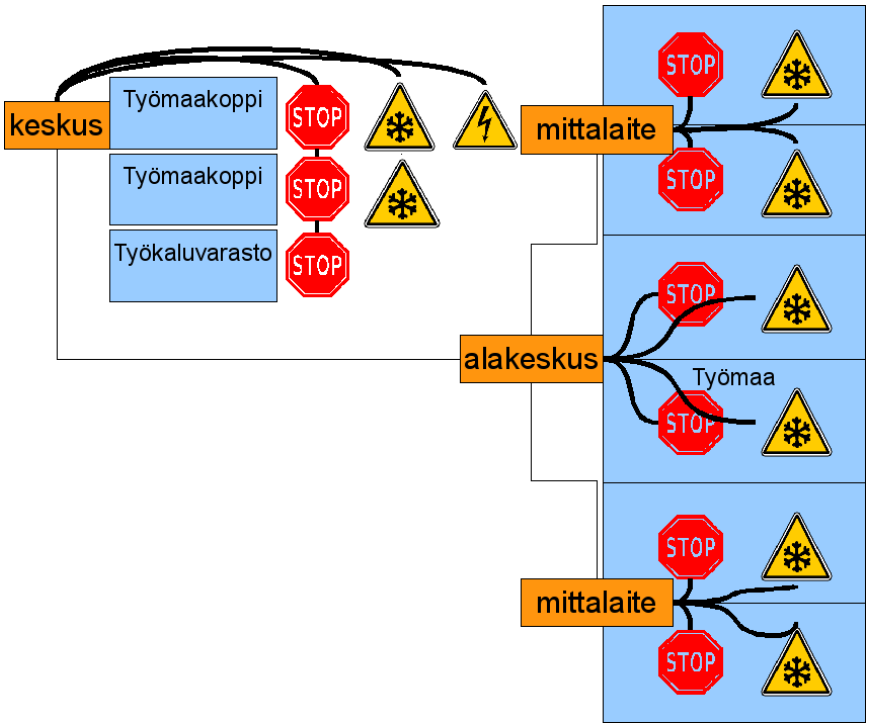
Kenttäverkon toteutusvaihtoehdoiksi karsiutui kolme melko erilaista ratkaisua, joita ei tiettävästi ole aikaisemmin sovellettu suoraan verrattavaan järjestelmään. Tekniikoiden arviointi on tehtävä erittäin huolellisesti erityisesti paneutuen toimintaympäristön asettamiin vaatimuksiin ja muihin käytännön seikkoihin. Kaikki vertailtavat tekniikat ovat riittävän koeteltuja, jotta on perusteltua olettaa tekniikoiden perustoiminnallisuuden olevan kunnossa.

Kenttäverkkoa varten arvioitavat tekniikat ovat Ethernet-verkko teollisuuslaatuisin komponentein toteutettuna. Toisena luonnosasteella olevaan IEEE 802.11s standardiin pohjautuva WiFi-Mesh silmukkaverkko. Kolmantena tekniikkana erityisesti anturiverkkoja varten kehitetty ZigBee.

4.1.1 Ethernet

Ethernet-tekniikat 100Base-TX ja 1000Base-T ovat nykyään ylivoimaisesti yleisimmät lähiverkkotekniikat, joita silmällä pitäen mm. kiinteistöjen yleiskaapelointijärjestelmät suunnitellaan (*Yleiskaapelointijärjestelmät 2005, 192*). Vaikka Ethernet on lunastanut paikkansa toimistojen verkkoratkaisuna teollisuuden merkittävästi haasteellisimmissa olosuhteissa se tekee vasta tuloaan perinteisten automaatioväylien rinnalle.

Ethernet-tekniikalla toteutettuna kenttäverkko koostuu kolmesta laitetyypistä. Työmaan keskukseen sijoitetaan Ethernet-kytkin, jotta keskukseen voidaan kytkeä useita lähtöjä. Toinen laitetyyppi on alakeskus, joka koostuu kytkimestä, sekä virtalähteestä, joka syöttää käyttöjännitteen verkkolähtöihin. Virtalähdeosa on sijoitettu alakeskuksiin, koska kaapelointi kestää vain noin kymmenen aktiivilaitteen vaatiman virran (*Yamaichi Electronics 2009*). Kolmas laitetyyppi on mittalaite, joka saa käyttöjännitteensä Ethernet-kaapelista. Esimerkkikäyttötapauksessa verkko koostuu kahdesta mittalaitteesta, alakeskuksesta ja työmaakeskuksesta (*Kuvio 4*).



Kuvio 4: Käyttötapaus UC2 Ethernet-tekniikalla toteutettuna

Teoria

Ethernet-tekniikalla viitataan 1970-luvulla alkunsa saaneisiin CSMA/CD tekniikkaan perustuviin IEEE 802.3-standardiperheen pari- tai valokaapelia hyödyntäviin pakettikytkentäisiin lähiverkkotekniikoihin. Näistä yleisimmät ovat 100Base-TX, 100Base-FX, 1000Base-T ja 1000Base-SX (IEEE 802.3u ja IEEE 802.3z). Ethernet-protokolla itsessään toimii OSI-mallin (Open Systems Interconnection Reference Model) 1 ja 2 kerroksissa, eli fyysisellä ja siirtoyhteystasolla, joten korkeamman tason datasiirto toteutetaan käytännössä aina TCP/IP protokollalla OSI-mallin 3 ja 4 kerroksissa (*Wendell 2005, 59*). Syyt Ethernet verkkojen yleisyyteen ovat selviä, sillä parikaapelitekniikalla toteutettuna verkot ovat ylivertaisen nopeita, luotettavia ja kustannustehokkaita kaikkiin kilpaileviin tekniikoihin verrattuna.

Topologialtaan tässä sovellettava Ethernet-verkko on laajennettu tähti. Kaikki verkon päätelaitteet yhdistetään keskuspisteeseen enintään neljän kytkimen kautta. Näin saadaan rakennettua laajalle alueelle leviävä verkko, jossa uusia päätelaitteita voidaan kytkeä varsin joustavasti lähimpään kytkimeen.

Luotettavuus

Ethernet on osoittanut luotettavuutensa suurten ja pienten organisaatioiden lähiverkkoratkaisuna, joten on perusteltua olettaa tekniikan itsessään olevan riittävän luotettava useimpiin käyttötarkoituksiin. Vaativissa olosuhteissa aktiivilaitteiden merkitys kuitenkin korostuu. Apuna luotettavuuden arviointiin käytetään SWOT-taulukkoa (Taulukko 9), jonka avulla oleellisimmat luotettavuuteen vaikuttavat tekijät saadaan esille.

Taulukko 9: SWOT analyysi Ethernet-tekniikan luotettavuudesta

Strenghts – Vahvuudet Erittäin yleinen tekniikka Normaalitilanteessa hyvin luotettava	**Weaknesses – Heikkoudeth** Kuluvat liitokset ja kaapelit Ei valmista vikailmoitusjärjestelmää Riippuvuus sähkönjakelusta
Oppoturnities – Mahdollisuudet Helppo vian haku ja korjaus	**Threats – Uhat** Kaapelointi mekaanisesti haavoittuva Sähköiset häiriöt kaapelointiin

SWOT-taulukko tuo armottomasti esille Ethernet-tekniikan alttiuden mekaanisille häiriöille. Vaikka verkon häiriöt ovat toisaalta melko helppoja korjata, ne edellyttävät asen-

tajan käyntiä työmaalla, mikä saattaa aiheuttaa pitkiä katkoksia. Kappaleessa 3.1 esitellyn laskentatavan mukaisesti Ethernet-tekniikan luotettavuus saa arvon -2.

Kustannukset

Vaikka Ethernet on yleinen tekniikka, johon sopivia laitteita löytyy sadoilta toimittajilta komponenttien kustannukset kohoavat yllättävän paljon käytettäessä teollisuuskäyttöön soveltuvia erikoiskomponentteja. Järjestelmä voitaisiin toteuttaa myös ns. white-box komponenteilla, mutta tällöin tarvittavat häiriösuojaukset pitäisi lisätä erikseen. Virtalähde pitäisi sovittaa järjestelmään sopivaksi tässä käytettävän teollisuusvirtalähteen sijaan.

Kuten alla oleva taulukko 10 osoittaa, merkittävimmän osan tekniikan kustannuksista muodostaa erikoiskestävä verkkokaapeli. Se mahdollistaa käyttöjännitteen jakelun samassa kaapelissa. Virtalähde on 12V DC teollisuusvirtalähde akkuvarmennuksella.

Taulukko 10: Ethernet-tekniikan kustannusvaikutus käyttötapauksessa UC2

Osa		Tarve	Kustannus	Yhteensä
Kaapelit	YconCable-1	60	5.70 €	342.00 €
Liittimet	Ycon*	6	26.05 €	156.30 €
Kytkimet	ISW800	2	99.00 €	198.00 €
Virtalähde	ADD-55	1	90.00 €	90.00 €
				786.30 €

Yhteensopivuus

Yhteensopivuuden puolesta Ethernet on vertailtavien tekniikoiden mallioppilas. Varsinainen datasiirto tapahtuu IEEE 802.3 standardin määrittelemin tekniikoin TCP/IP protokollaa käyttäen. Yhteensopivia CE-merkittyjä tuotteita on tarjolla tuhansia ja ohjelmistorajapintaan on tarjolla lukematon määrä työkaluja. Ainoan poikkeus standardien noudattamiseen tulee käytettävästä kaapelointijärjestelmästä, joka käytännössä pakottaa käyttämään yhden valmistajan tuotteita kautta linjan. Taulukkoon 11 on kerätty tekniikan yhteensopivuuden pisteytys.

Taulukko 11: Ethernet-tekniikan yhteensopivuus

Yhteensopivuus	Pisteet	Max pisteet
Standardi	2.5	2.5
Avoin SW API	2.5	2.5
Useita HW toimittajia	2.5	2.5
Komponentit CE-merkittyjä	2.5	2.5
	10	**10**

Turvallisuus

Turvallisuus on Ethernet-ratkaisun heikkous, sillä Ethernet ja TCP/IP tekniikat eivät sisällä sisäänrakennettuja turvaominaisuuksia ja sellaisten toteuttaminen verkkoyhteyden ylemmillä tasoilla (esim. 801.1x tai VPN) monimutkistaisi toteutusta epäkäytännöllisen paljon. Turvaominaisuuksien puute yhdistettynä maailman yleisimpään lähiverkkotekniikkaan, johon pääsee liittymään millä tahansa kannettavalla tietokoneella luo heikot lähtökohdat turvallisuuskriittisen järjestelmän toiminnalle. Tästä syystä tekniikan turvallisuusominaisuuksien testaus ja haavoittuvuudet eivät ole relevantteja. Oheiseen taulukkoon 12 on pisteytetty Ethernet-tekniikan turvallisuusominaisuudet.

Taulukko 12: Ethernet-tekniikan turvallisuus

Turvallisuus	Pisteet	Max pisteet
Luotettava tunnistus	0	2
Eheydenvarmistus	0	2
Salaus	0	2
Testattu	2	2
Haavoittuvuudet	2	2
	4	**10**

Mittapisteiden määrä ja maasto

Koska Ethernet-tekniikka on kehitetty suurten yritysten lähiverkkojen tarpeisiin suorituskyky ja skaalautuvuus eivät muodosta merkittävää ongelmaa tekniikan puolesta. Ethernet-verkkoon pystyy teoriassa liittämään lähes rajattoman määrän päätelaitteita, mikäli verkon rakenne suunnitellaan huolellisesti. Teknisesti 100Base-TX-tekniikalla toteutetussa verkossa kahden aktiivilaitteen väli voi olla enintään 100 m (*Marshall & Rinaldi 2005, 22*), joka riittää tässä tapauksessa erinomaisesti. Rakennustyömaan esteisyys ei varsinaisesti haittaa Ethernet-ratkaisussa, sillä data kulkee siellä, mistä kaapeli saadaan kulkemaan. Kaapeloinnin ongelmista ja muista olosuhteiden aiheuttamista

ongelmista lisää Mekaaniset ja Sähköiset vaatimukset kappaleessa. Tekniikan soveltumisen pisteytys on oheisessa taulukossa 13.

Taulukko 13: Ethernet-tekniikan soveltuminen mitapisteiden määrään ja maastoon

Mittapisteiden määrä ja maasto	Pisteet	Max pisteet
300 päätelaitetta mahdollinen	5	5
Minimisuorituskyky	2.5	2.5
Soveltuu esteiseen maastoon	0	2.5
	7.5	**10**

Mekaaniset ja sähköiset vaatimukset

Toimiakseen työmaaolosuhteissa Ethernet-verkko on siis ensinnäkin koottava tarkoitukseen soveltuvista teollisuuslaatuisista komponenteista. Merkittävimmät haasteet Ethernet-tekniikan hyödyntämisessä kulminoituvat kaapelointijärjestelmään, jonka pitää kestää em. olosuhteet. Yleisesti käytetyt UTP Cat 5e/6 kaapeloinnit eivät sovellu jatkuvaan liikutteluun ja mekaaniseen kulutukseen, vaan kaapeleiden on oltava ulkokäyttöön soveltuvaa, häiriösuojattua ja taipuisaa. Useilla valmistajilla on tarjota häiriösuojattu IP57 luokiteltu Ethernet-liitinjärjestelmä, joka kestää mekaanista rasitusta ja mahdollistaa pöly- ja roiskevesitiiviit liitokset. Näistä lupaavimmaksi karsiutui Yamaichin valmistama Y-Con-järjestelmä (Kuvio 5). Sen avulla myös aktiivilaitteiden käyttöjännite pystytään kuljettamaan samassa erikoisvalmisteisessa Cat 5 STP kaapelissa.

Kuvio 5: Yamaichi Y-ConRJ45 Liitinjärjestelmä (Yamaichi Electronics 2009)

Verkossa ei voida käyttää tavallisia aktiivilaitteita, vaan laitteiden on toimittava joko 12 V tai 24 V jännitteellä, joka toimitetaan verkkokaapelin ylimääräisissä johtimissa. Verkon aktiivilaitteiden pitää myös olla suojattuja sähköisiä häiriöitä, kuten virtapiikkejä ja indusoituneita jännitteitä vastaan. Nämä kriteerit täyttävistä laitteista kustannustehokkaimmaksi osoittautui taiwanilaisen Planet Technology Corporation valmistama ISW-800 teollisuusethernet-kytkin. Tarkemmin soveltumista arvioiva pisteytys esitetään ao. taulukossa 14.

Taulukko 14: Ethernet-tekniikan sähköisten ominaisuuksien pisteytys

Mekaaninen	**Pisteet**	**Max pisteet**
Sähköiset häiriöt	1	3.33
EMC-vaatimustenmukaisuus	3.33	3.33
Onnistuneita sovelluksia	1.5	3.33
	6	**10**

Mukautuminen

Vaikka Ethernet-verkkoa ei normaalikäytössä tarvitse muokata useinkaan, voidaan verkkoa muokata melko paljon kyseessä olevin liikennemäärin. Verkon aktiivilaitteet eli kytkimet huolehtivat siitä, että data löytää oikeaan paikkaan verkon rakenteen muuttuessakin. Verkkoa rakennettaessa ja muokattaessa huomioitavaa on, ettei päätelaitteen ja keskuksen välille jää yli neljää kytkintä ja ettei verkkoon synny silmukkaa. Mukautumiskyky pisteytetään taulukossa 15.

Taulukko 15: Ethernet-tekniikan mukautumiskyky

Mukautuminen	**Pisteet**	**Max pisteet**
Langattomuus	0	2.5
Automaattinen reititys	1	2.5
Tiladiagnostiikka	0	2.5
Akkukäyttö	1	2.5
	2	**10**

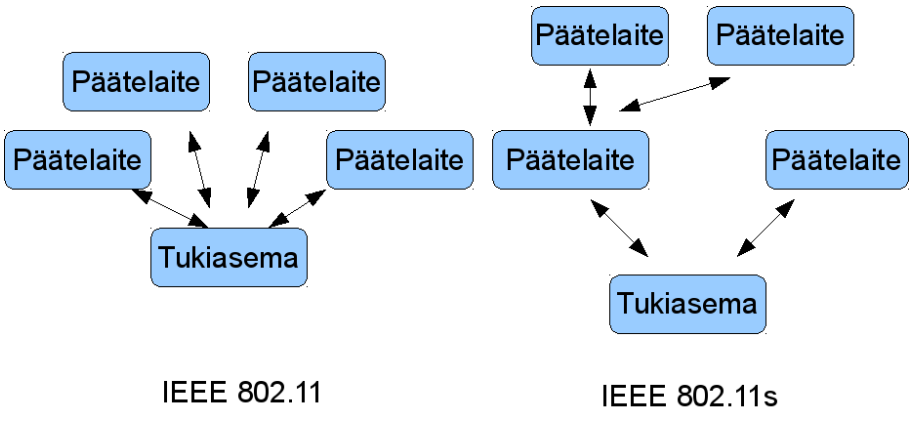
4.1.2 WiFi & WiFi-mesh

WiFi on kauppanimi WiFi Alliancen hallinnoimille keskenään yhteensopiville IEEE 802.11 standardiperheeseen perustuville tekniikoille, jotka on tarkoitettu verrattain

nopeaan tiedonsiirtoon lyhyellä kantamalla käyttäen lupavapaita 2,4 GHz ja 5 GHz ISM-taajuuksia (Industrial Scientific Medical). Nykyiset WiFi verkot ovat arkkitehtuuriltaan point-to-multipoint-tyyppisiä, jossa useat päätelaitteet ovat yhteydessä yhteen tukiasemaan. Verkon kattavuutta laajennetaan käyttämällä useampaa tukiasemaa, jotka liittyvät ns. runkoverkkoon Ethernet-väylän kautta.

WiFi-tekniikat ovat osoittautuneet tehokkaaksi ja edulliseksi tavaksi muodostaa langattomia verkkoyhteyksiä esimerkiksi yleisiin tiloihin ja yrityksiin. Yksittäisen tukiaseman pystyttäminen on äärimmäisen yksinkertaista. Laajemman verkoston rakentaminen vaatii merkittävästi suunnittelua, tietotaitoa ja käytännössä myös erillisen WLAN-ohjaimen hallitsemaan tukiasemien taajuuksia ja liikennettä. Näistä syistä päädyttiin jo karsintavaiheessa hylkäämään perinteinen WiFi-tekniikka kenttäverkon toteutusvaihtoehtona. Tekniikasta on kuitenkin kehitteillä ja jo osittain käytössä uusi versio, joka soveltuu merkittävästi paremmin työmaan olosuhteisiin.

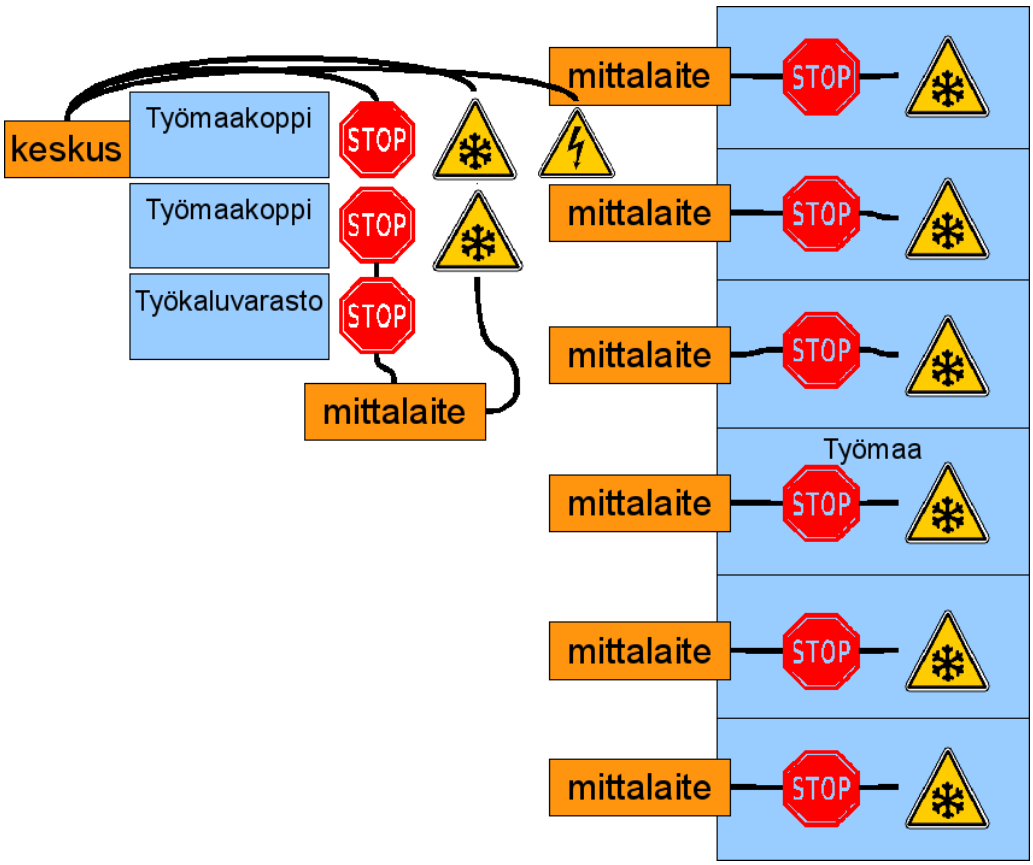
Uusi sukupolvi WiFi-tekniikassa on vielä virallisesti luonnosasteella oleva IEEE 802.11s standardi, joka mahdollistaa WiFi-laitteiden toiminnan silmukkaverkkona. Silmukkaverkossa jokainen päätelaite toimii myös tukiasemana. Reitti tiedonsiirtoon etsitään tarvittaessa useiden päätelaitteiden kautta (multihop) edistyneiden reititysprotokollien avulla. Oheinen kuva selvittää tekniikoiden topologioiden erot (Kuvio 6). Perinteisessä WiFi-verkossa kaikki päätelaitteet yhdistyvät suoraan tukiasemaan. WiFi-Mesh-verkossa päätelaitteet muodostavat yhteyden tukiasemaan (portaali) tarvittaessa toistensa kautta.



Kuvio 6: WiFi ja WiFi-Mesh verkkojen topologiat

Silmukkaverkkotekniikka on varsin uusi tulokas tietoverkkojen joukossa, mutta tekniikka yleistyy nopeasti monella rintamalla sen tarjoamien uusien mahdollisuuksien ansiosta. Tällä hetkellä yleisimmät silmukkaverkkojen sovellukset ovat lukuisat erityyppiset sensoriverkot ja One Laptop Per Child projekti, jonka XO-tietokoneet verkottuvat keskenään käyttäen 802.11s standardiluonnokseen perustuvaa verkkotekniikkaa (*One Laptop Per Child 2009*).

Standardin 802.11s mukaisella silmukkaverkolla toteutettuna kenttäverkko koostuu kahdesta laitteesta. Työmaan keskusyksiköstä, joka yhdistää kenttäverkon ja palvelinjärjestelmän, sekä hallitsee kenttäverkkoa. Verkon toinen komponentti on langattomaan verkkoon liittymisen mahdollistavalla moduulilla varustettu mittalaite, johon mitta-anturit kytkeytyvät ja joka toimii silmukkaverkon solmuna (Kuvio 7). Solmut sijoitetaan kohteeseen siten, että jokainen laite pystyy yhdistymään vähintään kahteen toiseen laitteeseen. Tällöin verkon toiminta varmistetaan, vaikka jokin yhteys katkeaisikin esimerkiksi fyysisen esteen johdosta.



Kuvio 7: Käyttötapaus UC2 WiFi-Mesh-tekniikalla toteutettuna

Teoria

Jotta voitaisiin ymmärtää, miten IEEE 802.11s standardin mukainen silmukkaverkko toimii, ensin on tutustuttava hieman alkuperäisen IEEE 802.11 suosituksen mukaisen WiFi-verkon toimintalogiikkaan. Kuten kaikki IEEE 802.x tekniikat myös WiFi-tekniikat toimivat OSI-mallin ensimmäisellä ja toisella kerroksella, joten ne toimivat käytännössä näkymättömästi ylemmän tason protokollien, kuten TCP/IP ja sen muodostaman loogisen topologian kannalta.

IEEE 802.11

Alkuperäisen 802.11 standardin määrittämää topologiaa noudattavat tekniikat mahdollistavat kolme eri tapaa muodostaa tietoverkko (Service Set) päätelaitteiden (STAtion) välille. Vähemmälle käytölle on jäänyt Ad-Hoc-topologia eli IBSS (Independent Basic Service Set), jossa päätelaitteet muodostavat suoraan yhteyden toisiinsa. IBSS-verkossa ei ole reititysominaisuuksia, joten kukin päätelaite voi olla yhteydessä vain suoraan toiseen laitteeseen. (*IEEE 802.11 2007, 25.*)

Toinen tapa muodostaa langaton tietoverkko on käyttää verkossa tukiasemaa (Access Point), johon päätelaitteet liittyvät ja viestivät keskenään tukiaseman kautta. Perusmuodossaan ns. BSS (Basic Service Set) verkko mahdollistaa vain päätelaitteiden välisen kommunikoinnin. (*IEEE 802.11 2007, 24.*)

Ylivoimaisesti yleisin verkkomalli on kuitenkin ESS (Extended Service Set). Siinä BBS-verkkoon lisätään yhdyskäytävä (Portal), jonka avulla useita langattomia verkkoja voidaan yhdistää samaan runkoverkkoon (DS Distribution System). Tällöin voidaan laajentaa langattoman verkon peittoa ja tarvittaessa reitittää data eteenpäin esim. internettiin. Käytännössä yhdyskäytävä on aina rakennettu tukiaseman yhteyteen. (*Granlund 2001, 230-233.*)

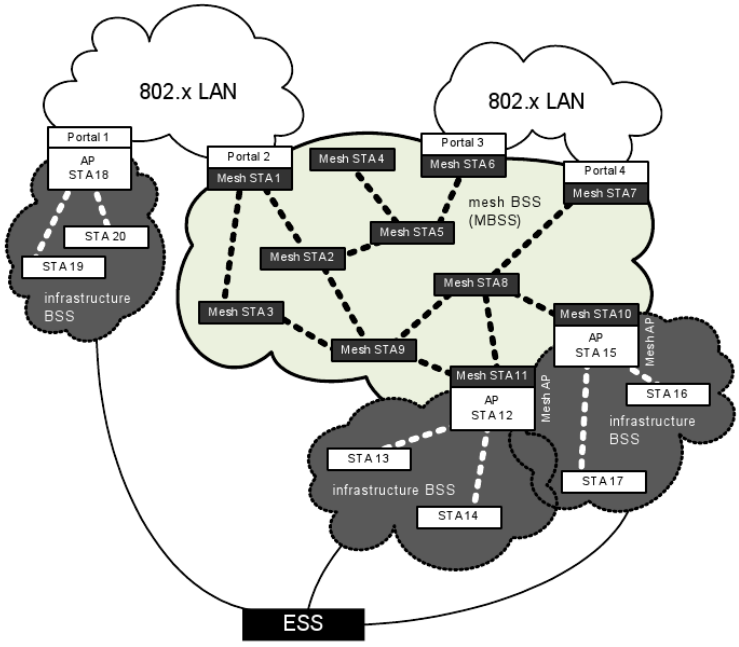
Verkon yksinkertaisen rakenteen ansiosta BSS:n jäsenten välinen liikenne ohjautuu samaan tapaan, kun Ethernet-kytkimissä. Tukiasema kerää MAC-tauluun tiedon tukiasemaan liittyneistä päätelaitteista. Taulun avulla osataan lähettää data eteenpäin joko takaisin radiotielle tai eteenpäin runkoverkkoon. (*Puska 2005, 140.*)

IEEE 802.11s

Koska vuodesta 2003 kehitetty 802.11s standardi on tällä hetkellä vielä luonnosvaiheessa eikä virallisen version valmistumisajankohdasta ole varmaa tietoa, on mahdollista, että tekniikkaan tulee vielä muutoksia. Todennäköisesti luonnos on kuitenkin oleellisimmilta osiltaan jo lopullisessa muodossaan, sillä useat laitevalmistajat ovat jo valmistaneet standardiluonnoksen pohjalta 802.11s-verkon laitteita ja One Laptop Per Child-projekti on käyttänyt standardiin perustuvaa verkkotekniikkaa laitteissaan jo vuosien ajan (*One Laptop Per Child 2009*).

Silmukkaverkon topologia poikkeaa merkittävästi perinteisestä ratkaisusta, sillä verkossa ei ole yhtä solmupisteenä toimivaa tukiasemaa, vaan jokainen päätelaite toimii myös tukiasemana muiden toimiensa ohella. 802.11s-verkon topologiassa ei mainitakaan erikseen tukiasemia, vaan lähtökohtaisesti kaikki verkon laitteet ovat päätelaitteita (Mesh STA), joihin saattaa olla yhdistettynä myös esimerkiksi yhdyskäytävä (Portal) tai perinteisen 802.11-verkon tukiasematoiminnallisuus. (*IEEE 802.11s 2009, 28.*)

Silmukkatekniikalla muodostetusta verkosta käytetään nimitystä MBSS (Mesh Basic Service Set). Kuten standardiluonnoksesta lainattu kuva (Kuvio 8) tuo esille, silmukkaverkko on suunniteltu myös osittain korvaamaan ja jatkamaan DS runkoverkkoa.



Kuvio 8: MBSS-verkko jossa yhdistetty useita verkkotyyppejä. (IEEE 802.11s 2009, 28.)

Silmukkaverkon toiminnan tekee mahdolliseksi uudenlainen OSI-mallin linkkikerroksella toimiva reititysprotokolla, joka pystyy päättelemään parhaan reitin kahden päätelaitteen tai päätelaitteen ja portaalin välille. Hybrid Wireless Mesh Protocol (HWMP) on 802.11s-standardia varten kehitetty etäisyysvektoriprotokolla, jonka toiminta perustuu L2-tasolle siirrettyyn Ad Hoc On Demand Distance Vector (AODV) protokollaan. Yksinkertaistettuna AODV toimii kuten lähiverkkojen reitittimistä tutut RIP ja IGMP-reititysprotokollat, etsien lyhimmän reitin kahden pisteen välille etäisyysvektoreiden avulla. HWMP:n tapauksessa reititys ei kuitenkaan tapahdu verkkokerroksessa (L3) IP-osoitteiden avulla vaan linkkikerroksella (L2) hyödyntäen MAC-osoitteita. (*IEEE 802.11s 2009.*)

Luotettavuus

Vaikka silmukkaverkkojen yksi suurimmista eduista on verkon silmukoinnin tuoma luotettavuus, on luonnosasteella olevan IEEE 802.11s-tekniikan luotettavuutta vaikea arvioida. Muutamat laitevalmistajat tarjoavat jo standardiin pohjautuvia laitteita, mutta dokumentoituja käyttöönottoja, joiden pohjalta arvioida tekniikan luotettavuutta ei juurikaan ole. Taulukossa 16 tutkitaan tarkemmin WiFi-Mesh tekniikan ominaisuuksia luotettavuuden valossa.

Taulukko 16: SWOT analyysi WiFi-Mesh-tekniikan luotettavuudesta

Strenghts – Vahvuudet Vähän mekaanisesti vaurioituvia osia Silmukkaverkko hyvin vikasietoinen	**Weaknesses – Heikkoudet** Radiotien häiriöt vaikea havaita Tekniikka ei vielä valmista
Oppoturnities – Mahdollisuudet Automaattisesti korjautuva silmukkaverkko	**Threats – Uhat** Radiotien häirintä helppoa

WiFi-Mesh tekniikka mahdollistaa teoriassa luotettavan verkon rakentamisen, kunhan laitevalmistajat aloittavat tekniikkaan perustuvien laitteiden valmistuksen. Tekniikan ongelmana on kuitenkin radiotekniikka, jonka häiriönsietokyky on melko rajallista. Paras luotettavuus WiFi-mesh tekniikalla saavutetaan kiinteästi asennettuna, jolloin radiotien olosuhteet pysyvät melko vakioina. Tekniikan luotettavuus saa pistearvon 0.

Kustannukset

WiFi-Mesh verkon kustannuksissa arvioitavien komponenttien määrä on varsin vähäinen, sillä ainoat tarvittavat osat ovat mittalaitteiden yhteyteen asennettavat WiFi-moduulit, sekä hieman edistyneempi portal-moduuli työmaan keskuksen yhteydessä. Taulukosta 17 selviää niiden arvioitu kustannusvaikutus.

Taulukko 17: WiFi-Mesh tekniikan kustannusvaikutus käyttötapauksessa UC2

Osa		**Tarve**	**Kustannus**	**Yhteensä**
Radiomoduuli	Mini G OEM	7	60.00 €	420.00 €
Portal moduuli		1	80.00 €	80.00 €
				500.00 €

Yhteensopivuus

Koska arvioitava silmukkaverkkotekniikka perustuu suoraan standardiluonnokseen, on tekniikka yhteensopivuuden kannalta varsin otollisessa asemassa. Vaikka toistaiseksi harvat järjestelmätoimittajat tukevat standardia, on perusteltua odottaa tekniikan muodostuvan verrattain suosituksi sen ratkaisemien teknisten ongelmien ja käytetyn edullisen laitteiston ansiosta.

Eräs merkittävimmistä 802.11s standardia käyttöön ottoa edistävistä tahoista on open80211s.org, joka on mm. Nortel Networksin ja Googlen tukema avoimen lähdekoodin hanke kehittää 802.11s-standardia toteuttava ohjelmistoratkaisu käytössä olevalle

802.11 laitteistolle. Tällä hetkellä projektin tuottamat ajurit ovat jo testattavissa, mutta kaikkea toiminnallisuutta, kuten standardin määrittelemiä salaus- ja tunnistustoiminnallisuutta, ei ole vielä implementoitu. (*open80211s.org 2009.*)

Teknisesti 802.11s-standardin kanssa yhteensopivia ovat lähes kaikki perinteistä 802.11-tekniikkaa varten kehitetyt langattomat päätelaitteet, kunhan laitteiden ohjelmisto päivitetään uudelle standardille. Tästä syystä tarjolla on monipuolisesti erilaisiin olosuhteisiin soveltuvia, toimivia ja vaatimukset täyttäviä laitteita. Varsinaisesti 802.11s-standardin mukaisia päätelaite- tai kokonaisjärjestelmätoimittajia ei toistaiseksi markkinoilla ole, vaikkakin monet alan yritykset tiettävästi kehittävät omia ratkaisujaan. Yhteensopivuus pisteytetään oheisessa taulukossa 18.

Taulukko 18: WiFi-Mesh-tekniikan yhteensopivuus

Yhteensopivuus	**Pisteet**	**Max pisteet**
Standardi	2	2.5
Avoin SW API	1	2.5
Useita HW toimittajia	2.5	2.5
Komponentit CE-merkittyjä	2.5	2.5
	8	**10**

Turvallisuus

IEEE 802.11s-standardin kehityksessä on ansiokkaasti otettu opiksi aikaisempien 802.11-tekniikoiden puutteista. Standardiluonnoksessa määritellään valmiiksi tekniikat vahvaan tunnistukseen, liikenteen salaamiseen. Standardissa on varauduttu myös man-in-the-middle ja replay-hyökkäyksiin. Salaus- ja tunnistusominaisuudet perustuvat WPA2-tekniikkaan (802.11i), jonka avulla solmupisteiden väliset yhteydet suojataan. Verkkoon pyrkivien laitteiden tunnistamiseen voidaan käyttää myös 802.1x-tekniikkaa, jolloin verkkoon tarvitaan RADIUS- (Remote Authentication Dial In User Service) tai TACACS-palvelin (Terminal Access Controller Access-Control System) hallitsemaan tunnistustietoja. Yhteenveto WiFi-Mesh tekniikan turvallisuuden arvioinnista taulukossa 19. (*IEEE 802.11s 2009, 88-95.*)

RADIUS-palvelin mahdollistaa varsin luotettavan päätelaitteiden ja pääsyn keskitetyn hallinnan kun työmaan keskusyksikköön asennetaan palvelinjärjestelmästä itsensä repli-

koiva RADIUS-palvelinohjelmisto. RADIUS-palvelimen avulla myös kaikki autentikointitapahtumat tallentuvat palvelinjärjestelmän lokitietoihin.

Taulukko 19: WiFi-Mesh-tekniikan turvallisuus

Turvallisuus	Pisteet	Max pisteet
Luotettava tunnistus	2	2
Eheydenvarmistus	1	2
Salaus	2	2
Testattu	0	2
Haavoittuvuudet	1	2
	6	**10**

Mittapisteiden määrä ja maasto

IEEE 802.11s-standardi on suunniteltu pieniä ja keskisuuria verkkoja (alle 32 solmupistettä) varten, mutta teknisesti myös suurempi solmumäärä on mahdollista. Solmumäärän kasvaessa ongelmaksi nousee tarvittavien hyppyjen määrä (viive) ja radiotien ruuhkautuminen. Ongelmia voidaan kiertää esimerkiksi rakentamalla 802.11s-tekniikalla runkoverkko, jonka solmupisteet toimivat tukiasemana perinteistä 802.11-tekniikkaa käyttäville mittalaitteille. Toinen vaihtoehto on jakaa kenttäverkko pienempiin osiin, jotka yhdistetään toisiinsa siltoina verkkojen välillä toimivin portaaliasemin. Molemmat toteutustavat tekevät verkon suunnittelusta ja käytännön toteutuksesta huomattavan monimutkaista. (*Yan, Jijun & Honglin 2006, 407.*)

Verkon nopeuden suhteen 802.11s-tekniikka on vähintäänkin riittävä, sillä verkossa voidaan käyttää vähintään 802.11a- ja 802.11g-tekniikoiden mahdollistamaa 56Mb/s nopeutta, mahdollisesti jossain vaiheessa myös 802.11n-tekniikan 600Mb/s nopeutta.

Soveltuvuutta työmaan maastoon on melko vaikea arvioida ilman kunnollista kenttätestausta, mutta verrattaessa esimerkiksi Ethernet-tekniikkaan silmukkaverkko sietää muuttuvia olosuhteita merkittävästi paremmin ja verkon komponentit on helpompi suojata mekaanisilta rasitteilta. Vaikka 2.4GHz tai 5GHz taajuusalueella toimiva radiosignaali vaimeneekin kovin herkästi esimerkiksi teräsbetoniseinissä, silmukointi parantaa verkon toimintaedellytyksiä merkittävästi. WiFi-Mesh tekniikan soveltuvuuden pisteytys taulukossa 20.

Taulukko 20: WiFi-Mesh-tekniikan soveltuminen mitapisteiden määrään ja maastoon

Mittapisteiden määrä ja maasto	Pisteet	Max pisteet
300 päätelaitetta mahdollinen	1	5
Minimisuorituskyky	2.5	2.5
Soveltuu esteiseen maastoon	2.5	2.5
	6	**10**

Mekaaniset ja sähköiset vaatimukset

Koska varsinaisesti 802.11s-standardia varten suunniteltuja päätelaitteita ei vielä markkinoilta löydy, on laitteiden fyysisiä ominaisuuksia arvioitava markkinoilta löytyvien 802.11-laitteiden perusteella. Koska molemmat tekniikat käyttävät samaa radiotekniikkaa, on perusteltua olettaa, että useisiin laitteisiin tulee saataville 802.11s-standardin mukaisen toiminnan mahdollistavat ajurit. WiFi-Mesh-tekniikalla toteutetun verkon sähköisten ominaisuuksien arviointi taulukossa 21.

Sähköisiin häiriöihin 802.11s-tekniikassa on varauduttu mahdollistamalla kanavan uudelleenneuvottelu (vaihto), mutta automaattisesti tämä toimii ainoastaan ruuhkautuneen kanavan tunnistamiseen. Kanavaa häiritsevää muuta signaalilähdettä ei kyetä tunnistamaan (*IEEE 802.11s 2009, 136*). Häiriöiden tunnistaminen on merkittävä puute, sillä yleisimmin käytetty 2.4 GHz taajuusalue on erittäin käytetty mitä moninaisimmissa sovelluksissa. Samalle taajuusalueelle saattavat tuottaa häiriöitä mm. mikroaaltouunit ja loisteputkivalaisimet. Pieni helpotus radiotien ruuhkautumiseen saadaan käyttämällä 802.11a-standardin mukaista 5 GHz taajuusaluetta, jolla liikennettä on vähemmän. Korkeamman taajuuden ansiosta radiosignaalin läpäisykyky kuitenkin heikkenee. (*Cisco Systems Inc 2007.*)

Koska järjestelmässä voidaan käyttää olemassa olevan 802.11-standardien mukaisia komponentteja on tarjolla hyvä valikoima valmiiksi CE-hyväksyttyjä laitteita. Tavoitteena on hyödyntää valmista laitetta, jolloin valmistajan vastuu laitteen vaatimustenmukaisuudesta on laitteen todellisella valmistajalla, eikä siirry soveltajalle.

802.11-tekniikkaan perustuvia verkkoja on sovellettu hyvin erilaisissa olosuhteissa mm. videovalvonnan runkoverkkona ja yleisten tilojen avoimina ja suljettuina lähiverkkoina.

Perustekniikka on osoittanut olevansa erittäin sopeutumiskykyinen. Merkittävimmät tekijät haastavissa ympäristöissä ovat laitteiden fyysinen suojaus, käyttöenergian turvaaminen ja käyttäjien tunnistaminen. Tekniikan sähköisten ominaisuuksien pisteytys taulukossa 21.

Taulukko 21: WiFi-Mesh-tekniikan sähköisten ominaisuuksien pisteytys

Mekaaninen	**Pisteet**	**Max pisteet**
Sähköiset häiriöt	2	3.33
EMC-vaatimustenmukaisuus	3.33	3.33
Onnistuneita sovelluksia	1	3.33
	6	**10**

Mukautuminen

Verrattaessa vanhempiin 802.11-standardeihin uusi silmukkaverkko tuo merkittäviä parannuksia nimenomaan verkon mukautumiskykyyn mahdollistamalla ainakin jollain tasolla ”drop in networking”-toiminnan. Siinä varsinaista verkko infrastruktuuria ei tarvitse erikseen rakentaa, vaan laitteet neuvottelevat keskenään yhteydet, jotka muodostavat kokonaisuuden ilman asentajan toimia.

Jotta kuvaillun kaltainen toiminta voidaan saavuttaa luotettavasti täytyy laitteiden käytännössä olla akkukäyttöisiä. Tässä kohdataankin 802.11-tekniikan heikkous, sillä tekniikkaa ei ole suunniteltu akkukäyttöiseksi. Vaikka 802.11s-standardi sisältää energiansäästöominaisuuksia, ei energiatehokkuudessa päästä alusta asti akkukäyttöön suunniteltujen laitteiden tehokkuuteen. (*IEEE 802.11s 2009, 180.*)

Eräs merkittävimmistä uuden standardin mukanaan tuomista uudistuksista on HWMP-protokolla, joka mahdollistaa verkon topologian automaattisen hallinnan. Kunhan verkon laitteita asennettaessa varmistetaan, että jokainen solmupiste saa yhteyden vähintään kahteen toiseen, toimii verkon reititys automaattisesti myös useimmissa ongelmatilanteissa.

Verkon tilan seurantaa varten pitää rakentaa oma ohjelmisto, mutta ainakin open80211s.org projekti tarjoaa perustyökalut, joiden avulla verkon tietoja saa tarkastel-

tua. Kattavampia valmiita ratkaisuja tulee todennäköisesti saataville standardin yleistyessä. Tekniikan mukautumiskyvyn pisteytys taulukossa 21.

Taulukko 22: WiFi-Mesh-tekniikan mukautumiskyky

Mukautuminen	Pisteet	Max pisteet
Langattomuus	2.5	2.5
Automaattinen reititys	2.5	2.5
Tiladiagnostiikka	2.5	2.5
Akkukäyttö	0.5	2.5
	8	**10**

4.1.3 ZigBee

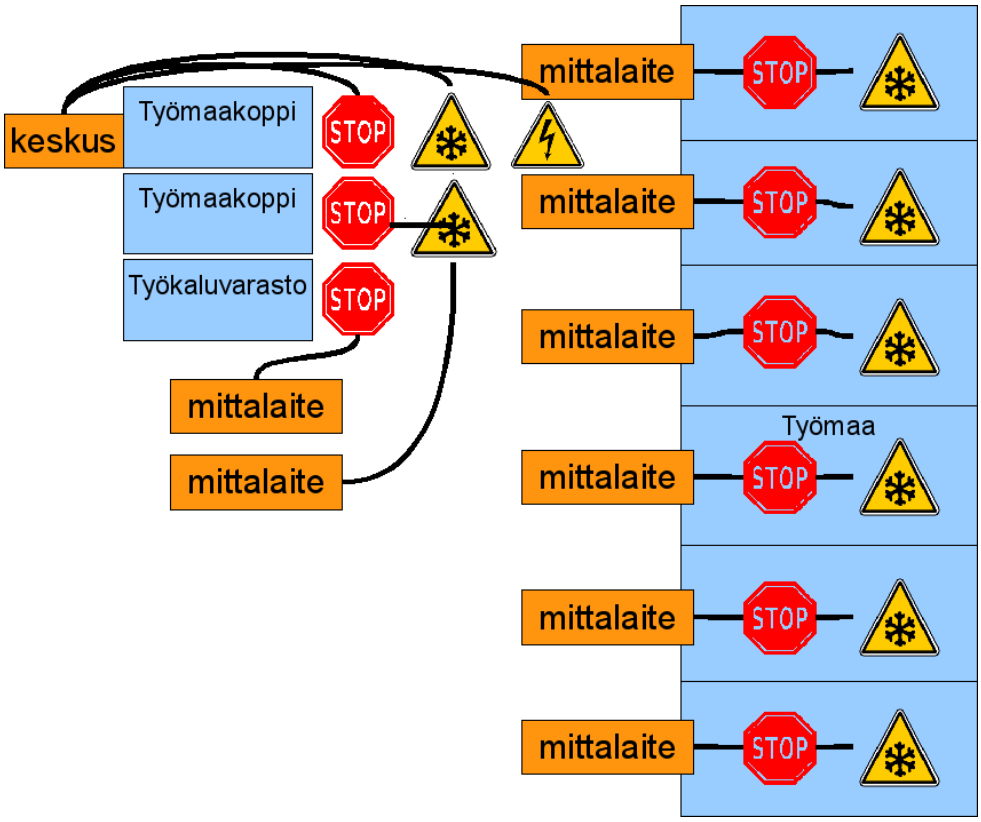
ZigBee lienee tässä dokumentissa esiteltävistä tekniikoista vierain perinteisiin tietoverkkoihin perehtyneille. Tekniikka on varsin uusi tulokas langattomien verkkotekniikoiden kentällä, eikä yleensä paini samassa sarjassa lähiverkkotekniikoiden kanssa. ZigBee tekniikan kehitystä hallinnoi ZigBee Alliance, joka on useiden tietoliikennealan yritysten perustama yhteisö tehtävänään kehittää IEEE 802.15.4-standardin mukaisen radiotekniikan pohjalta yhtenäistä määrittelyä lyhyen kantaman langattomalle tietoverkolle. ZigBee määrittelyn lähtökohtana on ollut kehittää edullinen, energiatehokas ja luotettava verkkoratkaisu valvonta ja ohjaustarpeisiin. Niissä siirrettävät datamäärät ovat verrattain pieniä, mutta laitteiden on toimittava akkukäyttöisinä jopa vuosia.

ZigBee Alliance ei pyri kehittämään valmista universaalisti yhteensopivaa ratkaisua, kuten WiFi Alliance, vaan pikemminkin tuotealustan, josta on hyvä jatko kehittää valmis tuote. ZigBee Alliancen sertifiointiohjelma määritteleekin erikseen sertifiointitasot, jossa laite toimii muiden ZigBee-laitteiden kanssa ja tason, jossa laite ei häiritse muiden ZigBee-laitteiden toimintaa.

Vaikka vastaaviin tarpeisiin on tarjolla useita muita verkkoratkaisua, ZigBee on saavuttanut hyvän jalansijan markkinoilla. Useat valmistajat kehittävät uusia sovelluksia mm. teollisuuden ja maatalouden tarpeisiin. ZigBeen vahvuus kilpaileviin tekniikoihin nähden on 802.15.4-standardin mukainen radiotekniikka, jonka mukaisia radiomoduuleita

löytyy usealta valmistajalta huokeaan hintaan ja määrittelyn avoimuus. (*ZigBee Alliance 2009.*)

ZigBee-tekniikka mahdollistaa työmaan valvonnan lähestymisen uudesta näkökulmasta aiemmin esiteltyihin tekniikoihin nähden. Edullinen tekniikka ja hyvin skaalautuva aito silmukkaverkko mahdollistavat laajojenkin alueiden valvonnan ilman, että verkkoa tarvitsee juurikaan suunnitella. Verkko koostuu työmaan keskukseen sijoitetusta kontrollerista ja päätelaitteesta, joka sisältää oleellisimmat anturit, liitäntämahdollisuudet lisäantureille ja router-tilassa toimivan ZigBee moduulin. Verkkoa rakennettaessa asentajan on huolehdittava, että kukin päätelaite saa yhteyden vähintään kahteen toiseen päätelaitteeseen, jolloin saadaan aikaan toimintavarma, silmukoitu verkko. (Kuvio 9)

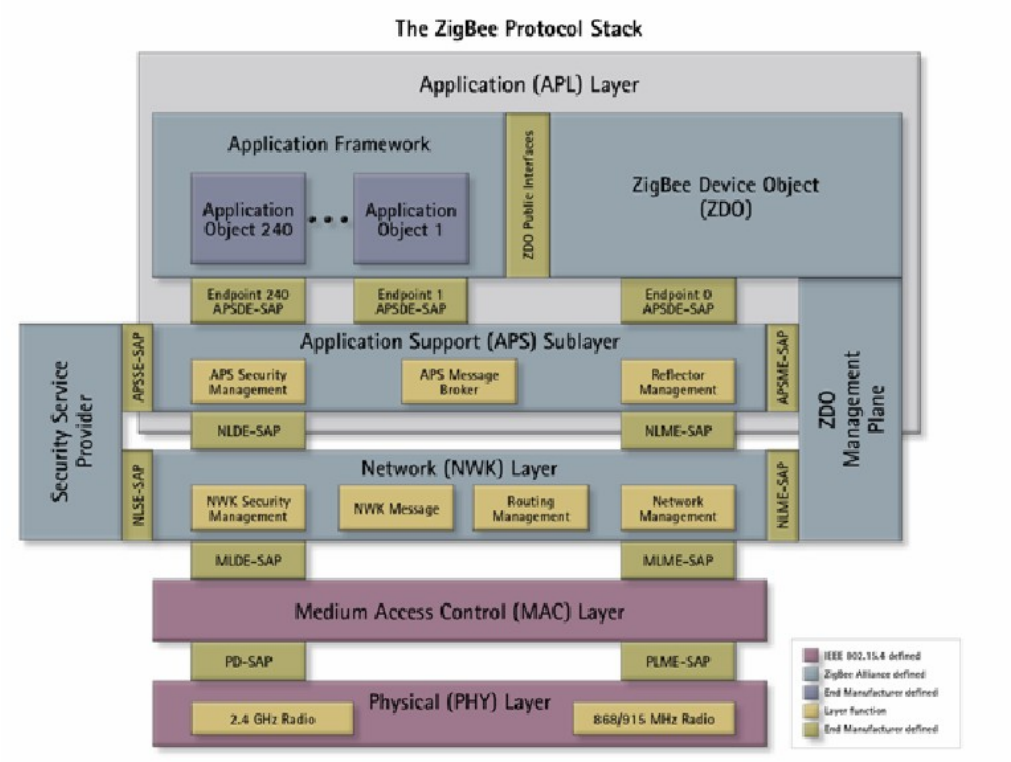


Kuvio 9: Käyttötapaus UC2 ZigBee-tekniikalla toteutettuna

Radiotiellä käytetään 868 MHz taajuusaluetta, joka on vähemmän käytetty, läpäisee paremmin esteitä ja kantaa kauemmas kuin 2,4 GHz taajuusalue. Verkkoratkaisun laitteet ja ZigBee ohjelmistopino hankitaan kokonaisuutena järjestelmätoimittajalta, joka varmistaa verkon toiminnan määritelmän mukaisesti.

Teoria

Koska ZigBee rakentuu IEEE 802.15.4-standardin päälle, on tarpeen ymmärtää molempien määrittelyjen sisältö ainakin oleellisimmilta osin, jotta ZigBee-tekniikalla toimivaa järjestelmää voidaan arvioida ja toisaalta jotta ymmärretään myös määrittelyn tarjoamat variointimahdollisuudet. Yksinkertainen rajanveto 802.15.4-standardin ja ZigBee Alliancen määrittelyn välille syntyy verrattaessa ZigBee protokollapinoa (Kuvio 10) OSI-malliin. IEEE:n standardi määrittelee ensimmäisen ja toisen tason toiminnan, eli fyysisen radiotien signaloinnin ja radiotien käytön periaatteet kuten vuoronvarausmetodin. ZigBee-määrittely kattaa loput verkkokerrokset aina kolmannen tason verkkokerroksesta sovelluskerrokseen asti tarjoten järjestelmälle turvallisuus- ja laitehallintarajapinnat, sekä sovelluskehyksen, jossa sovellukset eli profiilit toimivat.



Kuvio 10: ZigBee protokollapino (Daintree Networks Inc. 2008, 8.)

IEEE 802.15.4 on vuonna 2003 julkaistu standardi, joka määrittelee OSI-mallin mukaisen fyysisen- ja siirtokerroksen toiminnan lyhyen kantaman radioverkoille, jotka toimivat lisenssivapailla 868 MHz, 900 MHz (vain USA ja Australia) ja 2.4 GHz taajuusalueilla. 802.15.4 on suunniteltu ns. WPAN (Wireless Personal Area Network) sovelluk-

siin. Standardi mahdollistaa varsin monimuotoisten ratkaisujen toteuttamisen erilaisina taajuuden, topologian, laitetyypin ja siirtotien varausmenetelmän kombinaatioina. Myös standardiin nojaava ZigBee-määrittely mahdollistaa hyvin laajan sovelluskirjon. (*IEEE 802.15.4 2006.*)

Euroopassa standardin mukaisista taajuusalueista on mahdollista käyttää joko 868 MHz tai 2.4 GHz alueita. Näistä 2.4 GHz alue on jaettu 16 kanavaan, mutta 868 MHz alue sisältää vain yhden kanavan. Myös taajuusalueiden datanopeudessa on merkittävä ero, sillä 868 MHz taajuudella saavutetaan 20 kB/s nopeus ja 2.4 GHz taajuudella peräti 250 kB/s. Molemmilla taajuusalueilla radiotien häiriönsietokyky on varsin hyvä ilmarajapintana käytettävän DSSS (Direct Sequence Spread Spectrum) tekniikan ansiosta (*Silvola 2004, 15*). Nopeuden lisäksi merkittävä ero taajuusalueiden välille syntyy niiden kyvystä läpäistä rakenteita. Verrattaessa 868 MHz ja 2.4 GHz taajuuksien vaimentumaa rakennetussa ympäristössä huomataan 868 MHz taajuudella vaimentuman olevan jopa 9 dB pienempi 50 m matkalla, joten vastaava verkon kattavuus voidaan saavuttaa merkittävästi pienemmällä lähetysteholla (*ITU Model for Indoor Attenuation, Wikipedia 2009*).

IEEE 802.15.4 mahdollistaa perinteisen tähtitopologian, silmukkaverkon ja näiden yhdistelmän. Yhdistelmätopologiassa silmukkaverkon FFD (full-function device) päätelaitteet toimivat tukiasemina kevyemmille RFD (reduced-function device) laitteille, jotka eivät kykene toimimaan varsinaisessa silmukkaverkossa. FFD-laitteet toimivat verkon reitittiminä joten jokaisessa verkossa on oltava vähintään yksi FFD-laite. Yksi verkon FFD-laitteista pitää myös osoittaa koordinaattoriksi, joka ohjailee verkon toimintaan esimerkiksi lähettämällä majakkasignaalit koko verkkoon.

Eräs oleellisimmista energiansäästöön tähtäävistä ominaisuuksista 802.15.4-tekniikassa on majakkasignaaleihin (beacon) perustuva siirtotien varausmenetelmänä. Siinä laitteet tahdistavat lähetyksensä koordinaattorin lähettämän majakkasignaalin perusteella pyytämättä erillistä lähetyslupaa kuten esimerkiksi CSMA-CA (Carrier Sense Multiple Access – Collision Avoidance) tekniikkaa käyttävät 802.11-standardiperheen tekniikat. Niin haluttaessa 802.15.4-standardi mahdollistaa myös CSMA-CA tekniikan käytön vaihtoehtona majakkatekniikalle. (*IEEE 802.15.4 2006, 23.*)

ZigBee-määrittelyn alin kerros eli verkkokerros (NWK) huolehtii verkon osoitteista, reitityksistä, dataliikenteestä verkkoon, verkon hallinnasta ja tiettyjen turvallisuusominaisuuksien täytäntöönpanosta (*ZigBee Specification 2008, 259-260*). Reititys ZigBee-verkoissa toteutetaan AODV-protokollan avulla.

Sovellukset ZigBee ympäristössä tunnetaan profiileina, jotka määrittelevät sovelluksen rajapinnat. Käytännössä ZigBee-sovellusprofiilien toimintaa voidaan verrata esimerkiksi SNMP-protokollan (Simple Network Management Protocol) toimintaan, jossa kohteelta kysellään ja asetetaan parametreja. Profiilit voivat olla joko julkisia, jolloin esimerkiksi kaikki kiinteistöautomaatioratkaisuja kehittävät pystyvät luomaan yhteensopivia laitteita, tai valmistajakohtaisia, jolloin ei tähdätä yhteensopivuuteen muiden toimittajien kanssa.

ZigBee-määrittelyn turvallisuusominaisuudet perustuvat 128-bittiseen AES-algoritmiin (Advanced Encryption Standard), jonka avulla suojataan paitsi verkossa liikkuva data myös verkon ohjaustapahtumat, kuten verkkoon liittyminen. Huomattavaa ZigBee-verkon turvaominaisuuksissa on avaintenhallinnan keskitys kontrolleriin (tai muuhun tehtävään nimettyyn laitteeseen), joka mahdollistaa esimerkiksi avainten vaihdon määräajoin, mikäli tavoitellaan suurta turvallisuustasoa. (*Daintree Networks Inc 2008, 18.*)

Luotettavuus

Zigbee-tekniikassa on monia luotettavuutta edesauttavia tekijöitä ja tekniikka on suunniteltu aktiivisesti muuttuviin ympäristöihin, joten periaatteessa lähtökohdat luotettavaan verkkototeutukseen ovat hyvät. Luotettavuuden tasoon vaikuttaa kuitenkin muutama keskeinen valinta, kuten käytettävä taajuus. Käytettäessä 868 MHz taajuutta saadaan monia etuja kapasiteetin ja kanavavaihtoehtojen kustannuksella. SWOT-analyysi (Taulukko 23) paljastaa tarkemmin luotettavuuden osatekijät.

Taulukko 23: SWOT analyysi ZigBee-tekniikan luotettavuudesta

Strenghts – Vahvuudet Silmukkaverkko hyvin vikasietoinen Valmiit seurantatyökalut Vähän mekaanisesti vaurioituvia osia 868 Mhz taajuudella hyvä läpäisy ja kantavuus	**Weaknesses – Heikkoudet** Nuori tekniikka ei täysin vakiintunut Puolueetonta tietoa vähän saatavilla
Oppoturnities – Mahdollisuudet Itsekorjautuva silmukkaverkko	**Threats – Uhat** 868 Mhz taajuudella vain yksi kanava

ZigBee-tekniikalla toteutetun verkon luotettavuuden analysointi vahvisti tekniikan soveltuvan hyvin suunniteltuun käyttöön. Tekniikka on vielä melko nuori ja aidosti puolueettomia kokemuksia tekniikan käyttöönotosta ja luotettavuudesta on heikosti saatavilla. Vikasietoisen verkon ja valmiiden hallinta- ja analyysityökalujen ansiosta taulukon pisteluvuksi tulee +2 pistettä.

Kustannukset

Kuten WiFi-Mesh tekniikassa, myös ZigBee verkon yksinkertainen rakenne karsii tarvittavaa komponenttimäärää, mutta ZigBee-tekniikan kustannustehokkuus pääsee oikeuksiinsa tiputtaessaan kustannukset lähes puoleen WiFi-tekniikan kustannuksista. Kustannuserittely löytyy taulukosta 24.

Taulukko 24: ZigBee-tekniikan kustannusvaikutukset käyttötapauksessa UC2

Osa		**Tarve**	**Kustannus**	**Yhteensä**
Radiomoduuli	JN5148	9	24.48 €	220.32 €
Controller moduuli		1	40.00 €	40.00 €
				260.32 €

Yhteensopivuus

Yhteensopivuuden ja standardoinnin osalta ZigBee-tekniikka poikkeaa aiemmin arvioiduista vahvasti standardoiduista tekniikoista, joissa eri valmistajien ratkaisut toimivat samassa verkossa lähes täydellä varmuudella. Vaikka ZigBee-protokollapino (ml. IEEE 802.15.4) määrittelee käytettävän tekniikan varsin tarkasti varsinkin radiotien käytön osalta, jättää se järjestelmätoimittajille reilusti liikkumavaraa kehittää juuri omiin tarpeisiin soveltuvia ratkaisuja tarvittaessa yhteensopivuuden kustannuksella.

ZigBee-määrittely on periaatteessa avoin ja kaikkien saatavilla. Kaupallinen käyttö kuitenkin edellyttää ZigBee Allianceen liittymistä ja laitteen sertifiointia suositellaan. Sertifiointi edellyttää laitteen määrittelynmukaisuuden varmentamista ZigBee Alliancen hyväksymän testausorganisaation toimesta. Sertifiointi osoittaa laitteen olevan teknisesti yhteensopiva muiden ZigBee laitteiden kanssa. Yhteensopivuuden kannalta on kuitenkin tärkeää huomata, että järjestelmätoimittajan kehittämät profiilit eivät välttämättä ole standardoituja, vaan ne voivat olla ns. yksityisiä profiileja (*ZigBee Alliance 2009*). Hankittaessa ZigBee-järjestelmää on siis järkevää varmistaa, että toimittajan kehittämät profiilit ovat joko avoimesti lisensoituja tai toimittaja luovuttaa tarvittavat määrittelyt joko toimituksen yhteydessä tai escrow-sopimuksella. Näin varmistetaan, että tarvittaessa järjestelmässä voidaan käyttää myös muiden järjestelmätoimittajien kehittämiä komponentteja.

Koska ohjelmistorajapinta, jolla ZigBee-verkko liittyy muihin verkkoihin ja jolla ZigBee-verkkoa hallitaan, ei sisälly ZigBee määrittelyyn, riippuu rajapinnan tyyppi ja avoimuus järjestelmätoimittajasta. Järjestelmän hankinnan yhteydessä on syytä varmistaa tarjoaako järjestelmätoimittaja rajapinnan esimerkiksi valmiina apuohjelmina, sarjaportin kautta AT-komennoin vai ohjelmistokirjastona. Parhaassa tapauksessa toimitukseen sisältyvät valmiit apuohjelmat lähdekoodeineen ja hyvin dokumentoidut ohjelmistokirjastot vapaasti lisensoituina.

Tätä kirjoitettaessa ZigBee Alliance ilmoittaa sertifioineensa 41 ZigBee tuotealustaa, joille ratkaisuja kehittää 165 yritystä. ZigBee-määrittelyn mukaisten komponenttien saatavuutta voidaan pitää turvattuna, kunhan edellä mainitut lisensointi/määrittelyasiat huomioimalla varmistetaan profiilien ja rajapintojen yhteensopivuus. (*ZigBee Alliance 2009.*)

Laajan tuotealusta ja ZigBee-moduulitarjonnan ansioista useilta järjestelmätoimittajilta löytyy valmiiksi CE-merkinnän vaatimukset täyttäviä tuotteita, joten myös järjestelmän vaatimustenmukaisuus on helppo saavuttaa tällä tekniikalla. Tekniikan yhteensopivuusvaatimusten pisteytys on kirjattu taulukkoon 25.

Taulukko 25: ZigBee-tekniikan yhteensopivuus

Yhteensopivuus	Pisteet	Max pisteet
Standardi	2.5	2.5
Avoin SW API	1.5	2.5
Useita HW toimittajia	2.5	2.5
Komponentit CE-merkittyjä	2.5	2.5
	9	**10**

Turvallisuus

Turvallisuusnäkökohdat on huomioitu ZigBee-määrittelyssä kiitettävästi ja turvallisuuden tasoa pystyy mukauttamaan kohteen vaatimustason mukaan, sillä lisätty turvallisuus vääjäämättä vaatii uhrauksia esimerkiksi muistin kulutuksessa, akkukestossa tai ylläpidettävyydessä. IEEE 802.15.4-standardi määrittelee tärkeimmät turvallisuuden työkalut, kuten radiotiellä käytettävän AES 128-salauksen, jonka ZigBee-määrittely ottaa käyttöön mahdollistamalla mm. keskitetyn avaintenhallinnan ja datan eheyden varmistuksen laajentamalla salauksen linkkien välisestä koko reitille. (*Reddy 2006.*)

Päätelaitteiden luotettava tunnistus toteutetaan salausavaimin. Verkkoon liitettävään uuteen laitteeseen asetetaan verkon senhetkinen salausavain, jonka perusteella verkon koordinaattori hyväksyy laitteen verkon jäseneksi. Palvelinjärjestelmään ja työmaan keskukseen pitää kehittää järjestelmä avainten hallintaan, jotta verkon avain voidaan ohjelmoida laitteeseen ennen laitteen lähettämistä työmaalle.

Verkossa siirrettävän datan eheys varmistetaan ZigBee-määrittelyn turvallisuusominaisuuksien mukaisesti siten, että datan lähettävä laite allekirjoittaa datan ns. MIC-koodilla (Message Integrity Code). Se sisältää datan tarkistussumman ja laitteen tunnisteen. Mikäli data on muuttunut alkuperäisestä se hylätään. (*Cragie 2009.*)

Kaikki verkon radiotiet on salattu käyttäen 128-bittistä AES-algoritmia, jota voidaan pitää varsin turvallisena. Ainoa toistaiseksi tunnettu murtometodi on ns. brute force, jossa yritetään kaikkia mahdollisia kombinaatioita, eli 2^128 kombinaatiota (*Advanced Encryption Standard, Wikipedia 2009*). Vaikka todennäköisyys brute force-hyökkäykseen ja sen onnistumiseen on häviävän pieni, vaihdetaan koko verkon salausavaimet säännöllisin väliajoin. Toinen mahdollinen hyökkäysvektori on, että varastetusta pääte-

laitteesta urkitaan salausavain esimerkiksi analysoimalla radiopiirin ja mikrokontrollerin välistä dataa, kuten tietoturvatutkija Travis Goodspeed esittelee blogikirjoituksessaan Breaking 802.15.4 AES 128 Encryption by Syringe (*Goodspeed 2009*). Fyysiseen hyökkäysvektoriin on mahdollista varautua myös valitsemalla integroitu moduulityyppi, jossa dataa ei siirretä salaamattomana piiriltä toiselle.

ZigBee-tekniikka on ollut käytössä vuodesta 2004 ja sen avulla on toteutettu lukematon määrä hyvin erilaisia järjestelmiä mm. taloautomaation ja energiankäytön hallintaan, sekä rikosilmoitinkäyttöön (*Telegesis Ltd 2009*). ZigBee Alliancen oman sertifiointiohjelman edellyttämä testausprosessi on varsin kattava, varmistaen osaltaan tuotteiden toimivuuden.

ZigBee ja 802.15.4-tekniikoiden yleistymisen myötä myös mielenkiinto niiden turvallisuuden tutkimiseen on herännyt tietoturvapiireissä. Yhdysvaltalainen tietoturvatutkija Travis Goodspeed on onnistunut paikallistamaan tietyistä ZigBee-pinon toteutuksista ylivuotohaavoittuvuuksia ja 802.15.4-laitteista muistiliikenteen kuuntelun mahdollistavia suunnitteluvirheitä (*Goodspeed 2009*). Varmaa on, että tulevaisuudessa haavoittuvuuksia tullaan löytämään lisää ZigBee ratkaisujen yleistyessä. Tärkein tapa suojautua tulevilta haavoittuvuuksilta on varmistaa ZigBee pinon toimittajan turvallisuuskulttuuri, jotta ainakin huolimattomuusvirheiltä vältytään ja varmistetaan, että haavoittuvuuksien löydyttyä niihin saadaan korjaukset mahdollisimman nopeasti.

Taulukkoon 26 on kerätty ZigBee-tekniikan tuvallisuusominaisuuksien pisteytys.

Taulukko 26: ZigBee-tekniikan turvallisuus

Turvallisuus	**Pisteet**	**Max pisteet**
Luotettava tunnistus	2	2
Eheydenvarmistus	2	2
Salaus	2	2
Testattu	2	2
Haavoittuvuudet	2	2
	10	**10**

Mittapisteiden määrä ja maasto

Koska ZigBee tekniikka on suunniteltu suuret anturiverkkokokonaisuudet huomioiden, on verkon teoreettinen maksimikoko jopa yli 64000 päätelaitetta (*ZigBee Alliance 2009*). Vaikka käytännön kokoraja jää huomattavasti alhaisemmaksi, ei tässä sovelluksessa edellytetty 300 päätelaitteen enimmäismäärä tuota ongelmia.

Käytettäessä 868 MHz taajuutta on tekniikan maksiminopeus 20 kB/s eli määritelty vähimmäissuorituskyky saavutetaan. Vaihtamalla ZigBee-moduuli 2,4 Ghz taajuusalueella toimivaksi saavutetaan 250 kB/s nopeus mikäli suurempaa suorituskykyä kaivataan syystä tai toisesta tulevaisuudessa.

Tässä vertailtavista tekniikoista ZigBee soveltuu rakennustyömaan esteiseen ja muuttuvaan ympäristöön ylivoimaisesti parhaiten, sillä 802.11s-tekniikasta poiketen ZigBee mahdollistaa aidon langattoman silmukkaverkon, joka pystyy akkukäyttöisenä toimimaan riippumattomana työmaan sähköjärjestelmästä. Silmukkaverkko pystyy mukautumaan ympäristön muutoksiin etsimällä uuden reitin, mikäli jokin linkkijänne katkeaa esimerkiksi väliin rakennetun seinän ansiosta. Tekniikan soveltuminen käyttöympäristöön tarkemmin taulukossa 27.

Taulukko 27: ZigBee-tekniikan soveltuminen mitapisteiden määrään ja maastoon

Mittapisteiden määrä ja maasto	Pisteet	Max pisteet
300 päätelaitetta mahdollinen	5	5
Minimisuorituskyky	2.5	2.5
Soveltuu esteiseen maastoon	2.5	2.5
	10	**10**

Mekaaniset ja sähköiset vaatimukset

Lienee osittain 802.15.4- ja ZigBee-tekniikoiden verrattain nuoren iän ansiota, että 802.15.4-standardin suunnittelussa on huomioitu radioteiden ruuhkautuminen ja muut radiotien häiriöt varsin kattavasti. Tärkeimmät tavat, joilla 802.15.4-standardin mukaiset radiolaitteet pyrkivät vähentämään ja välttämään ruuhkautumisongelmia ovat DSSS-modulaatio (Direct Spread Spectrum Signal), FDMA-kanavointi, (Freqvency Division Multiple Access), CSMA-CA-kanavavarausmetodi ja metodit radiotien ruuhkaisuuden seuraamiseen. Edellämainitut tekniikat yhdistettynä melko vähän käytettyyn 868 MHz

taajuuden käyttöön antaa varsin lupaavat lähtökohdat sähköisiin häiriöihin varautumiselle ja niiden välttämiseen. (*ZigBee Alliance 2007, 6-9.*)

Kuten jo tekniikan yhteensopivuutta arvioitaessa tuli esille, useat valmistajat ovat kehittäneet valmiita CE-hyväksyttyjä moduuleja, joiden avulla voidaan verrattain helposti kehittää ZigBee järjestelmiä tarvitsematta itse kehittää radiolaitteita yms. elektroniikkaa. Suurin etu valmiin moduulin käytössä on varmuus siitä, että laite täyttää CE-merkinnän edellytykset tarvitsematta teettää kallista EMI-testausta (Electro Magnetic Interference).

Saatavilla olleiden tietojen perusteella ZigBee-tekniikkaa ei ole sovellettu aikaisemmin suoraan rakennustyömaakäyttöön, mutta tekniikalla on monitoroitu esimerkiksi talotekniikan toimintaa, teollisuudessa venttiilien toimintaa, merikonttien lämpötilaa, ajoneuvojen toimintaa ja kylmäsäilytystilojen lämpötilaa. Edellä mainittujen toteutusten valossa on perusteltua olettaa tekniikan taipuvan vastaaviin ympäristöihin. (*Telegesis Ltd 2009.*)

Tekniikan sähköisten ominaisuuksien pisteytys taulukossa 28.

Taulukko 28: ZigBee-tekniikan sähköisten ominaisuuksien pisteytys

Mekaaninen	**Pisteet**	**Max pisteet**
Sähköiset häiriöt	3.33	3.33
EMC-vaatimustenmukaisuus	3.33	3.33
Onnistuneita sovelluksia	3.33	3.33
	10	**10**

Mukautuminen

Mukautumiskykyä arvioitaessa ZigBee menestyy hyvin, sillä tekniikka on kehitetty myös tilapäisasennuksia silmällä pitäen (Taulukko 29). Verkon reititys AODV-protokollaa hyödyntäen mahdollistaa verkon muutokset ilman tarvetta muokata asetuksia, kunhan muutosten yhteydessä varmistetaan, että siirretty päätelaite saa yhteyden vähintään kahteen toiseen päätelaitteeseen.

Tekniikka mahdollistaa verkon tilan reaaliaikaisen seurannan ja katkosten yms. virhetilanteiden nopean havainnoinnin. Verkon diagnostiikkaominaisuudet ovat pitkälti kiinni järjestelmätoimittajasta ja käytettävästä ZigBee-protokollapinosta, mutta toimittajalta vaaditaan vähintään rajapinta, jonka avulla esimerkiksi päätelaitteen tippuminen verkosta havaitaan välittömästi. Diagnostiikkaominaisuuksia voidaan hyödyntää myös verkon asennusvaiheessa riittävän silmukoinnin havainnointiin. ZigBee verkossa voidaan käyttää myös kolmannen osapuolen valmistamaa analyysiohjelmaa, kuten Daintree Sensor Network Analysator, joka soveltuu erinomaisesti mm. vikatilanteiden analysointiin.

Taulukko 29: ZigBee-tekniikan mukautumiskyky

Mukautuminen	**Pisteet**	**Max pisteet**
Langattomuus	2.5	2.5
Automaattinen reititys	2.5	2.5
Tiladiagnostiikka	2.5	2.5
Akkukäyttö	2.5	2.5
	10	**10**

4.2 Siirtoyhteys

Vertailtavien siirtoyhteystekniikoiden valinnassa rajoittavin kriteeri oli selvästi verkon kattavuusvaatimus, joka karsi vertailtavien joukosta pois muutamia vain tietyillä alueilla saatavilla olevia yhteystyyppejä, kuten WiMax ja paikalliset WLAN-operaattorit. Vertailuun jäi kuitenkin kolme teknisesti hyvin poikkeavaa tekniikkaa, jotka kuitenkin pystyvät toimittamaan vastaavan palvelun.

Vertailtaviksi tekniikoiksi valittiin asiakkaan toiminttamaan Internet-yhteyteen tukeutuminen, Digitan @450-verkko ja GSM-verkon datapalvelut. Toisistaan merkittävästi poikkeavat tekniikat osoittautuivat arviointijärjestelmän kannalta haasteellisiksi, mutta teknologiariippumattomuus vaatimusmäärittelyssä mahdollisti tasapuolisen arvioinnin tekniikoiden välillä.

4.2.1 Olemassaoleva yhteys

Eräs varteenotettava vaihtoehto siirtoyhteyden toteutukseen on käyttää työmaalla ennestään olevaa kiinteää Internet-yhteyttä, mikäli sellainen työmaalle on järjestetty. Yleisin yhteystyyppi työmailla on ADSL-tekniikalla (Asymmetric Digital Subscriber Line) toteutettu yhteys, joka jaetaan työasemien kesken ADSL-reitittimen tekemän NAT-muunnoksen (Network Address Translation) avulla. Työmaan yhteys voi olla toteutettu myös muilla tekniikoilla, kuten WiMax, GSM tai WLAN.

Tämä toteutusmalli poikkeaa muista vertailtavista tekniikoista merkittävästi. Käytännössä yhteyden toteutustekniikalla ei ole merkitystä, vaan lähdetään olettamuksesta, että työmaalle on toimitettu Internet-yhteys, joka otetaan käyttöön liittämällä työmaan keskusyksikkö työmaan toimistokoppiin sijoitettuun verkkokytkimeen. Yhteyden toiminta on asiakkaan vastuulla.

Jotta asiakkaan toimittamaa verkkoyhteyttä voidaan käyttää toteutustekniikasta riippumatta, pitää työmaan keskuksen ja palvelinjärjestelmän välinen yhteys tunneloida siten, että työmaan keskus muodostaa tunnelin. Tällöin todennäköisesti vältytään mahdollisen NAT-muunnoksen ja palomuurien aiheuttamilta esteiltä ja ratkaistaan vaihtuvan IP-osoitteen aiheuttamat ongelmat.

Luotettavuus

Asiakkaan järjestämän yhteyden luotettavuuden arviointi on varsin haastavaa, sillä vaikka yleisin tekniikka on ADSL, ei arviointia voidata tehdä pelkästään sen varaan. Yhteyden käyttöaste voi myös vaihdella työmaan aikana ja mahdollisuus käyttäjävirheistä aiheutuviin häiriöihin kasvaa useiden käyttäessä samaan yhteyttä. Tarkemmin luotettavuuteen pureudutaan taulukossa 30.

Taulukko 30: SWOT analyysi olemassa olevan yhteyden luotettavuudesta

Strenghts – Vahvuudet Kaapeloidut yhteydet normaalisti luotettavia	**Weaknesses – Heikkoudet** Ei mahdollisuuksia hallita yhteyttä Ei oikeuksia hallita yhteyttä Riippuvuus sähkönjakelusta
Oppoturnities – Mahdollisuudet Vastuu yhteydestä asiakkaalla	**Threats – Uhat** Yhteyden tahallinen tai tahaton katkaisu helppoa Yhteys voi ruuhkaantua

Vaikka asiakkaan hankkima yhteys olisikin normaalissa työkäytössä riittävän luotettava, ovat valvonta ja mittaussovelluksen vaatimukset luotettavuuden suhteen aivan eri luokkaa. Yhteyskatkoksista aiheutuva toimimattomuus on asiakkaan vastuulla, mutta käytännössä ongelmat kohdistuvat valvontajärjestelmän toimittajaan. Toinen merkittävä ongelma on, että yhteysvirheiden ilmetessä ainoastaan asiakkaalla on oikeus asioida yhteyden toimittajan kanssa. SWOT-analyysin tuloksena tekniikka sai pisteluvun -3.

Kustannukset

Käytettäessä työmaalla jo olevaa Internet-yhteyttä siirtoyhteyden toteutukseen vältytään erillisiltä yhteyskustannuksilta ja yhteyden vaatiman päätelaitteen hankinnalta, joten lähestymistapa ei aiheuta arvioitavia kustannuksia lainkaan.

Yhteensopivuus

Koska tilaaja tarjoaa yhteyden valmiina Ethernet-liitäntänä, yhteensopivuus ei aiheuta ongelmia. Kuten jo aikaisemmin on todettu, Ethernet on standardoitu ja selvästi käytetyin lähiverkkotekniikka, jossa käytännössä kaikkien valmistajien laitteet toimivat ongelmitta. Yhteensopivuuden pisteytys löytyy taulukosta 31.

Taulukko 31: Olemassaolevan tekniikan yhteensopivuus

Yhteensopivuus	**Pisteet**	**Max pisteet**
Standardi	2.5	2.5
Avoin SW API	0	2.5
Useita HW toimittajia	2.5	2.5
Komponentit CE-merkittyjä	2.5	2.5
	7.5	**10**

Turvallisuus

Koska verkko ei ole omassa hallinnassa ja yhteys on salaamaton, pitää yhteyden turvaamiseksi muodostaa VPN-tunneli työmaan keskuksen ja palvelinjärjestelmän välille. Tunneloinnilla mahdollistetaan samalla datan eheyden varmistus, päätelaitteiden luotettava tunnistus ja suojaudutaan mahdollisilta siirtoyhteyden murroilta ja haavoittuvuuksilta.

Liityttäessä yhteiseen verkkoon muiden työmaan tietokoneiden kanssa on tärkeää varmistaa myös työmaan keskuksen tietoturva karsimalla kaikki tarpeettomat palvelut verkkorajapinnasta ja lisäämällä ohjelmistopalomuuri rajoittamaan verkkoliikenteen sallittuihin muotoihin (esim. VPN ja ssh). Turvallisuus on pisteytetty tarkemmin alla olevassa taulukossa 32.

Taulukko 32: Olemassolevan-tekniikan turvallisuus

Turvallisuus	**Pisteet**	**Max pisteet**
Luotettava tunnistus	0	2
Eheydenvarmistus	0	2
Salaus	0	2
Testattu	1	2
Haavoittuvuudet	1	2
	2	**10**

Suorituskyky

Käytännössä kaikki ns. laajakaistayhteydet, joilla työmaan Internet-yhteys voidaan toteuttaa, tarjoavat vähintään 1 Mb/s nopeuden, jonka jakavat tyypillisesti muutama työasema melko kevyessä käytössä. Yhteyden nopeus riittää erinomaisesti järjestelmän tarpeisiin. Mikäli yhteys on toteutettu ADSL-tekniikalla, on nopeuden nostaminen aina 24 Mb/s asti usein helppoa. Tarvittaessa samaa yhteyttä hyödyntäen voidaan siirtää esimerkiksi videokuvaa, mikäli järjestelmään halutaan liittää kameravalvonta tulevaisuudessa. Suorituskyvyn arviointi löytyy oheisesta taulukosta 33.

Taulukko 33: Olemassaolevan siirtoyhteyden suorituskyvyn pisteytys

Suorituskyky	Pisteet	Max pisteet
Vähimmäisnopeus saavutetaan	5	5
Dataliikenteen priorisointi mahdollista	0	5
	5	**10**

Saatavuus

Koska ei sitouduta mihinkään yksittäiseen tekniikkaan voidaan olettaa, että kaikkialla Suomessa on saatavilla vähintään 1 Mb/s Internet-yhteys. Sen toteutumiseksi tulisi valtion pitää kiinni tavoitteistaan saattaa vähintään 100 Mb/s yhteys kaikkien saataville vuoteen 2010 mennessä (*Liikenne ja viestintäministeriö 2009*). Kuten jo aiemmin on todettu, tämä liityntätekniikka ei edellytä erillisiä laitehankintoja, kuten ulkoisia antenneja tai päätelaitteita toimiakseen. Taulukossa 34 on olemassa olevan yhteyden saatavuuden pisteytys.

Taulukko 34: Olemassa olevan yhteyden saatavuuden pisteytys

Saatavuus	Pisteet	Max pisteet
Kattaa koko Suomen	5	5
Ei edellytä lisäantennia	5	5
	10	**10**

4.2.2 Flash OFDM

Paremmin kauppanimellä @450 tunnettu Flash OFDM-tekniikka on varsin uusi tulokas Suomen laajakaistamarkkinoilla. Kyseessä on Digita Oy:n operoima 450 Mhz taajuusalueella toimiva langaton verkko, joka lupaa toimittaa 1 Mb/s laajakaistayhteyden käytännössä kaikkialle Suomeen. Digita toimii verkon operaattorina ja jälleenmyynti tapahtuu palveluoperaattorien, kuten TeliaSoneran, Fujitsu Servicen, LynxNetin, Academican ja Emtelen kautta. (*Digita Oy 2009.*)

Tätä kirjoitettaessa Flash-ODFM-tekniikkaa hyödyntäviä laajakaistaverkkoja on käytössä Suomessa, Slovakiassa ja Yhdysvalloissa. Lisäksi Norjassa, Tanskassa ja Alanko-

maissa on testattu tekniikkaan perustuvia verkkoja (*Flash-OFDM 2009*). Osassa Suomea Digita tarjoaa myös 2 Mb/s nopeudella toimivaa yhteyttä.

Verkon tekniikan ja ominaisuuksien arviointi on huomattavan vaikeaa muihin vertailtaviin tekniikoihin nähden, sillä verkon yksityiskohdista on tietoa tarjolla hyvin vähän. Digitan 450laajakaista.fi sivusto on suunnattu lähinnä kuluttajille, eikä tekniikan omistaja Qualcomm kerro kotisivuillaan käytännössä mitään tekniikasta. Parhaaksi lähteeksi on osoittautunut Wikipedia, johon on koottu useista eri lähteistä löydetyt tiedonmurut tekniikasta, mutta osittain epätäydellisin lähdeviittein.

Teoria

Ytimekkäästi nimetty Flash-OFDM (Fast Low-latency Access with Seamless Handoff – Orthogonal Frequency Division Multiplexing) on alunperin Flarionin kehittämä mobiili laajakaistatekniikka, jota nykyään kehittää Qualcomm. Muihin tässä vertailtaviin tekniikoihin nähden Flash-OFDM poikkeaa olemalla täysin standardoimaton tekniikka. Sen kehitystä ja käyttöä säätelee oikeuksienhaltija Qualcomm Inc.

Flash-OFDM verkko on tekniikaltaan puhdas IP-verkko, sillä paitsi loppukäyttäjän yhteys, myös runkoverkko on toteutettu IP-tekniikalla. Tällöin dataa ei tarvitse muuntaa siirron aikana ja viivehävikit pysyvät maltillisina. Itse Flash-OFDM-verkon rakenne on varsin yksinkertainen, sillä lähes kaikki toiminnallisuus on runkoverkon reunoille sijoitetuissa radioreitittimissä, jotka toimivat kuten WiFi-verkon tukiasemat toimien rajapintana ja reitittiminä radioverkon ja kiinteän verkon välillä. (*Penttinen 2007.*)

Radiotien fyysinen toteutus hyödyntää hajaspektritekniikkaa, joka mahdollistaa radiotien tehokkaan ja häiriösietoisen hyödyntämisen.Lisäksi radiotekniikkaan on rakennettu mobiilikäytön kannalta merkityksellinen doppler-efektin kompensointi, jonka ansiosta tekniikalla toteutettuja verkkoja on käytetty jopa 250 km/h nopeudella liikkuvalla päätelaitteella. Tekniikan MAC- ja linkkikerrokset huolehtivat virheenkorjauksesta ja kaistanhallinnasta. (*Penttinen 2007.*)

Luotettavuus

Kuten kaikkien muidenkin Flash-OFDM tekniikan ominaisuuksien vertailussa luotettavuuden arviointia vaikeuttaa merkittävästi puolueettoman tiedon puute. Taulukkoon 35 kerättiin saatavissa olevien tietojen valossa tekniikan luotettavuuden arvioinnin kannalta oleelliset seikat.

Taulukko 35: SWOT analyysi Flash-OFDM-tekniikan luotettavuudesta

Strenghts – Vahvuudet Normaalisti luotettava	**Weaknesses – Heikkoudet** Mahdollinen lisäantenni haavoittuva Verkon huoltotyöt katkovat yhteyksiä
Oppoturnities – Mahdollisuudet Toistaiseksi ruuhkaton verkko Liikenteen priorisointi mahdollista	**Threats – Uhat**

Flash-OFDM-tekniikan luotettavuuden kannalta positiiviseksi asiaksi osoittautui verkon vähäinen käyttö ja mahdollisuus lisämaksusta priorisoida liikennettä yhteyden turvaamiseksi. Heikkoutena on kuitenkin nähtävä se, että verkon huoltotyöt saattavat ajoittain katkaista liikenteen alueellisesti (*Digita Oy 2009*). SWOT analyysi sai pistearvon +1.

Kustannukset

Vaikka itse @450-verkon liittymähinnat ovat kohtuullisia saatavaan palveluun nähden, päätelaitteiden hankintahinnoissa kostautuu tekniikan harvinaisuus ja pieni käyttäjäpopulaatio. Lisäksi kustannuksia aiheuttaa lisäantenni, joka kuuluvuuskartoista päätellen on lähes välttämätön. Kustannuserittely alla olevassa taulukossa 36.

Taulukko 36: Flash-OFDM-tekniikan kustannusvaikutus käyttötapauksessa UC2 (LynxNet Oy 2009)

Osa		Tarve	Kustannus	Yhteensä
Päätelaite	TW-3G Flash	1	299.00 €	299.00 €
Antenni		1	65.00 €	65.00 €
Liittymä	@450 512Kb	12 kk	38.00 €	456.00 €
				820.00 €

Yhteensopivuus

Flash-OFDM tekniikka ja @450-verkko eivät perustu millekään viralliselle määrittelylle, joten ainoastaan tekniikan oikeuksienhaltijan lisensoimat valmistajat voivat val-

mistaa komponentteja, kuten päätelaitteita verkkoon. Yksi kolmesta 450info.net sivustolla mainitusta laitevalmistajasta ilmoittaa tukevansa myös Linux-käyttöjärjestelmiä Windowsin lisäksi ja tarjoaa PCMCIA-verkkokortin kernel-modulin lähdekoodeja suljetun lisenssin alaisena. Käytännössä verkkoon liittyminen pitäisi toteuttaa Ethernet-väyläisella Flash-OFDM-reitittimellä, jolloin rajapintaongelmat vältetään. (*450info.net 2009.*)

Koska Flash-OFDM tekniikka on hyvin vähän käytetty maailmalla ja yhteensopivien laitteiden valmistus edellyttää Qualcomin lisenssiä laitetarjonta on kovin vähäistä. Digitan ilmoittaman laitteiden maahantuojan Brightpoint Finland Oy:n ylläpitämän 450info.net sivuston mukaan laitteita valmistavat vain Qualcomm, Netgear ja Leadtek, joten valinnanvaraa ei juurikaan ole. Toisaalta kun laitekirjo on pieni voidaan olettaa, että yhteensopivuusongelmia ei juurikaan ole ja laitteet ovat testattuja ja CE-merkittyjä. Taulukossa 37 on listattu tekniikan yhteensopivuuden ansaitsemat pisteet.

Taulukko 37: Flash-OFDM-tekniikan yhteensopivuus

Yhteensopivuus	**Pisteet**	**Max pisteet**
Standardi	0	2.5
Avoin SW API	1	2.5
Useita HW toimittajia	0	2.5
Komponentit CE-merkittyjä	2.5	2.5
	3.5	**10**

Turvallisuus

Tekniikan suljetun ja standardoimattoman luonteen huonot puolet tulevat esille tekniikan turvallisuutta arvioitaessa. Tekniikan turvallisuusominaisuuksista ei ole annettu mitään tietoa tekniikkaa käsittelevissä artikkeleissa ja jälleenmyyjät toteavat vain tekniikan olevan turvallinen. Vaikka tehdään olettamus, että operaattorin runkoverkkoon voi luottaa, ei esimerkiksi päätelaitteen ja tukiaseman välisen yhteyden suojauksesta ole tietoa. Tällöin joudutaan olettamaan, että liikenne on kuunneltavissa, mahdollisesti jopa häirittävissä tai altis man-in-the-middle hyökkäyksille. Tekniikan vähäisen maailmanlaajuisen käytön johdosta sen turvallisuuden koettelemiseen ei ole juurikaan kiinnostusta puolueettomien turvallisuustutkijoiden osalta, eikä siten varsinaisia haavoittuvuuksia ole löydetty tai julkaistu.

Siirtoyhteyden turvallisuuden varmistamiseksi on välttämätöntä suojata yhteys salatulla tunnelilla, jonka avulla voidaan myös varmistua datan muuttumattomuudesta ja tunnistaa yhteyden päätelaitteet luotettavasti. (Taulukko 38)

Taulukko 38: FlashOFDM-tekniikan turvallisuus

Turvallisuus	**Pisteet**	**Max pisteet**
Luotettava tunnistus	0	2
Eheydenvarmistus	0	2
Salaus	0	2
Testattu	0	2
Haavoittuvuudet	1	2
	1	**10**

Suorituskyky

Koska Flash-OFDM on suunniteltu laajakaistatekniikaksi riittää sen nopeus erinomaisesti järjestelmän tarpeisiin. Tällä hetkellä saatavilla on 512 kb/s, 1 Mb/s ja 2 Mb/s liittymiä, joissa uplink-nopeus (päätelaitteelta tukiasemalle) on joko 256 kb/s tai 512 kb/s (*LynxNet 2009*). Tulevaisuudessa on mahdollista, että nopeus vielä kasvaa kolmeen megabittiin, sillä tekniikan teoreettinen maksiminopeus on 3,2 Mb/s / 900 kb/s (*Penttinen 2007*).

Flash-OFDM on arvioiduista tekniikoista ainoa, jossa operaattori tarjoaa mahdollisuutta priorisoituun dataliikenteeseen. Priorisoidun liittymän kuukausimaksu on lähes kaksinkertainen vastaavaan tavalliseen liittymään verrattuna, joten tähän mahdollisuuteen turvaudutaan vain tarpeen vaatiessa. Suorituskykyvaatimukset on pisteytetty taulukkoon 39.

Taulukko 39: Flash-OFDM siirtoyhteyden suorituskyvyn pisteytys

Vähimmäisnopeus saavutetaan	5	5
Dataliikenteen priorisointi mahdollista	5	5
	10	**10**

Saatavuus

Verkon maantieteellinen saatavuus on ehdottomasti @450-verkon vahvuuksia muihin tekniikoihin verrattuna, sillä se on tällä hetkellä ainoa tekniikka, joka kattaa jopa 98% väestöstä ja toimii myös haja-asutusalueilla (*Digita Oy 2009*). Edellämainittu peittoaste edellyttää monin paikoin korkealle asennetun erillisen suunta-antennin käyttöä. Tekniikan saatavuus pisteytettiin taulukkoon 40.

Taulukko 40: Flash-OFDM-tekniikan saatavuus

Saatavuus	Pisteet	Max pisteet
Kattaa koko Suomen	5	5
Ei edellytä lisäantennia	2	5
	7	**10**

4.2.3 GSM-tekniikat

Matkapuhelinverkko tarjoaa hyvin kattavan verkkoratkaisun, jonka avulla lähes missä tahansa Suomessa saadaan jonkinasteinen datayhteys. Yhteyksien nopeudet ja laatu vaihtelevat kuitenkin merkittävästi sijaintien ja operaattoreiden välillä. Operaattoreiden mainostamat esimerkiksi 1 Mb/s nopeudet toteutuvat käytännössä kovin harvoissa ja valituissa paikoissa, sillä ns. 3G verkot kattavat lähinnä suurempien kaupunkien keskustat. Käytännössä haja-asutusalueilla ja pienemmissä kaupungeissa joudutaan tyytymään joko EDGE-tekniikalla (Enhanced Data rates for Gsm Evolution) toteutettuun datasiirtoon tai vielä hitaampaan GPRS-yhteyteen (General Packet Radio Service), joka mahdollistaa parhaimmillaankin vain 50 kb/s datanopeuden.

GSM-tekniikan (Global System for Mobile communications) käyttöönotto siirtoyhteysmediana onnistuu käyttämällä esimerkiksi työmaan keskusyksikön USB-väylään liitettävää modeemia, joita on tarjolla erinomaisen laaja valikoima erilaisiin tarpeisiin. Modeemin valinnassa huomioitavaa on sen tukemat siirtotekniikat ja nopeudet, mahdollisuus käyttää ulkoista antennia tarvittaessa ja ajureiden saatavuus.

Teoria

Puhepalvelujen osalta matkapuhelinverkot ovat kehittyneet varsin vähän sitten GSM-tekniikan käyttöönoton vuonna 1991. Datapalvelut sen sijaan ovat kehittyneet huikeasti ja nykyään termi langaton laajakaista ja lupaukset jopa 5 Mb/s siirtonopeuksista ovat arkipäivää ainakin operaattoreiden markkinointimateriaalissa. Todellisuudessa monin paikoin matkapuhelinverkot toteutetaan vanhemmilla tekniikoilla, joita useimmat päätelaitteet osaavat sulavasti käyttää.

Alkuperäinen GSM-tekniikka mahdollisti piirikytkentäisen datasiirron teoreettisellä 14.4 kb/s nopeudella käyttäen yhtä kahdeksasta aikavälistä ja ½ konvoluutiokoodausta samaan tapaan kuin puhetta siirrettäessä. Dataliikenteen määrän kasvaessa kehitettiin HSCSD-tekniikka (High Speed Circuit Switched Data), joka mahdollisti useamman aikavälin yhdistämisen yhdeksi loogiseksi tietoliikennekanavaksi vaatimatta laitteistotason muutoksia GSM-verkon tai päätelaitteiden tekniikkaan. Uusi tekniikka paransi siirtonopeuksia merkittävästi jopa teoreettiseen 57.6 kb/s nopeuteen, mutta käytännössä radiotien ja laitteiden viiveet sekä ruuhkautuminen rajoittivat nopeutta merkittävästi. (*Granlund 2001, 164-172.*)

Vastauksena jatkuvasti kasvavaan datasiirron tarpeeseen ja HSCSD-tekniikan melko tehottomaan piirikytkentäiseen tekniikkaan kehitettiin GPRS-tekniikka, joka mahdollistaa yhteydettömän pakettikytkentäisen dataliikenteen 172,2 kb/s huippunopeudella (21,2 kb/s aikaväliä kohden). Käytännössä operaattorit rajoittavat yhteyden nopeuden esimerkiksi 50 kb/s välttääkseen verkon ruuhkautumista. Merkittävin ero aiempiin tekniikoihin on GPRS:n tapa käyttää ainostaan tarvittaessa saatavilla olevan määrän aikavälejä datapaketin lähetykseen tai vastaanottoon (*Granlund 2001, 173-197*). Tällä hetkellä kaikki kolme Suomen GSM verkko-operaattoria tarjoavat GPRS-palvelua koko verkkonsa alueella.

EDGE-tekniikka on suora jatke perinteiseen GSM-tekniikkaan pohjautuville datasiirtotekniikoille. Operaattoreiden kannalta päivitys EDGE-verkkoon on ollut melko edullista verrattuna kolmannen sukupolven UMTS-tekniikoihin (Universal Mobile Telecommunications System), jotka vaativat laajempaa verkon uudistusta. Tekniikka mahdollistaa teoriassa jopa 1 Mb/s datanopeuden lähinnä tehokkaamman modulaation ansiosta

(*Ericsson 2007*). Käytännössä operaattorit tarjoavat EDGE-verkossaan korkeintaan 200 kb/s datanopeutta. Kaikilla kolmella verkko-operaattorilla EDGE-verkko kattaa eteläisen Suomen ja suuren osan kaupungeista pohjoisempana.

Mobiilidatatekniikoiden kärjessä ovat tällä hetkellä kolmannen sukupolven UMTS-tekniikat, kuten HSDPA (High Speed Downlink Packet Access), joka mahdollistaa jo nyt 21 Mb/s nopeuden. UMTS-tekniikka uudistaa matkapuhelinverkon rakennetta järjestelmäarkkitehtuurin ja käytettävien radiotekniikoiden osalta merkittävästi ja luo uuden pohjan, jonka varaan tulevaisuuden tekniikoita kehitetään (*Penttinen 2006, 64*). Suomen verkko-operaattorit ilmoittavat 3,6 Mb/s – 21 Mb/s nopeuksia verkoilleen, jotka tällä hetkellä kattavat käytännössä ainoastaan suuret kaupungit.

Luotettavuus

GSM-tekniikka on useimmiten luotettava ja siihen luotetaan henkilökohtaisessa viestinnässä lähes sokeasti. Lähes jokainen joutuu kuitenkin aika-ajoin toteamaan GSM-verkon ruuhkautumisen aiheuttamat ongelmat esimerkiksi massatapahtumissa tai muissa poikkeustilanteissa. SWOT-analyysi (Taulukko 41) paljasti GSM-tekniikan luotettavuuden näkökohdat mittausjärjestelmän osana.

Taulukko 41: SWOT analyysi GSM-tekniikan luotettavuudesta

Strenghts – Vahvuudet Kattava verkko ilman lisäantennia Paljon käytetty ja testattu	**Weaknesses – Heikkoudet** Nopeus vaihtelee Ei liikenteen priorisointia
Oppoturnities – Mahdollisuudet	**Threats – Uhat** Joukkotapahtumat voivat tukkia verkon

Normaaliolosuhteissa erinomaisesti hyvällä nopeudella toimivan GSM-verkon heikkoudeksi osoittautuu juuri luotettavuus. Dataliikennettä ei lähtökohtaisesti priorisoida pääasiassa puheliikenteelle suunnatussa verkossa, joten puheliikenteen kasvaessa äkillisesti saattaa data-yhteys hidastua tai katketa kokonaan. SWOT-analyysin pisteytys johti tulokseen -1 juurikin tästä syystä.

Kustannukset

GSM-tekniikan laaja levinneisyys ja markkinoiden aktiivinen kilpailutilanne ovat painaneet sekä päätelaitteiden, että liittymien hinnat varsin matalalle tasolle. Tarkemmin kustannukset eritellään alla olevassa taulukossa 42.

Taulukko 42: GSM-tekniikan kustannusvaikutukset käyttötapauksessa UC2 (Microdata Oy 2009) (DNA Oy 2009)

Osa		**Tarve**	**Kustannus**	**Yhteensä**
Modeemi	EDGE-E1	1	69.00 €	69.00 €
Liittymä	Data-liittymä	12 kk	9.90 €	118.80 €
				187.80 €

Yhteensopivuus

Vaikka standardeja ja verkkotekniikoita on markkinoilla merkittävä määrä, on Suomen tilanne sikäli hyvä, että kaikki verkko-operaattorit ovat päätyneet samoihin tekniikoihin, joten samat laitteet toimivat kaikkien Suomessa toimivien operaattoreiden verkoissa. Suomessa ja Euroopassa matkapuhelinverkot on totutettu yksinomaan GSM-tekniikkaan pohjautuviin ratkaisuihin, jotka ovat keskenään yhteensopivia.

Matkapuhelinverkkojen teknologiaa kehitetään alan yritysten erittäin tiiviissä yhteistyössä nykyisin lähinnä 3GPP organisaation kautta, joka johtaa kolmannen sukupolven verkkojen kehitystä. Tekniikoiden kehitys tapahtuu alan standardointielinten kautta ja valmiit määrittelyt ovat vapaasti saatavilla, joten kehitysprosessi on varsin avoin. (*3GPP 2009.*)

Tekniikoiden vahvan standardoinnin ja avoimuuden ansiosta tarjolla on hyvä valikoima päätelaitteita, jotka mahdollistavat verkkoon kytkeytymisen. Monet laitevalmistajat ovat myös julkaisseet päätelaitteilleen tarvittavat ajurit ja ohjelmistot Linux-ympäristöön. (*TuxMobil 2009.*)

GSM-tekniikoiden yhteensopivuus on pisteytetty taulukossa 43.

Taulukko 43: GSM-tekniikan yhteensopivuus

Yhteensopivuus	Pisteet	Max pisteet
Standardi	2.5	2.5
Avoin SW API	2.5	2.5
Useita HW toimittajia	2.5	2.5
Komponentit CE-merkittyjä	2.5	2.5
	10	**10**

Turvallisuus

Matkapuhelinjärjestelmien turvallisuus ei syystä tai toisesta ole ollut kovinkaan kehuttava, sillä ensimmäisen sukupolven NMT-järjestelmät (Nordic Mobile Telephone) eivät käyttäneet minkäänlaista salausta. GSM-tekniikassa käytettävästä A5 algoritmista on löydetty vakavia haavoittuvuuksia, jotka mahdollistavat esimerkiksi man-in-the-middle tyyppiset hyökkäykset. (*Barkan, Bihan & Keller 2006.*)

Käytännössä matkapuhelinverkon läpi toteutettu Internet-yhteys ei tarjoa todellista tietoturvaa, sillä päätelaitteita ei pysty luotettavasti tunnistamaan, datan eheyttä ei varmisteta, eikä yhteys ole salattu kuin päätelaitteen ja tukiaseman välisellä radiotiellä ja silloinkin haavoittuvalla algoritmilla. Käytännössä matkapuhelinverkon käyttö edellyttää yhteyden salattua tunnelointia, mikäli tavoitellaan todellista turvallisuutta. (Taulukko 44)

Taulukko 44: GSM-tekniikan turvallisuus

Turvallisuus	Pisteet	Max pisteet
Luotettava tunnistus	0	2
Eheydenvarmistus	0	2
Salaus	1	2
Testattu	2	2
Haavoittuvuudet	2	2
	5	**10**

Suorituskyky

Nykyiset matkapuhelinverkot täyttävät suorituskykyvaatimukset pääsääntöisesti hyvin, sillä vaadittu 2.6 kB/s nopeus saavutetaan jo GPRS-tekniikalla, joka on saatavilla lähes kaikkialla Suomessa. Vaikka GSM-verkkojen tekniikka mahdollistaa dataliikenteen priorisoinnin tiettävästi kaikki operaattorit ovat päätyneet priorisoimaan puheliikenteen.

GSM-tekniikan suorituskyvyn vastaavuus vaatimusmäärittelyyn on pisteytetty taulukkoon 45.

Taulukko 45: GSM-tekniikalla toteutetun siirtoyhteyden suorituskyvyn pisteytys

Suorituskyky	Pisteet	Max pisteet
Vähimmäisnopeus saavutetaan	5	5
Dataliikenteen priorisointi mahdollista	0	5
	5	**10**

Saatavuus

Kaikilla kolmella Suomessa toimivalla verkko-operaattorilla on varsin hyvin kattavat verkot, jotka ulottuvat aina Ahvenanmaan saaristosta Nuorgamiin asti. Ne kattavat operaattoreiden ilmoituksen mukaan jopa 98% Suomen asukkaista. (Taulukko 46)

Taulukko 46: GSM-tekniikan saatavuus

Saatavuus	Pisteet	Max pisteet
Kattaa koko Suomen	4	5
Ei edellytä lisäantennia	4	5
	8	**10**

4.3 Tunnelointi

Kuten jo edellisissä kappaleissa on jouduttu toteamaan, salattu tunnelointi on käytännössä välttämätön tietoturvallisen yhteyden muodostamiseen työmaan ja palvelinjärjestelmän välille. Tunnelointi voidaan toteuttaa useilla eri tekniikoilla, joista osa perustuu laitteistotason ratkaisuihin. Valittavana on myös useita toimivaksi osoittautuneita ohjelmistotasolla toimivia ratkaisuja. Koska työmaan keskuksen laitteisto mahdollistaa tunneloinnin toteuttaminen ohjelmistotasolla, on ohjelmistoratkaisun hyödyntäminen kustannustehokasta ja turvallista. Dataa ei siirretä salaamattomana esimerkiksi keskuksesta erilliseen VPN-laitteeseen (Virtual Private Network).

Parhaiksi ehdokkaiksi tunneloinnin toteutukseen karsiutui kaksi melko erilaista lähestymistapaa virtuaalisiin yksityiverkkoihin. Molemmista tekniikoista arvioitavaksi pyrittiin

löytämään kirjoitushetkellä yleisin ja koetelluin toteutus. Vertailtavien tekniikoiden päällimmäinen ero on salauksen toteutuksessa, mutta myös tekniikkaa toteuttavat sovellukset ja niiden hallintamahdollisuudet poikkeavat toisistaan arvioinnin kannalta merkittävästi. Vertailtavat tekniikat ovat IPSec (Internet Protoco Security) Openswan sovelluksella toteutettuna ja SSL-VPN (Secure Socket Layer – Virtual Private Network) OpenVPN-ohjelmistolla toteutettuna.

Arvioinnissa tunneloinnin kannalta epäoleelliset kustannus ja saatavuus-aihepiirit jätetään käsittelemättä, sillä molemmat toteutukset ovat GPL-lisenssin alla julkaistuja avoimia ohjelmistoja, jotka ovat yhtäläisesti saatavilla ilmaiseksi.

4.3.1 IPSec

IPSec lienee tunnetuin tunnelointiprotokolla, vaikka oikeammin IPSec on kokoelma protokollia, joiden avulla muodostetaan turvallinen yhteys kahden pisteen välille. Huomioitavaa IPSec-tekniikassa verrattuna muihin VPN-tekniikoihin on, että se toimii kokonaan OSI-mallin kolmannella, eli verkkokerroksella ollen täten näkymätön kaikille ylemmillä tasoilla toimiville tekniikoille. IPSec tekniikalla voidaan toteuttaa myös autentikoitu tunneli ilman salausta, mutta tässä sovelluksessa tunnelin tulee olla salattu.

Openswan on selvästi yleisin IPSec ohjelmisto Linux-ympäristöissä. Sovellus perustuu vuodesta 1999 aina vuoteen 2004 asti kehitettyyn FreeS/WAN sovellukseen ja on siten varsin pitkälle kehitetty ominaisuuksiltaan ja luotettavuudeltaan. Openswan ohjelmisto on saatavilla sekä lähdekoodimuodossa, että valmiina pakettina kaikille yleisimmille Linux-jakeluversioille.

Teoria

IPSec käyttää kolmea protokollaa toteuttaakseen turvallisen tunneloinnin kahden pisteen välille. Todennusotsikko AH (Authentication Header) mahdollistaa pakettien alkuperän tunnistamisen ja eheyden varmistuksen. Salausotsikko ESP (Encapsulated Security Payload) toteuttaa varsinaisen datan salaamisen ja varmistaa paketin alkuperän ja eheyden.

Avaintenhallintaprotokolla IKE (Internet Key Exchange) nimensä mukaisesti vastaa salausavainten hallinnasta.

Yksinkertaistettuna IPSec-tekniikalla toteutettu salattu tunneli muodostetaan kapseloimalla IP-paketti kokonaisuudessaan uuteen IP-pakettiin, johon lisätään AH tai ESP protokollien otsikkotiedot ja data salataan valitulla tavalla. IKE-protokolla huolehtii, että sekä lähettäjä että vastaanottaja käyttävät samoja salausavaimia, joilla kapseloidut paketit palautetaan alkuperäiseen muotoonsa. (*Heikkilä 2002, 65.*)

Luotettavuus

IPSec-tekniikan ja Openswan ohjelmiston luotettavuuden arviointi rakentuu IPSec-tekniikan saaman yleisen kritiikin ja rakenteellisten rajoitteiden varaan. Ne eritellään tarkemmin SWOT-analyysin (Taulukko 47) avulla.

Taulukko 47: SWOT analyysi IPSec-tekniikan luotettavuudesta

Strenghts – Vahvuudet Paljon käytetty ja testattu Avoin lähdekoodi varmistaa saatavuuden	**Weaknesses – Heikkoudet** Toimii huonosti NAT-muunnoksen läpi
Oppoturnities – Mahdollisuudet Mahdollisuus käyttää eri valmistajien ratkaisuja	**Threats – Uhat** Monimutkaisuus lisää virheiden todennäköisyyttä

Tietoturvatutkijoidenkin kritisoima IPSec-tekniikan monimutkaisuus on merkittävä luotettavuusongelmille altistava tekijä, joka tulee huomioida muuten käytännössä toimivaksi todetun ja hyvin yhteensopivan ratkaisun luotettavuutta arvioitaessa (*Ferguson & Schneier 2003*). SWOT-analyysin pistearvoksi saatiin +1.

Yhteensopivuus

IPSec perustuu IETF:n RFC dokumentteihin, joten tekniikkaa voidaan pitää standardoituna. Määrittelydokumentit ovat vapaasti kaikkien saatavilla ja hyödynnettävissä. Valitettavasti pitkään eri valmistajien VPN-tuotteiden yhteensopivuus on ollut vähintäänkin epävarmaa, vaikka ne periaatteessa ovatkin toteuttaneet samaa tekniikkaa ja noudattaneet samoja määrittelyjä. Openswan projektin kotisivuilla on listattuna useita VPN-toteutuksia asennusohjeineen, joiden on todettu toimivan Openswan IPSec toteutuksen

kanssa. IPSec-tekniikan yhteensopivuutta on arvioitu oheisessa taulukossa 48. (*Openswan 2009.*)

Taulukko 48: IPSec-tekniikan yhteensopivuus

Yhteensopivuus	Pisteet	Max pisteet
Standardi	2.5	2.5
Avoin SW API	2.5	2.5
Useita HW toimittajia	2.5	2.5
Komponentit CE-merkittyjä	2.5	2.5
	10	**10**

Turvallisuus

IPSec tekniikka toteuttaa asetettua tavoitetta AAA-turvallisuudelle esimerkillisesti. Vahvalla salauksella varustettu IPSec tunnelointi tunnistaa samalla yhteyden päätepisteiden oikeellisuuden esimerkiksi julkisen avaimen tekniikalla, varmistaa datan eheyden tarkastussummilla ja pakettien sarjanumeroilla sekä salaa datan valittua algoritmia käyttäen. (*Kent & Atkinson 1998.*)

Sekä IPSec-tekniikka että Openswan-ohjelmisto ovat erittäin käytettyjä tekniikoita, minkä johdosta niiden turvallisuutta myös tutkitaan hyvin aktiivisesti. Molempien avoimen luonteen ansiosta löydetyt haavoittuvuudet julkaistaan ja myös korjaus ongelmiin saadaan varsin nopeasti. Tietoturvayhtiö Secunia listaa Openswan ohjelmiston 2.x sukupolven historiasta viisi haavoittuvuutta, joista uusin havaittiin kesäkuussa 2009. Kaikki haavoittuvuudet on korjattu nykyisissä versioissa. IPSec tekniikan turvallisuutta lisää osaltaan modulaarinen rakenne, joka mahdollistaa eri salaus- ja varmennusalgoritmien käytön. Mikäli käytettävässä algoritmissa havaittaisiin vakava haavoittuvuus voidaan vaihtaa käytettävää algoritmia verrattain pienellä vaivalla. (*Secunia 2009a.*)

IPSec tekniikan turvallisuus ei ole voittanut kaikkien alan asiantuntijoiden varauksetonta tunnustusta varsin monimutkaisen rakenteensa ansiosta. Tunnetut tietoturvatutkija Bruce Schneier ja Niels Ferguson toteavatkin IPSec tekniikan turvallisuutta käsittelevässä artikkelissaan IPSecin olevan liian monimutkainen voidakseen olla turvallinen (*Ferguson & Schneier 2003*). Tekniikan turvallisuuden arvioinnissa (Taulukko 49) kri-

tiikin arvioitiin olevan ennemminkin luotettavuustekijä, sillä monimutkaisuus altistaa käyttäjän tekemille virheille.

Taulukko 49: IPSec-tekniikan turvallisuus

Turvallisuus	Pisteet	Max pisteet
Luotettava tunnistus	2	2
Eheydenvarmistus	2	2
Salaus	2	2
Testattu	2	2
Haavoittuvuudet	2	2
	10	**10**

4.3.2 SSL-VPN

SSL-tekniikka tunnetaan paremmin Web-sivujen suojaamiseen käytettävästä https-protokollasta, mutta sama OpenSSL-kirjasto mahdollistaa tehokkaan VPN-yhteyden suojaamisen. Vaikka markkinoilla on useita SSL-tekniikkaan perustuvia VPN-ratkaisuja ja itse SSL-salaus on IETF:n standardoima ei SSL-VPN-tekniikoille ole mitään yhteistä standardia, eivätkä eri valmistajien ratkaisut ole käytännössä yhteensopivia.

OpenVPN on noussut nopeasti erittäin suosituksi VPN-ratkaisuksi pitkälti avoimuutensa, laajan käyttöympäristötuen ja yksinkertaisuutensa ansiosta. Siinä missä esimerkiksi Openswan vaatii kokonaisen ohjelmakirjaston toimiakseen, OpenVPN käyttää vain yhtä binääritiedostoa ja asetustiedostoa. OpenVPN-ohjelmistoa kehittävän OpenVPN Technologies Inc.-yrityksen sivuston mukaan ohjelmiston käyttäjäyhteisössä on yli 3 miljoonaa jäsentä ja ohjelmistoa ladataan yli 150 000 kertaa kuukaudessa, joten ohjelmisto on selvästi varsin laajasti käytössä. (*OpenVPN Technologies Inc 2009.*)

Teoria

SSL-VPN ratkaisujen kuten OpenVPN-ohjelmiston tärkein komponentti on SSL/TLS-salaustekniikka, joka perustuu jo vuonna 1994 Netscape Communications Corporationin julkaisemaan SSL-määrittelyyn. Myöhemmin IETF on ottanut tekniikan kehitysvastuun Transport Layer Security (TLS) nimellä. (*Transport Layer Security 2009.*)

Kuten nimi viittaa, TLS-tekniikka on suunniteltu toimimaan TCP/IP-mallin siirto ja sovelluskerrosten välissä, jolloin sen toimintaan ei vaikuta alempien tasojen tekniikat, kuten IP-osoitemuunnos. Toisaalta sovellustason protokollat voidaan kuljettaa muuttumattomina. Monet sovellukset, kuten HTTP-palvelimet (HyperText Transfer Protocol), toteuttavat SSL/TLS-salauksen sisällyttämällä salauksenhallinnan ohjelmiston käyttöliittymään, jolloin ainostaan kyseisen ohjelmiston välittämä data salataan. VPN-käytössä erillinen ohjelmisto muodostaa SSL/TLS-tekniikalla suojatun tunnelin, jonka läpi kaikki päätepisteiden välinen data ohjataan. (*Transport Layer Security 2009.*)

Itse TLS protokolla koostuu kättelyprotokollasta (Handshake protocol), jonka avulla suojattavan yhteyden osapuolet tunnistautuvat ja sopivat käytettävistä salaus ja varmennusalgoritmeista sekä tietueprotokollasta (Record protocol), joka vastaa itse siirrettävän datan salaamisesta ja pilkkomisesta sopiviksi paketeiksi. Kuten IPSec-tekniikassakin, käytettävä tunnistus ja salausalgoritmi voidaan valita tarpeen mukaan.

Oletusasetuksin OpenVPN muodostaa tunnelin UDP-protokollalla (User Datagram Protocol), sillä OpenVPN ohjelmisto varmistaa pakettien perillemenon. Näin vältytään kaksinkertaiselta varmistukselta joka kuluttaisi turhaan resursseja ja kaistaa. (*Yonan 2004.*)

Luotettavuus

OpenVPN poikkeaa Openswan ohjelmistosta perustekniikaltaan ollen rakenteeltaan huomattavasti yksinkertaisempi ja toimien ylempänä OSI-mallissa. Tarkemmin luotettavuuden arviointiin perehdytään SWOT-analyysin avulla (Taulukko 50).

Taulukko 50: SWOT analyysi SSL-VPN-tekniikan luotettavuudesta

Strenghts – Vahvuudet Yksinkertainen ohjelmisto Avoin lähdekoodi varmistaa saatavuuden NAT-muunnos ei häiritse Hyvät hallintatyökalut Hyvä tunnelin luotettavuuden hallinta	**Weaknesses – Heikkoudet** Ei yhteensopiva muiden toteutusten kanssa
Oppoturnities – Mahdollisuudet Hyvin dokumentoitu rajapinta integrointiin	**Threats – Uhat** Ohjelmiston kehitys nojaa yritykseen

Standardoimaton toteutus ja kehityksen keskittyminen yksittäisen yrityksen haltuun vaikuttavat negatiivisesti OpenVPN:n luotettavuuden arvioon. Ohjelmiston yksinkertaisuus, toiminta ylempänä OSI-mallissa ja hyvät hallintatyökalut puhuvat ohjelmiston puolesta. Pistearvoksi SWOT-analyysistä saatiin +4.

Yhteensopivuus

Vaikka OpenVPN-ohjelmisto perustuu standardoituihin SSL/TLS-tekniikoihin, ei itse ohjelmisto ole minkään standardin mukainen. Koska itse ohjelmisto on julkaistu GPL-lisenssin alaisena, ovat sen lähdekoodit vapaasti saatavilla, mikäli kehitystyö syystä tai toisesta päättyisi.

Muutamat laitevalmistajat kuten, Vyatta ja Nokia, ovat lisänneet tuen OpenVPN-tunneloinnille omiin tuotteisiinsa. Periaatteessa myös kolmannet osapuolet voivat valmistaa asiakasohjelmistoja OpenVPN ympäristöön, sillä ohjelmistorajapinta on hyvin määritelty. Yhteensopivuus on pisteytetty taulukossa 51. (*OpenVPN Technologies Inc 2009.*)

Taulukko 51: SSL-VPN-tekniikan yhteensopivuus

Yhteensopivuus	Pisteet	Max pisteet
Standardi	0	2.5
Avoin SW API	2.5	2.5
Useita HW toimittajia	0.5	2.5
Komponentit CE-merkittyjä	2.5	2.5
	5.5	**10**

Turvallisuus

Yleisin tapa muodostaa laajempia VPN-kokonaisuuksia OpenVPN-ohjelmistolla on hyödyntää vahvaan tunnistukseen julkisen avaimen tekniikkaa ja sertifikaatteja, jolloin saavutetaan erittäin turvallinen yhteyden osapuolten varmennus.

Kun osapuolet on tunnistettu, voidaan yhteyden salaamiseen käyttää lähes mitä hyvänsä algoritmia riippuen yhteyden kriittisyydestä, laskentakapasiteeista ja algoritmien turvallisuustilanteesta. Laajasti käytettyjen ohjelmistojen turvallisuutta koetellaan jatkuvasti, mutta varsinaisesta OpenVPN ohjelmistosta on löytynyt haavoittuvuuksia viimeksi vuonna 2006. Nämä haavoittuvuudet on luonnollisesti paikattu. (*Secunia 2009b.*)

Taulukko 52: SSL-VPN-tekniikan turvallisuus

Turvallisuus	**Pisteet**	**Max pisteet**
Luotettava tunnistus	2	2
Eheydenvarmistus	2	2
Salaus	2	2
Testattu	2	2
Haavoittuvuudet	2	2
	10	**10**

5 Valinta

Valinta käytettävien tekniikoiden välillä tehtiin pisteyttämällä tekniikoiden ja vaatimusmäärittelyn vastaavuus luvussa 3 esitellyllä tavalla. Vertailemalla tekniikoiden ansaitsemia pisteitä löydettiin parhaiten vaatimuksia vastaava tekniikoiden yhdistelmä. Seuraavissa kappaleissa esitellään valintapisteytyksen tulokset kunkin järjestelmän osan kohdalta ja perustellaan valinta.

5.1 Kenttäverkko

Kenttäverkon vaihtoehdot olivat teknisesti keskenään hyvin poikkeavia. Ethernet-tekniikan korkeat kustannukset ja kaapeloinnin aiheuttamat ongelmat työmaaolosuhteissa tekivät siitä käytännössä mahdottoman ratkaisun langattomiin tekniikoihin verrattaessa. WiFi-Mesh-tekniikka tarjosi monia hyviä ominaisuuksia, mutta standardin vakiintumattomuus, alttius sähköisille häiriöille ja skaalautumattomuus suuriin (300 päätelaitetta) verkoihin jättivät sen toiselle sijalle. Ylivoimaisesti parhaaksi kenttäverkon tekniikaksi osoittautui ZigBee, joka on suunniteltu juuri tämän tyyppisiin verkkoihin ja siten loisti kaikilla osa-alueilla. Tarkempi pisteytys eritellään taulukossa 53, johon kaikki arvioitavat osa-alueet on pisteytetty kappaleessa 3 esitellyllä tavalla.

Taulukko 53: Kenttäverkon tekniikan valintapisteet

	Max pisteet	Ethernet	WiFi-Mesh	ZigBee
Luotettavuus	10	6	8	10
Kustannukset	10	6	8	10
Yhteensopivuus	10	10	8	9
Turvallisuus	10	4	6	10
Mittapisteiden määrä ja maasto	10	7.5	6	10
Mekaaniset ja sähköiset	10	6	6	10
Mukautuminen	10	2	8	10
		41.5	**50**	**69**

5.2 Siirtoyhteys

Siirtoyhteyden valinnassa vastakkain asetettiin kolme erilaista lähestymistapaa tietoverkkoyhteyden toteutukseen. Ehkä hieman yllättäenkin Digitan ylläpitämä Flash-OFDM-verkko jäi vertailun viimeiseksi tekniikan suljetun luonteen ja sen kerrannaisvaikutusten, kuten korkeiden kustannusten ansiosta. Mikäli katsottaisiin läpi sormien se, ettei tekniikasta ole saatavilla kunnollisia teknisiä tietoja ja että päätelaitteiden valmistajia on vain muutama olisi tekniikka erittäin varteenotettava vaihtoehto varsinkin alueilla, joissa GSM-verkko on heikko tai ruuhkainen.

Pisteytyksessä toiseksi ylsi ratkaisumalli, jossa hyödynnetään asiakkaan järjestämää yhteyttä, joka useimmiten on työmaan tietokoneiden kanssa jaettu ADSL-yhteys. Ratkaisun ongelmana on turvattomuuden lisäksi kaapeloidun yhteyden alttius vaurioille työmaaolosuhteissa ja yhteysongelmien yhteydessä ilmenevät toimivaltaongelmat operaattorin kanssa asioitaessa.

Turvallisuus ja luotettavuusongelmistaan huolimatta GSM-tekniikalla toteutettu siirtoyhteys osoittautui parhaaksi tavaksi toteuttaa työmaan ja palvelinjärjestelmän välinen yhteys. Tekniikkaa käytettäessä on kuitenkin hyvä huomioida mahdollisen verkon ruuhkautumisen vaikutukset. Esimerkiksi suurten kaupunkien keskusta-alueilla saattaa olla aiheellista harkita vaihtoehtoista tekniikkaa, mikäli yksikään operaattori ei tarjoa dataliikenteen priorisointia. Tarkemmin tekniikoiden pisteytys selviää taulukosta 54.

Taulukko 54: Siirtoyhteystekniikan valintapisteet

	Max pisteet	Olemassaolev	Flash-OFDM	GSM
Luotettavuus	10	6	10	8
Kustannukset	10	10	6	8
Yhteensopivuus	10	7.5	3.5	10
Turvallisuus	10	2	1	5
Suorituskyky	10	5	10	5
Saatavuus	10	10	7	8
		40.5	**37.5**	**44**

5.3 Tunnelointi

Tunnelointitekniikoita arvioitaessa lupaavimmiksi vaihtoehdoiksi valikoitui kaksi päällisin puolin melko samankaltaista avoimen lähdekoodin ohjelmistoa, jotka toteuttavat salatun tunneloinnin hieman eri lähestymistavoin. Täpärästi toiseksi jääneen OpenVPN-ohjelmiston heikkoudeksi osoittautui standardeista poikkeava toteutus, jonka ansiosta se ei ole käytännössä yhteensopiva muiden ohjelmistojen kanssa. Sen käyttö esimerkiksi laitepohjaisen VPN-yhdyskäytävän kanssa olisi varsin vaikeaa.

Paremmin tarpeita vastaavaksi ohjelmistoksi osoittautui IPSec-tekniikkaan perustuva Openswan ohjelmisto, joka monimutkaisuudestaan huolimatta tarjosi merkittäviä etuja standardoituun IPSec-tekniikkaan pohjautuvalla lähestymistavallaan. IPSec toteutus mahdollistaa esimerkiksi palvelinjärjestelmässä VPN-tunneleiden hallinnan laitepohjaisella VPN-yhdyskäytävällä ja muiden IPSec ohjelmistojen käytön tarvittaessa. Tekniikoiden välinen ero käy ilmi alla olevasta taulukosta 55.

Taulukko 55: Tunnelointitekniikan valintapisteet

	Max pisteet	**IPSec**	**SSL-VPN**
Luotettavuus	10	8	10
Yhteensopivuus	10	10	5.5
Turvallisuus	10	10	10
		28	**25.5**

6 Loppuanalyysi

Tämän työn tarkoitukseksi asetettiin teknisin perustein parhaiden tietoverkkoratkaisujen löytäminen olosuhdevalvontajärjestelmään. Työssä perehdyttiin kaikkiaan kahdeksaan tekniikkaan hieman pintaa syvemmin, mutta ennen tätä työn taustatutkimusvaiheessa arvioitiin kymmenien tekniikoiden soveltuvuutta määriteltyihin raameihin. Lopputuloksena työ paljasti kolmen eri tekniikan kombinaation, joiden avulla on erinomaiset mahdollisuudet rakentaa toimiva, kestävä ja kustannustehokas tietoverkko rakennustyömaiden valvontaan.

Merkittävä arvo, joka työllä saavutettiin on kattavat perustiedot käytettävistä tekniikoista ja muista vastaaviin käyttötarkoituksiin soveltuvista tekniikoista. Laajat taustatiedot osoittautuvat varmasti hyödyllisiksi yhteistyökumppaneita kartoittaessa ja integroitaessa tekniikoita kokonaisjärjestelmään.

Vaikka huolellinen kirjallisuusselvitys on hyvä lähtökohta teknisten ratkaisujen toteuttamiskelpoisuuden tutkimiseen, se ei korvaa käytännön testausta. Mikäli aikataulu ja resurssit olisivat sen mahdollistaneet, olisi tekniikat pitänyt testata myös käytännössä sekä yksitellen että järjestelmänä. Varsinkin työmaaolosuhteiden aiheuttamat sähköiset, mekaaniset ja inhimilliset muuttujat ovat mahdottomia hallita totuudenmukaisesti pelkästään paperilla.

Yksi suurimmista yllätyksistä siirtoyhteystekniikoiden vaihtoehtoja arvioitaessa oli Digitan @450-verkon heikko menestys, sillä verkko soveltuu mainospuheidensa perusteella hyvin järjestelmän tarpeisiin. Ehkä tekniikan suurin ongelma oli juuri mainospuheiden määrä ja olematon oikean tieto. Tällöin arvioinnissa jouduttiin lähestymään tekniikkaa melko negatiivisella asenteella. Tarkempi kuvaus tekniikan toiminnasta olisi edellyttänyt asiantuntijahaastatteluja, joita ei käytettävissä olleen ajan puitteissa pystytty tekemään. Vaikka tekniset tiedot olisivatkin tarkentuneet tekniikan kannalta suotuisammiksi, ei se muuttaisi tekniikan sietämättömiä kustannuksia ja siten valinnan lopputulosta oleellisesti.

Aivan ongelmitta ei valintaprosessi edennyt, sillä alkuvaiheessa teknologiariippumattomien vaatimusten laatiminen tekniikoiden valintaperusteeksi osoittautui varsin haasteelliseksi tehtäväksi. Vaatimusten selvittyä piti myös laatia arvostelujärjestelmä, joka kohtelisi kaikkia tekniikoita tasapuolisesti, mutta painottaisi tärkeimpiä kriteerejä. Oman lisämausteensa antoivat myös tiettyjen tekniikoiden kohdalla puolueettomien lähteiden vähäinen määrä ja toisaalta kokonaisjärjestelmän salassa pidettävät yksityiskohdat julkaistavassa työssä.

Järjestelmässä hyödynnettävien tekniikoiden selvittyä jatketaan kokonaisjärjestelmän kehitystä suunnittelemalla valittuja tekniikoita hyödyntävät verkot ja valitsemalla yhteistyökumppanit verkkojen toteutukseen. Koska järjestelmän kehittämiseen käytettävät resurssit ovat varsin rajalliset on vaikeaa arvioida järjestelmän markkinoilletulo ajankohtaa. Varmaa on kuitenkin, että lähivuosien aikana rakennustyömaiden olosuhteiden seurannassa tullaan ottamaan käyttöön teknisiä ratkaisuja olivatpa ne sitten Salon Rakennuskonevuokraamon tai jonkin muun tahon kehittämiä.

Lähteet

Julkaisemattomat lähteet

SRKV Oy 2009a. Olosuhdevalvontajärjestelmän vaatimusmäärittely

SRKV Oy 2009b. Olosuhdevalvontajärjestelmän arkkitehtuurisuunnitelma

SRKV Oy 2009c. Olosuhdevalvontajärjestelmän käyttötapausanalyysi UC2

Painetut lähteet

Cisco Networking Academy Program 2003. CCNA 1 and 2 Companion Guide. Indianapolis USA: Cisco Press

Granlund, Kaj 2001. Langaton tiedonsiirto. Porvoo: Docendo Finland Oy

IEEE 802.11. 2007. Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications. New York: IEEE

IEEE 802.11s. 2009. Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications. Amendment 10: Mesh Networking. Draft 3.0. New York: IEEE

IEEE 802.15.4. 2006. Part 15.4: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low-Rate Wireless Personal Area Networks (WPANs). New York: IEEE

Marshall, Perry S.; Rinaldi, John S. 2005. Industrial Ethernet. USA: The Instrumentation, Systems and Automation Society

Penttinen Jyrki 2007. Laajakaistapalvelut alkavat 450 megahertsillä. Prosessori-lehti 6-7 / 2007

Penttinen Jyrki 2006. Tietoliikennetekniikka: 3G ja erityisverkot. Helsinki: WSOY

Wendell, Odom 2005. Tietoverkot – Perusteet. Helsinki: IT Press

Yleiskaapelointijärjestelmät 2008. Espoo: Sähkötieto Ry

Sähköiset lähteet

3GPP 2009. [online]. [viitattu 16.11.2009] http://www.3gpp.org

450info.net 2009. [online]. [viitattu 10.11.2009]. http://www.450info.net

Advanced Encryption Standard, Wikipedia 2009. [online]. [viitattu 4.11.2009]. http://en.wikipedia.org/wiki/Advanced_Encryption_Standard

Barkan, Elad; Biham, Eli; Keller, Nathan 2006. Instant Ciphertext-Only Cryptanalysis of GSM Encrypted Communication. [online]. [viitattu 16.11.2009]. http://www.cs.technion.ac.il/users/wwwb/cgi-bin/tr-get.cgi/2006/CS/CS-2006-07.pdf

Euroopan Komissio 2008. CE-merkintä: tuote vastaa vaatimuksia. [online]. [viitattu 20.5.2009]. http://ec.europa.eu/finland/news/press/101/10779_fi.htm

Cisco Systems Inc 2007. White Paper: 20 Myths of WiFi Interference. [online]. [viitattu 23.11.2009]. http://www.cisco.com/en/US/prod/collateral/wireless/ps9391/ps9393/ps9394/prod_white_paper0900aecd807395a9_ns736_Networking_Solutions_White_Paper.html

Cragie, Robert 2009. ZigBee Security [online]. [viitattu 4.11.2009]. http://www.zigbee.org/imwp/idms/popups/pop_download.asp?contentID=16564

Digita Oy 2009a. @450 [online]. [viitattu 8.11.2009]. http://www.450laajakaista.fi/at450

Digita Oy 2009b. Ajankohtaista & Huoltokatkokset [online]. [viitattu 8.11.2009]. http://www.450laajakaista.fi

DNA Oy 2009. [online]. [viitattu 2.12.2009]. http://www.dna.fi

Ericsson AB 2007. White Paper: The Evolution of EDGE. [online]. [viitattu 16.11.2009]. http://www.ericsson.com/technology/whitepapers/3107_The_evolution_of_EDGE_A.pdf

Ferguson Niels, Schneier Bruce 2003. A Cryptographic evaluation of IPSec [online]. [viittattu 17.11.2009]. http://www.schneier.com/paper-ipsec.pdf

Flash-OFDM, Wikipedia 2009. [online]. [viitattu 10.11.2009]. http://fi.wikipedia.org/wiki/Flash-OFDM

Goodspeed, Travis 2009. Breaking 802.15.4 AES 128 By Syringe [online] [viitattu 5.11.2009] http://travisgoodspeed.blogspot.com

Heikkilä, Tommi 2002. Verkonhallintajärjestelmän suojaaminen IPSecin avulla. pro gradu. Jyväskylän yliopisto. [online]. [viitattu 17.11.2009]. http://tisu.it.jyu.fi/terabitti/20021028-vh-ipsec-gradu-final-2.pdf

ITU Model for Indoor Attenuation, Wikipedia 2009. [online] [viitattu 4.11.2009] http://en.wikipedia.org/wiki/ITU_Model_for_Indoor_Attenuation

Jacobs, David B 2008. 802.11s mesh networks. [online]. [viitattu 8.10.2009]. http://searchenterprisewan.techtarget.com/tip/0,289483,sid200_gci1324249,00.html

Kaskela Lauri 2005. Tietotekniikan hankinta. TIEKE Tietoyhteiskunnan kehittämiskeskus ry. [online]. [viitattu 19.11.2009]. http://www.tieke.fi/verkkokaveri/teemat/tietotekniikkahankinnat/tietotekniikan_hankinta/hankintaprosessi/1_vaatimusmaarittely/

Kent, S. ja Atkinson R. 1998. RFC 2406 - IP Encapsulating Security Payload (ESP). The Internet Society, Network Working Group [online]. [viitattu 17.11.2009]. http://www.ietf.org/rfc/rfc2406.txt?number=2406

Liikenne ja viestintäministeriö 2009. Laajakaista kaikille [online]. [viitattu 8.11.2009]. http://www.lvm.fi/web/fi/243

LynxNet Oy 2009. Tuotteet [online]. [viitattu 13.11.2009]. http://www.lynxnet.fi/index.php/page/tuotteet.html

Microdata Oy 2009. [online]. [viitattu 01.12.2009] http://www.microdata.fi

Network Stuff 2009. IPSec bandwidth overhead using AES [online]. [viitattu 21.11.2009]. http://www.networkstuff.eu/index.php/IPsec_Bandwidth_Overhead_Using_AES

One Laptop Per Child 2009. [online]. [viitattu 2.12.2009]
http://www.laptop.org

Open80211s.org 2009. [online]. [viitattu 2.12.2009]
http://www.open80211s.org

Openswan 2009. [online]. [viitattu 18.11.2009].
http://www.openswan.org

OpenVPN Technologies Inc 2009. [online]. [viitattu 18.11.2009].
http://www.openvpn.net

Secunia 2009a. Vulnerability Report: Openswan 2.x [online]. [viitattu 17.11.2009].
http://secunia.com/advisories/product/3624

Secunia 2009b. Vulnerability Report: OpenVPN 2.x [online]. [viitattu 18.11.2009].
http://secunia.com/advisories/product/5568

Silvola Risto 2004. ZigBee ja Bluetooth 1.2 ja niiden soveltuminen automaation käyttöön. Raportti [online]. [viitattu 29.10.2009].
http://ae.tut.fi/research/AIN/Publications/ZigBee_BT1.2_Silvola.pdf

STEK - Sähköturvallisuuden edistämiskeskus: IP-numeroiden merkitys [online]. [viitattu 5.10.2009].
http://www.sahkoturva.info/sahkon_kaytto_kotona/sahkolaitteiden_ip_luokitus/fi_FI/ip_numeroiden_merkitys/

Telegesis Ltd 2009. ZigBee Case Studies [online]. [viitattu 7.11.2009].
http://www.telegesis.com/zigbee_overview/zigbee_case_studies.htm

Transport Layer Security, Wikipedia 2009. [online]. [viitattu 18.11.2009].
http://en.wikipedia.org/wiki/Transport_Layer_Security

TuxMobil 2009. Linux compability guides for 3G [online]. [viitattu 21.11.2009].
http://tuxmobil.org/linux_on_laptops_with_umts_cards.html

Yamaichi Electronics 2009. Y-ConRJ45 Series. [online]. [viitattu 22.11.2009].
http://www.yamaichi.com

Yan Zhang, Jijun Luo ja Honglin Hu 2006. Wireless Mesh Networking: Architectures, Protocols and Standards. CRC Press. [online]. [viitattu 7.11.2009].
http://books.google.fi/books?id=7t4szWRwnFkC&lpg=PA407&ots=tSbOp46-DUm&dq=802.11s%2032%20node%20limit&pg=PA407#v=onepage&q=&f=true

Yonan James 2004. User-Space VPN and OpenVPN. [online]. [viitattu 18.11.2009].
http://www.openvpn.net/papers/BLUG-talk/index.html

ZigBee Alliance 2009. [online]. [viitattu 28.10.2009].
http://www.zigbee.com

ZigBee Alliance 2007. ZigBee and Wireless Radio Frequency Coexistense. [online]. [viitattu 7.11.2009].
http://www.zigbee.org/imwp/idms/popups/pop_download.asp?contentID=11745

Reddy, Joseph 2006. ZigBee Security Layer Technical Overview. [online]. [viitattu 4.11.2009].
http://www.zigbee.org/imwp/idms/popups/pop_download.asp?contentID=9436