MAANPUOLUSTUSKORKEAKOULU

AD HOC -REITITYSPROTOKOLLIEN HYÖDYNTÄMISMAHDOLLISUUDET TULEVAISUUDEN TAISTELUKENTÄLLÄ

Kandidaatintutkielma
Kadetti
Ismo Reunamäki
Kadettikurssi 98
Maavoimien JOJÄ-opintosuunta
maaliskuu 2014

MAANPUOLUSTUSKORKEAKOULU

Kurssi	Linja
Kadettikurssi 98	Maavoimien johtamisjärjestelmälinja
Tekijä	
Kadetti Ismo Reunamäki	
Tutkielman nimi	
Ad hoc -reititysprotokollien hyödyntämismahdollisuudet tulevaisuuden taistelukentällä	
Oppiaine, johon työ liittyy Sotatekniikka	Säilytyspaikka Kurssikirjasto (MPKK:n kirjasto)
Aika Maaliskuu 2014	Tekstisivuja 22 Liitesivuja 4

TIIVISTELMÄ

Tulevaisuuden taistelukenttä tulee asettamaan useita haasteita asevoimille. Joukot liikkuvat enemmän ja nopeammin sekä sijaitsevat hajaantuneemmin taistelualueilla. Tilannetietoa pystytään tuottamaan kehittyneillä järjestelmillä, jolloin niiden siirtämiseen käytettyjen viestijärjestelmien pitää pystyä toimittamaan tätä kasvanutta informaation määrää. Ad hoc ja Mobile Ad Hoc Network (MANET) -verkoilla voidaan siirtää suuria määriä informaatiota tai dataa joukkojen välillä. Verkoissa käytetyt reititysprotokollat määrittävät miten lähetetty tieto liikkuu verkossa. Oikealla reititysprotokollan valinnalla pystytään vaikuttamaan verkon ruuhkautumiseen, tiedon siirtymisen varmuuteen, tiedonsiirtonopeuksiin, kaluston toimintakykyyn sekä siirtotien toimivuuteen.

Päätutkimuskysymykseni on: Mitä käyttömahdollisuuksia AD HOC -reititysprotokollilla on tulevaisuuden taistelukentällä? Tutkimusta tukevat alakysymykset: Mitä viestillisiä vaatimuksia tulevaisuuden taistelukenttä voi asettaa MANET-verkolle? Mitä eroja erilaisilla ad hoc -reititysprotokollilla on? Mitä vaikutuksia erilaisilla siirtoteillä on MANET-verkossa?

Tutkimukseen käytetty aineisto on kerätty internet- sekä kirjallisuuslähteistä. Lähteisiin sisältyy aihepiirin kuuluvia tutkimuksia, artikkeleita, oppaita ja yritysten tuote-esitelmiä. Johtopäätöksenä voidaan todeta, että taistelukentän muuttujat määrittävät parhaan käytettävän reititysprotokollan. Olennaisena tekijänä on hahmottaa verkkoa käyttävän joukon tarve sekä minkälaista dataa verkossa liikkuu. Erilaiset reititysprotokollat soveltuvat paremmin erilaisille joukoille ja erilaiseen toimintaympäristöön. Reititysprotokollaa valittaessa tulee huomioida käytössä olevat siirtotiet, jotta tiedonsiirtokaistaa ei tuhlata ja tällä tavalla ruuhkauteta verkkoa.

AVAINSANAT
TULEVAISUUDEN TAISTELUKENTTÄ, AD HOC, MANET, REITITYSPROTOKOLLA, SIIRTOTIE, VERKKOTOPOLOGIA,

SISÄLLYSLUETTELO

AD HOC -REITITYSPROTOKOLLIEN HYÖDYNTÄMISMAHDOLLISUUDET TULEVAISUUDEN TAISTELUKENTÄLLÄ

1 JOHDANTO

1.1 Aihealueen esittely

Tulevaisuuden sodankäynnissä armeijat turvautuvat entistä enemmän parempaan informaatioteknologiaan. Verkot, joissa informaatio liikkuu, voidaan karkeasti jakaa kahteen eri luokkaan: strategisiin ja taktisiin verkkoihin. Nykyaikana sodankäynti tukeutuu enemmän informaatioteknologian hyödyntämiseen ja siihen, miten viestimme keskenämme. Taktisella tasolla tilannetietojen ylläpito ja jakaminen omille joukoille korostuu enemmän teknologian tarjotessa mahdollisuuden lähettää esimerkiksi suorassa lähetyksessä videokuvaa taistelukentältä tai muita vastaavia palveluita. Myös taistelukentällä olevien joukkojen liikkeestä johtuviin ongelmiin pitää pystyä vastaamaan entistä paremmin. [1]

Erilaiset ad hoc -verkkosovellutukset ovat käytössä kansainvälisesti erilaisilla sovelluksilla. Ad hoc ja sen liikkuvat versiot mahdollistavat sotilaskäyttöön lupaavan määrän erilaisia hyödyntämismahdollisuuksia [2]. Asevoimien järjestelmien verkottumisen myötä erilaisilla reititysprotokolilla on tärkeä osa toimivan verkon muodostamiseksi. Ad hoc, Mobile Ad hoc Network (MANET) -verkot sekä niiden tarjoama haasteellinen ympäristö reititysprotokolille on paljon tutkittu ala nykyään, kuten lähteet [2], [3] ja [4] osoittavat. Useat eri asevoimat käyttävät erilaisia MANET-verkkoja ja jopa yksityisen sektorin yritykset tarjoavat niitä sotilaskäyttöön [5]. Eri tutkimuksien pohjalta voidaan todeta, että erilaisen reititysprotokollan valinta voi merkitä paljon taistelukentällä.

1.2 Tutkimuskysymykset

Tutkimuksen tarkoituksena on selvittää, miten erilaisia reititysprotokollia voidaan hyödyntää tulevaisuuden taistelukentällä. Tutkimuksessa vertaillaan erilaisia reititysprotokollia ja niiden mahdollisia käyttömahdollisuuksia. Erilaiset reititysprotokollat tarjoavat erilaisia etuja ja haittoja toisiinsa nähden; isoimpana muuttujana voidaan pitää käyttöympäristöä, joka suurimmilta osin määrää minkälaista reititysprotokollaa on tehokkainta käyttää. Tutkimuksessa tarkastellaan myös lyhyesti siirtotien vaikutusta MANET toimintaan.

Tutkimuksen pääkysymys on: Mitä käyttömahdollisuuksia on ad hoc -reititysprotokollilla tulevaisuuden taistelukentällä?

Tutkimuksen alakysymykset:

1. Mitä viestillisiä vaatimuksia tulevaisuuden taistelukenttä voi asettaa MANET-verkolle?
2. Mitä eroja erilaisilla ad hoc -reititysprotokollilla on?
3. Mitä vaikutuksia erilaisilla siirtoteillä on MANET-verkossa?

1.3 Tutkimusaineisto

Tutkimus perustuu suurimmilta osin Guide To Wireless Ad Hoc Networks -kirjaan. Teoksen tueksi olen valinnut kotimaista kirjallisuutta joka käsittelee aihetta enemmän sotilasnäkökulmasta. Tutkimuksessa käytetyistä internetlähteistä saatu tieto on varmennettu kirjallisuuslähteistä.

Ad hoc -reititysprotokollia käsitellessä teosten ikä ei nouse ongelmaksi, sillä niistä saatua tietoa voidaan pitää edelleen totena. Lähteissä käytetyt termit, käsitteet ja kokonaisuudet säilyvät pääosin samoina tulevaisuudessa [6]. Poikkeuksena on mahdollisesti tulevaisuudessa muuttuvat tekijät kuten miten taistelukenttä tulee muuttumaan 20 vuoden kuluessa [7]. Tällöin olen pyrkinyt käyttämään mahdollisimman uutta aineistoa [1] ja [8].

1.4 Tutkimusmenetelmä

Tutkielma on kirjallisuustutkimus. Lähdekritiikki ja tulevaisuudentutkimus ovat tutkielman päämenetelmät. Lähdekritiikki on huomioitu käyttämällä useita lähteitä ja vertaamalla ristiin niiden tietoa. Tutkimuksessa on otettu huomioon lähteiden alkuperä ja se, missä muualla niitä on käytetty. Tulevaisuudentutkimus perustuu kerätyn tiedon arvioimiseen ja vertaamalla niitä mahdollisiin tulevaisuuden trendeihin.

Tutkimuksessa ei ole hypoteesia, vaan siinä selvitetään eri lähteitä tutkimalla ja vertailemalla, onko tiettyihin ympäristöihin paremmin soveltuvia reititysprotokollia. Tutkimuksen alussa arvioidaan mahdollista käyttöympäristöä MANET-verkoille johon erilaisia reititysprotokollia verrataan.

1.5 Tutkimuksen rakenne

Tutkimus koostuu viidestä pääluvusta ja niiden alle tuotetuista alaluvuista. Tärkeimmät luvut ovat 2, 3 ja 4, jotka sisältävät varsinaisen tutkivan osan. Tämän jälkeen tulee johtopäätösluku, joka sisältää aikaisempien lukujen perusteella tehdyt havainnot ja päätelmät.

Ensimmäinen luku on johdanto, joka esittelee tutkittavan aiheen sekä perusteet millä tutkimus on tehty.

Toinen luku sisältää tutkimukseen liittyvät suuremmat kokonaisuudet ja niihin liittyvän teorian. Luvussa esitellään lyhyesti tulevaisuuden taistelukenttää ja sen viestillisiä vaatimuksia. Lisäksi esitellään infrastruktuurinen, ad hoc ja MANET-verkko ja niiden eroavaisuuksia vertaillaan keskenään.

Kolmas luku sisältää tutkimukseen liittyvät ad hoc -verkoissa käytettävät reititysprotokollat. Alaluvuissa esitetään reititysprotokollien käyttäytymismalleja ja pohditaan niiden käyttömahdollisuuksia tulevaisuuden taistelukentällä. Reititysprotokollien eroja vertaillaan toisiinsa ja niiden hyötyjä sekä haittoja esitellään erilaisissa ympäristöissä.

Neljännessä luvussa käsitellään MANET-verkkoihin liittyviä siirtoteitä. Eri siirtoteiden teknisiä ominaisuuksia vertaillaan niiden mahdollisiin vaikutuksiin muun muassa verkkotopologiaan ja mahdollisiin käyttömalleihin tulevaisuuden taistelukentän eri ympäristöissä.

Viidennessä luvussa aikaisempien lukujen päätelmät kootaan yhteen. Niistä muodostetaan vastaukset aikaisemmin esitettyihin tutkimuksen pää- ja alakysymyksiin. Mahdolliset jatkotutkimuksen tarpeet tuodaan esille myös tässä luvussa.

1.6 Rajaukset ja käsitteet

Tutkimuksessa selvitetään miten reititysprotokollien erilaisten käyttäytymismallit toimivat sekä kuinka hyvin ne mukautuvat muuttuvaan verkkotopologiaan. Esimerkiksi reititysprotokollien ohjelmointia tai MANET-verkoissa käytössä olevien laitteiden ominaisuuksia ei tutkimuksessa käsitellä. Tutkimuksessa on kuvattu miten eri reititysprotokollat vaikuttavat verkkotopologiaan laitteiden ollessa esimerkiksi liikkeessä.

Tutkimuksen keskeiset käsitteet kuten MANET, ad hoc, verkkotopologia, infrastruktuurinen verkko, proaktiiviset ja reaktiiviset reititysprotokollat sekä tulevaisuuden taistelukenttä on määritelty liitteessä. Isolle osalle käsitteistä ei ole suomenkielistä vastinetta, josta syystä tutkimuksessa käytetään niistä englanninkielisiä termejä.

2 AD HOC JA MANET OSANA TULEVAISUUDEN TAISTELUKENTTÄÄ

2.1 Tulevaisuuden taistelukenttä

Nykypäivänä ja vielä enemmän tulevaisuudessa kaikki taistelukentällä sijaitsevat järjestelmät yhdistyvät kokonaisuudeksi, jota kutsutaan digitaaliseksi taistelukentäksi [8]. Kolmen aikaisemman ulottuvuuden lisäksi (maa, meri, ilma) taistelukentällä ovat kasvaneet neljännen (aika) sekä viidennen (sähkömagneettinen spektri) elementin merkitykset. Neljäs ja viides elementti ovat ajaneet asejärjestelmien integroitumisen toisiinsa.

Sodankäynnin neljäs ulottuvuus eli aika korostaa, miten omia voimavaroja käytetään. Voiman keskittäminen oikeana aikana halutussa kohteessa lisää tarvetta yhtenäisille keskenään kommunikoiville asevoimille. Hyökkäyksessä koordinoidut iskut ja puolustuksessa voimavarojen oikea-aikainen sijoittaminen ovat osa nykypäivän sodankäyntiä. [8]

Sähkömagneettinen spektri muodostaa viidennen ulottuvuuden. Johtajien kyky päivittää tilannetietoisuuttaan perustuu sähkömagneettisen spektrin avulla tehtyihin havaintoihin. Nykyään joukkojen johtaminen tukeutuu vahvasti sähkömagneettisen spektrin tuomaan teknologiseen kehitykseen. Jos johtajalta viedään sähkömagneettisen spektrin hallinta, hän ei kykene tehokkaasti käyttämään muita resurssejaan kuten tulivoimaa. [8]

Nykyinen tietoyhteiskunta on siirtänyt sodankäynnin johtamis- ja tietosodankäynnin aikaan [8]. Aikaisemmat sodankäynnin periaatteet ovat muokkaantumassa tai kokonaan poistumassa taistelukentiltä.

Tärkeänä muuttujana tulevaisuuden taistelukentällä voidaan pitää tilannetietoisuutta. Sitä voidaan pitää mahdollisuutena sekä haasteena, sillä komentaja jolla on parempi kuva taistelukentän fyysisestä ympäristöstä, pystyy myös hahmottamaan paremmin viholliskomentajan ymmärryksen taistelun tilasta. Tulevaisuuden parempi tilannetietoisuus voi aiheuttaa ongelmia esimerkiksi esikuntien johtosuhteiden kanssa, jos saatavaa tietoa ei pystytä analysoimaan tarpeeksi tehokkaasti ja jos organisaatiorakenteet aiheuttavat tiedonkululle hidasteita. Tärkeää tilannetietoisuuden hyödyntämisen kannalta on myös käytettävät viestijärjestelmät, joilla informaatiota siirretään eteenpäin. [9]

Massan ja sodassa käytetyn materiaalin merkitys on vähentynyt suhteessa taistelussa tarvittavaan tiedon määrään sekä laatuun [8]. Tietoylivoima ei yksinään riitä, vaan sillä luodaan puitteet käyttää muita voimavaroja. Pyrkimyksenä on omien resurssien säästeliäs ja tehokas käyt-

täminen. Viestijärjestelmissä tämä tarkoittaa sitä, että meidän tulee saada tarvittava määrä tietoa mahdollisimman nopeasti halutulle organisaatiolle. Tiedon määrän ja laadun kasvaessa lähetettävän datan koko kasvaa. Puolustusvoimien kyky vastata kasvavaan datavirtaan riippuu tutkimuksesta, jonka avulla säästetään resursseja sekä tarpeiden tunnistamisesta ja niille oikeiden ratkaisujen kehittämisestä [6].

Taistelu voidaan jakaa neljään elementtiin: 1) Tiedustelu, valvonta ja johtaminen 2) Tulivoima 3) Liike 4) Taistelukyvyn säilyttäminen [8]. Kaikkien joukkotasojen taistelualueet syvenevät ja laajenevat teknologian tarjotessa tehokkaampaa kalustoa sotilaiden käyttöön. Kehittyneiden asejärjestelmien, elektronisen vaikuttamisen keinojen ja informaatiosodankäynnin menetelmillä kyetään vaikuttamaan vastustajan koko suorituskykyyn. Isolle alueelle hajaantuneet joukot ovat pakottaneet asevoimat ja yritykset kehittämään järjestelmiä, joilla pystytään toteuttamaan joukkojen välinen tiedonsiirtäminen [10]. Paremmilla laitteilla pystytään käyttämään myös niille sopivampia uusia ohjelmistoja ja protokollia, joilla toiminnasta saadaan edelleen tehokkaampaa.

Järjestelmien keventyessä liikkeellä tulee olemaan merkittävämpi vaikutus taistelussa kuin niiden tulivoimalla [8]. Liikkeellä suojataan omat joukot ja mahdollistetaan neljännen dimension eli ajan hallinta. Seuraavan 20 vuoden aikana asejärjestelmien siirtymisnopeudet kasvavat ja niiden polttoainekulutus laskee [1]. Samalla järjestelmiä kehitetään kykeneväisiksi toimimaan liikkeen aikana (esim. AMOS). Hajautetut, nopeat sekä koordinoidusti hyökkäävät joukot asettavat viestijärjestelmille vaatimukseksi, että ne kykenevät toimittamaan tietoa nopeasti ja katkeamatta asejärjestelmiä käyttävien joukkojen välillä.

Joukkojen liikkumisen ja tulivoiman kasvaessa niiden johtamisen merkitys tulee kasvamaan entisestään. Liikettä ja asejärjestelmien tulta pitää pystyä synkronoimaan joukkojen välillä tai muuten vaikutusta ei saada halutulla tavalla. Paremmalla tilannetietoisuudella ja kyvyllä koordinoida joukkojen liikettä voidaan saavuttaa ylivoima millä taistelu voitetaan. Tulevaisuudessa viestijärjestelmien kyky vastata tähän liikkeeseen ja tietoliikenteen määrään korostuu.

2.2 Ad hoc

Ad hoc -verkko tarkoittaa verkkoa jolla ei ole keskitettyä asemaa, joka kontrolloisi verkon muodostumista. Verkon solmut lähettävät, vastaanottavat ja välittävät sen sisällä liikkuvaa dataa. Tällöin kaikki välittävät solmut toimivat verkossa myös reitittiminä. Koska ad hoc -

verkossa ei yleensä ole pysyvää infrastruktuuria ja kaikki sen solmut kykenevät välittämään viestejä, on se helppo pystyttää nopeasti halutulle alueelle. Jos verkon solmut vioittuvat tai tuhoutuvat, niin ad hoc -verkossa on mahdollista ylläpitää eri yhteysvälit, koska solmut automaattisesti reitittyvät keskenään uudelleen. Ad hoc -verkkojen siirtotiet on usein toteutettu langattomilla yhteyksillä. Nämä langattomat verkot yleensä liittyvät kiinteän infrastruktuurin verkkoihin yhden tai useamman pisteen kautta. Kytkemällä ad hoc -aliverkot kiinteään verkkoon voidaan tämän ylemmän verkon palveluita tarjota ad hoc -verkon käyttäjille. [4]

Ad hoc -verkkojen perusta on luotu 1970- ja 1980-luvulla, kun DARPA kehitti radioverkkoon parempaa ja kestävämpää ratkaisua jota pystyttäisiin käyttämään taistelukentällä. Vaikka ad hoc -verkot suunniteltiin alun perin sotilaskäyttöön, niin suurin osa käytöstä ja aiheeseen liittyvästä tutkimuksesta tehdään kuluttajapuolella. Sotilaskäytössä olevat ad hoc -verkot hyötyvät kuluttajapuolen kehityksestä, mutta sotilaskäytöllä on erikoisvaatimuksia käytettävälle teknologialle. Esimerkiksi laitteiden tulee kestää ympäristöstä tulevia haittoja ja verkon tulee kyetä vastaamaan siinä nopeasti tapahtuviin topologian muutoksiin. [11]

Ad hoc -verkot tarjoavat paljon sellaisia ominaisuuksia joita tarvitaan haastavassa sotilaskäytössä. Ad hoc -verkosta voidaan rakentaa paljon kestävämpiä verrattuna kiinteisiin verkkoihin johtuen niiden kyvystä automaattisesti korjata ja muokata verkkotopologiaansa [2]. Langattomuus ja nopeat muutokset asettavat paljon vaatimuksia käytettäville laitteille ja verkossa käytettäville protokollille. Tulevaisuuden taistelukentällä ad hoc -verkot soveltuvat joukkojen tilannetietoisuuden ylläpitämiseen.

2.3 MANET

Liikkuva ad hoc -verkko (Mobile ad hoc network, MANET) pystytään rakentamaan solmujen ollessa liikkeessä ja normaalin ad hoc -verkon tapaisesti ilman keskitettyä kontrolloivaa yksikköä [12]. MANET-verkot kykenevät itsenäisesti muodostamaan monimutkaisia verkkoja vaikka solmut olisivat liikkeessä. MANET-verkko tarvitsee käyttäjältä vain vähän valvontaa tai manuaalista työtä. Näiden ominaisuuksien vuoksi MANET-verkot soveltuvat erittäin hyvin sotilaskäyttöön. Esimerkiksi nopeasti liikkuvat ja laajalle alueelle hajautetut tiedustelijat pystyvät liikkeestään huolimatta pysymään yhteydessä toisiinsa ja ylempään johtoportaaseen.

MANET-verkoilla on monia erilaisia käyttösovellutuksia erilaisiin toimintaympäristöihin ja tilanteisiin. Esimerkiksi liikkuvat vaunut kykenevät ylläpitämään verkkoaan maastossa, jossa korkeuserot estävät suorat yhteydet solmujen välillä. MANET-verkot tarjoavat mahdollisuu-

den toteuttaa haastavia sotilasoperaatioita. MANET-verkko kyetään pystyttämään sellaiselle alueelle minne ei ole mahdollista rakentaa kiinteää verkkoa. Tällä tavalla sotilaille voidaan muodostaa verkko esimerkiksi vihollisen alueella tai sellaiselle alueelle minne ei ole aikaa rakentaa muita verkkoja. [2]

Vaikka MANET-verkot tarjoavat paljon etuja sotilaskäyttöön niin asettaa se samalla isoja haasteita verkolle ja siinä käytettäville laitteille. Verkon solmujen liikkeen takia sen reititysprotokollan pitää pystyä ylläpitämään yhteysvälit ja mahdollistamaan viestien liikkuminen koko verkossa. Yhteysvälit voivat nopeasti muodostua ja poistua verkosta, jolloin solmuilla pitää olla kyky ylläpitää verkkotopologiaansa. Kiinteän verkon reititysprotokollat eivät kykene vastaamaan liikkuvien solmujen asettamia vaatimuksia. Koska jokainen solmu toimii sekä isäntänä sekä reitittimenä, ne joutuvat pakettien liikkuessa jokaisen yhteysvälin aikana tekemään reitittimen työt. Vaikka MANET-verkot tarjoavat huomattavia etuja taistelukentällä, niin niiden asettamat vaatimukset ohjelmistoille ja laitteille vaatii lisää tutkimusta. [12]

3 REITITYSPROTOKOLLAT

Solmujen jatkuva liike, maasto, viestintävälineiden muuttuminen kiinteistä varmoista yhteyksistä langattomiin epävarmempiin aiheuttavat isoja haasteita MANET-verkkojen reititysprotokollille. Langattomien yhteyksien kaistan leveydet ovat huomattavasti pienempiä verrattuna esimerkiksi kuituyhteyksiin tai muihin kiinteisiin yhteyksiin, jolloin reititysprotokollan pitää pystyä pitämään verkko ruuhkautumatta [4]. Taistelukentällä tiedusteluun, valvontaan ja johtamiseen käytettyjen yhteyksien ylläpitämisen merkityksen kasvaessa on olennaista, että reititysprotokollat pystyvät toimimaan halutulla tavalla [1]. Tästä syystä MANET-verkkoihin on kehitetty useampia erilaisia reititysprotokollia, jotka pystyvät vastaamaan erilaisiin tilanteisiin.

MANET-verkoissa käytettäville reititysprotokollille asetetaan selviä vaatimuksia jotta ne vastaavat haluttuun tarpeeseen. Reititysprotokollan tulee kasvattaa verkon varmuutta. Jokaisella solmulla tulee olla kyky itsenäisesti tehdä päätöksiä verkossa yhteistyössä naapuriensa kanssa. Koska kaksisuuntainen liikenne ei yhteysväleillä aina ole mahdollista, niin reititysprotokollat on suunniteltava oletuksella, että kaikki yhteysvälit olisivat yksisuuntaisia. Koska laitteet, mitä joukot kantavat mukanaan, on suunniteltu mahdollisimman pieniksi, se myös yleensä vaikuttaa niiden akkukokoon. Pienillä akuilla akkukesto on myös yleensä heikompi, joten reititysprotokollien tulee jakaa reitityskuormaa mahdollisimman tehokkaasti pidentääkseen akkukestoa.

MANET-verkkojen suojaus on huomattavasti vaikeampaa kuin esimerkiksi kiinteiden verkkojen. Langattomia yhteyksiä pystytään tiedustelemaan ja häiritsemään helpommin kuin kiinteitä. Fyysisen tason ongelmilta on helpompi suojautua esimerkiksi taajuushypinnällä, mutta reititystason suojaus asettaa enemmän haasteita. Tapoja joilla reititystasolla yritetään suojata viestintää, on esimerkiksi viestien kryptaus tai solmujen välille asennetut todennusjärjestelmät.

Viimeiseksi pitää ottaa huomioon QoS (Quality of Service). Nykyään taistelukentältä vaaditaan reaaliaikaista videokuvaa ja muita raskaita lähetteitä, jolloin reititysprotokollan pitää pystyä suoriutumaan vaatimuksiin nähden. [12]

Reititysprotokollat jakautuvat kahteen luokkaan: reaktiivisiin ja proaktiivisiin. Proaktiivisia protokollia kutsutaan myös taulukko-ohjatuiksi (table-driven) ja reaktiivisia vaatimusohjatuiksi (on-demand). Proaktiiviset protokollat tiedustelevat jatkuvasti naapureiltaan tietoja

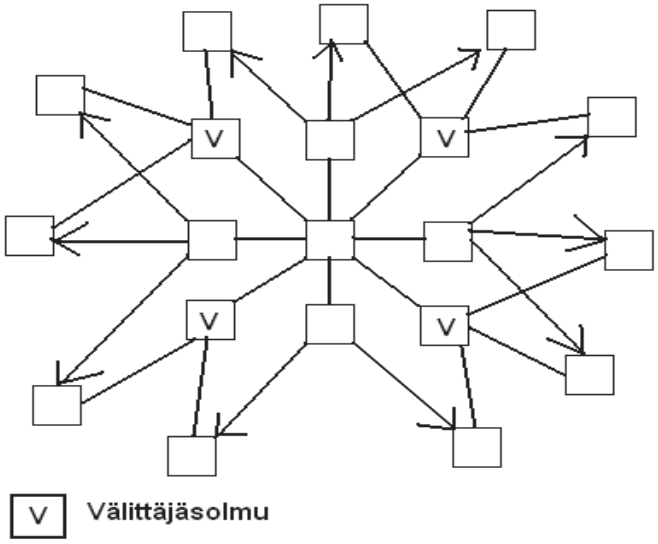
muodostaakseen kuvan verkon rakenteesta. Näistä muodostuvat taulukot joiden avulla verkossa liikennöinti solmujen välillä onnistuu haluttuun tapaan. Reaktiiviset protokollat toimivat herättämällä halutut solmut tarpeen mukaan. Datan liikkuessa verkossa solmut tarpeen mukaan tiedustelevat naapureilta parhaan tavan reitittää liikennettä. Kolmantena luokkana voidaan pitää hybridiluokkaa, jossa sovelletaan kahden aikaisemmin mainitun luokan ominaisuuksia. Hybridiprotokollat joko jatkuvasti toimivat osittain reaktiivisesti ja proaktiivisesti, tai tilanteen mukaan vaihtelevat kokonaan näiden kahden protokollatyypin välillä. Esimerkiksi sotilaiden ollessa lähellä toisiaan verkko toimii proaktiivisesti, mutta hajaantuessa kauemmas toisistaan ja yhteysvälien kasvaessa pidemmiksi verkko vaihtaa protokollan reaktiiviseen. [4]

Verkossa reitittämisessä pitää ottaa myös huomioon viestitystapa. Unicast-lähetykset (yhdeltä yhdelle), multicast-lähetykset (ryhmään lähetykset) ja geocast-lähetykset (maantieteelliseen tietoon perustuva lähetys) asettavat erilaiset haasteet eri reititysprotokollille. Riippuen verkon solmujen määrästä ja tavasta millä lähetykset verkossa toteutetaan voi reititysprotokollalla olla suuri merkitys. [4] [11]

3.1 Optimized Link State Routing

Optimized Link State Routing (OLSR) on paranneltu versio perinteisestä link state routing -reititysprotokollasta. Se perustuu edelleen samaan algoritmiin, mutta tiettyjä asioita on kehitetty aiempiin protokolliin verrattuna. Perinteisessä link state -reitityksessä kaikki naapurisolmujen kanssa muodostetut yhteydet on tunnistettu ja tieto niiden välillä on koko verkossa vuodettu. OLSR:ssä erona on, että se suorittaa tiedon jakamista solmujen uusimmalla tiedolla. Tällä tavalla paketit löytävät kohdesolmun aina, vaikka solmut olisivat liikkeessä. Solmujen liikenopeus ei saa olla liian suuri, koska tällöin solmut eivät välttämättä pysty pitämään kirjaa naapureistaan.

OLSR:ssä optimisaatio on toteutettu kahdella tavalla. Ensimmäiseksi OLSR:ssä solmut eivät enää välitä tietoa kaikkien naapurisolmujen kanssa muodostettujen yhteyksien välillä. Solmuille on käsketty muutama yhteysväli, jonka kautta se reitittää viestinsä. Toiseksi turhia uudelleen lähetyksiä on vähennetty määrittämällä tietyt solmut toimimaan lähetysliikenteen välittäjinä. Tällä tavoin verkon kontrollointiliikennettä minimoidaan, koska vain nämä valitut solmut pystyvät uudelleen lähettämään omia viestejään verkossa lähetyksen aikana. [12]



Kuva 1 Esimerkki OLSR-verkkorakenteesta [12]

Lähettävät solmut laskevat reitin kohdesolmuun näiden välittäjäsolmujen kautta. Välittäjäsolmut valitaan siten, että ne ovat verkossa yhden yhteysvälin päässä solmuista joilla on kaksisuuntaiset yhteydet [12]. Kuva 1 näyttää esimerkin yksinkertaisesta OLSR-verkkorakenteesta ja välittäjäsolmujen sijoittelusta. Välittäjäsolmujen oikealla asettelulla pystytään minimoimaan verkossa tapahtuvaa liikennöintiä.

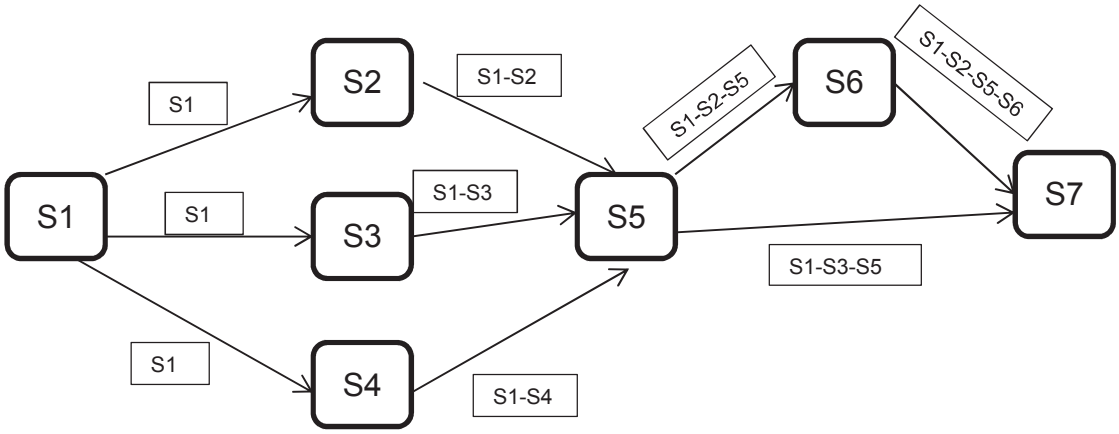
OLSR soveltuu parhaiten verkkoihin joissa on paljon solmuja ja sijaitsevat toisiinsa nähden lähekkäin. Mitä suurempi ja tiheämpi verkko on, niin sitä enemmän solmujen välistä liikennettä pystytään optimoimaan [7]. Tulevaisuudessa maastossa tapahtuvat taistelut ovat hajautettuja, joten OSLR ei välttämättä sovellu parhaiten liikkuvaan sodankäyntiin metsämaastossa. OLSR soveltuu hyvin asutuskeskuksissa tapahtuviin puolustustaisteluihin tai metsämaastossa tapahtuvaan aluepuolustukseen.

3.2 Dynamic Source Routing

Dynamic Source Routing (DSR) perustuu solmujen kykyyn itse muodostaa reitti kohdesolmuun useiden yhteysvälien kautta. Liikkeessä olevien solmujen tulee päivittää omaa reittitietokantaansa kaikista solmulle tiedetyistä reiteistä. Tietokanta päivittyy, kun solmujen välisissä yhteysväleissä tapahtuu muutoksia esimerkiksi liikkeen takia. [12]

Reititys DSR:ssä tapahtuu kahdessa vaiheessa. Ensimmäiseksi solmu tarkistaa omasta tietokannastaan onko sillä jo valmiiksi tiedossa reitti haluttuun kohdesolmuun. Jos reitti on jo tiedossa, niin solmu pystyy suoraan lähettämään paketin kohteeseen. Jos kohteeseen ei ole valmista reittiä tiedossa, niin solmu aloittaa reitin etsimisen lähettämällä tiedustelulähetyksen naapurisolmuihin. Reitin tiedustelulähetykseen sisältyy alkuperäisen viestin kohdesolmun osoite sekä yksilöllisen tunnistenumeron. Tiedustelulähetys kulkee muiden solmujen välityksellä aina kohdesolmuun asti. Tämän jälkeen solmujen reittitietokannat päivittyvät ja paketit voi kulkea normaalisti solmujen välillä. [12]

Solmut käsittelevät tiedustelulähetykset vain siinä tapauksessa jos se ei ole aikaisemmin käsitellyt sitä tai sillä ei ole rekisteröity reittiä haluttuun kohteeseen. Vastaus reitin tiedusteluun lähetetään alkuperäiselle lähettäjälle, kun reitti on selvitetty välissä olevien reitittävien solmujen avulla tai kohdesolmussa. [12]



Kuva 2 Esimerkki DSR-verkkorakenteesta [3]

Kuva 2 esittää esimerkin mahdollisesta DSR-verkkorakenteesta ja reitin etsimisestä. DSR pyrkii hakemaan reitin missä on mahdollisimman vähän solmuja välissä.

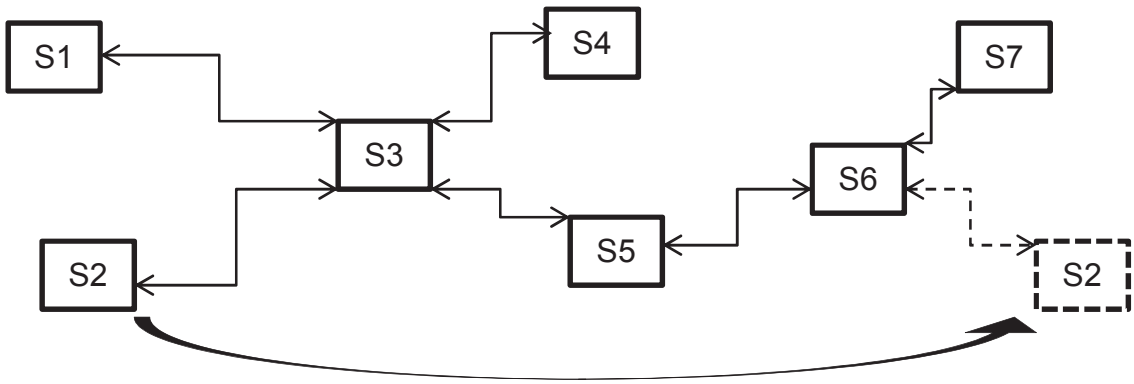
DSR-protokollaa voidaan pitää varmana reititysprotokollana, koska solmut reaktiivisesti itse ylläpitävät verkon kuntoa. Ongelmaksi nousee, että verkon kasvaessa se voi ruuhkautua helposti ja solmujen välisten etäisyyksien kasvaessa tiedonsiirto voi hidastua tai katketa kokonaan. DSR:ää voi käyttää liikkuvassa sodankäynnissä, mutta solmujen määrä ei saa kasvaa liian suureksi.

3.3 Dynamic Destination-Sequenced Distance-Vector Routing Protocol

Dynamic Destination-Sequenced Distance-Vector Routing Protocol (DSDV) perustuu Bellman-Ford-reititysalgoritmiin, mutta siihen on tehty muutoksia. Jokainen verkon solmu ylläpitää reittitietokantaa, joka sisältää mahdolliset kohdesolmut ja niiden välillä olevan yhteysväli-

en määrän. Jokainen kohde on merkitty sarjanumerolla, joka määräytyy kohdesolmun perusteella. Verkon solmut pitävät yllä topologiaansa kahdella tavalla. Verkon solmut ylläpitävät reittitietokantaansa jaksottaisilla päivityslähetyksillä tai jos verkossa tapahtuu suurempia muutoksia – esimerkiksi solmu tai tärkeä yhteysväli katoaa verkosta – niin päivityslähetykset suoritetaan välittömästi. DSDV-verkossa solmut mainostavat omaa reittitietokantaansa broadcasting- tai multicasting-menetelmällä sen hetkisille naapureilleen. Koska solmut mainostavat omia tietokantojaan niin verkon kaikilla solmuilla on sen hetken uusin tieto verkon topologiasta ja siinä tapahtuneista muutoksista. Jatkuvat reittitietokantojen mainostamiseen tehdyt lähetykset voivat ruuhkauttaa verkkoa turhaan. [12]

DSDV-verkot pitävät yllä reititystietokantojaan kahdella tavalla. Solmu pystyy lähettämään koko reititystietokannan tai osan siitä naapureilleen. Solmut lähettävät harvemmin koko reititystietokantaansa naapureille, jos verkossa ei tapahdu paljoa liikettä. Jos verkon topologiassa ei tapahdu paljoa muutoksia, niin solmujen on tehokkaampi lähettää vain osa reittitietokannastaan. Jos verkon solmujen välille syntyy paljon liikettä, niin näitä osapäivityksiä tulee liikaa ja niistä saattaa kasvaa liian suuria, jolloin verkko saattaa ruuhkautua (NPDU). Tällaisissa tapauksissa koko reititystietokannan lähettäminen on yleensä tehokkaampaa. Lähetetyt paketit, joilla päivitetään solmujen reittitietokantoja, sisältävät sarjanumeron joka määräytyy lähdesolmun perusteella. Korkein sarjanumero tarkoittaa, että se on uusin, jolloin solmut päivittävät reittitietokantansa sen perusteella. Solmut lähettävät mainoslähetyksiään tietyillä aikaintervalleilla, jolloin reitit on muodostettu uusimmalla tiedolla ja ne toimivat parhaiten. [12]



Kuva 3 Esimerkki DSDV-verkkorakenteesta [12]

Kuvan 3 esimerkin mukaisesti, jos solmu 2 (S2) siirtyy S6:n viereen, niin koko verkonkuvaa ei tarvitse muokata vaan pelkästään S2:n siirto tarvitsee päivittää reititystietokantoihin. Tieto siirrosta siirtyy solmujen välillä ja päivittyy tietokantoihin.

DSDV:tä tulisi käyttää silloin jos verkon topologiaa halutaan ylläpitää jatkuvasti ja tarkasti. Eri komentopaikkojen välisten yhteyksien varmistaminen soveltuu DSDV:lle hyvin. Myös

virran kulutus tai kaluston tehokkuus ei ole ongelmana, sillä komentopaikkojen yhteydessä on tehokkaampaa kalustoa sekä mahdollisesti verkkovirtaa, mitä jalkaisin liikkuvilta joukoilta ei välttämättä löydy.

3.4 Ad hoc On-Demand Distance Vector Routing

Ad Hoc On-Demand Distance Vector Routing (AODV) on kehittyneempi versio DSDV:stä. DSDV:n ollessa proaktiivinen reititysprotokolla, niin AODV on reaktiivinen. AODV:ssä vähennetään lähetyksien määrää muodostamalla reittejä vain tarpeen vaatiessa. DSDV:ssä lähdesolmun lähettäessä paketteja sen tulee lähettää naapurisolmuihin reitintiedustelupaketti. Naapurisolmujen tulee välittää tiedustelupakettia kunnes se löytää kohdesolmun. Tiedustelulähetyksen aikana välittäjäsolmut tallentavat tietokantaansa reitin naapurisolmuun mistä tiedustelulähetys saapui. Tällä tapaa liikenne vastakkaiseen suuntaan nopeutuu.

Jos välittäjäsolmuihin tai kohdesolmuun saapuu sama tiedustelulähetys, niin ne hylätään. Vastaus kohdesolmusta lähdesolmuun toteutetaan muodostettua reittiä pitkin. [12]

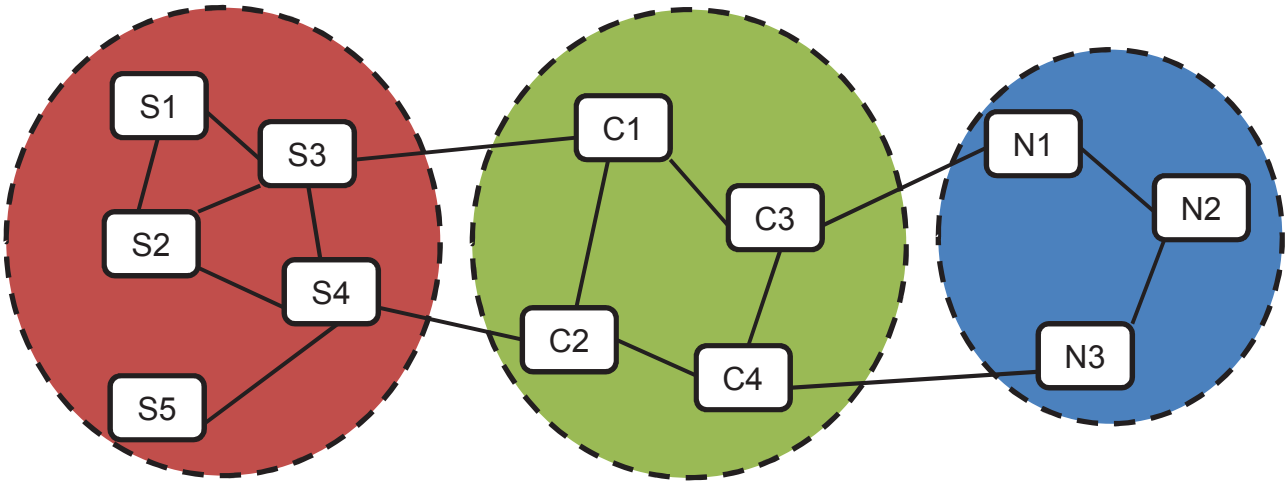
Lähdesolmun liikkuessa se lähettää uuden reitintiedustelulähetyksen. Jos reitillä oleva välittäjäsolmu liikkuu sen naapurit pystyvät lähettämään tiedon tästä kohdesolmuun, tämän jälkeen kohdesolmu päättää tarvitseeko uutta reittiä solmujen välillä tiedustella. AODV:n ero DSDV:hen on, että paikallisen linkin katketessa se ei lähetä lähetystä koko verkkoon. Poikkeuksena on jos reitti toimii käynnissä olevan yhteyden reitillä tai jos se kuuluu olemassa olevaan multicast-puuhun [4]. AODV suorittaa reitintiedustelulähetyksiä reaktiivisesti, eli silloin jos lähetykselle on tarve. [4] [12]

AODV ei ruuhkaudu niin helposti kuin DSDV, jolloin sitä voidaan käyttää esimerkiksi sellaisissa verkoissa, joissa solmut liikkuvat paljon. Myös virrankulutus on pienempää. AODV soveltuu taktisen tason sodankäyntiin – esimerkiksi ryhmien väliseen viestintään maastossa.

3.5 Zone Routing Protocol

Zone Routing Protocol (ZRP) soveltuu hyvin verkkoihin, joissa solmut ovat levinneet suurelle alueelle ja liikkuvat paljon. ZRP on proaktiivinen protokolla, jossa solmut ylläpitävät reittitietokantaansa aluekohtaisesti. Tätä aluetta kutsutaan reititysalueeksi. [12]

Solmut muodostavat reitit tiedustelemalla naapureiltaan yhteysväliä ja saamalla vastauksen kohdesolmulta. Reititysalueet muodostuvat useista solmuista, jotka tietävät omat naapurisolmunsa. Naapurisolmu määritellään solmuna, jonka kanssa voidaan muodostaa suora yhteys ilman välittäjäsolmuja. ZRP:ssä pakettien lähettäminen suoritetaan reitin tiedustelulla missä tiedustelulähetys ohjataan poispäin lähdesolmusta ja katetuista reititysalueista. Tiedustelulähetyksen edetessä yksittäinen solmu tunnistaa, onko kohdesolmu sen reititysalueella ja merkitsee kaikki solmut katetuiksi, jos kohdesolmu ei kuulu niihin. Lähetys etenee reititysalueesta seuraavaan, kunnes välittäjäsolmu tunnistaa kohdesolmun ja ohjaa lähetyksen siihen. Kohdesolmu vastaa lähdesolmulle käyttäen käänteisesti muodostettua reittiä. [12]



Kuva 4 Esimerkki ZRP-verkkorakenteesta [13]

ZRP:tä kyetään hyödyntämään suurien verkkojen reitityksessä. Suuri verkko voi olla esimerkiksi prikaatitason verkko. Kuvan 4 eriväriset ympyrät voisivat kuvata prikaatin pataljoonia ja neliöt niiden sisällä niiden yksiköitä. Alueiden sisällä voi olla myös mahdollista käyttää eri reititysprotokollia kuitenkin niin, että koko ZRP-verkon alla toimivien solmujen väliset yhteydet pysyvät yllä liikkeestä riippumatta.

4 AD HOC -SIIRTOTIET

Fyysinen kerros sisältää viestiliikenteen tekniikan jossa yhteyden raakabitit kulkevat. OSI-malli (liite 2) kuvaa eri kerrosten vastuut ja niiden alle kuuluvat protokollat. Langattomissa verkoissa, kuten MANET-verkoissa, fyysisen kerroksen tehtävänä on muodostaa yhteydet muiden solmujen välille. Tämä tapahtuu esimerkiksi radioteitse. Fyysisen kerroksen muita tehtäviä on väylän kapasiteetin jakaminen kanavien kesken, kanavakoodaus, virheenkorjaus sekä joissain tapauksissa myös salaaminen. Ad hoc -verkoissa voi olla useita solmuja, jonka takia fyysisen kerroksen toimivuus on olennaista. [4]

Vaihtoehtoja langattoman verkon fyysisen kerroksen toteutukseen on useita. Sotilasympäristöissä yleisin toteutusmalli on radiotaajuuksien käyttäminen. Muita vaihtoehtoja ovat infrapunataajuudet tai lasersäteily. Oikeanlaisen tekniikan valinta fyysiselle kerrokselle on tärkeää viestiyhteydelle, koska se määrittelee pitkälle verkon topologian toimivuuden sekä solmujen välisen tiedonsiirtokapasiteetin. [4]

Sotilasympäristöissä ad hoc -verkkoja on toteutettu usein myös langallisin yhteyksin. Tällöin verkosta voidaan käyttää nimitystä semi ad hoc -verkko [4]. Langattomiin verrattuna langalliset yhteydet ovat varmempia ja tarjoavat myös vakaamman tiedonsiirtokapasiteetin.

Tutkimuksessa tarkastellaan MANET-verkkoihin soveltuvia siirtoteitä. Langalliset yhteydet ovat solmujen liikkeestä johtuen hankala toteuttaa, joten tutkimuksessa käsitellään ainoastaan langattomia yhteyksiä, joita voidaan muodostaa suoraan solmulta toiselle.

4.1 VHF-kaista

Very high frequency eli VHF-kaista soveltuu liikkuvaan sodankäyntiin useasta syystä. Se tarjoaa kenttäolosuhteisiin nähden sopivan tasapainon kantaman, tiedonsiirtonopeuden ja tehonkulutuksen välillä. VHF-kaistalla toimivien radioiden taajuus on yleensä 30-88 MHz:n välillä. [8]

Käytettävien radioiden tehot vaihtelevat 0,25 W:n ja 50 W:n välillä riippuen siitä, onko laite jalan kannettavana vai ajoneuvossa. 30-88 MHz:n taajuusvälillä voidaan päästä alemmilla lähetystehoilla 8-9 kilometrin ja ylemmillä 50 kilometrin kantamaan. Pitkän kantaman ja korkean lähetystehon käyttö ei välttämättä ole tarkoituksenmukaista, sillä se lisää todennäköisyyttä lähettäjän havaitsemiseen elektronisella tiedustelulla. [8]

Nykypäivän ja tulevaisuuden sodankäynnissä radioiden määrä on kasvanut, jonka takia niiden väliset kantamat ovat keskimäärin pienentyneet. Tämä sen sijaan mahdollistaa korkeampien taajuuksien käyttämistä, jolloin radioiden välistä siirtokapasiteettia kyetään kasvattamaan. Radioiden laskentateho on myös kasvanut teknologian kehityksen ohessa, jolloin niitä on mahdollista käyttää MANET-verkossa reititykseen. [8]

4.2 TETRA

Trans-European Trunked Radio (TETRA) toimii trunking-järjestelmänä, joten siinä voidaan luoda yhteys radioiden välillä suoraan tai tukiaseman kautta. Yleisesti yksityisen ja viranomaissektorin käytössä oleva standardi mahdollistaa tiedon välityksen vaativissa olosuhteissa. Normaalisti radiot keskustelevat tukiaseman kautta, mutta jouduttuaan esimerkiksi katveeseen tukiasemasta, ne kykenevät muodostamaan suoria yhteyksiä keskenään (Direct Mode Operation, DMO), joka on merkittävä taktinen etu verrattuna esimerkiksi GSM-verkkoon. [8]

TETRA-järjestelmä käyttää Euroopassa 380-400 MHz:n ja 410-430 MHz:n kaistoja [8]. 410-430 MHz:n taajuusalue on kaupallisille lisensseille varatussa käytössä. Yhden kanavan nopeus on 7,2 kbit/s, jolloin kaikkien neljän kanavan ollessa käytössä suurin tiedonsiirtonopeus on 28,8 kbit/s. Tilaajaradioiden teholuokka on 1-30 W. Tilaajat sekä tukiasemat kykenevät toimimaan liikkeestä, joka lisää järjestelmän taktisen käytön mahdollisuuksia. [8] [6]

TETRA:n tietoturvaominaisuudet mahdollistavat sen liikenteen siirtämisen muihin verkkoihin [8]. Taistelukäytössä ongelmat esiintyvät sen häirintäsietokyvyssä. Toimiessaan alemmalla toimintataajuudella järjestelmän etenemisvaimennus on pienempi, jonka takia TETRA:lla on huonompi suoja häirintää vastaan.

4.3 WLAN-standardit

Wireless local area network (WLAN) -standardit toimivat 2,4 GHz:n ja 5 GHz:n taajuusalueilla. Korkeilla taajuusalueilla kyetään luomaan suuren tietosiirtonopeuden omaavia yhteyksiä, mutta yhteysvälit jäävät lyhyiksi. Institute of Electrical and Electronics Engineers (IEEE) -järjestön 802.11-standardit toimivat näillä taajuusalueilla ja tavallisimmat käytetyt modulointitekniikat ovat Frequency-hopping spread spetrum (FHSS) ja Direct-sequence spread spectrum (DSSS). Kaikki standardit mahdollistavat liikennöinnin 100 metrin etäisyydellä esteettömässä tilassa, mutta kantamaa on mahdollista kasvattaa suuremmaksi. [14]

4.3.1 802.11-standardit

Alkuperäisen 802.11 legacy -standardin pohjalta muokattiin 802.11a WLAN -standardi. Standardi kykenee teoriassa 5 Mbit/s tiedonsiirtonopeuksiin, vaikka käytännön nopeudet ovat 1-2 Mbit/s alueella. 802.11a:n taajuusalue on 5GHz jonka takia yhteydet tarvitsevat esteettömän näköyhteyden. Tästä syystä standardi soveltuu huonosti taktisesti hyödylliseen käyttöön. [14]

802.11b toimii 2,4 GHz:n taajuusalueella. Sen tukee ainoastaan 11 Mbit/s tiedonsiirtonopeutta. 2,4 GHz:n taajuusalue on siitä ongelmallinen, että sitä ei ole säännöstelty tiettyä käyttöä varten (vrt. TETRA 380-400 MHz ja 410-430 MHz). Tästä syystä lähetykset ja laitteet saattavat kärsiä muista samalla taajuusalueella toimivista laitteista. Kantama riippuu ympäristöstä, lähetystehosta ja vastaanottimesta. [14] [15]

802.11g toimii 2,4 GHz:n taajuusalueella ja kykenee jopa 54 Mbit/s siirtonopeuksiin. Standardissa yhdistetään 802.11a:n ja 802.11b:n hyviä puolia. Standardeja yhdistämällä on saatu yhteysväleille parempi kantama ja tiedonsiirtonopeudet ovat myös kasvaneet. 2,4 GHz:n alueella toimimisesta esiintyy kuitenkin samoja häiriöongelmia, kuin aikaisemmin. [14]

802.11n tarkoituksena on kasvattaa tiedonsiirtonopeudet WLAN-verkoissa jopa 600 Mbit/s tasolle. Käytännön nopeudet ovat kuitenkin 100-200 Mbit/s luokkaa. Tekniikka perustuu usean antennin käyttöön jolloin tiedonsiirtonopeuksia pystytään kasvattamaan. 802.11n pystyy toimimaan 2,4 GHz:n ja 5 GHz:n taajuusalueilla. Kantamat voivat olla parhaimmillaan 800 m luokkaa. [14] [16] [17]

4.3.1 Bluetooth

Bluetooth toimii 2,4 GHz:n taajuusalueella. Yhteysvälin kantama riippuu minkä luokan laite on kyseessä. Bluetooth-laitteet on luokiteltu kolmeen eri luokkaan lähetystehon ja kantaman perusteella:

1. luokka: Suurin lähetysteho 100 mW, kantama noin 100 m
2. luokka: Suurin lähetysteho 2,5 mW, kantama noin 10 m
3. luokka: Suurin lähetysteho 1 mW, kantama noin 1 m

Toistaiseksi Bluetooth ei ole soveltunut lähiverkkojen rakentamiseen pienen tiedonsiirtokykynsä johdosta, mutta vuonna 2009 ilmestynyt Bluetooth 3.0 kykenee jo 24 Mbit/s tiedonsiirtonopeuksiin. Tiedonsiirtonopeuden kasvun myötä Bluetooth soveltuu myös lähiverkkojen muodostamiseen. [14] [18]

Samalla taajuusalueella toimivien laitteiden häirinnän välttämiseksi käytetään Bluetoothissa taajuushypintää [14]. Bluetooth soveltuu hyvin pinta-alallisesti pienen alueen tiedonsiirron toteuttamiseen. Tietoturva on toteutettu kahdella eri tekniikalla: laitteiden todennuksella ja lähetyksen salaamisella. Näin Bluetooth on myös käytössä tietoturvallinen [14] [18].

4.4 Siirtoteiden vertailu

Reititysprotokollan toiminnan kannalta on olennaista valita tarpeeseen sopiva siirtotie. Vaikuttavia muuttujia on solmujen etäisyys toisistaan, toimintaympäristö sekä minkälaista dataa yhteysvälillä tulee liikkumaan.

Taulukko 1 Eri siirtoteiden perusominaisuuksia

Siirtotie	Taajuus	Teho	Kantama*	Tiedonsiirtokyky**
VHF	30-88 MHz	0,25W, 50W	8-9 km, 50 km	16 kbit/s (puhe), 9600 bit/s (data)
TETRA	380-400 MHz, 410- 430 MHz	1-30 W	250 m (DMO)	28,8 kbit/s
802.11a	5 GHz	100 mW	120 m	1-2 Mbit/s
802.11b	2,4 GHz	100 mW	140 m	11 Mbit/s
802.11g	2,4 GHz	100 mW	140 m	54 Mbit/s
802.11n	2,4 GHz, 5 GHz	100 mW	250 m	600 Mbit/s
Bluetooth	2,4 GHz	1 mW, 2,5 mW, 100 mW	1 m, 10 m, 100 m	24 Mbit/s

* Tyypillinen kantama maastossa, riippuu käytettävästä kalustosta, antennista ja maastosta.
** Suurin tiedonsiirtokyky, riippuu käytettävien kanavien määrästä.

Taulukosta 1 voidaan havaita, että taajuuden noustessa myös tiedonsiirtokyky paranee, mutta tehokkaan kantaman etäisyydet huononevat. Langattomissa yhteyksissä joissa tarvitaan suuria tiedonsiirtokykyjä, on yleensä turvauduttava WiFi-tekniikkaan.

Teho vaikuttaa käytettävän kaluston kokoon. Suuret virtalähteet ja akustot vaikuttavat joukon liikkumiskykyyn hidastavalla tavalla. Suuria määriä sähkömagneettista säteilyä tuottavat joukot ovat myös helpommin havaittavissa. Solmujen välisen yhteyden ylläpito on siirtotietä valittaessa prioriteetti, mutta on huomioitava kuinka pitkään tätä siirtotietä voidaan ylläpitää ilman huoltoa, sekä mitä muita riskejä sen valinnassa mahdollisesti on.

Siirtotietä valittaessa on huomioitava muut sen mukana tulevat ominaisuudet. VHF:llä voidaan muodostaa pitkiä yhteysvälejä, mutta sen havaitseminen on suhteellisen helppoa tutkaamalla. WiFi-tekniikassa käytettävät pienet lähetystehot ja pienet kantamat voivat tehdä yhteysväleistä vaikeasti havaittavia, mutta helposti häirittäviä ja kuunneltavia.

5 JOHTOPÄÄTÖKSET

Erilaisten ad hoc -reititysprotokollien soveltuvuus riippuu toimintaympäristöstä, verkon rakenteesta, kalustosta sekä tehtävästä. Joukon liikkuvuus vaikuttaa siihen kykeneekö reititysprotokolla pitämään yllä verkkotopologiaansa vaaditulla tasolla. Taistelukentällä ei ole enää samanlaisia statiivisia puolustustaisteluja mitä ennen on ollut, joten kaikki taistelun lajit vaativat reititysprotokollilta kykyä vastata solmujen liikkeeseen.

Johtaminen korostuu nykysodankäynnissä ja siinä eteenkin tilannetietoisuuden ylläpitäminen. Joukkojen hajauttaminen ja niiden liikkeessä oleminen vaikuttaa tiedon siirtymiseen komentopaikoille. Jotta tieto saadaan alajohtoportailta yläjohtoportaille, niin tarvitaan taisteluun soveltuvat siirtotiet ja joukon rakenteelle sopivat reititysprotokollat.

OLSR soveltuu parhaiten suuriin tiheisiin verkkoihin. Jos joukot ovat laajalle alueelle hajautettuna ja solmujen välinen liike kasvattaa etäisyydet niiden välillä liian suuriksi, niin kyseinen reititysprotokolla ei välttämättä tue joukon taistelua parhaalla tavalla. Paras tapa soveltaa kyseistä reititysprotokollaa on silloin, kun solmut liikkeestään huolimatta pysyvät toisistaan verkkotopologian rakenteen ylläpitämisen tarvittavissa rajoissa. OLSR-verkossa eri siirtoteitä voitaisiin hyvinkin yhdistellä. Jos joukolta ei tarvita tietoa mikä vaatii suurta tiedonsiirtonopeutta, se voisi käyttää VHF-yhteyksiä. Tarvittaessa tieto voitaisiin siirtää korkeammilla taajuuksilla esimerkiksi käyttämällä 802.11-, TETRA- tai Bluetooth-yhteyksiä.

DSR toimii reaktiivisena reititysprotokollana resurssitehokkaasti. Ainoana ongelmana siinä esiintyy, että verkon solmujen määrän kasvaessa se saattaa helposti ruuhkautua. DSR soveltuu myös MANET-verkkoihin ja liikkuvaan sodankäyntiin, mutta solmujen väliset etäisyydet eivät saa kasvaa liikkaa, koska tällöin liikennöinti verkossa hidastuu. Yksi tapa hyödyntää DSR:ää on pitää sitä esimerkiksi käytössä joukkueen kokoisissa verkoissa ja jatkaa yhteys yläjohtoportaisiin eri kanavaa sekä reititysprotokollaa pitkin. Joissain tapauksissa siirtotienä pystyttäisiin käyttämään jopa korkeita 2,4 GHz:n taajuuksilla olevia (esim. 802.11n) yhteyksiä. Tällöin voisi olla mahdollista esimerkiksi siirtää suoraa videokuvaa joukkojen välillä reititettynä yläjohtoportaille. Yleensä jatkoyhteys yläjohtoportaille jouduttaisiin etäisyyksien vuoksi jatkamaan kiinteällä yhteydellä, kuten valokuidulla.

AODV:n resurssitehokkuus ja kyky ylläpitää melkein samalla tasolla verkkotopologiaansa DSDV:hen verrattuna tekee siitä taktisesti käyttökelpoisemman reititysprotokollan edeltäjäänsä verrattuna. Liikkeestä riippumatta AODV kykenee ylläpitämään verkkotopologiansa.

AODV ei silti sovellu käyttöön liian suuriin verkkoihin, koska niissä se kärsii yhteyksien ylläpitämisestä sekä tiedonsiirron hidastumisesta. AODV voidaan käyttää esimerkiksi komppanian hyökkäys- tai puolustustaistelussa. Tällöin verkon solmujen määrä ei kasva liian suureksi ja niiden liike ei haittaa verkkotopologian ylläpitoa.

ZRP:tä voidaan käyttää suurissa verkoissa joissa solmujen välillä tapahtuu paljon liikettä. Tätä reititysprotokollaa kyetään käyttämään hyväksi suurien joukkojen hyökkäys- ja puolustustaisteluissa. Riippuen mitä dataa solmujen välillä halutaan liikkuvan, niin siirtoteitä voidaan jälleen kerran vaihdella. Pidemmille yhteysväleille soveltuvat parhaiten VHF-siirtotiet, mutta tällöin tulee muistaa, että tiedonsiirtonopeus hidastuu. Jos suuria määrää tietoa halutaan siirtää pidempiä matkoja, niin tehokkaampana voidaan pitää kiinteiden yhteysvälien hyödyntämistä. Tällöin paljon liikkuvien, mutta tiiviiden sekä pienten joukkojen sisällä voidaan käyttää esimerkiksi 802.11- tai Bluetooth-yhteyksiä, ja näiltä joukoilta yhteydet voidaan jatkaa käyttämällä tukiasemalta lähtevää kiinteää yhteyttä.

Ad hoc -reititysprotokollien jatkotutkimuksia tulisi suorittaa kenttätutkimuksin. Suomen ollessa maa, jossa voidaan taistella vahvasti hajautettujen joukkojen kanssa, tarvitaan viestijärjestelmiä, joilla nämä liikkuvat hajautetut joukot kykenevät kommunikoimaan ja päivittämään tilannetietojaan. Jo taistelijatasolla voidaan kerätä sekä jakaa tietoa esimerkiksi sotilaan terveydentilasta [19]. Useasta kohteesta tällaisen data siirtäminen kuormittaa siirtoväylää raskaasti.

Mahdollinen jatkotutkimusaihe voisi olla reititysprotokollien kokeilu eri sovelluksissa. Tutkimalla eri joukkotasoilla saman sovelluksen toimintaa, mutta vertaamalla siirtoteiden sekä reititysprotokolla valintojen vaikutusta tiedonsiirtoon, voitaisiin selventää eri sovelluksille sopivimmat vaihtoehdot. Asejärjestelmä joka huomattuaan vihollisen toteuttaa automaattisesti vastatoimet siihen, mutta välittää myös tiedon havainnosta ja käskyn vastatoimista lähellä oleville maa-, meri- ja ilmajoukoille, vaatisi reititysprotokollalta nopeaa verkkotopologian päivityskykyä laajalla alueella erilaisiin viestijärjestelmiin. Muita tutkimuskohteita on uuden kaluston sisäänotto ja sille sopivimman reititysprotokollan löytäminen riippuen sen käyttötarkoituksesta.

LÄHTEET

[1] Kosola J., *Teknologisen kehityksen vaikutuksia sodankäyntiin 2015-2025*, Helsinki, Maanpuolustuskorkeakoulu, 2011, ISBN 978-951-25-2166-1 (verkkojulkaisu)

[2] Jormakka J., Oksa S., *Technical Solutions for Network Enabled Defence,* Helsinki, Maanpuolustuskorkeakoulu, 2006, ISBN 951-25-1723-X

[3] Jormakka J., Candolin C., *Military Ad Hoc Networks*, Helsinki, Maanpuolustuskorkeakoulu, 2004, ISBN 951-25-1544-X

[4] Kuosmanen P., *Taktisten ad hoc-radioverkkojen toteuttamismahdollisuudet erilaisissa toimintaympäristöissä*, Helsinki, Maanpuolustuskorkeakoulu, 2004, ISBN 951-25-1562-8

[5] *Wireless Mesh Networks for Military and Public Safety*, MeshDynamics, Saatavuus: http://www.meshdynamics.com/military-mesh-networks.html

[6] Jyri Kosola, *Sotateknisen arvion ja ennusteen kehittäminen*, Diplomityö, Maanpuolustuskorkeakoulu, 2005.

[7] Petteri Kuosmanen, *Classification of Ad Hoc Routing* Protocols, Merisotakoulu, Saatavuus: http://www.netlab.tkk.fi/opetus/s38030/k02/Papers/12-Petteri.pdf

[8] Kosola J., Solante T., *Digitaalinen taistelukenttä: Informaatioajan sotakoneen tekniikka*, Helsinki, Maanpuolustuskorkeakoulu, 2003, ISBN 951-25-1449-4

[9] NATO, Land Operations in the year 2020 (LO2020), 1999 Saatavuus: http://ftp.rta.nato.int/public//PubFulltext/RTO/TR/RTO-TR-008///$$TR-008-ALL.PDF

[10] RAND, Improving communications in Urban Warfare, 2002, Saatavuus: http://www.rand.org/pubs/research_briefs/RB3029/index1.html

[11] Kuosmanen P., *Choosing routing protocol for military ad hoc networks based on network structure and dynamics,* Helsinki, Helsinki University of Technology, 2002, Saatavuus: http://www.netlab.tkk.fi/opetus/s38310/01-02/kuosmanen_030902.pdf

[12] Misra S., Woungang I., Misra S.C., *Guide to Wireless Ad Hoc Networks*, Springer, 2009, s. 59-96, ISBN 978-1-84800-327-9

[13] Nicklas Beijar, Zone Routing Protocol (ZRP), Helsinki University of Technology, Saatavuus: http://fb.yenol.net/2007fall/advcomnet/papers/ZRP.pdf

[14] Mäkynen Jaakko, *WLAN tekniikan soveltuvuus MESH-käytössä sotilasvoimissa.* Pro gradu-tutkielma, Maanpuolustuskorkeakoulu, 2009.

[15] http://en.wikipedia.org/wiki/IEEE_802.11b-1999

[16] http://en.wikipedia.org/wiki/IEEE_802.11n-2009

[17] http://en.wikipedia.org/wiki/IEEE_802.11#802.11n

[18] http://fi.wikipedia.org/wiki/Bluetooth

[19] Hock Beng Lim, A Soldier Health Monitoring System for Military Applications, Singapore, 2010

[20] Nilsson R., *Differnce Between 2.4 GHz and 5 GHz Wireless Lan,* Digi-Key, 5.3.2012, Saatavuus: http://www.digikey.com/us/en/techzone/wireless/resources/articles/difference-between-24-ghz-5-ghz-wireless-lan.html

[21] Hirvonsalo J-H., *Sotilaan paikkatiedon siirtäminen tietoverkoissa,* Maanpuolustuskorkeakoulu, 2011, Saatavuus: https://www.doria.fi/bitstream/handle/10024/74442/SM636.pdf?sequence=1

[22] http://fi.wikipedia.org/wiki/TETRA

[23] TETRA, Direct Mode Applications (DMO), TCCA, Saatavuus: http://www.tandcca.com/about/page/12026

LIITELUETTELO

Liite 1 Tutkimuksessa käytettävät keskeisimmät käsitteet

Ad hoc: Verkossa käytettävä viestimistapa jossa laitteiden välinen liikennöinti suoritetaan ilman tukiasemia. Langattomassa ad hoc -verkossa verkon rakentaminen ja ylläpito tapahtuu automaattisesti.

MESH: MESH-verkossa jokaisen verkon solmun on omien viestien vastaanottamisen lisäksi kyettävä reitittämään muiden solmujen viestejä. MESH-verkot ovat automaattisesti reitittyviä. MESH-verkko pystyy itsenäisesti vaihtamaan tukiasemiaan ja pystyy näin korjaantumaan verkkoon tullessa muutoksia.

MANET: (Mobile Ad hoc Network) MANET-verkot muistuttavat paljon MESH-verkkoja, mutta verkon solmut ovat liikkeessä. Usean langattoman laitteen MANET-verkko voidaan muodostaa nopeassa ajassa ilman valmista infrastruktuuria.

QoS: (Quality of Service) Kuvaa verkon kykyä toteuttaa siinä tapahtuvaa liikennettä. Arvioitavia ominaisuuksia on esimerkiksi viive, palvelun saatavuus ja datapakettien häviämisen todennäköisyys.

Verkkotopologia: Verkkotopologian muodostaa verkossa olevat solmut ja niiden välille muodostuvat yhteydet. Verkon perusrakenne rakentuu näistä yhteysväleistä ja solmuista.

Solmu: Solmu on verkossa oleva yhteyspiste joka välittää viestin eteenpäin tai on yhteysvälin päätepiste. Fyysisellä tasolla solmu on verkossa oleva laite joka vastaanottaa, lähettää ja välittää dataa.

Reititysprotokolla: Reititysprotokolla määrittää kuinka verkon reitittimet tai solmut keskustelevat keskenään. Solmut jakavat tietoa välittömästi naapurissa olevien solmujen kanssa ja tämän jälkeen tieto jaetaan eteenpäin jolloin jokaiselle solmulle muodostuu kuva verkkotopologiasta..

Proaktiivinen protokolla: Proaktiiviset reititysprotokollat jakavat jatkuvasti tietoa solmujen sijainneista ja tilasta verkossa. Jokaisella solmulla on tällöin välittömästi tiedossa verkon topologia datan lähettämistä, vastaanottamista tai välittämistä varten.

Reaktiivinen protokolla: Reaktiiviset reititysprotokollat alkavat jakaa tietoa toisilleen vasta siihen tullessa tarvetta. Esimerkiksi viestin lähtiessä yhdeltä solmulta toiselle välissä olevat solmut heräävät tiedustelemaan naapurisolmuilta verkkotopologiaan liittyvää tietoa.

Trunking-järjestelmä: Suljettu radiojärjestelmä, jonka kantamaa on vahvennettu tukiasemaverkon kautta.

Frequency-hopping spread spectrum (FHSS): FHSS tunnetaan myös taajuushyppelynä. Radiolähetyksessä taajuutta vaihdetaan tietyn algoritmin mukaisesti. Algoritmi voi olla satunnainen tai etukäteen sovittu. Jotta yhteys toimisi, sekä lähettäjän että vastaanottajan tulee tietää algoritmista johtuva taajuusvaihtelevuus.

Direct-sequence spread spectrum (DSSS): Suorasekventointia käyttäessä lähetys puretaan pieniin paloihin ja lähetetään koko käytettävällä taajuusalueella yhtenä signaalina.

Reititystaulu: Solmu voi tallentaa tietokantaansa mahdollisien eri reittien tietoja. Reititystaulu sisältää tietoja naapurisolmujen etäisyydestä, eli kuinka monen hypyn päässä kukin solmu sijaitsee toisestaan. Muita tallennettavia tietoja voivat olla esimerkiksi väylien nopeudet, solmujen nimet ja muu verkkokuvan ylläpitoon tarvittava informaatio.

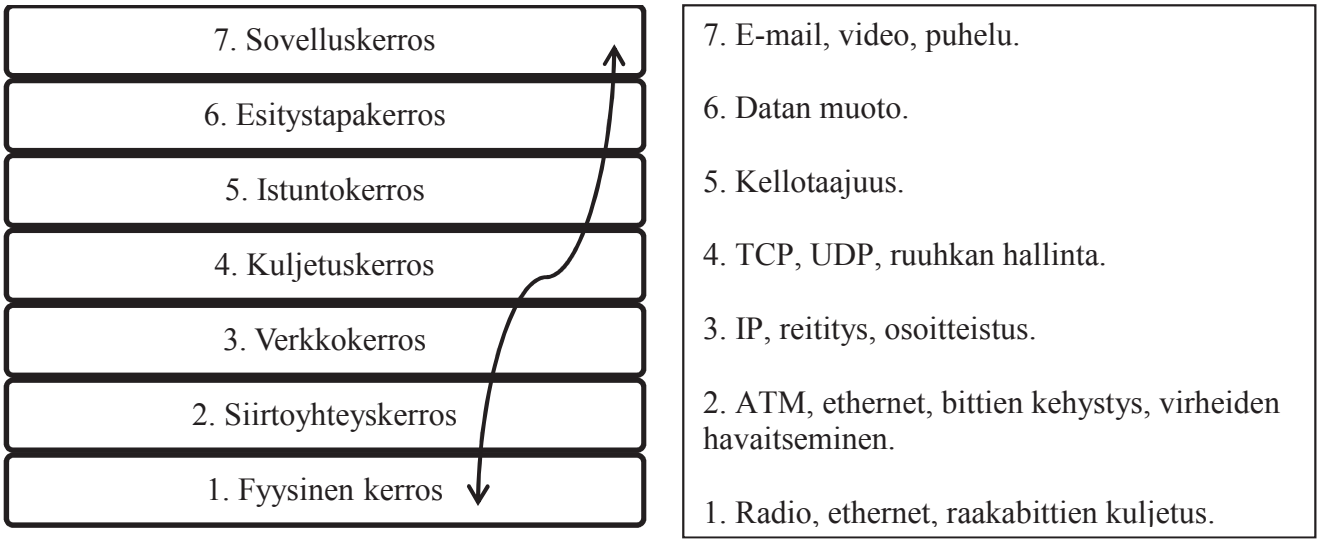
NPDU: Network Protocol Data Unit. Yksikkö jonka tarkoituksena on määrittää kyseisen verkkokerroksen protokollan sisältämää informaatiota esimerkiksi käyttäjätietoja tai osoitetietoja.

Liite 2 OSI-malli (Open System Interconnection)

Kansainvälinen standardointiorganisaatio ISO (International Organization for Standardization) kehitti tietoverkkojen yhteensopimattomuusongelmien poistamiseksi seitsenkerroksisen OSI-mallin, jonka avulla tutkijat ja yritykset kykenisivät yhtenäistämään verkkonsa.

OSI-malli ei ole enää nykyaikana suosittu, mutta soveltuu edelleen yksinkertaisena työvälineenä verkkojen tarkasteluun. OSI-mallin ymmärtäminen auttaa ymmärtämään muita pinomalleja.

Jokainen kerros on oma itsenäinen kokonaisuutensa, mutta kerroksilla on riippuvuussuhde naapuri kerroksista. Tiedon siirtyessä eteenpäin kerros käyttää alempana olevan kerroksen palveluita hyväkseen, sekä tarjoaa omia palveluita ylemmälle kerrokselle.



Kuva 5 OSI-mallin kerrokset

1. Fyysinen kerros käsittelee joko langallista tai langatonta fyysistä tekniikkaa jossa raakabitit kulkeutuvat. Esimerkkejä käytetyistä tekniikoista on radiotie, valokuitukaapeli sekä liittimet.

2. Siirtoyhteyskerros rakentaa kehyksen. Kerroksen toiminta on raskaasti riippuvainen fyysisen kerroksen toiminnasta.

Liite 2 OSI-malli (Open System Interconnection)

3. Verkkokerros hoitaa globaalin reitityksen sekä kohdesolmun löytämisen verkosta.

4. Kuljetuskerros huolehtii siitä, että paketit tulevat perille oikeassa järjestyksessä. Kuljetuskerros voi toimia kahdella eri yhteyskäytännöllä: TCP ja UDP.

5. Istuntokerros huolehtii useiden, saman yhteyden sisällä kulkevien istuntojen multipleksoinnista.

6. Esitystapakerros muuttaa datan käyttäjälle hyödylliseen muotoon. Esimerkiksi Unicode-tekstin kiinankielisiksi merkeiksi tai bittisarjat ääniksi.

7. Sovelluskerros sisältää itse käytettävät sovellukset, kuten sähköpostit tai kuvankäsittelyohjelmat.

Lähde: Kosola J., Solante T., *Digitaalinen taistelukenttä: Informaatioajan sotakoneen tekniikka*, Helsinki, Maanpuolustuskorkeakoulu, 2003, ISBN 951-25-1449-4