Jukka Valvanne

Ad-Hoc-verkot

Projektit, protokollat ja reititys

Metropolia Ammattikorkeakoulu
Tietotekniikka
Tietoverkot
Insinöörityö
30.05.2014

Metropolia

Tiivistelmä

Tekijä(t) Otsikko Sivumäärä Aika	Jukka Valvanne Ad-Hoc-verkot: projektit, protokollat ja reititys 36 sivua 30.05.2014
Tutkinto	Insinööri
Koulutusohjelma	Tietotekniikka
Suuntautumisvaihtoehto	Tietoverkot
Ohjaaja(t)	Lehtori Jukka Louhelainen

Tämän insinöörityön aiheena on tutustua langattomissa verkoissa vähemmän tunnettuihin Ad-Hoc– ja mesh-topologiaratkaisuihin.

Insinöörityössä käydään aluksi läpi pintaraapaisu 802.11-lähiverkkostandardin peruskäsitteistä. Tämän jälkeen käsitellään syvemmin ns. Ad-hoc– sekä mesh-tyyppisiä verkkoja, tutustutaan muutamaan näitä hyödyntäviin sekä kehittäviin projekteihin sekä mahdollisiin käyttökohteisiin.

Suuri osa työstä käsittelee Mesh-verkkoja, eli sellaista langattoman Ad--Hoc-verkon muotoa, joissa tukiasemaa ei tarvita, sillä jokainen solmu voi toimia viestien välittäjänä.

Esittelen erään harrastelijavoimin toteutetun mesh-verkkoja käyttävän projektin verkkorakennetta, sekä käyn läpi useita nimenomaan Ad-Hoc-verkkoon toteutettuja ja suunniteltuja reititysprotokollia.

Lopussa kerrotaan hieman yleisiä tietoturva-asioita, jotka koskevat avoimia verkkoja yleisellä tasolla. Kerron mm. PGP-salausohjelman periaatteesta.

Tarkoitus on kertoa mahdollisimman selkeästi, mitä tukiasematon (Ad-Hoc) verkko tarkoittaa, missä tällaisia verkkoja käytetään ja voitaisiin käyttää sekä antaa lukijalle perustason ymmärrystä reitityksestä langattomissa verkoissa.

Työtä tehdessä opittiin, että avoimesti ja harrastelijavoimin toteutetuilla projekteilla voi olla suuri merkitys kaupungin tai kylän asukkaille sekä taloudelliselle tilanteelle. Työ osoitti myös, että projektit ovat hajanaisia, heikosti dokumentoituja ja usein vielä heikommin tunnettuja.

Avainsanat	Mesh, Ad-Hoc, WLAN, langaton reititys, PGP, SSL

Metropolia

Abstract

Author(s) Title Number of Pages Date	Jukka Valvanne Ad-Hoc Networks: projects, protocols and routing 36 pages 30. May. 2014
Degree	Insinööri
Degree Programme	Tietotekniikka
Specialisation option	Tietoverkot
Instructor(s)	Jukka Louhelainen, Lecturer

The subject of this thesis is to take a look on the less well known Ad-Hoc and mesh-network topologies used in Wireless networks.

At first, this thesis will cover very basic understanding of the concepts of the 802.11 wireless network standard. After that, the document will dive a little deeper into the Ad-Hoc and mesh network models. We will also take a look at a few projects which develop and target areas, which take advantage of these sort of networks.

A large portion of this thesis cover mesh-networks, which are the kind of networks without bases tations, in which every node can participate in forwarding the routing messages.

I present the contruction of a particular network, which was put together by hobbyists - based on meshes, I also cover several routing protocols specificly aimed and designed for Ad-Hoc networks.

Lastly, a few general security issues are discussed shortly f.ex. The very basics of the PGP-encryption software is provided.

The purpose is to as simply as possible put, to tell what does it mean to have a network without a base station, where these kind of networks are and could be used, and to give rough understanding about routing in wireless networks.

Writing this thesis taught me, that openly developed, hobbyist-driven projects can have a significant impact on people and the economics of a city or village.

It was also discovered, that the projects are highly diverse, not well documented and even less known by general public.

Keywords	Mesh, Ad-Hoc, WLAN, wireless routing, PGP, SSL

Sisällys

LYHENTEET

802.11 IEEE-standardointijärjestön langattoman WLAN-verkkojen päästandardi.

Ad-Hoc Tukiasematon verkkotopologia.

ALFRED *Allmighty Lightweight Fact Remote Exchange Daemon,* Langattomien verkkojen tietojen, kuten sää- ja sijaintitietojen vaihtoon suunniteltu palvelu.

AODV *Ad-Hoc On-Demand Distant-Vector routing protocol* Mobiiliin Ad-Hoc–verkkoon suunniteltu reititysprotokolla.

B.A.T.M.A.N.
Better Approach To Mobile Ad-hoc Networks, Ad-Hoc-verkkoja varten suunniteltu sekä 2. että 3. tason reititysprotokolla.

EAP *Extensible Authentication Protocol,* Laajennettava autentikointiprotokolla.

EIGRP *Enhanced Interior Gateway Routing Protocol*
Kaupallinen, vuoteen 2013 asti Cisco Networksin omistama suljettu reititysprotokolla.

ETX *Expected Transmission Count.* Eräissä langattomissa reititysprotokollissa käytetty reitin luotettavuutta kuvaava suure.

GNU *GNU's Not Unix,* projektin tarkoitus on luoda täysin vapaa käyttöjärjestelmä (GNU) ja ohjelmia.

IEEE *Institute of Electrical and Electronics Engineering,* kansainvälinen tekniikan alan järjestö.

MANET *Mobile Ad-Hoc Network,* Ad-Hoc-tyyppinen verkko, jossa laitteet eivät ole kiinteitä.

MIMO *Multiple Input Multiple Output*, Langattomissa 802.11 -standardin laitteissa käytetty useamman antennin hyödyntämismenetelmä.

OFDM *Orthogonal Frequency-Division Multiplexing.* Langattomissa verkoissa käytetty modulointitekniikka.

OLSR *Optimized Link-State Routing Protocol*, avoin ja standardoitu reititysprotokolla.

PGP *Pretty Good Privacy,* viestien salaukseen tarkoitettu ohjelma.

SOWN *Secure, Open Wireless Network,* SSL-varmenteisiin perustuva ehdotus avoimen langattoman verkon suojaamiseksi.

SSL *Secure Socket Layer,* Digitaalisiin varmenteisiin perustuva protokolla, jota esimerkiksi pankkipalveluissa käytetään.

WLAN *Wireless Local Area Network,* langaton lähiverkko.

QAM *Quadrature Amplitude Modulation*, modulaatiomenetelmä, jossa sekä signaalin vaihetta että amplitudia muunnetaan halutun binaariluvun (symbolin) välittämiseksi.

1 Johdanto

Tämän insinöörityön tarkoitus on esitellä langatonta 802.11-lähiverkkostandardin tekniikoita yleisesti sekä tutustua tukiasemattomiin langattomiin verkkoihin. Työssä tutustutaan sellaisiin tukiasemattomiin lähiverkkoratkaisuihin, tekniikoihin, protokolliin, toteutuksiin sekä projekteihin, jotka voisivat tuoda lähiverkon sekä internetin myös esim. köyhien maiden ulottuville.

Työssä käsitellään harrastelijapohjalta lähteneitä projekteja, joiden tarkoitus on hyödyntää tukiasemattomia, langattomia verkkoja luovalla ja uudenlaisella tavalla. Esittelen projektin, jonka pyrkimys on tuoda internetyhteys köyhään kaupunkiin. Esittelen myös kaksi sellaista projektia, joiden tuotosta käyttämällä voidaan mahdollistaa verkon toimivuus sellaisissa hätä- ja erikoistilanteissa, joissa varsinainen puhelinverkko ei syystä tai toisesta toimi, tai kestä poikkeustilanteen aiheuttamaa ylimääräistä kuormaa. Esittelen myös joukon vähemmän tunnettuja nimenomaan langattomiin lähiverkkoihin kehitettyjä reititysprotokollia.

Dokumentin tarkoitus on pyrkiä kertomaan tekniikoista, toteutuksista, tulevaisuudennäkymistä sekä tekniikoiden tuomista mahdollisuuksista ymmärrettävällä ja kansantajuisella kielellä. Tarkoitukseni on, että lukija saa työstäni perusajatuksen reitityksestä. Lisäksi pyrin siihen, että tämä työ antaa lukijalle ymmärrystä siitä, mistä Ad-Hoc- ja erityisesti mesh-verkoissa on kyse, millaisia käyttökohteita ja ongelmia näihin liittyy, sekä hieman kuvaa siitä, millaisia asioita tällaiset verkot voivat suotuisasti kehittyessään mahdollistaa.

Tämä insinöörityö on kirjoitettu jokaiselle, joka on kiinnostunut tekniikan tuomista mahdollisuuksista siitäkin huolimatta, että kyseisten tekniikoiden käyttöönotto ei toistaiseksi olisi taloudellisesti kannattavaa. Työ on kirjoitettu halusta auttaa lukijaa ymmärtämään vaihtoehtoisia ajatus- sekä toimintamalleja tietoverkkoja toteuttaessa. Tavoitteeni on, että lukija saa sekä yleistä, konkreettista että teknistä ymmärrystä tietoverkkojen soveltuvuudesta sekä suunnittelusta uudenlaisiin, mahdollisesti haastaviinkin olosuhteisiin, tilanteisiin ja ympäristöihin.

Uskon, että suurin osa uusista ideoista, ajatuksista ja tekniikoista on lähtenyt liikkeelle nähdystä epäkohdasta sekä halusta korjata se, onnistumisesta tai lopputuloksesta huolimatta.

Hakkerikulttuurin edustajana sekä osana yhteiskuntaa koen paitsi kunnia-asiaksi, myös eettiseksi velvollisuudekseni jakaa kaikki tekninen tietoni ja osaamiseni jokaisen ideasta, asiasta tai tekniikasta kiinnostuneen kanssa.

Tulevana insinöörinä ja tekniikan alan osaajana minulle on kunnia-asia käyttää osaamistani siten, että edistän toiminnallani jokaisen oikeuksia vapaaseen tiedon ja kulttuurin jakamiseen tietotekniikkaa hyödyntämällä.

Käsitteitä ja termistöä-osuudessa kerron pintapuolisesti tässä työssä käytetyistä keskeisimmistä termeistä, käsitteistä sekä konsepteista. Selitän tukiasemallisen ja tukiasemattoman verkon erot sekä reitityksen peruskonseptin. Kerron myös, mitä eroa on vapaalla ohjelmalla ja avoimella lähdekoodilla.

WLAN-verkoista yleisesti-osuudessa tutustutaan 802.11-standardissa tänä päivänä yleisesti käytettäviin tekniikoihin, kuten modulointiin, lähetteen paloitteluun sekä useamman antennin yht' aikaiseen käyttöön lähetyksessä.

Ad-Hoc-verkot-osuudessa kerron yleisesti Ad-Hoc-verkoista, niiden ominaisuuksista, niihin liittyvistä pulmista, käytetyistä tekniikoista, reititykselle asetettavista vaatimuksista sekä eroista tukiasemallisiin ratkaisuihin verraten.

Projektit ja tekijät-osiossa kerron tapahtumista, järjestöistä, meneillään olevista sekä päättyneistä projekteista, joiden tarkoitus on edistää, kehittää tai hyödyntää Ad-Hoc-verkkoja uudella tavalla. Käsittelen hieman tarkemmin erästä kaupunkitason WLAN-toteutusta, jossa nuori opiskelija tarjoaa kotiseudulleen langattoman internetyhteyden käyttäen mesh-verkkoja lähes koko verkon luomisessa.

Protokollat ja reititys-osiossa syvennytään nimenomaan mesh-verkkoihin suunnitelluista reititys-, määrittely- ja tiedonkeruuprotokollista sekä niiden erityispiirteistä ajatellen nimenomaan langatonta reititystä ajatellen. Lisäksi kerron langattomaan reititykseen liittyvistä ongelmista.

Tietoturva-osiossa kerrotaan yleisesti internetissä käytettyjen protokollien ongelmista sekä niihin liittyvistä ratkaisuista. Osiossa tutustutaan lyhyesti konseptiin turvallisesta, avoimesta langattomasta verkosta. Osiossa valotetaan myös SSL-varmennusta ja PGP-salausta.

Yhteenvedossa niputan yhteen ne asiat ja havainnot, jotka olen tätä työtä kirjoittaessa tehnyt tai oppinut.

2 Käsitteitä ja termistöä

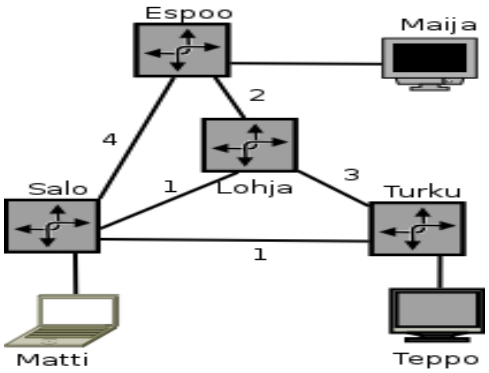
Tukiasema on laite, joka luo verkon sekä välittää liikenteen siihen liittyneille laitteille. Tukiasemaan nojautuvassa ratkaisussa kaikki liikenne kulkee tukiaseman kautta, jolloin koko verkon toiminta on myös riippuvainen tukiasemasta. Tällainen malli on toimiva, edullinen ja usein tehokas lähestymistapa silloin, kun tukiaseman tiedetään olevan vakaassa ympäristössä ja sen kuuluvuusalue kattaa koko fyysisen verkkoalueemme.

Tukiasemattomassa verkossa ei tällaista laitetta ole. Yksinkertaisimmillaan Ad-Hoc-verkon laitteet keskustelevat suoraan toistensa kanssa, ilman välikäsiä. Tällöin halutun verkon jokainen laite on toistensa kantomatkan ulottuvilla sekä yhdessä verkkoalueessa tai *segmentissä*.

Tämä työ käsittelee edellä mainitun kaltaisia verkkoja muutamaa laitetta suuremmissa verkoissa. Tällaisissa verkoissa osa laitteista sijaitsee toistensa kuuluvuusalueen ulkopuolella. Tällöin laitteille täytyy voida kertoa jokin *reitti*, jota pitkin toiselle laitteelle, eli *solmulle* tarkoitettu viesti lähetetään.

Tätä reittien välitystä varten on kehitetty erilaisiin tilanteisiin ja vaatimuksiin soveltuvia reittien välitys- ja havainnointikieliä, *reititysprotokollia*. Reititysprotokollaa ajavaa laitetta nimitetään *reitittimeksi*. Se yhdistää yhden tai useamman verkon solmut toisiinsa.

Reititysprotokolla on siis verkon reitittimien välinen kommunikointikieli. Yleisesti puhuen reititysprotokollien päätarkoitus on sekä kertoa toisille reitittimille, mitä kautta vastaanottajalle osoitettu viesti pitäisi seuraavaksi lähettää.



Kuva 1: Reititys

Tarkastellaan kuvaa 1 ensin Lohjan reitittimen kannalta. Reititin kertoo Saloon ja Turkuun, että sillä on yhteys Espooseen etäisyydellä 2. Reititin kertoo Espoolle, että sillä on yhteys Saloon ja Turkuun etäisyydellä 1 ja 3. Salolla on yhteys Espooseen etäisyydellä 4, ja Turkuun etäisyydellä 1. Lohja saa tiedon Salosta, että sitä kautta etäisyys Turkuun on 1. Lohja laskee, että 2 < 3, joten oletusreitti Lohjasta Turkuun kulkee Salon kautta. Kun Matti haluaa lähettää viestin Maijalle, reitti kulkee Salo-Lohja-Espoo. Kun Maija haluaa jutella Tepolle, reitti on Espoo-Lohja-Salo-Turku.

Reititys langattomassa lähiverkossa toimii pitkälti saman perusajatuksen mukaan, mutta koska yhteydet ovat epävarmoja, ovat reititysprotokollalle asetettavat vaatimukset toisenlaisia.

Langaton tiedonsiirto tapahtuu radioaalloilla. Radioaalloilla viestit sovitetaan *siirtotielle*, jotta se kulkisi häiritsemättä toisia lähetteitä ja jotta se voitaisiin vastaanottajan päässä myös erottaa siirtotien muusta taustahälinästä. Tätä sovittamista sanotaan *modulaatioksi.* Yksinkertaisia modulointitapoja ovat esimerkiksi AM (*Amplitude Modulation*), jossa kiinteän taajuuden *amplitudia* muutellaan siirrettävän informaation tahdissa.

Amplitudilla tarkoitetaan signaalin ylä- ja alahuippuarvon välistä erotusta, signaalin voimakkuutta. Esimerkiksi äänen voimakkuus on sitä kovempi, mitä suurempi sen amplitudi on.

Vapaalla ohjelmalla tarkoitetaan ohjelmaa, joka antaa käyttäjälleen vapaudet käyttää, opiskella, muuttaa sekä levittää ohjelmaa ja sen lähdekoodia joko sellaisenaan tai muutettuna käyttäjän haluamalla tavalla [1.]. Lähde-

koodin edellytetään myös olevan ohjelmoijalle ymmärrettävässä muodossa, ei esimerkiksi binaarinä.

3 WLAN-tekniikoista yleisesti

IEEE 802.11 on kokoelma WLAN-verkkoihin liittyviä standardeja. Tänä päivänä kuluttajille on tarjolla 802.11ac-standardi, jonka teoreettiseksi enimmäisnopeudeksi luvataan 1 Gbit/s. Tämä teoreettinen maksiminopeus kuitenkin vaatii useamman lähetin-vastaanotinparin, lyhyen etäisyyden sekä hyvän radiosään. Verkon radioalueella ei saa olla muita lähetteen kanssa päällekkäin meneviä lähetteitä. Tällaiset lupaukset ovat aina joko teoriaa tai myyntipuhetta, eikä ne käytännössä koskaan toteudu.

Kehitteillä on myös 802.11HEW (*High Efficiency WLAN*) -standardi. IEEE 802.11HEW Study Group (SG) on pitänyt asian tiimoilta konferensseja, tapaamisia ja keskusteluita, viimeksi maaliskuussa 2014, mutta varsinainen työryhmä (Task Group, TG):n on tarkoitus aloittaa toimintansa heinäkuussa 2014 [2].

802.11HEW:n tarkoitus on toimia jo käytössä olevien 2.4 GHz sekä 5 GHz taajuuksien lisäksi sekä 1 GHz että 6 GHz taajuuksilla, kunhan ne tulevat saataville [3].

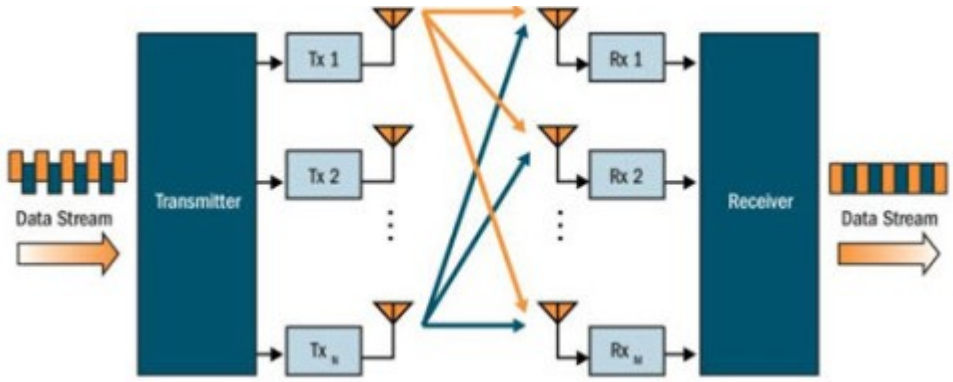
3.1 MIMO-tekniikka

Multiple Input Multiple Output on tekniikka, joka mahdollistaa useamman kuin yhden lähettimen ja vastaanottimen käytön tiedonsiirrossa. Tekniikka tuli käyttöön 802.11n-standardin myötä. Tämä parantaa radiosignaalin tiedonsiirtokykyä, kun lähetys ja vastaanotto eritellään käytetyn kanavan eri taajuuksille. MIMO kasvattaa suoritustehoa ja kuuluvuutta ilman kaistanleveyden lisäämistä, mutta radion lähetystehoa täytyy samalla kasvattaa useamman antennin takia. [5]

Vanhemmissa 802.11g-sarjan reitittimissä saattaa myös olla kaksi antennia, mutta tämä ei ole MIMO-tekniikkaa, vaan .11g -standardissa on mahdollista käyttää eri antenneja lähetykseen ja vastaanottamiseen. Tämäkin parantaa suorituskykyä, mutta ei hyödynnä useampia lähetin-vastaanotin-pareja. MIMO-tekniikkaan liittyy olennaisesti myös *Spatial Multiplexing*, josta lisää seuraavassa luvussa.

3.2 Spatial Multiplexing -ominaisuus

Spatial Multiplexing tarkoittaa, että viesti pilkotaan laitteen useammalla lähettimelle yht' aikaa lähetettäväksi. Koska lähettimet käyttävät omia, fyysisesti erillään olevia antenneja, niiden lähetteet myös saapuvat eri aikaan vastaanottajalle. Lisäksi lähetteet heijastuvat tilan pinnoista, jolloin myös pakettien fyysinen reitti poikkeaa jonkin verran. Lähete pilkotaan pieniin osiin ja lähetetään yhdessä aikajaksossa. Vastaanottaja kokoaa viestin osat, ja lopputulos on alkuperäinen viesti. Idea on siinä, että hajottaminen ja kokoaminen useampaa ”kanavaa” pitkin nopeuttaa tiedonsiirtoa jonkin verran. Ilman Spatial Multiplexing -ominaisuutta viestit pitäisi lähettää yhdessä pötkössä.



Kuva 2: Spatial Multiplexing

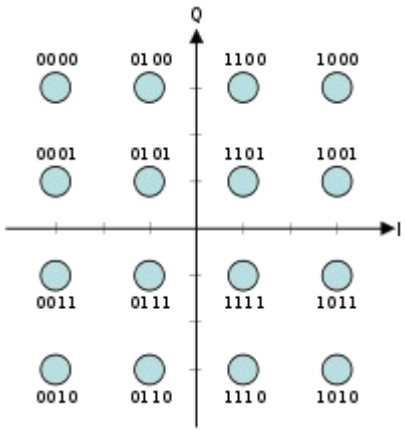
Kuvan tilanteessa viesti pilkotaan kahteen osaan. Lähetin (*Transmitter*) lähettää viestit kahdella antennilla (Tx1 ja Tx3). Vastaanottimen (*Reciever*) viestin palaset saapuvat jokaiselle kolmelle antennille (Rx1...Rx3). Vastaanotin kokoaa tulleet palaset yhteen.

3.3 OFDM- ja QAM-modulointitekniikat

OFDM (*Orthogonal Frequency Division Multiplexing*) on vanha modulointitekniikka, jota käytetään WLAN-verkkojen lisäksi mm. antenniverkon DigiTV:n, WiMAX:n ja 4G-verkkojen yhteydessä.

OFDM-moduloinnissa useita siniaaltoja moduloidaan käyttäen jotakin toista modulaatiomenetelmää, ikään kuin kahta sisäkkäistä modulaatiota. WLAN-verkoissa käytetään 256-QAM-modulaatiota OFDM:n sisällä. [6, s. 17]

Mitä monimutkaisempi modulointitapa on käytössä, sen suurempi symbolinopeus voidaan saavuttaa [6, s. 18]. Symbolinopeuden kasvattaminen toisaalta myös pienentää jokaiselle symbolille jäävää aluetta.



Kuva 3: 16-QAM

QAM-modulointitekniikka perustuu sekä signaalin amplitudin että vaiheen muutteluun siten, että haluttu arvo (symboli) saadaan liitettyä lähetykseen. Haluamme lähettää arvon 0010. Meidän on lähetettävä kompleksiluku (-3, -3i). Vastaanottajalle riittää, että se kuulee signaalin olevan jotain 0010:aa riittävän lähellä olevan luvun, että symbolille tarvitsisi suorittaa korjausta. Tämä korjaus voidaan tehdä yhdelle bitille, joten myös kuvassa olevat binääriluvut on sijoitettu siten, että yksi bitti voidaan nopeasti korjata. WLAN-verkoissa käytetty 256-QAM tarkoittaa, että kompleksiluvuilla voidaan osoittaa 256 eri bittijonoa. Havainnollisesti tämä tarkoittaisi sitä, että kuvan 3 koordinaatistossa olisi niin ikään 256 pistettä.

4 Ad-Hoc-verkot

Ad-Hoc-verkko on yleisnimi sellaiselle verkolle, jossa verkkoalueen laitteet keskustelevat keskenään ilman, että viestejä välitetään tukiaseman kautta.

Tässä insinöörityössä käsitellään mesh-tyyppisiä Ad-Hoc-verkkoja. Mesh-verkolla tarkoitetaan sellaista verkkoa, jossa jokainen verkon laite osallistuu reititykseen. Jatkossa käytetään lyhyesti termiä ”mesh-verkko” tai ”mesh”.

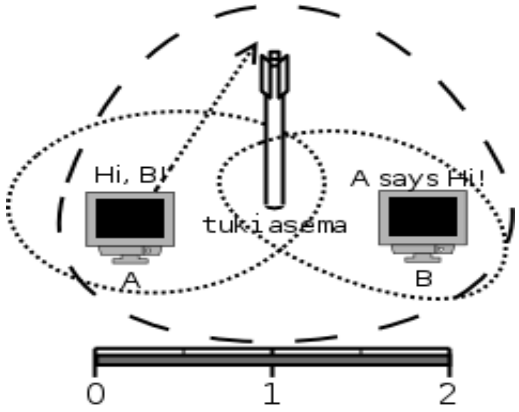
Reititykseen osallistuvaa laitetta nimitetään yleisesti *reitittimeksi*. Jokaisella verkon reitittimellä on tiedossaan reitti toiseen verkkoon tai *solmuun,* joko suoraan tai toisen reitittimen kautta. Kaikki reitittimet tuntevat verkon rakennetta ainakin jollain tavalla. Tuntemuksen taso riippuu verkon suunnittelutavan tehokkuudesta - esimerkiksi siitä, voidaanko useita verkkoalueita yhdistää yhteen ilmoitukseen.

Tukiaseman puuttuminen aiheuttaa erilaisia haasteita ja vaatimuksia verkossa käytettäville tekniikoille. Langattoman siirtotien käyttö vaatii reititysprotokollalta ymmärrystä niin pitkistä *vasteajoista*, pakettien hukkumisesta, häiriöistä kuin lähetys- ja vastaanottovirheistäkin. [4, s. 138]

Langattomalta reititykseltä toivotaan vähäistä kaistankäyttöä, jotta siirtotie olisi käytettävissä myös varsinaisen tiedon siirrolle [4, s. 138]. Niin sanotut tulva- ja silmukkatilanteet (*broadcast storm, routing loop*) eivät käy päinsä, sillä jokainen lähetetty viesti varaa osan siirtotieltä lähetyksen ajaksi. Tällöin toiset samalla kanavalla olevat laitteet myös estyvät kommunikoimasta keskenään.

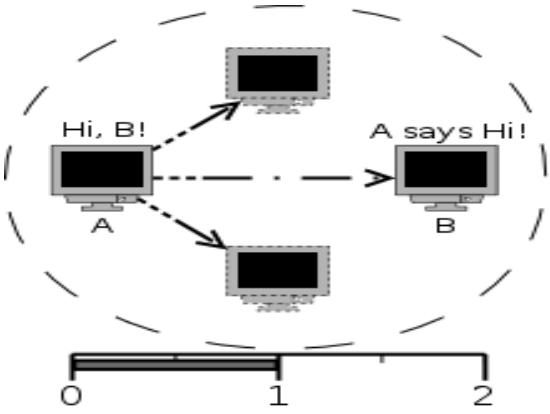
4.1 Ominaisuuksia

Ad-Hoc-tilassa toimivan verkon tiedonsiirtokapasiteetti on teoriassa tukiasemallista verkkoa hieman parempi.



Kuva 4: Verkko, jossa tukiasema

Tukiasemaan pohjautuvassa ratkaisussa (kuva 4) laitteelta A lähtevät viestit joutuvat kulkemaan tukiaseman kautta vastaanottajalle B. Viestin lähetys vaatii itse asiassa kaksi lähetyskertaa – ensin A:lta tukiasemalle ja sitten tukiasemalta B:lle – joten myös lähetysaika on kaksinkertainen. Toisaalta tukiaseman käyttö kasvattaa verkon kuuluvuusaluetta, sillä A:n ja B:n tarvitsee olla vain tukiaseman kanssa samalla kuuluvuusalueella (pitkä katkoviiva), ei toistensa kanssa samalla alueella (pisteviivat).



Kuva 5: Ad-Hoc verkko

Ad-Hoc-tilassa (kuva 5) laite A yksinkertaisesti huudahtaa B:lle osoitetun viestinsä taivaalle. Jokainen laite A:n kuuluvuusalueella kuulee, että A:lla on asiaa, mutta koska viesti on osoitettu B:lle, vain B katsoo viestin sisällön. Tässä lähetysaika on vain yhden viestin lähetysaika, mutta sekä lähettäjän että vastaanottajan on oltava toistensa kuuluvuusalueella. Tämän vuoksi mesh-verkoissa käytetään reititystä, jotta erillisillä kuuluvuusalueilla olevat laitteet saadaan yhdistettyä ja viestit kulkemaan.

Ad-Hoc-verkon siirtonopeus yhden solun sisällä on karkeasti ajateltuna se siirtonopeus, jonka ”sääolosuhteet” sekä laitteistot sallivat. *Siirtonopeudella* tarkoitetaan koko yhteyden kaikkea siirtonopeutta (data + signalointi + salaukset + reititys), ei pelkkää ns. *tehollista* kapasiteettia.

Liikkuvuuteen sopeutuvaa langatonta Ad-Hoc-verkkoa nimitetään myös MANET:iksi (*Mobile Ad-Hoc Network*). MANET:n täytyy myös selviytyä eräästä siirreltävyydestä aiheutuvasta ongelmasta: miten taataan, että asiakkaan yhteydet, kuten puhelut eivät katkea siirryttäessä paikasta toiseen?

Toinen liikkuvuuteen liittyvä ongelma on IP-osoitteiden säilyvyys tai uudistaminen mahdollisimman pian, kun laite ilmestyy - tai siirtyy - verkosta toiseen. Miten laitteiden IP-osoitteet, oletusyhdyskäytävä ja nimipalvelinasetukset määritellään, jos verkkoalue äkkiä muuttuu?

Yritysverkoissa nämä kaksi pulmaa ratkaistaan ns. *roaming*-toiminnallisuudella. Tämä voidaan toteuttaa esim. siten, että eri verkot on *tunneloitu* toisiinsa. Kun päätelaite ottaa yhteyden verkkoon, se pyytää DHCP-palvelimelta (*Domain Host Control Protocol)* IP-osoitteen. Jos päätelaite siirtyy toiseen verkkoon, on uusi verkko tunneloitu siihen verkkoon, josta laite alun perin osoitteen sai. Liikenne ohjataan tunnelin kautta alkuperäiseen verkkoon ja sitä kautta kohteeseensa. Tällainen ratkaisu toimii luotettavissa ja nopeissa lankaverkoissa, mutta aiheuttaa paljon liikennettä alkuperäistä verkkoa kohti. Jos alkuperäinen verkko sijaitsee monen hypyn päässä, voi tästä aiheutua kohtuutonta ruuhkaa puhtaasti langattomissa verkoissa.

Kaupunkiverkoissa (*Municipal Wireless*) voidaan roaming-pulmaan myös osittain vastata määrittelemällä päätelaitteiden osoitteet kiinteiksi. Jos käy-

tetään esim. 10.0.0.0/8-verkkomaskia, saadaan yhteen verkkoalueeseen sopimaan jopa 16,7 miljoonaa laitetta. Kaupunkitasolla tällainen osoitemäärä riittäisi vallan mainiosti useimpiin tilanteisiin.

Yksi ratkaisuajatus voisi olla ns. hybridit, joissa yksi tai useampi reunareititin olisi yhteydessä jotain kautta (kuten Internet) toisiin reunareitittimiin. Samalla voitaisiin yhtä hyvin toteuttaa pääsy myös julkiseen internetverkkoon näiden reunareitittimien kautta.

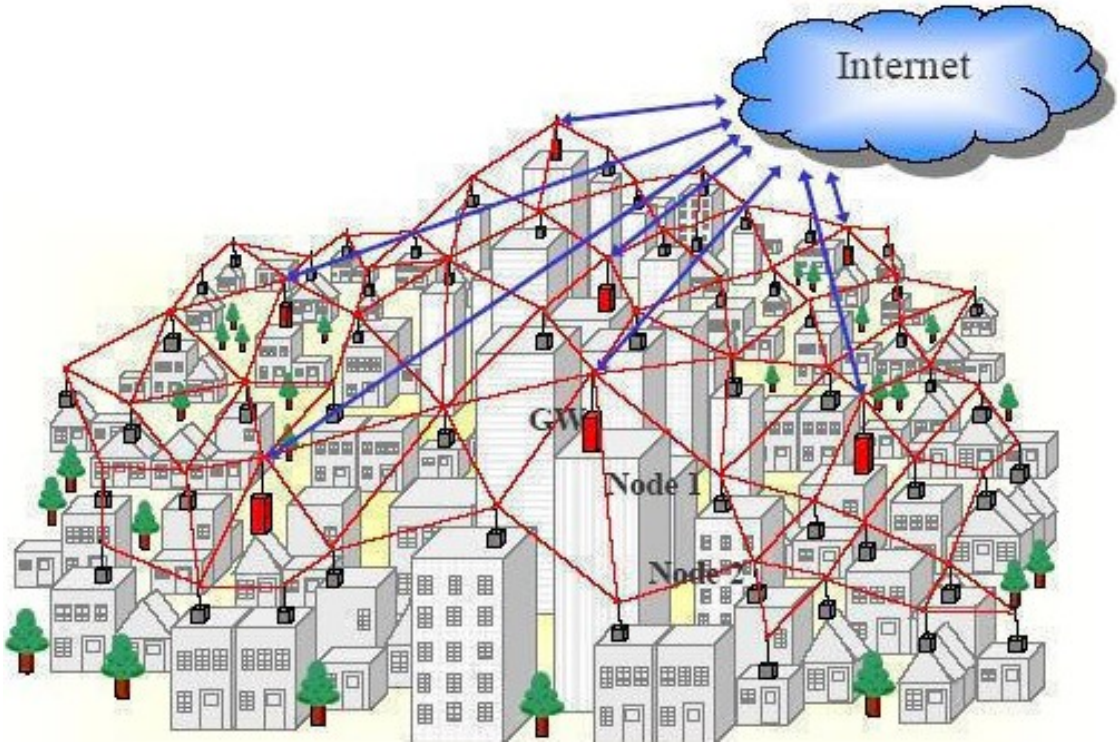
Tällaisessa ratkaisussa käytettäisiin sopivaa vikasietoisuusprotokollaa, kuten VRRP (*Virtual Router Reduncancy Protocol*) tai CARP (*Common Address Redundancy Protocol*). Protokollien päätoiminto on siirtää liikenne kulkemaan toisen *reunareitittimen* kautta siinä tilanteessa, että alkuperäinen laite vikaantuu tai sen yhteys katkeaa. Tämä toiminto toteutetaan luomalla näennäinen, ns. *virtuaalinen* reititin. Tämän virtuaalisen reitittimen osoite kerrotaan päätelaitteille reitiksi ulkomaailmaan. Käytetty vikasietoisuusprotokolla pitää huolen siitä, mikä reunareititin milloinkin vastaa virtuaalisen reitittimen osoitteeseen kulkeviin pyyntöihin.

Päätelaitteille, kuten tietokoneille ja matkapuhelimille riittää usein ns. oletusyhdyskäytävä, aliverkon peite, nimipalvelin sekä IP-osoite. Nämä tiedot on jollain menetelmällä tarjottava ja uusittava siirtymistilanteessa.

IP-osoitteiden tarjoamiseen yleisesti käytetty DHCP-protokolla tarjoaa ns. *Lease Time* -tietueen, jolla IP-osoitetta pyytävälle laitteelle voidaan pakottaa osoitteen uusimisaikaväli. Jatkuva verkon kysely mahdollisesti uutta IP-osoitetta varten ei kuitenkaan tunnu kovin järkevältä ajatukselta, varsinkaan jos langattomassa verkossa on useita laitteita ja uusimisväli on kovin lyhyt.

Kolmas pulma muodostuu verkon fyysisestä rakenteesta. Ajatellaan tilanne, jossa solmut A, B ja C ovat peräkkäin siten, että C ei ole A:n kantoalueella. Jos solmu B katoaa, katoaa myös yhteys solmujen A ja C välillä. Jos solmu B siirtyy solmun A kantoalueelle, mutta solmu C:n kantoalueen ulkopuolelle, ei yhteyttä solmujen A ja C välillä edelleenkään ole. Joko A:n täytyy saada tai laskea itse reitti C:hen jotain toista kautta, tai todeta C:n olevan saavuttamattomissa.

4.2 Mesh-verkot



Kuva 6: Mesh-verkko kaupungissa.

Kuvan 6 mesh-verkko on käytännössä muuttumaton. Verkon laitteet ovat suoraan tai toistensa kautta yhdyskäytäviin (GW), jotka ovat edelleen yhteydessä Internetiin.

Mesh-verkko on yksi Ad-Hoc-verkon muoto. Mesh-verkolla tarkoitetaan sellaista Ad-Hoc-verkkoa, joka koostuu aktiivilaitteista, kuten jo mainituista reitittimistä ja silloista (*bridge*). Sillalla voidaan yhdistää kaksi fyysisesti toisistaan eroavaa verkkoa, (esimerkiksi satelliitti- ja lankaverkko) toisiinsa.
Niin sanotussa *Full Mesh* -verkossa jokaisella solmulla on suora yhteys jokaiseen toiseen solmuun. Langattomiin mesh-verkkoihin liitetään usein myös ajatus laitteiden liikkuvuudesta, koska fyysinen kaapelointi ei ole tarpeen.

4.3 Käyttökohteet

Ad-Hoc-verkkoja toteutettiin alun perin lähinnä sotilaskäyttöön, mutta muutamia vuosia sitten sekä standardien kehityksen alettua ja edettyä sekä Ad-Hoc– että mesh-verkkoja alettiin käyttää myös muihin tarkoituksiin.

Muutamia mesh-verkkoja hyödyntäviä projekteja ovat esimerkiksi *One Laptop Per Child* (myöh. OLPC) sekä *Kansas City Free Network*. Hätätilanteen kommunikointitarpeisiin mesh-verkkoja hyödyntää *Project SPAN*. Tekniikoiden ja standardien ympärille syntyi myös reititysprotokollia, laitteita ja ohjelmistoja kehittäviä projekteja, kuten *B.A.T.M.A.N.* sekä *FreedomBox.* Verkkojen toteutusalustoja ja malleja kehittää *Free Network Foundation* sekä *guifi.net*. Kaikkia näitä harrastajia, projekteja ja järjestöjä yhdistämään on perustettu *BattleMesh*-kokoontumistapahtuma. Projekteista lisää myöhemmin kohdassa ”Toteutukset”.

Mesh-verkon voi toteuttaa paitsi täysin langalliseksi, myös osittain tai täysin langattomaksi. Täysin tai osittain langattomat toteutukset sopivat hyvin toteutettuna sellaisiin ympäristöihin, jossa fyysisen kaapelin veto laitteiden välille olisi joko kallista, mahdotonta tai molempia. Kompromissina on tietysti yhteyden luotettavuus ja nopeus, mutta joskus hidas ja epäluotettavakin yhteys on käyttökelpoisempi kuin ei yhteyttä ollenkaan. Kansas City Free Networkin vaikutus on tästä hyvä esimerkki.

Wireless Networking in Developing World -kirja käsittelee nimensä mukaisia toteutuskohteita, eli langattomien verkkojen toteuttamista kehittyviin maihin. Koska jatkuvaa sähkönsyöttöä ei tällaisessa ympäristössä voida aina taata, tulee tietoverkon palautua toimintakuntoon sähkön palattua ja ilman minkäänlaisia huolto- tai ylläpitotoimenpiteitä. Yksi kirjan 17 luvusta kertoo ns. *off-grid*-sähkönsyötöstä, eli sellaisesta tilanteesta, jossa laitteiston on toimittava irrallaan virallisesta sähköverkosta esimerkiksi tuuli-, vesi- tai aurinkoenergiaan nojautuen. [4] Teos mainitaan työssä nimeltä, sillä se on toiminut mm. Ghanan yliopiston referenssiteoksena [39].

4.4 Perusteluita ja toteutustapoja

Sekä Ad-Hoc- että mesh-verkot puoltavat asemiaan sellaisissa paikoissa ja tilanteissa, joissa joillekin tai millekään tukiasemalle ei voida taata jatkuvaa sähkönsyöttöä. Esimerkiksi OLPC-projektille tämä on yksi peruste käyttää nimenomaan tukiasematonta verkkoa. Vaikka joltain verkon alueelta katkeaisi sähkö, voidaan muiden verkon solmujen liikennöinti reitittää jotain toista kautta. Koko verkko ei kaadu, vaikka yksi tai useampi alue putoaisi pois syystä tai toisesta.

Vaikka tukiasemattomuus tuokin mukanaan omat haasteensa, voidaan toteutusmallilla kuitenkin tuoda langaton verkko sellaisiin paikkoihin, jonne fyysiset kaapelit ja perinteiset tukiasemalliset ratkaisut sopivat heikommin.

Joskus kommunikaatio ei saa katketa siinäkään tilanteessa, että alueelta katkeaisi sähkönsyöttö tai että virallinen puhelinverkko tukkiintuisi. Tällaisia tilanteita on esimerkiksi hätäapujoukkojen kommunikaatio katastrofitilanteissa. Mesh-verkoilla voidaan kiertää esim. katastrofitilanteessa puhelin- tai internetverkon kaatumisesta aiheutuva hätäavun tiedonkulun estyminen. *ProjectSPAN* -projektin pyrkimys on tarjota ratkaisuja juuri tähän ongelmaan.

Jos verkko toteutetaan puhtaasti avoimilla standardeilla, laitteilla sekä vapailla ohjelmilla, saadaan lopputuloksena yhdestä valmistajasta, poliittisista toimenpiteistä sekä itse verkkotekniikkaan liittymättömistä ongelmista vapaa verkko. Verkko voidaan rakentaa reitittämään ongelma-alueen ohi niin, että tähän ei ole poliittista valtaa kellään.

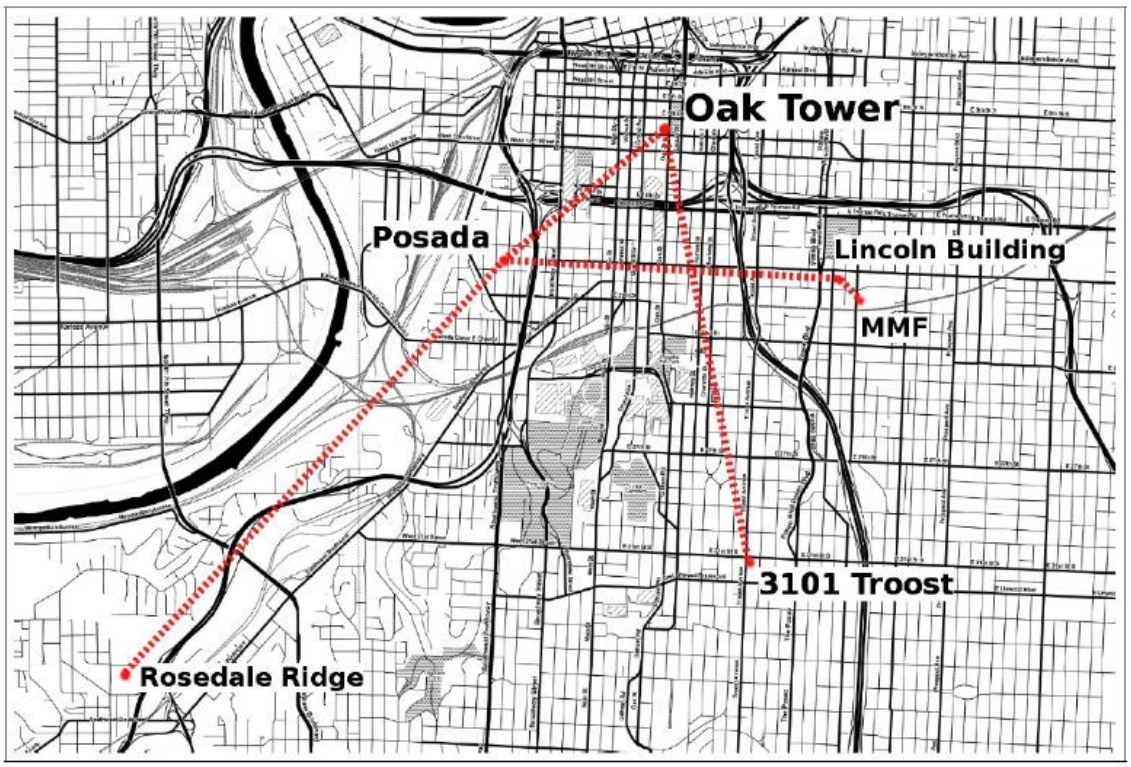
Joidenkin mesh-verkkoja hyödyntävien projektien tavoitteet ovat myös puhtaasti ideologisia: *FreedomBoxi*n pyrkimys on palauttaa internet takaisin juurilleen. Projekti vannoo hajautettujen palveluiden ja verkkojen nimiin, toivoen niiden vapauttavan käyttäjänsä keskitetyltä seurannalta, hallinnalta tai jopa vakoilulta.

5 Projektit ja tekijät

5.1 Free Network Foundation ja Kansas City Freedom Network

Free Network Foundation (myöh. FNF) on **Isaac Wilder**in perustama järjestö, jonka pyrkimys on tarjota työkalut, joilla vapaa internetyhteys voidaan taata kaikelle kansalle. Järjestö tarjosi internetyhteyden mm. *Occupy Wall Street* -ryhmän aktivisteille vuonna 2011.

Parhaillaan FNF panostaa vapaan verkon, *Kansas City Freedom Network:in* (myöh. KCFreeNet) toteuttamiseen ja laajentamiseen Kansas Cityn alueella [8]. Kansas City valittiin kohteeksi paitsi siksi, että Wilder on kotoisin Kansas Citystä, mutta myös siksi, että kaupallisen tarjonnan ratkaisu katsottiin paitsi eriarvoistavaksi, myös mahdottomaksi kustantaa kaupungin talousahdingon ja alueen köyhyyden vuoksi [9]. FNF yhdisti voimansa *Connecting for Good* sekä *guifi.us* -järjestöjen kanssa kesällä 2013.



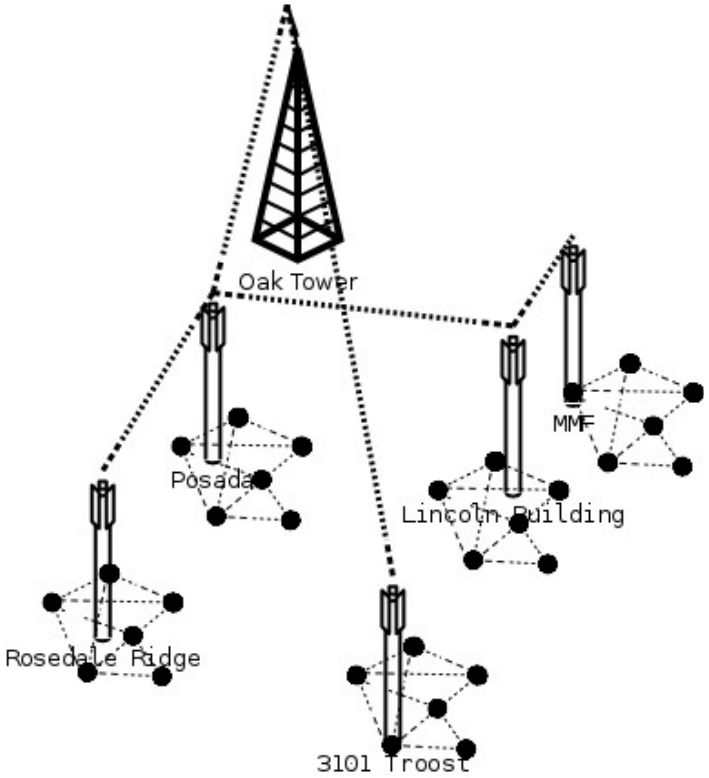
Kuva 7: KCFN:n verkko elokuussa 2013

Kuvassa 7 näkyy KCFreeNet:in rakenne. Päälinkki sijaitsee *Oak Tower*:ssa, ja se tarjoaa yhteyden *Posadan*, *3101 Troost*:n sekä *Rosedale Ridge*:n mastoille. Posada tarjoaa yhteyden *Lincoln Building*:n sekä *Mutual Musician Foundation*:n (kuvassa MMF) mastoille.

Wilder katsoo projektin merkittävimmäksi saavutukseksi Rosedale Ridgen yhteyden: "*So I think the most significant thing to have happened is that the Rosedale Ridge project, ... It's providing connectivity to about 200 families, only one of which, I believe, had connectivity in their home before the network was built. So it's quite a difference in the lives of these couple hundred families. ... Because Rosedale Ridge is up on top of a big hill, and there's poor bus service, it has always had trouble leasing out their apartments. Since the installation of the network, they have leased every apartment in the complex.*" - Isaac Wilder [9].

KCFreeNet:n mallissa luodaan oma, alueellinen verkko. Nämä alueelliset verkot yhdistetään ensin toisiinsa, sitten alueelliseen tukiasemaan ja edelleen internetiin. Alueelliset tukiasemat voidaan vielä tunneloida toisiinsa käyttämällä internetiä siirtotienä.

KCFreeNet:n mallissa verkko koostuu vähintään kolmesta osasta: linkistä (*FreedomLink*), mastosta (*FreedomTower*) sekä solmusta *(FreedomNode)*.



Kuva 8: Periaate FNF:n mallista

Kuvassa 8 *Oak Tower* toimii KCFreeNetin linkkimastona, FreedomLink:inä. FreedomLink tarjoaa yhteyden kahdelle naapuruston mastolle, FreedomTowerille. FreedomTowerit ovat keskenään mesh-verkossa. *Posada*-masto tarjoaa yhteyden Rosedale Ridgelle sekä Lincoln Building:lle. Lincoln Building tarjoaa Posadalta saamansa yhteyden edelleen MMF:lle (Mutual Musician Foundation -järjestön päämaja).

Kaikki FreedomLinkit toimivat siltana oman mesh-verkkonsa alueelle ja välittävät jälleen niihin yhteydessä oleville FreedomNodeille yhteyden. FreedomNodet ovat taas yhteydessä toisiinsa ja toimivat siltana, tarjoten paikallisen verkon esimerkiksi ethernetillä.

FreedomNode on päätelaite, joka tarjoaa laitteen kantoalueelle langattoman verkon. Laite yhdistää alueen muut FreedomNodet toisiinsa mesh-verkon kautta, sekä toimii siltana *FreedomToweriin*.

FreedomTower on torni, joka yhdistää naapurustot olemalla toisiin FreedomTowereihin, niin ikään mesh-verkon kautta. FreedomTowerit voivat ajaa

useita reititysprotokollia, kuten OLSR, B.A.T.M.A.N. tai Babel. FreedomTower on edelleen yhteydessä *FreedomLink*:iin.

FreedomLink on alueellisen verkon päätepiste välittäen lopulta internetiin kuuluvat viestit sinne. Laite keskustelee BGP (*Border Gateway Protocol)* -protokollan avulla internetin toisten reitittimien kanssa. FreedomLinkillä voidaan myös tehdä tunneli (*FreedomTunnel*) toisiin FreedomLinkeihin, jolloin useita verkon alueita saadaan yhdistettyä toisiinsa.

Wilder katsoo, että vapaiden verkkojen mallissa ei ole yhtä ainoata rahoitustapaa. Jokainen verkkoalue (*site*) saa päättää mallistaan. Verkot voisivat rahoittaa toimintansa esimerkiksi voittoa tavoittelemattomana järjestönä, julkisena toimijana tai erilaisten kampanja- ja yhteisötointen kautta. [9 s. 130]

5.2 BattleMesh–kokoontumistapahtuma

BattleMesh on pienimuotoinen tapahtuma, jossa alan harrastajat, hakkerit sekä ammattilaiset kokoontuvat yhteen edistääkseen ja kehittääkseen mesh-verkkojen tekniikoita, ohjelmia, protokollia ja muita projekteja. Tapahtuman teemana ovat mm. reititysprotokollien ja niiden suorituskyvyn kehittäminen, testaus, parantaminen sekä ylipäätään eri tekijäryhmien ideoiden jakaminen, kehitys ja toteutus. Seuraava BattleMesh järjestetään 12. - 18. toukokuuta 2014 Leipzig:ssä, Saksassa.

5.3 One Laptop Per Child -projekti

Projektin tavoite on mahdollistaa jokaiselle maailman lapselle kannettava tietokone. Laitteet (joita projekti kutsuu XO:ksi) suunnitellaan edullisiksi, kevyiksi ja vähävirtaisiksi. Jokainen laite voi toimia mesh-solmuna osallistuen siten alueen langattoman verkon toimintaan (tai sen puuttuessa luoda itse sellaisen).

One Laptop Per Child:n tavoitteena oli alun perin toteuttaa verkko jokaiseen XO-koneeseen siten, että jokainen XO toimisi verkon solmuna. Toteutus kuitenkin kompasteli muun muassa käytetyn reititysprotokollan puutteiden

vuoksi. OLPC on toiminut langattomalle yhteisölle opettavana pioneeriprojektina. Käytetyn HWMP-reititysprotokollan reititys- ja tervehdysviestit tukkivat kaistan, mikäli laitteita kasaantuu useita toistensa kuuluvuusalueelle. Tällainen tilanne voi olla esimerkiksi koulun luokkahuone, jossa voi olla kymmeniä, satojakin koneita suhteellisen pienessä tilassa.

5.4 Wireless Networking in Developing World – kirja

Internetistä ladattavissa oleva 520-sivuinen ja 17-osainen kirja kertoo langattoman verkon toteutuksesta kehittyviin maihin. Kirjassa perehdytään radiotekniikkaan, Ad-Hoc-verkkoihin, tietoturvaan, suunnitteluun, laitteistohankintoihin, sisä- ja ulkokäyttöön, off-grid-sähköistykseen, ylläpitoon sekä taloudelliseen kestävyyteen. Kirjasta on julkaistu 3. painos, ja edellisiä painoksia on tällä hetkellä (11.9.2013) luettavissa kuudella kielellä. Kirja on toiminut referenssinä mm. Ghanan yliopiston kampuksen langattoman verkon toteutuksessa [22].

5.5 ProjectSPAN – mesh-verkkoja älypuhelimilla

GSM-verkot koostuvat soluista, jotka mitoitetaan kestämään tietty määrä laitteita. Kun tämä määrä ylittyy, verkko joko estyy välittämästä kapasiteetin ylittäviä puheluita, tai kaatuu kokonaan. Tällaisia tilanteita voi olla esimerkiksi erilaiset luonnonkatastrofit, joiden projektin perustaja **Josh Thomas** kertoo olevan pääsyitä sekä kantava voima projektille. Thomas nimeää mm. hurrikaani Katrinan (v. 2005) sekä Fukushiman ydinvoimalaonnettomuuden (v. 2011) tällaisiksi katastrofeiksi.

ProjectSPAN muuttaa älypuhelinten ohjelmistoa siten, että laitteen langaton WLAN-piiri saadaan Ad-Hoc-tilaan. Näin puhelin saadaan kytkettyä edelleen mesh-verkkoon, jolloin sitä voidaan käyttää ilman tukiasemaa. Puhelimen verkkoa käyttävät ohjelmat toimivat aivan samalla tavalla kuin ennenkin, sillä ohjelmille näkyviä verkkorajapintoja ei muuteta - ainoastaan alemman tason ohjelmia joka huolehtii tiedonsiirrosta, muutetaan. Projekti haluaa mahdollistaa sen, että katastrofitilanteissa apujoukot pystyvät kommunikoi-

maan keskenään siitäkin huolimatta, että yleinen GSM-verkko kaatuu eikä lähettyvillä ole toimivaa verkkoa apujoukkojen käytettävissä. [11]

5.6 FreedomBox

FreedomBox on ***Eben Moglen***in aloittama projekti, jonka tavoite on paketoida vapautta, yksityisyyttä, sekä tietoturvaa parantava ohjelmistoympäristö pienille, halvoille ja vähävirtaisille plug-in-tietokoneille. Tavoite on, että jokainen FreedomBox-laitteen tai ohjelmiston käyttäjä voisi parantaa sekä yksityisyyttä että tietoturvaansa internetissä. [13]

Ohjelmisto koostuu pelkästään vapaasta ohjelmistosta, jotta käyttäjä voisi niin halutessaan muuttaa sen toimintaa tai varmistaa ohjelmiston tekevän mitä pitääkin, eikä mitään muuta.

Laitteen voi ottaa käyttöön esimerkiksi puhelimella tai toisella lähiverkkoon liitetyllä tietokoneella. Kaikki tähän tarvittava ohjelmisto on olemassa, tehtävä on vain saada se helpoksi ja toimivaksi kokonaisratkaisuksi.

Vaikka projektin virallinen kohdearkkitehtuuri onkin ARM-ytimellä varustettu, puhelinlaturin kokoinen DreamPlug, voi ohjelmistoa ajaa millä tahansa Debian GNU/Linux:n tukemalla laitteistolla - aina perus-PC:stä verkkokovalevyihin ja sulautettuihin projektialustoihin.

Tuotteena FreedomBox on seinään kytkettävä, noin puhelinlaturin kokoinen minitietokone. Laitteen ohjelmisto yhdistää salatun yhteyden muihin tuntemiinsa FreedomBoxeihin viestien, kuten sähköpostin, pikaviestien ja IP -puheluiden välitystä varten. Kiinteän verkkoyhteyden katketessa ohjelmisto liittyy mesh-verkkoon, yrittäen käyttää sitä yhteytenä muihin FreedomBox:eihin. [13]

Alun perin FreedomBoxin piti olla puhtaasti ohjelmistoprojekti, joka paketoi tarvittavat osat yhteen ja yhdistää ne sopivaan laitteeseen. Projektin johtoryhmän jäsen ***Bdale Garbee*** kertoo FOSDEM 2013 -tilaisuudessa antamas-

saan tilannekatsauksessa, että projektilla on kulunut liian paljon aikaa ja voimia suljettujen laiteajureiden kanssa taistellessa. [12]

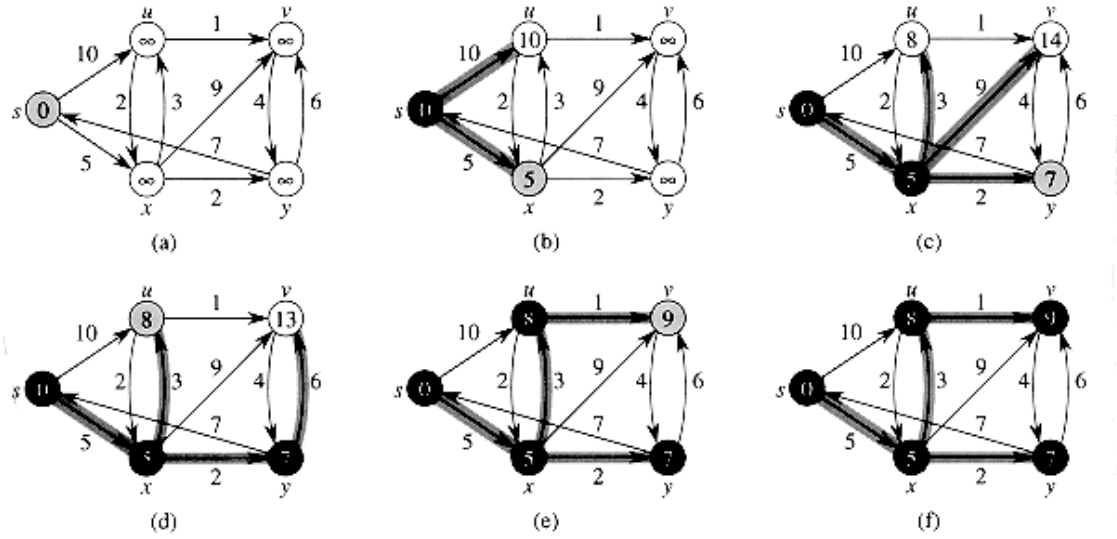
6 Protokollat ja reititys

Jotta mesh-verkon laitteet voisivat välittää viestejä toisille laitteille, täytyy siinä olevien solmujen osata kertoa tuntemistaan reiteistä toisilleen. Tähän tarkoitukseen on kehitetty useita erilaisia reititysprotokollia, jotka soveltuvat kukin erilaisiin ympäristöihin hieman eri tavoin.

Tutustun tässä osiossa muutamaan mesh-verkkoja varten kehitettyä tai kehitteillä olevaan reititysprotokollaan, kuten OLSR *(Optimized Link-State Routing Protocol)*, B.A.T.M.A.N. *(Better Approach To Mobile Ad-Hoc Networking)* sekä Babel.

Ad-Hoc-verkkojen yksi ominaispiirre on usein liikkuvuus, eli jokin laite siirtyy fyysisesti tai topologisesti toisen verkon alueelle. GSM-puhelimen siirtymistä vaikkapa Helsingistä Ouluun voidaan pitää vastaavanlaisena analogiana. Yhteydet eivät saa katketa, eikä siirtyminen saa aiheuttaa käyttäjälle kohtuutonta vaivaa. Parhaassa tilanteessa siirtyminen ei tulisi näkyä loppukäyttäjälle millään lailla. Tätä kutsutaan nimellä ”roaming”. Se on GSM-verkossa onnistuttu toteuttamaan kohtuullisen hyvin, mutta IP-pohjaisissa Ad-Hoc--verkoissa tilanne saattaa olla toinen. Laitteen siirtyessä toiseen aliverkkoon myös IP-osoite vaihtuu.

Reitityksestä puhuttaessa törmätään lähes poikkeuksetta ns. Dijkstran algoritmiin. Algoritmi on sarja loogisia operaatioita, joita toistamalla voidaan laskea lyhin reitti lähteestä kohteeseen.



Kuva 9: Dijkstran algoritmi

Dijkstran algoritmin toimintaperiaate (kuva 9). Lähdetään liikkeelle pisteestä s, ja halutaan tietää lyhyimmät reitit kaikkiin muihin pisteisiin. Katsotaan kyseessä olevasta etäisyydet muihin pisteisiin, (u ja x). Siirrytään sinne, missä on pienin etäisyys (x). Tätä toistetaan, kunnes kaikki pisteet on käyty läpi. Lopuksi lasketaan reittien pienimmät arvot yhteen. Tuloksena on lyhyimmät etäisyydet pisteestä s kaikkiin muihin pisteisiin.

6.1 802.11s -standardi

802.11s on IEEE :n hyväksymä lisäys, joilla tuodaan mesh-verkot 802.11--standardin piiriin. 802.11s tukeutuu jo olemassa oleviin 802.11-standardin verkkolaitteisiin varsinaisessa tiedonsiirrossa. Se ei itsessään ole tekniikka eikä protokolla, vain lisämääritelmä mesh-verkkojen toteutuksista.

Jo mainitussa OLPC-projektissa käytetään 802.11s:n draft-versiossa ehdotettua HWMP-reititysprotokollaa (*Hybrid Wireless Mesh Protocol*). Reititysprotokollan ongelmaksi on osoittautunut siirtotien tukkeutuminen reititysviesteistä, mikäli laitteita kertyy liian tiiviiksi ryppääksi toistensa kuuluvuusalueen kanssa päällekkäin. Sekä 802.11s että OLPC ovat kuitenkin toimineet eräänlaisina pioneeri- ja suunnannäyttäjäprojekteina mesh-verkoille sekä niihin liittyville projekteille.

6.2 AHCP, IP-osoitteiden hallintaprotokolla

Perinteinen DHCP-protokolla (*Domain Host Control Protocol)* sopii usein kiinteisiin tai vain hyvin vähän muuttuviin verkkoihin, mutta mobiileihin tai alati muuttuviin verkkoihin se soveltuu heikommin. Jos reitittävä laite siirtyy loogisesta verkkoalueesta toiseen, niin paitsi verkon topologia, myös monet reitit muuttuvat tästä siirtymisestä johtuen.

AHCP *(Ad-Hoc Configuration Protocol)* on ***Juliusz Chroboczek***in suunnittelema kehitysasteella oleva protokolla, jonka tarkoitus on tarjota IPv6- tai IPv4-osoitteet nimenomaisesti Ad-Hoc-verkon laitteille. Protokollan toimintaperiaate on hyvin samankaltainen kuin DHCP:llä. Protokollasta löytyy toimiva ohjelmakoodi sekä toimintaperiaatteen kuvaava draft-vedos, mutta virallisempaa RFC:tä siitä ei ole [7].

6.3 OLSR-reititysprotokolla

Optimized Link-State Routing Protocol (RFC 3626) on reititysprotokolla, joka on pyritty optimoimaan langattomia verkkoja varten. OLSR-reititin lähettää sekä *Hello* että *Topology Control* -viestejä, joilla havaitaan naapureita kahden hypyn päähän. Tässä luvussa puhutaan myös *OLSRd*:stä, jolla tarkoitetaan vapaan lähdekoodin toteutusta OLSR-reititysprotokollasta.

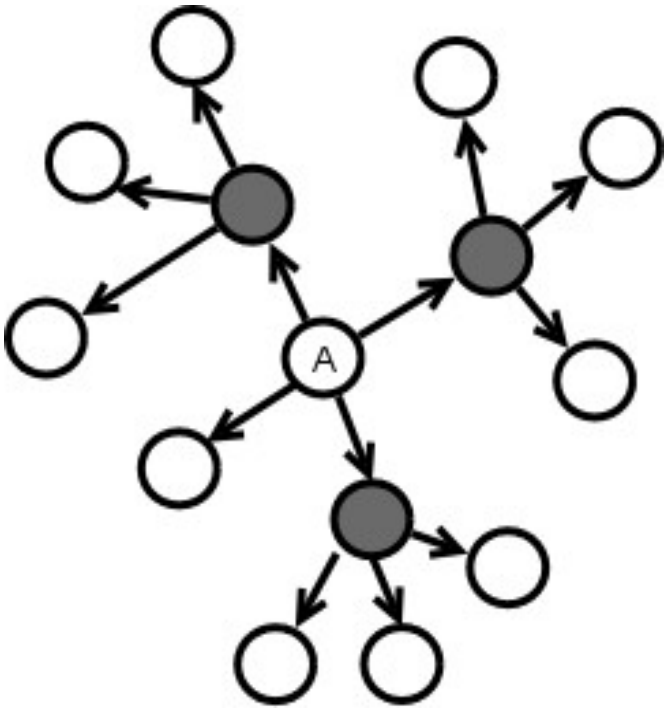
OLSR:n käyttämä, toistuvien tervehdysviestien lähetys (Link-State-reititysprotokollien ominaisuus) toimii hyvin pienessä mesh-verkossa, mutta laitemäärien kasvaessa ne aiheuttavat tarpeetonta liikennettä.

Link-State-reititysprotokollat tarvitsevat reititystietojen synkronointia. Siinä, missä lankaverkossa käytetty OSPF (*Open Shortest Path First*) -protokolla käyttää luotettavuusalgoritmeja reittien valitsemiseen, niin OLSR yksinkertaisesti kuuluttaa topologiatiedot ”riittävän usein”, jotta toisten reitittimien reititystaulukot eivät ajautuisi epäsynkroniseen tilaan pitkäksi aikaa.
Koska reititystaulukon säännöllinen lähetys jokaiseen solmuun aiheuttaa nopeasti skaalautuvuusongelmia, päätettiin OLSR:ssä ottaa käyttöön ns. MPR (*Multipath Relay)* -toiminto.

Vaikka MPR-toimintoa käyttämällä saadaankin jonkin verran kasvatettua verkon kokoa, se ei korjaa Link-State-reitityksen ja OLSR:n toiminnallisista ominaisuuksista aiheutuvaa ruuhkaa.

Kun reititin lähettää tervehdyksen, valitaan MPR:ksi ne reitittimet, joiden kautta kyseinen reititin saa tietoja kahden hypyn päästä. Jokainen reititin kuuluttaa säännöllisesti listan niistä laitteista, jotka ovat valinneet kyseisen reitittimen MPR:ksi.

Näin vähennetään kuormaa, kun koko verkon kaikkia vaihtoehtoisia reittejä ei kuuluteta jokaiselle laitteelle – ainoastaan ns. olennaiset reitit välitetään.



Kuva 10: MPR:n valinta

Kuvassa 10 laite A lähettää ”Hello”-viestin ympäröiville laitteille. Jos vastaanottajalla on tiedossaan lisää reittejä, lähettää se edelleen tiedon eteenpäin lisäten, että A on valinnut hänet MPR:ksi. Harmailla laitteilla on lisäyhteyksiä, joten niistä tulee A:lle MPR-reitittimet.

OLSR on paljon käytetty reititysprotokolla mm. sen vapaan ohjelmiston toteutuksen, OLSRd:n suhteellisen pienen resurssitarpeen ansiosta. Langattomiin kotireitittimiin tarkoitetun DD-WRT-ohjelmiston avulla osoitettiin, että reititys onnistuu OLSRd:llä varsin pienillä resursseilla. Toteutetut verkot ovat muutaman kymmenen reitittimen luokkaa. Suositussa, Linksysin WRT54-sar-

jan tukiasemissa on noin 200 MHz MIPS-suoritin ja vähintään 8 MB keskusmuistia. DD-WRT-ohjelmisto toimii myös lukuisissa muissa langattomissa reitittimissä [14]. OLSR-protokollasta löytyy useita toteutuksia eri käyttöjärjestelmille sekä laitteille, mm. Nokia N900 -älypuhelimelle.

Suhteellisen vähäinen resurssien tarve voi esimerkiksi tarkoittaa sitä, että heikkotehoisilla, muutoin jo tiensä päähän tuomituilla tietokoneilla voidaan toteuttaa ainakin osa OLSR-reititystä käyttävistä mesh-verkoista.

Varhaiset OLSRd:n versiot kärsivät pahoista skaalautuvuusongelmista. Tämä johtui pääasiassa siitä, että reittien laskennassa käytettiin yksinkertaisinta mahdollista Dijkstran algoritmin toteutustapaa. Algoritmin toteutustapa kasvatti verkon sekä reitittimien kuormaa lähes lineaarisesti suhteessa reitittimien määrään.

David Johnsonin, **Ntsibane Ntlatlapa**n sekä **Corinna Aichele**n julkaisema, OLSR:ää sekä seuraavassa kappaleessa käsiteltävää B.A.T.M.A.N.-protokollaa käsittelevä raportti osoittaa vertailussaan OLSR:n olevan varteenotettava vaihtoehto pienikokoisissa verkoissa. Raportin mukaan OLSR-reititysprotokollan kaistantarve kasvaa lineaarisesti suhteessa laitemäärään. Tutkimuksessa käytettiin OLSRd:n versiota 0.5.5. Raportista käy ilmi, että OLSRd:ssä ei ollut tutkimuksen tekohetkellä MPR-toimintoa vielä oletuksena käytössä [15]. Myöhemmin OLSRd:n skaalautuvuutta on parannettu korjaamalla Dijkstra:n algoritmin toteutusta tehokkaammaksi, sekä ottamalla MPR käyttöön oletuksena.

6.4 B.A.T.M.A.N. -reititysprotokolla

a Better Approach To Mobile Ad-Hoc Networking eli ”parempi lähestymistapa mobiileihin Ad-Hoc-verkkoihin” on reititysprotokolla, joka kehitettiin aiemman, nyt jo vanhentuneen OLSR-version pohjalta.

Vanha OLSRd:n versio ei käyttänyt MPR-reitittimien valintaominaisuutta ollenkaan hyväksi, vaan lähetti täydelliset reititystaulukot eteenpäin. Osa OLSRd:n kehittäjistä siirtyi kehittämään B.A.T.M.A.N.:ia.

Edellisessä luvussa mainittu tutkimus osoitti, että B.A.T.M.A.N. skaalautui silloista OLSRd:n versiota paremmin. Vertailukohtina käytettiin lähtevien reititysviestien määrää sekunnissa (vähempi parempi), muistin kulutusta sekä suoritinkuorman tasoa suhteessa solmumäärän kasvuun. Tutkimus osoitti OLSRd:n soveltuvan hyvin pieniin verkkoihin ja B.A.T.M.A.N.:in isompiin. Tuloksista havaitaan, että B.A.T.M.A.N.:in resurssitarpeet kasvavat maltillisemmin ja näyttävät hakeutuvan tiettyä raja-arvoa kohti reititinmäärän kasvaessa. [15, s. 8]

B.A.T.M.A.N.:sta löytyy sekä siirto- (OSI Layer 2) että verkkokerroksen (OSI Layer 3) -toteutukset. Layer 2 -toteutusta kutsutaan B.A.T.M.A..N.-adv:ksi (lue: *”advanced”*). B.A.T.M.A.N.-adv tarjoaa mielenkiintoisia ominaisuuksia, joilla se eroaa muista reititysprotokollista varsin mielenkiintoisella tavalla.

Kun perinteiset reititysprotokollat toimivat Layer 3 -tasolla, kuljettaen vain reititysprotokollan omia tietoja, B.A.T.M.A.N.-adv kuljettaa sisällään myös kaiken liikenteen, kunnes ne saavuttavat määränpäänsä – ikään kuin laitteet olisivat samassa fyysisessä verkossa, autuaan tietämättöminä verkon topologiasta tai sen muutoksista.

Layer 2 -tason protokollan sisällä voi kuljettaa ylemmän, Layer 3 -tason liikennettä, kuten esimerkiksi IP-, IPX-, IGMP- tai AppleTalk -paketteja. Mikään ei myöskään estä ajamasta vaikkapa 3-tason reititysprotokollaa B.A.T.M.A.N.-adv:n kautta.

Tämä mahdollistaa mm. *broadcast* (kaikille lähetettävä viesti) sekä *multicast* (tietylle joukolle osoitettu viesti) -tyyppisten lähetteiden käytön uudella tavalla (joskin yhteysnopeudet huomioon ottaen).

Solmut voivat lisäksi osallistua ja toimia mesh-verkossa ilman, että niillä on IP-osoitetta, joten IP-osoitteiden jakamisesta syntyvät pulmat katoavat, sillä DHCP-palvelin on 3. tason protokolla – joka siis kulkee B.A.T.M.A.N.-adv:n sisällä. Miten tämä vaikuttaa *roaming*-tilanteeseen on avoin kysymys, sillä ominaisuuden mahdolliset käyttö- ja sovelluskohteet sekä vaikutukset ovat vielä tutkimatta.

B.A.T.M.A.N.-adv sisältää myös visualisointikomponentin, *B.A.T.M.A.N.-vis*:n. Komponentilla voidaan kartoittaa verkon topologista rakennetta. Komponentti luo näkemyksen naapureistaan sekä suoraan kytketyistä laitteista. Tiedot lähetetään ALFRED-palvelun kautta toisille naapureille, jotka tekevät saman tehtävän. Kerätyn tiedon perusteella muodostetaan kuva verkon rakenteesta, laitteiden fyysisestä sijainnista ja linkkien laadusta.

ALFRED (*Allmighty Lightweight Fact Remote Exchange Daemon*) on tiedonkeruu- ja välityspalvelu, jota käytetään verkon lisätietojen vaihtoon. Protokollan yli voi jakaa käytännössä mitä tahansa hyödylliseksi katsottua tietoa – kuten GPS - tai säätietoja [17]. ALFRED-protokollaa voidaan käytettään myös visualisoimaan B.A.T.M.A.N.-adv-protokollaa ajavia verkkoja.

6.5 Babel-reititysprotokolla

Babel (RFC 6126) on silmukoita välttävä distance-vector-tyyppinen reititysprotokolla sekä langattomiin että langallisiin verkkoihin. Babel perustuu DSDV-, AODV- sekä EIGRP-reititysprotokolliin.

Reittien kustannusten laskemiseen Babel käyttää muunneltua ETX (*Expected Transmission Count*) -menetelmää hyppyjen lukumäärän summaamisen sijaan. Tämä siksi, että hyppyjen lukumäärä ei kerro solmujen välisistä radiotien laadusta tai sen luotettavuudesta riittävästi.

$$ETX = \frac{1}{\left(LQ * LQ_n\right)}$$

Kaava 1: Expected Transmission Count

Kaava 1 esittää ETX (*Expected Transmission Count*)-suureen laskukaavan. LQ (Link Quality) tarkoittaa vastaanotettujen pakettien määrää suhteessa ajanjaksoon. LQ_n tarkoittaa naapurisolmun meiltä saamien pakettien määrää ajanjaksossa. ETX-arvo kuvaa yhteyden luotettavuutta ollen aina 1:tä pienempi luku.

Babel-protokollaa voidaan ajaa myös lankaverkossa. Tällöin lankaverkosta tuleviin reitteihin ei käytetä ETX-arvoja, koska lankaverkon linkin laatu voidaan useimmiten olettaa hyväksi.

Babel välttää reitityssilmukoita hidastamalla ja kuolettamalla reititysviestejä. Jos reititin havaitsee useamman kuin yhden reitin samalla linkin laadulla (ETX), Babel katsoo historiatiedoista, kumpaa reittiä viimeksi on käytetty. Tällä vältetään tilanne, jossa reititin ei osaisi päättää kumpaa käyttää, kun kustannukset ovat yhtä suuret [18 s. 4].

Edellä mainittua tilannetta, jossa reitin tila vaihtelee nopeasti, kutsutaan termillä *route flap*. Tilaansa nopeasti vaihteleva reitti on epäluotettava ja tilan vaihtelu aiheuttaa ylimääräisiä tilaviestien ja reititystaulukoiden vaihtoa verkossa. Reititystietojen vaihdon hidastamisesta edelleen aiheutuu se, että protokolla on epäideaalinen nopeasti muuttuvaan, mobiiliin Ad-Hoc-verkkoon.

Suureen, kiinteään ja langattomaan verkkoon Babel soveltuu kuitenkin paremmin kuin esim. OLSR, sillä reititysviestien tarkoituksellisen hidastamisen ja kuolettamisen takia itse reititysprotokolla tarvitsee muihin protokolliin verrattuna vähemmän tilaa verkon varsinaiselta datalta.

Toisaalta, kun Babel havaitsee reiteissä muutoksia, se voi myös pakottaa kaikkien reititystaulukoiden päivittämisen. Babel:in sanotaan toipuvan lähes välittömästi, mikäli kaikkien reittien luotettavuusarvot on laskettu ennen pakotettua reititystaulukoiden päivitystä [18 s. 4].

6.6 Ongelmia ja ideoita

Reititys langattomassa verkossa ei ole ongelmatonta. Useiden reitittimien lähettämät, toistuvat tervehdysviestit vaativat oman aikansa radioaalloilla. Tänä aikana mikään muu viesti ei kulje samalla radiokanavalla toimivan laitteen välillä.

Toisaalta verkon voi myös paloitella sillä tavalla, että useammalla radiolaitteella varustetut solmut laitetaan eri WLAN-kanaville. Tämän jälkeen reitit välitetään reititysprosessilta toiselle. Lähekkäiset solmut voitaisiin sen jälkeen asettaa sillaksi eri kanavien verkkojen välille liittäen useammat verkot yhteen.

Tällainen rakennelma vaatisi tietysti ainakin kaksi langatonta verkkokorttia, sekä sillan ajamista yhdistävissä laitteissa. Tästä herää edelleen kysymys, voisiko reititystiedot jollain keinoin viedä erilleen varsinaisesta datasta niin, että itse dataverkkoon jäisi paremmin tilaa?

ALFRED-palvelua voidaan käyttää mm. sijainti- ja säätietojen välittämiseen verkon toisille reitittimille. Koska ProjectSPAN käyttää älypuhelimia reitittiminä ja koska puhelimet ovat monesti akun varassa, voisiko ALFRED-palvelulla välittää toisille puhelimille tietoja akun varauksesta? Tällöin puhelin voisi pyytää toisia kiertämään kyseinen puhelin.

Vastaavasti jos puhelin on esimerkiksi laturissa kiinni, se voisi kertoa tämän tiedon. Tällöin laturissa oleva puhelin voisi saada akulla toimivia puhelimia korkeamman prioriteetin, eli kyseistä puhelinta käytetään reittinä mieluummin, kuin niitä, jotka eivät laturin päässä ole.

7 Tietoturva

7.1 Avoin vai suljettu verkko?

Tietoturva on Ad-Hoc-verkoissa tietenkin tärkeä seikka. Jos ajatellaan OLPC:n, FNF:n tai FreedomBoxin visioita, niin tietoturvalla ei tarkoiteta sitä, että verkko olisi suljettu ja salasanojen takana. Mainituissa visioissa ei keneltäkään voida kieltää pääsyä verkkoon, sillä tällainen ajatus olisi ristiriidassa projektien arvomaailmojen kanssa. Sitä paitsi, kenellä tulisi olla oikeus päättäisi siitä, kuka verkkoa saisi käyttää?

Kaikki kolme projektia lähtevät liikkeelle siitä periaatteesta, että internet kuuluu kaikille. Verkko ei siis voi vaatia salausavaimia, toteuttaa MAC-suodatuksia tai valikoida käyttäjiään. Verkon pitää olla kaikille avoin, ja sitä pitää saada käyttää sekä laajentaa vapaasti. Toisaalta kannattaa myös muistaa, että liikennettä voi kuunnella ja häiritä melko pienellä vaivalla huolimatta siitä, minkälainen verkon fyysinen rakenne on.

7.2 SOWN – varmennettu avoin verkko

SOWN (*Secured Open Wireless Network*) on *proof-of-concept*-tasolla oleva lähestymistapa avoimiin, mutta turvallisiin langattomiin verkkoihin. Tekniikkaa ei ole suunnattu nimenomaisesti Ad-Hoc-verkoille, mutta ajatus avoimesta, salatusta verkosta on kuitenkin mielenkiintoinen. SOWN perustuu SSL- ja EAP-protokollien salaukseen ja todentamiseen. Pääsy verkkoon olisi sallittu, mutta SOWN:n kehittäjä ehdottaa SSL-varmenteiden käyttöä todentamaan, että tietyn niminen langaton verkko todella liittyy jollain tapaa verkon oikeaan omistajaan tai haltijaan. Varmenteita käsitellään seuraavassa luvussa lyhyesti.

Kehittäjät esittävät Blackhat-konferenssissa, että SOWN:ia käyttävät verkot nimettäisiin ja nimi varmennettaisiin jollain auktoriteetilla siten, että vain yritys, järjestö tai yksityinen taho voisi luoda luotetun verkon, joka kantaa esimerkiksi nimeä ”sown.metropolia.fi” [19]. SOWN sinänsä ei estä verkon

sisällä tehtyjä tietoturvaloukkauksia, mutta sitä käyttämällä voitaisiin taata, että kyseinen verkko, jolla on nimi ”sown.metropolia.fi”, kuuluu todellakin Metropolialle, sillä osoitteen SSL-sertifikaatti on voimassa, maksettu sekä varmennettu ulkopuolisella varmentajalla (Certificate Authority).

7.3 Liikenteen häirintä ja seuranta

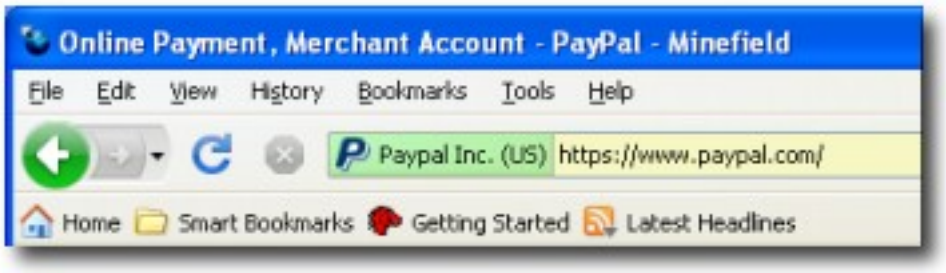
Laitteiden välinen tiedonsiirto on syytä salata. Palveluntarjoajat, kuten ISP (*Internet Service Provider)* tai sosiaaliset mediapalvelut voivat kerätä ja tallentaa kaiken liikenteen. Tiedämme, että naapurimaassamme Ruotsissa hyväksyttiin laki, jonka mukaan kaikki rajan ylittävä internetliikenne kerätään ja tallennetaan [20].

Toinen kasvava ongelma on ns. Web bugit. Tyypillisimpiä web bugeja ovat lukuisten sosiaalisten mediapalveluiden pikkuruiset ikonit. Web bugit haetaan sivun ulkopuoliselta palvelimelta, joka saa jokaisen ikonin latauksen yhteydessä tiedon IP-osoitteesta, sekä minkä kuvan, milloin ja minkä osoitteen kautta. Näillä web bugeilla seurataan yhä useamman sivun lukijoita ja liikkeitä riippumatta siitä klikkaako ikonia vai ei.

7.4 Salaus ja varmennus

Avoimessa verkossa kaikki liikenne solmujen välillä on oletettavasti salaamatonta. Kuka tahansa voi kuunnella liikennettä melko pienellä vaivalla. Tästä syystä muutama termi - kuten jo mainittu SSL *(Secure Sockets Layer)* sekä PGP *(Pretty Good Privacy)* ovat hyödyllisiä tuntea.

SSL on ulkoisen varmentajan (*Certificate Authority*, CA) myöntämään digitalliseen varmenteeseen perustuva menetelmä. SSL:ää käytetään laajimmin internetin HTTPS-protokollan yhteydessä WWW-sivuilla, kuten käytännössä kaikissa pankkipalveluissa sekä enenevissä määrin erilaisissa verkkoasiointipalveluissa varmentamaan sivuston alkuperä.



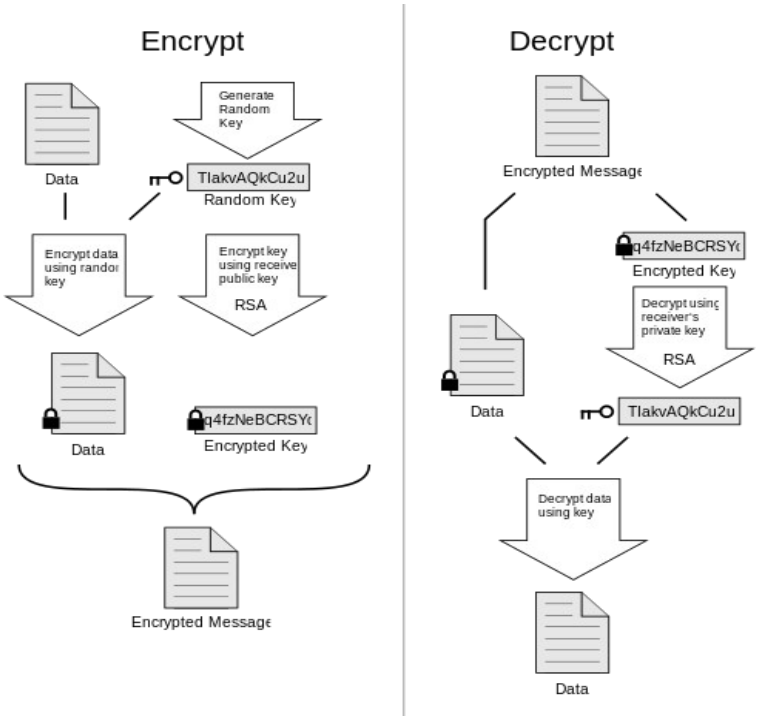
Kuva 11: Firefox SSL-salatulla sivulla

Firefox-selain ilmoittaa kelvollisesta SSL-varmennetusta sivusta värjäämällä osoitepalkin vihreäksi, jos varmenne on voimassa.

SSL:n heikkous on kuitenkin itse varmennetuissa varmenteissa. Näin kuka tahansa voi väittää olevansa oma itsensä - ja tämä kelpaa SSL:lle. Vaikka useimmat ohjelmat kuitenkin huomauttavat itse luoduista varmenteista, harva käyttäjä kuitenkaan reagoi huomautuksiin.

7. huhtikuuta 2014 yleiseen tietoon tullut HeartBleed-haavoittuvuus koski avoimen lähdekoodin SSL-toteutuksessa, OpenSSL:ssä ollutta haavoittuvuutta, jota hyödyntämällä palvelimelta voidaan pyytää kerrallaan 64 kilotavua keskusmuistin sisältöä. Asiasta nousi kova meteli, sillä tällä tavoin käyttäjien tietoja kuten käyttäjätunnuksia ja salasanoja voidaan pala kerrallaan pyytää palvelimelta. Vika on korjattu OpenSSL:n versiosta 1.0.1g lähtien.

PGP *(Pretty Good Privacy)* on asymmetrinen salausohjelma. Tämä tarkoittaa sitä, että siinä käytetään eri salausavainta salaukseen ja sen purkamiseen. Avaimia kutsutaan *julkiseksi* ja *yksityiseksi* avaimeksi. Kumpikaan avain ei kulje salatun viestin sisällä, vaan viestiin liitetään satunnainen avain, jota käytetään salauksen ja purun eri vaiheissa. Periaatekuva esitetään seuraavalla sivulla.



Kuva 12: PGP:n toimintaperiaate.

Kuva 12 esittää PGP:n toimintaperiaatteen. Ensin muodostetaan *satunnainen* avain. Seuraavaksi salataan viesti satunnaisella avaimella ja samaan aikaan salataan satunnainen avain vastaanottajan *julkisella* avaimella. Nyt meillä on satunnainen avain sekä tieto yhdessä viestissä.

Vastaanottaja saa viestin, joka sisältää tiedon sekä satunnaisen avaimen. Seuraavaksi vastaanottaja purkaa salatun viestin omalla *yksityisellä* avaimellaan. Nyt vastaanottajalla on hallussa satunnainen avain ja salattu tieto. Vastaanottaja käyttää satunnaista avainta salattuun tietoon, ja saa viestin.

PGP-salatun viestin alussa on PGP-viestin alkuilmoitus sekä versionumero. Lopussa on teksti ” ---- END PGP MESSAGE ---”. Kaikki muu sisältö näyttää vain kasalta ASCII-merkkejä ilman mitään muotoiluja, välilyöntejä tai rivinvaihtoja.

Tietoturva ei kuitenkaan ole yhtä kuin jokin tietty tuote tai ohjelma. Tietoturva on prosessi, jota tulee harjoittaa ja tarkistaa aika-ajoin. Pelkkä tekninen tuntemus tai ohjelmien lataaminen ei ole tietoturvallinen toimintatapa, ellei

lähetettyjä viestejä todellakin salata siinä koneessa, mistä viesti lähtee. Ensimmäinen välikäsi, jolle viesti lähtee salaamatta voi myös lukea viestisi.

WWW-liikenne (HTTP-protokollan yli) on tietysti salaamatonta. HTTPS on turvalliseksi väitetty protokolla, joka tarkoittaa yksinkertaisesti SSL-varmenteiden käyttöä HTTP-protokollan liikenteelle. Vaikka HTTPS-protokolla käyttääkin SSL-varmenteita, voi varmenteita luoda myös itse.

Sähköpostiliikenne (POP-, IMAP- ja SMTP-protokollat) ovat yleensä salaamatonta, ellei sähköpostiohjelmaa erikseen käsketä salaamaan kaikkea lähtevää ja tulevaa liikennettä. Ulkopuoliset palvelut eivät kuitenkaan useinkaan tue SSL-varmennusta, joten kunnollisille palveluille olisi tarvetta.

Tuore uutinen on, että Google aikoo pakottaa SSL-varmennuksen päälle kaikkiin uusiin ja vanhoihin sähköpostiosoitteisiin [21]. Tämä on hyvä edistysaskel, sillä se hankaloittaa ns. *Man in the middle* -hyökkäyksen toteuttamista. Tietenkään kukaan ei voi taata etteikö palveluntarjoaja itse lukisi postejasi, mutta jos viesti on myös PGP-salattu, ei palveluntarjoajakaan pysty itse viestin sisältöä purkamaan ilman vastaanottajan yksityistä salausavainta.

On edelleen huomattava, että vaikka salaisit sähköpostiviestisi esim. PGP:llä, viestin tunnisteet (lähettäjä, vastaanottaja(t), otsikko jne.) lähetetään edelleen puhtaana tekstinä. Tämä tarkoittaa, että vaikka viesti olisikin salattu, voidaan keskustelun osapuolet selvittää. Näiden perusteella saadaan selville osatotuuksia sosiaalisesta verkostostasi, kiinnostuksenkohteistasi, poliittisista agendoistasi jne.

Pikaviestimillä lähetetyt viesti ovat myös oletuksena puhdasta tekstiä. Jotkut ohjelmat osaavat kuitenkin salata viestin joko itse tai liitännäisen avulla. Yksi salausliitännäinen on nimeltään OTR (*Off The Record*). Liitännäinen huomauttaa, jos yhteytenne on salaamaton tai vastaanottajan varmenne ei täsmää omasi kanssa.

8 Yhteenveto

Langattomat verkot on aiheena hyvin laaja, sillä osoittautuu olevan monen laista mielenkiintoista ja tutkimatonta käyttökohdetta ja soveltamistapaa.

Ad-Hoc-tyyppisillä verkoilla on potentiaalia monenlaisessa muuttuvassa, kriittisessä tai muutoin haastavassa ympäristössä. Länsimaissa -verkkojen kasvualueita voi olla esimerkiksi erilaisissa valvontajärjestelmissä, kuten kameroissa, kulunvalvonnassa tai varashälyttimissä.

Harrastelijaprojekteilla, kuten tässä insinöörityössä käsitellyllä Kansas City Freedom Network:lla voi olla suuri merkitys köyhien, syrjäisten tai jakautuneiden alueiden asukkaiden elämään. Langattomia verkkoja käyttämällä voidaan tuoda tietoverkot ja internet uusille alueille vaikuttamalla sitä kautta myös alueiden elintasoon.

Köyhillä alueilla jo pelkkä infrastruktuurin puute asettaa vaatimuksia, joihin perinteiset mallit eivät välttämättä ole toimivia ratkaisuja. Ad-Hoc-verkko voi olla tällaisissa tilanteissa varteenotettava vaihtoehto.

Reititys langattomassa verkossa aiheuttaa myös isoja haasteita. Laitteet saattavat liikkua paikasta toiseen, siirtotiellä on monenlaista häiriötä, sääolosuhteet saattavat muuttua ja siirtotietkin ovat ahtaat.

Haasteet eivät kuitenkaan lannista alan harrastajia, vaan he kehittävät ja tulevat jatkossakin kehittämään lukuisia erilaisia ratkaisu- ja lähestymistapoja näihin ongelmiin. Harrastepohjalta kehitetyt projektit ovat usein heikosti dokumentoitu, sillä projekteja tehdään omalla ajalla, omien intressien pohjalta ja omin varoin.

Tietoturva, yksityisyydensuoja ja käytetyt protokollat ovat tavalla tai toisella kaikki rikki. Heikosti suunniteltujen protokollien sisällä voidaan kuitenkin tehdä erilaisia asioita, jotta kaikki yksityisyys ei olisi täysin menetetty. Kryptografia, kuten PGP toimii, ja se on ainoa tapa säilyttää edes jonkin tasoinen yksityisyyden suoja avoimessa tietoverkossa.

Lähteet

1 Free Software Foundation: What is free software? [Verkkodokumentti]. [Viitattu 24.04.2014]. Saatavissa: http://www.gnu.org/philosophy/free-sw.html.

2 Aboul-Magd, Osama. Huawei Technologies: High Efficiency WLAN (HEW) SG March 2014 Closing Report 20.03.2014. [esityskalvot, viitattu 24.04.2014]. Saatavilla: https://mentor.ieee.org/802.11/dcn/14/11-14-0457-00-0hew-high-effciency-wlan-hew-sg-march-2014-closing-report.pptx.

3 Aboul-Magd, Osama. Huawei Technologies: 802.11HEW SG Proposed PAR. [verkkodokumentti], [viitattu 24.04.2014]. Saatavilla: https://mentor.ieee.org/802.11/dcn/14/11-14-0165-01-0hew-802-11-hew-sg-proposed-par.docx.

4 Buettrich, Sebastian [ja monet muut]: Wireless Networking in Developing Countries [3. Engl. painos]. [Julkaistu Maaliskuussa 2013]. Saatavissa: http://wndw.net.

5 Wikipedia, MIMO [verkkodokumentti]. [viitattu 24.4.2014]. Saatavissa: https://en.wikipedia.org/wiki/MIMO.

6 Ravatti, Antti. Insinöörityö: DVB-lähetystekniikat ja teräväpiirtolähetykset suomessa. Tampereen Ammattikorkeakoulu, Tietotekniikka, Sulautetut järjestelmät ja elektroniikka. [Julkaistu Huhtikuussa 2013].

7 Chroboczek, Juliusz. Internet-draft: The Ad Hoc Configuration Protocol. [verkkodokumentti], [julkauistu: Elokuu 2009]. [viitattu 24.4-.2014, saatavissa:]http://www.pps.univ-paris-diderot.fr/~jch/software/ahcp/draft-chroboczek-ahcp-00.html.

8 Free Network Foundation, Q3 2013 review [julkaistu 5. Marraskuuta 2013]. [Viitattu 24.4.2014]. Saatavilla http://thefnf.org/2013-q3-review/.

9 The Cook Report on Internet Protocol: Do-It-Ourselves Telecommunications, Part Two: The Free Network Foundation. [Verkkodokumentti]. [Julkaistu huhtikuussa 2013]. [viitattu 24.4. 2014]. Saatavilla: http://www.cookreport.com/pdfs/march-april13diowireless.pdf.

10 The Cook Report on Internet Protocol: The Global Free Network Movement, Part Four: Isaac Wilder and the KC Freedom Network. [Verkkodokumentti]. [Julkaistu joulukuussa 2013]. [viitattu 24.4. 2014]. Saatavilla: http://www.cookreport.com/pdfs/nov-Dec_2013_CRpp.pdf.

11 Jeff Robble, Josh Thomas: Off-grid Off-Grid Communications with Android - Meshing the Mobile World.[Esityskalvot], [Julkaistu Marraskuussa 2012]. [Viitattu 24.4.2014]. Saatavilla: https://github.com/monk-dot/SPAN/blob/master/docs/IEEE HST 2012/Off-Grid Communications with Android.pdf.

12 Eben Moglen, Bdale Garbee: FreedomBox 1.0. [Puhe FOSDEM 2013 -tapahtumassa].[Viitattu 20.4.2014]. Video katsottavissa: http://yourfreedombox.org/2013/fosdem-2013-conference/.

13 FreedomBox Foundation: Learn about FreedomBox! [Verkkodokumentti]. [Viitattu 24.4.2014], Saatavilla: http://www.freedomboxfoundation.org/learn/.

14 DD-WRT: Supported Devices. [Verkkodokumentti]. [Viitattu 24.4-.2014]. [http://www.dd-wrt.com/wiki/index.php/Supported_Devices.

15 David Johnson, Ntsibane Ntlatlap, Corinna Aichele: A simple pragmatic approach to mesh routing using BATMAN [Verkkojulkaisu]. [Viitattu 24.4.2014]. https://www.cs.ucsb.edu/~davidj/Files/Batman_ifip.pdf.

16 OpenMesh: B.A.T.M.A.N. advanced [Verkkodokumentti]. [Viitattu 24.4-.2014].Saatavissa: http://www.open-mesh.org/projects/batman-adv/wiki/Wiki.

17 OpenBesh: ALFRED [Verkkodokumentti]. [Viitattu 24.4.2014]. Saatavissa: http://www.open-mesh.org/projects/open-mesh/wiki/Alfred.

18 M. Abolhasan, Brett Hagelstein, Jerry Chung-Ping Wang: Real-World performance of current proactive multi-hop mesh protocols. University of Wollongong Research Online, Faculty of Engineering and Information Sciences. [Verkkodokumentti], Saatavissa: http://ro.uow.edu.au/cgi/viewcontent.cgi?article=1747&context=infopapers.

19 Christopher Byrd, Tom Cross, Takehiro Takahashi: Secure Open Wireless Networking. BlackHat -konferenssi 2011. [Esityskalvot] Saatavissa: https://media.blackhat.com/bh-us-11/Arsenal/BH_US_11_Cross_Arsenal_Secure_Wireless_Slides.pdf.

20 Tiffen, Stuart: Sweden passes controversial data retention directive. Deutche Welle. [Julkaistu 22.3.2012], [Verkkodokumentti], saatavilla: http://www.dw.de/sweden-passes-controversial-data-retention-directive/a-15826462.

21 Nicolas Lidzborski: Staying at the forefront of email security and reliability: HTTPS-only and 99.978% availability [Verkkouutinen], [20-.3.2014], [viitattu 22.04.2014] Saatavissa: http://gmailblog.blogspot.ca/2014/03/staying-at-forefront-of-email-security.html.

22 Togo, Emmanuel. Case study: University of Ghana campus wireless network. [Verkkodokumentti], Saatavilla: http://wndw.net/CaseStudies/University_Of_Ghana.html.