LAUREA

# Kamerajärjestelmän uudistaminen ja langattoman tietoliikenne-yhteyden kehitys hätätilanteita varten

Vanhanen, Lauri

2009 Laurea Leppävaara

Laurea-ammattikorkeakoulu
Laurea Leppävaara

# Kamerajärjestelmän uudistaminen ja langattoman tietoliikenne-yhteyden kehitys hätätilanteita varten

Lauri Vanhanen
Tietojenkäsittelyn koulutusohjelma
Opinnäytetyö
Kesäkuu, 2009

**Laurea-ammattikorkeakoulu** **Tiivistelmä**
Laurea Leppävaara
Tietojenkäsittelyn koulutusohjelma
Yritysten tietoverkot

Lauri Vanhanen

**Kamerajärjestelmän tehostaminen ja tietoliikenneyhteyden kehitys kamerajärjestelmään hätätilanteita varten**

**Vuosi** **2009** **Sivumäärä** **42**

Tutkimuksen tavoitteena oli selvittää Laurean kamerajärjestelmän tehostamista ja kehittää kamerajärjestelmään langaton tietoliikenneyhteys hätätilanteita varten. Tutkimuksella pyritään selvittämään, kuinka hätätietoliikenneyhteys toimii oikeassa ympäristössä mahdollisimman tietoturvallisesti. Tutkimuksella myös pyritään selvittämään keinoja Laurean valvontajärjestelmän tehokkuuden ja tietoturvallisuuden tehostamiseksi.

Tutkimuksessa käytettiin konstruktiivista tutkimustapaa, jossa keskityttiin tutkimuksen spesifiointiin ja tavoitetilaan. Tutkimus kirjoitettiin kirja-, internet- ja online-kirjastohakupalvelulähteiden perusteella. Tutkimuksen tietoliikenneyhteysosiossa perehdyttiin langattomien tekniikoiden spesifiointiin ja vertailuun. Vertailun kohteena oli tuvallisuus- ja tehokkuuskriteerit. Kamerajärjestelmäosiossa ei käsitelty kameroita ja niiden eri vaatimuksia toimintaympäristössä. Osiossa syvennyttiin tallennuslaitteistojen ja käyttöliittymien ominaisuuksiin, jotta niiden avulla Laurean kamerajärjestelmän suorituskykyä voidaan parantaa.

Tutkimus osoitti nykyisen kamerajärjestelmän keskeisimmiksi kehitystarpeiksi tietoturvallisuuden, laitteiden fyysisen turvallisuuden ja järjestelmän skaalautuvuuden. Tutkimuksen perusteella päädyttiin kamerajärjestelmän käyttöliittymän päivittämiseen suorituskykyisempään ja monipuolisempaan ohjelmistoon. Digitaalisella pakkausformaatilla tehostetaan videokuvan tallennusta ja tallennuskapasiteetin käyttöä.

Tutkimuksen perusteella langattoman yhteyden keskeisimmät ominaisuudet ovat varma toiminta, tietoturvallisuus sekä yhteensopivuus viranomaislaitteiden kanssa. Yksi kriittisimmistä vaatimuksista hankkeen toteuttamisen kannalta on mahdollisuus kokoaikaiseen videokuvan reaaliaikaiseen katseluun. Tämän tutkimuksen perusteella Laureaan on mahdollista rakentaa langaton tietoliikenneyhteys kamerajärjestelmään ja parantaa kamerajärjestelmän toimintojen hallinnan tehokkuutta ja turvallisuutta.

Asiasanat: Kamerajärjestelmä, tietoliikenneyhteys, tallennus, pakkausformaatit

**Laurea-ammattikorkeakoulu**
Laurea Leppävaara
Data processing
Business networks

Lauri Vanhanen

**Abstract**

**To improve Laureas video surveillance system and to create emergency connection via data communications link**

**Year** **2009** **The number of pages** **42**

The purpose of the thesis was to develop Laurea's camera surveillance system to work more efficiently and to develop the emergency data communication link for the surveillance system. The thesis examines how the emergency connection would work in a real environment and how to make the data communication link as safe as possible information security wise.

The research paper was written based on the constructive method of researching. The research concentrated primarily on specifications and how to define the goal that is the recommendation based on the research. The research paper was written based on book, internet and online library search engine sources. The section of the data communication link concentrated solely on wireless systems and on comparing different wireless systems based on security and efficiency. In the section of surveillance systems the research did not cover the actual cameras and their different requirements in the working environment but the section covered how to update the surveillance systems recording machinery. The section also covered the software that operates the surveillance system and making it more efficient by researching the features of different software.

According to the research, the surveillance system has to be updated further on information security, physical security and more versatile operating software. In the section of storing data it is pointed out that the current systems storage capabilities are sufficient and they need to be improved for example using a better encoding compression format.

The research of the data communication link showed that the critical features are reliable hardware and software, information security and compatibility with most of the PC hardware. Real time viewing of the surveillance footage is critical for the success of the project. Based on this research it is possible to build the data communications link to the surveillance system and to improve the systems administrating efficiency and systems safety.

Keywords: video surveillance system, wireless link, Digital recording, compression formats

Sisällys

# 1 Johdanto

Tutkimusaiheen sain tietojenkäsitelykoulutusohjelman opinnäytetöiden ohjaajalta Jyri Rajamäeltä. Ohjaajani kanssa kävimme keskusteluja mahdollisista opinnäytetyöaiheista ja aiheeseen päädyttiin mielenkiinnon sekä työkokemuksen myötä. Tutkimukseni aihe kuuluu Opetusviraston hankkeeseen, jolla on tarkoitus parantaa korkeakoulujen turvallisuutta. Tutkimuksen kohteena oli Laurean kamerajärjestelmä ja langattoman tietoliikenneyhteyden kehittäminen. Laurean nykyisestä kamerajärjestelmästä sain tietoa tutustumalla kamerajärjestelmän tiloihin. Kamerajärjestelmän tiloihin tutustuin Laurean kouluisännän ja lehtori Jouni Viitasen kanssa, joka vastaa Laureassa meneillään olevasta kamerajärjestelmän päivittämishankkeesta. Kamerajärjestelmää haluttiin päivittää tehokkaammaksi ja monipuolisemmaksi toimintojen osalta.

Hanke käynnistettiin vuonna 2008 Jokelan ja 2009 Kauhajoen kouluissa tapahtuneiden onnettomuuksien vuoksi. Hanke on osa isompaa projektia, jolla Suomi tavoittelee asemaa Euroopan turvallisinpana maana vuonna 2015. Hankkeella on myös tarkoitus olla osa kuntien paikallisia turvallisuussuunnitelmia, jotka tullaan uusimaan vuoden 2010 aikana. Koko hankkeen tavoitteena on tuottaa käytännön ratkaisuja ja koulutusta turvallisuuden lisäämiseksi korkeakouluihin.
(Korkeakoulujen turvallisuusposteri 2009.)

Hankkeen hyödyntämiskohteet:

- korkeakoulujen turvallisuuskäsikirjassa
- turvallisuuden toimijaverkosto
- seminaarit
- koulutus
- internetsivusto
- tiedotus
- jatkotutkimushankkeet

(Korkeakoulujen turvallisuusposteri 2009).

# 2 Tutkimuksen tavoitteet

Tutkimuksen tavoitteena on selvittää Laurean kamerajärjestelmän päivittämismahdollisuudet laitteiden ja käyttöliittymän osalta. Lisäksi tavoitteena on kehittää kamerajärjestelmään langaton tietoliikenneyhteys hätätilanteisiin pelastusviranomaisia varten. Tutkimus toteutetaan käyttäen konstruktiivista tapaa. Tekniikoiden soveltumista käyttökohteeseen vertaillaan tavoitteen kriteerien täyttymisen ehdoilla.

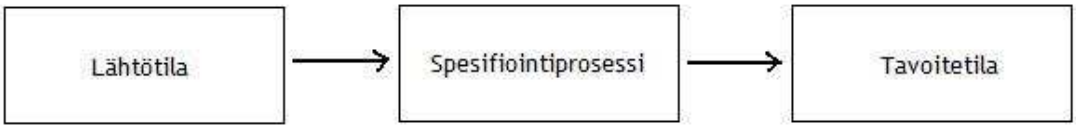
Tietoliikenneyhteyden tavoitteen vaatimuksina ovat yhteyden saatavuus, helppo käytettävyys, yhteensopivuus ja turvallisuus fyysisesti sekä tietoturvallisesti. Saatavuudella tarkoitetaan yhteyden vakaata toimivuutta vaihtuvassa ulkoympäristössä. Yhteyden yhteensopivuudella tarkoitetaan toimivuutta viranomaisten tietokoneiden langattomien yhteyksien kanssa. Yhteyden fyysinen turvallisuus tarkoittaa ulkoympäristössä olevien laitteiden suojaamista ratkaisulla, joka ei vaikuta negatiivisesti yhteyden saatavuuteen tai yhteensopivuuteen. Tietoliikenneyhteyden tutkimuksen ansiosta on mahdollista hätätapauksissa lääkintäavun koordinoinnin tehostaminen ja vaaratilanteiden havainnoinnin tehostuminen.

Kamerajärjestelmän tutkimuksessa perehdytään videokuvan tallennukseen ja tallennetun materiaalin saatavuuteen. Osiossa myös selvitetään kamerajärjestelmän tallennuslaitteiden, suorituskyvyn, skaalautuvuuden, tietoturvallisuuden sekä käyttöliittymän tehostamista. Videokuvan tallennuksessa perehdyn laitteiden tallennuskapasiteetin skaalautuvuuteen, tallennuslaitteen helppoon hallintaan sekä fyysiseen turvallisuuteen. Tallennuksen tietoturvallisuuteen ei tutkimuksessa paneuduta, koska tallennus tapahtuu sisäverkossa. Laurean sisäverkon tietoturvallisuus on jo riittävällä tasolla. Järjestelmän tallenninlaitteissa keskityn suorituskykyyn ja käyttöliittymän toimintojen ominaisuuksiin.

## 3 Tutkimustapa ja eri vaiheet

Tutkimus toteutetaan konstruktiivisella tutkimustavalla, jossa hyödynnetään Van Aikenin metodia. Van Aikenin tavalla tuotetaan perustutkimustieto suunnittelu- ja realisointitietoudesta kohteena olevaa järjestelmää sekä tietoliikenneyhteyttä varten. Tutkimustavalla voidaan selvittää kolmea tutkimusongelmaa: kamerajärjestelmän päivittämisongelman ja kamerajärjestelmän konstruktio-ongelman sekä tietoliikenneyhteyden konstruktio-ongelman. Tutkimuksessa käsitellään nämä ongelmat ja vertaillaan ratkaisujen toimivuutta keskenään. Tutkimuksen kamerajärjestelmän hyödyllisyys arvioidaan vertailemalla eri ratkaisuja nykyiseen järjestelmään. Tietoliikenneyhteyttä arvioidaan vertailemalla soveltuvuutta olemassa olevia langattomia tekniikoita nykyiseen toimintaympäristöön. (Järvinen & Järvinen 2004, 103–106.)

Eri tutkimustavat sisältyvät suunnittelutieteeseen ja tutkimuksessa toteutan artefaktin suunnittelun. Artefaktin suunnittelulla tarkoitetaan valmiin tuotteen suunnittelua sen konstruktiovaiheeseen saakka. Tässä tutkimuksessa tarkoitetaan videovalvontajärjestelmän ja tietoliikenneyhteyden suunnittelua hätätilanteita varten. Tutkimuksen algoritminen preskriptio on, että ”halutaan lähtötilanteesta Y tilanteeseen X käyttämällä tehostavia toimenpiteitä Z” (Y+Z=X).(Kuvio 1.) (Järvinen 2004, 106–108.)




Kuvio 1. Tutkimuksen läpivienti tavoitetilaan.

Tutkimus määrittelee tavoitetilan saavuttamisen vaatimukset verraten lähtötilaan. Tavoitteena tutkimuksella on kuvata järjestelmän suorituskyvyn tehostamisen tekniset ratkaisut selkeästi toiselle osapuolelle. Kamerajärjestelmän ja tietoliikenneyhteyden konstruktio voidaan toteuttaa tutkimuksen pohjalta. (Järvinen 2004, 108.)

## 3.1 Spesifiointiprosessi

Tutkimuksen spesifiointiprosessin aikana on tärkeää jäsentää ja kuvata tutkimuksen kokonaisuus. Tutkimuksen tavoitetilasta joskus jäädään tai tavoitetila ylitetään asiakkaan tarpeiden mukaan määritellystä kokonaisuudesta. Tavoitetila voi jäädä toteutumatta tai tavoitetila ylitetään esimerkiksi asiakkaan muuttuneiden tarpeiden tai tutkimuksen aikataulujen takia. Tutkimuksessa spesifioinnin tarkasta kuvauksesta ja tiedon jäsentämisestä on erittäin paljon apua tutkimuksen soveltamisessa käytäntöön. (Järvinen 2004, 108.)

Käytännön innovaatiot ovat usein järjestelmiä, joissa on monta osapuolta ja intressiryhmää vaikuttamassa. Tutkimuksen kokonaisuuden kartoittamiseksi on hyvä tietää, että mielipiteitä asioihin on niin monta kuin osapuolia ja lisäksi saattaa olla osapuolien välillä erimielisyyksiä kokonaisuuden vaatimuksista (Järvinen 2004, 109). Tämän takia spesifiointiprosessin aikana on hyvä tietää eri intressiryhmien tavoitteet. Tavoitteiden pohjalta voidaan luoda kompromissi kokonaisuudesta, mutta kontekstin säilyttäminen on tärkeää. Prosessin tuottava aineisto perustuu luotettaviin ja monipuolisiin lähteisiin. Tutkimuksen tietolähteet perustuvat suurelta osin englanninkielisiin ja erilaisiin sähköisiin julkaisuihin. Alan kirjallisuuden tiedot vanhenevat hyvin nopeasti ja kattavaa suomenkielistä materiaalia ei juuri ole aiheesta saatavilla. (Järvinen 2004, 109.)

## 3.2 Innovaation raportointiprosessi

Seuraavissa kappaleissa käsitellään millä tavalla innovaatio raportoidaan tutkimuksessa ja millä tavalla tutkimuksen lopputulos arvioidaan käyttäen erilaisia mittareita. Tutkimuksessa käytetään mittareita käsitteistön, mallin ja metodin arvioimiseen. Realisoinnin suunnittelua ei tutkimuksessa käsitellä. (Järvinen 2004, 113–115.)

Innovaation raportointiprosessin pohjana käytetään Marchin & Smithin laatimaa metodia. Raportointiprosessin aikana tuotetaan analysoitua tietoa innovaation käsitteistöstä, malleista, metodeista ja realisoinnista. Käsitteistön pohjalta toteutetaan spesifiointi, jonka pohjalta luodaan realisoinnin metodeja varten. Käsitteistö tulee uusia jos idean konseptiin tulee muutoksia tai tavoitetila muuttuu. Tutkimuksen malli toteutuu käsitteistön pohjalta ja kuvaa innovaation mahdollista realisaatiota. Mitä tarkemmin tavoitetila kuvataan, sitä paremmin voidaan arvioida järjestelmän toteutus ja järjestelmän hyödyt nykytilaan nähden. (Järvinen 2004, 113–115.)

### 3.3 Innovaation arviointimittarit

Marchin & Smithin(1995) määrittelevät suunnittelutieteen toimintatavassa mittareita arvioimaan eri vaiheiden onnistumista. Käsitteistön mittaamiseen käytetään seuraavia mittareita: täydellisyys, yksinkertaisuus, eleganssi, ymmärrettävyys ja helppokäytettävyys. Mittareilla tarkastellaan miten käsitteistö onnistuu vastaamaan tutkimusongelmaan. Helppokäytettävyys viittaa käsitteistön hyödynnettävyyteen ja neljä muuta käsittelevät käsitteistön yleistä rakennetta. Malli on käsitteistöstä koottu kuvaus, joka täydentyy ulkopuolisilla muuttujilla realisointivaiheessa. (Järvinen 2004, 118–120.)

## 4 Langattomat yhteydet

Seuraavaksi tutkimus kohdistuu langattomiin yhteystapoihin. Kappaleessa esitellään erilaisia langattomia yhteystapoja ja näistä kaksi esitellään tulevissa kappaleissa tarkemmin. Lisäksi selvitetään miksi nämä kaksi yhteystapaa tutkitaan tarkemmin.

Suurin osa langattomista yhteyksistä perustuu radiotaajuuksiin, mutta langattomat yhteydet voivat myös perustua valoon. Radiotaajuuksia lähetetään eri taajuuksilla ja voimakkuuksilla riippuen yhteystavasta. Radiotaajuuksien lähettämiseen käyteytään antenneja, joita on kehitetty erilaisia ympäristöjä ja käyttötarkoituksia varten. Radiotaajuuksilla toimivat yhteydet ovat herkkiä häiriöille. Yhteyden häiriöt voivat johtua sähkömagneettisesta säteilystä tai fyysisistä esteistä kuten betoniseinästä. Radiotaajuuden häiritseminen erikseen tarkoitetulla laitteella ja kyseisen laitteen hankkiminen on helppoa (Personal Cell Phone Signal Blocker Device 2009). Langattomien yhteyksien ominaisuudet vaihtelevat käyttöympäristön ja kantaverkon tarkoituksesta riippuen. Langattomien yhteyksien vasteajat vaihtelevat myös yhteystyypistä riippuen. Vasteaika tarkoittaa kuinka kauan kestää paketin siirto edestakaisin yhteyden kautta (Latenssi 2009).

Wlan (Wireless local area network) on yleisesti käytetty langaton yhteys. Yhteystavan tiedonsiirtonopeudet ovat suuria ja yhteyden kantomatka ilmassa vaihtelee välillä 30m-1500m. Wlan-yhteydelle on kehitetty salausmekanismit tiedonsiirron laittomalle kuuntelulle ja yhteyden muodostamiselle. Vasteajat yhteydessä ovat pienenmmät verrattuna toisiin markkinoilla oleviin langattomiin yhteyksiin kuten UMTS.
(What is a wireless LAN? – Knowledge Base 2009.)

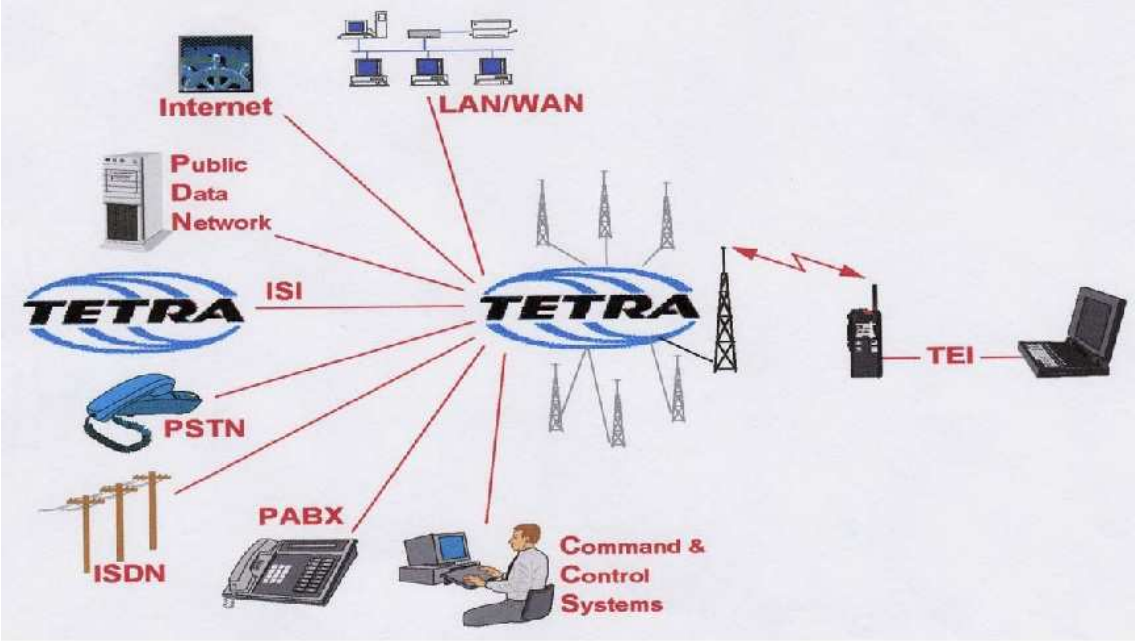
Wimax-yhteys (Worldwide Interoperability of Microwave Access) on kehitetty langattomaksi yhteydeksi, jolla saavutetaan suuri tiedonsiirtonopeus pitkillä käyttöetäisyyksillä. Yhteyden tiedonsiirtokantama vaihtelee jopa 50 km:iin asti ja tiedonsiirtonopeus on enintään 70 Mbit/s. (Wimax-An-Introduction 2005.) Yhteyden kantomatka sopii hyvin peittämään laajoja alueita suurilla tiedonsiirtonopeuksilla, mutta yhteyden yleistyminen käytössä ei ole toteutunut (Nokia Siemens hautaa oman wimaxin 2009).

Matkapuhelimissa on yleisesti käytössä UMTS-yhteys (Universal Mobile Telecommunications System), jota pystyy käyttämään myös tietokoneen tietoliikenneyhteyden luomiseen. UMTS-yhteyden toisin sanoen 3G-yhteyden (3rd Generation) hyötynä on liikuteltavuus ja yhteyden kantavuus maanlaajuisen matkapuhelintukiasemaverkoston ansiosta. 3G-yhteys mahdollistaa videokuvan reaaliaikaisen katselun ja tiedostojen nopean latauksen. Tietokoneen 3G-yhteyteen tarvitaan 3G-modeemi ja tukiasema yhteyden muodostamiseen kohdeverkon kanssa. (What is UMTS? 2009.)

@450 on Digitan rakentama langaton laajakaistaverkko, joka perustuu Flash-OFDM -tekniikkaan (Orthogonal Frequency Division Multiplexing). Flash-OFDM -tekniikkaa ei ole standardoitu. Verkko käyttää NMT-450 -verkon (Nordisk Mobiltelefon*)* entistä taajuusaluetta, joka matalan taajuusalueen vuoksi soveltuu kattavan verkon rakentamiseen suurella alueella. Suurin suunnattavalla antennilla toteutetun yhteyden välimatka on 60 km. Yhteyden käyttö kannettavassa tietokoneessa onnistuu PCMCIA (Personal Computer Memory Card International Association)-, USB (Universal Serial Bus)- tai Express card -modeemia käyttäen. Yhteyden vastaanottotiedonsiirtonopeus on enintään 2 Mbit/s ja lähetysnopeus on 512 Kbit/s. Yhteys sopii pitkille välimatkoille ja yhteyden kaistan leveyden vuoksi se ei sovi isojen tiedostojen tai videokuvan lataamiseen yhteyden kautta. (@450 2009.)

TETRA (TErrestrial Trunked RAdio) on digitaalinen matkapuhelinjärjestelmä. Suomessa TETRA on käytössä valtakunnallisessa viranomaisverkko VIRVE:ssä. (Kuvio 2.) TETRA tukee sekä puheen- että tiedonsiirtoa. TETRA:n Euroopassa käyttämät taajuudet ovat 380-400 MHz ja 410-430 MHz sekä Aasiassa noin 800 MHz. Tiedonsiirto on mahdollista sekä paketti- että piirikytkentäisenä. Tiedonsiirron enimmäisnopeus on 28,8 kbit/s jos käytössä on kanavan kaikki neljä aikaväliä. Kanavan yhden aikavälin nopeus on 7,2 kbit/s. TETRA-tekniikan

perusominaisuuksiin kuuluu todennus ja salaus. Salausprosessissa todentaminen tapahtuu haaste-vastaus-menetelmällä, joka tarkoittaa päätelaitteen tunnistautumista verkkoon ja verkon tunnistautumista päätelaitteeseen. Ilmarajapintasalaus on yleisesti käytössä oleva salaus, joka salaa päätelaitteen ja tukiaseman välisen liikenteen. TETRA:ssa on mahdollista salata liikenne myös koko matkalta kahden päätelaitteen välillä. TETRA:ssa on lisäksi sisäänrakennettuna ominaisuus, joka havaitsee häirinnän. Verkon havaitessa tahallista häiriötä tietyillä taajuusalueilla se vaihtaa automaattisesti taajuusaluetta verkossa. (Tetra: introduction to technology 2004.)




Kuvio 2. Tetra-tekniikan yhteysmahdollisuuksista (Tetra: introduction to technology 2004).

Tutkimuksessa esitellään Wlan- ja 3G-yhteys seuraavaksi tarkemmin, koska näillä yhteystavoilla saavutetaan tarvittava tiedonsiirtokapasiteetti. Lisäksi nämä yhteystavat sopivat tutkimukseen signaalin riittävän kantomatkan takia.

## 5 WLAN

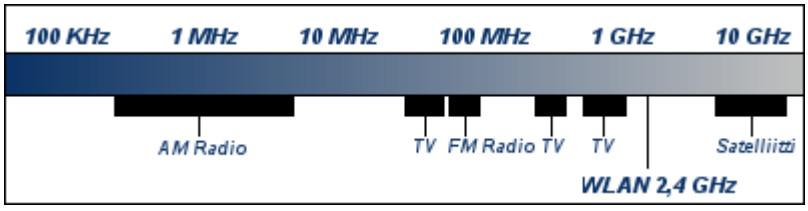
Wlan on lyhenne sanoista Wireless Local Area Connection ja usein Wlan:sta käytetään myös nimitystä WiFi (Wireless Fidelity). WiFi alliance perustettiin huolehtimaan uusien standardien yhteensopivuudesta. Wlan-yhteyden standardien yhteensopivuudessa pitää ottaa huomioon taajuusalue, yhteydenottotapa ja informaation siirtonopeus. Wlan-yhteyttä käytetään ympäristöissä, joissa se on taloudellisempi ratkaisu kuin runkoverkon asennus. Langaton lähiverkko käyttää radiosignaaleja luomaan peitealueita ympäristöön, jotta yhteys verkkoon olisi mahdollinen.

Wlan-yhteyden voi liittää myös osaksi langallista lähiverkkoa ja näin uusien lähiverkkojen luonti osaksi isompaa kokonaisuutta on helppoa. Wlan tarjoaa mahdollisuuden perustaa ns. Hot-Spot–peittoalueita, joista saa yhteyden esimerkiksi internetiin tai yrityksen intranet-yhteyksiin. Hot-Spot alueita sijaitsee kaupunkien keskustoissa ja muissa julkisissa ympäristöissä. (Harte, Bowler, Ofrane & Levitan 2005, 367-368.)

## 5.1 Wlan-taajuudet

802.11 on Wlan-standardimalli, joka sisältää monta eri kehitysmallia standardimallin perustamisesta lähtien. Wlan toimii radiotaajuksilla 2,4 GHz - 5,7 GHz, mutta Wlan voi myös toimia infrapunalla. (Harte ym. 2005, 407-408.) Ir Wlan-yhteyttä (Infrareded Wlan) käytettäessä linkki vaatii toimiakseen täydellisen näköyhteyden, eikä toimintasäde tämän takia sovellu muuttuviin ympäristöihin. Ir Wlan-yhteyden siirtonopeus on yleensä 1-2 megabitin alueella, kun taas radiotaajuuksilla saavutetaan enintään 300 Megabitin nopeus. Infrapunayhteyttä voidaan käyttää slloin, kun laitteiden välinen matka on lyhyt. Ir Wlan -yhteyden käyttö perustuu tietoturvallisuuden korkeaan tasoon, koska lähettimestä lähtevää valosädettä ei voi kaapata muualta käsin. (Infrared networking 2009.)

2,4 GHz ja 5,7 GHz ovat julkisia radiotaajuuksia, joita kuka tahansa voi käyttää. Tästä syystä taajuudet ovat häiriöille herkkiä. (Kuvio 3.) Esimerkiksi mikroaaltouuni toimii 2,4 GHz:n taajuusalueella. Wlan-yhteyden käyttöönoton aikana taajuusasetuksissa tulee ottaa huomioon taajuuden kanava, voimakkuus ja kanavan hallinta. Yleensä Wlan-laitteissa käytetään laajakaistaista tekniikkaa, mutta on myös mahdollista käyttää kapeakaistaista tekniikkaa. Kapeakaistatekniikka mahdollistaa pidemmän kantomatkan kapean kaistan ja suuremman lähetystehon vuoksi. Kapeakaistatekniikan käyttö vaatii lisenssin omalle taajuudelle ja tarkan antennisuuntauksen näköyhteydellä. Hajaspektritekniikassa käytetään yleensä 2,4 GHz:n taajuusaluetta ja tekniikkaa kutsutaan toisella nimellä ISM-kaistaksi (Industrial, Scientific, Medical). (WLAN 2003.)




Kuvio 3. Kuvassa Wlan-taajuus ja muut tuttujen laitteiden taajuuksia (WLAN 2003).

Hajaspektritekniikalla lähetysteho saa olla maksimissaan 0,1wattia, joka pienentää peittoaluetta, mutta mahdollistaa useiden yhteyksien rinnakkaiselon. Hajaspektritekniikkaa käyttävissä laitteissa signaali on ohjelmoitu niin, että laite hakee oikean signaalin muiden signaalien joukosta yhteyden muodostamiseksi. Hajaspektritekniikka jakautuu vielä kahteen

eri alitekniikkaan, jotka ovat suorasekvenssi- ja taajuushyppelytekniikka. Taajuushyppelytekniikka kuitenkin hylättiin, koska suorasekvenssitekniikalla on mahdollista saavuttaa tämänpäiväiset nopeudet(54-300Mbit/s). Tajuushyppelytekniikkaa käyttävät standardit eivät ole yhteensopivia suorasekvenssitekniikka standardien kanssa. (WLAN 2003.)

## 5.2 Siirtostandardit

Wlan-siirtostandardit kuuluvat IEEE:n (Institute of Electrical and Electronics Engineers) standardiluokkaan 802.11, joka sisältää eri ominaisuuksilla rakennettuja versioita. Pääasiassa standardit eroavat tiedonsiirtokyvyltään ja taajuudeltaan. Standardi kuvaa OSI-mallin fyysisen kerroksen ja siirtokerroksen alemman osan, jota kutsutaan nimellä MAC (Media Access control). Standardit on rakennettu luokan 802.3 pohjalta, jotta ne olisivat yhteensopivia Ethernet-tekniikan kanssa. 802.3 on Ethernet-teknologian standardiluokka. Seuraavissa kappaleissa tutkitaan standardeja, jotka ovat tällä hetkellä käytössä. (Taulukko 1.) (IEEE 802.11 2009.)

| | 802.11b | 802.11a | 802.11g | 802.11n |
|---|---|---|---|---|
| Siirtotekniikka | DSSS | OFDM | OFDM | MIMO |
| Taajuusalue | 2,4GHz | 5,15 – 5,25GHz | 2,4GHz | 2,4- ja 5GHz |
| Tiedonsiirtonopeus | 5,5-11MBit/s | 9-54MBit/s | 9-54MBit/s | 100-200Mbit/s |

Taulukko 1. 802.11 keskeisimpien standardien tiedot tiivistettynä.

### 5.2.1 802.11b

Heinäkuussa 1999 IEEE laajensi alkuperäistä 802.11 standardia luomalla mallin 802.11b. Versio tukee tiedonsiirtoa 11 Mbit/s asti ja oli verrattavissa silloin yleisessä käytössä olleeseen Ethernet-teknologiaan kaistan leveyden vuoksi.

802.11b-standardi käyttää julkista 2,4 GHz ISM-taajuusaluetta. Standardi käyttää kolmea toisistaan erossa olevaa kanavaa taajuusalueella ja yhdessä yhteyspisteessä voi olla enintään 32 eri käyttäjää.

- Hyvät puolet ovat: vähäinen hankintahinta, kantomatka ja yhteensopivuus g-standardin kanssa.
- Huonot puolet ovat: hidas tiedonsiirtokyky, taajuusalue on herkkä häiriöille (esim. mikroaaltouuni).

(WLAN 2003.)

### 5.2.2 802.11a

B-standardin kehityksen aikana IEEE kehitti a-standardia, mutta korkeampien kustannusten takia 802.11a on lähinnä yritysmaailman käytössä. 802.11a tukee 54 Mbit/s tiedonsiirtonopeutta ja taajuusalue on säännellyllä 5,15-5,25 GHz:n alueella (U-UNI-alue). Standardi käyttää OFDM (Orthogonal Frequency Division Multiplexing) kanavanjakotekniikkaa. Standardissa on 4 eri kanava-aluetta 25 MHz:n välein ilman ja käyttäjiä voi olla samaan aikaan 64 yhdessä AP(Access Point)-yhteyspisteessä. Standardin taajuusalueiden vuoksi b-standardi ei ole yhteensopiva a-standardin kanssa.

- Hyvät puolet ovat: tiedonsiirtonopeus ja häiriönsietokyky, koska taajuusalueella toimivat laitteet on säännöksin määritelty.
- Huonot puolet ovat: korkeat kustannukset, peittoalueen vähäinen kantomatka taajuusalueen vuoksi.

(WLAN 2003.)

### 5.2.3 802.11g

Standardi kehitettiin yhdistämään 802.11a:n ja 802.11b:n parhaat puolet samaan standardiin. Standardi tukee 54 Mbit/s tiedonsiirtonopeutta ja versio toimii julkisella 2,4 GHz ISM-taajuusalueella pidemmän kantomatkan tavoittelemiseksi. Standardi tuottaa neljä 20 MHz:n välein olevaa kanavaa ilman päällekkäisyyksiä. 802.11g on yhteensopiva taaksepäin b-standardin kanssa.

- Hyvät puolet ovat: Kaistan nopeus, peittoalueen kantomatka ja signaalin kuuluminen esteiden läpi.
- Huonot puolet ovat: hitaampi nopeudeltaan kuin nykyinen n-standardi, kodinkoneet voivat häiritä signaalia.

(WLAN 2003.)

### 5.2.4 802.11n

Uusin IEEE-standardi on 802.11n ja standardi kehitettiin tiedonsiirtokyvyn kasvattamiseksi. N-standardi käyttää MIMO (multiple input, multiple output) tekniikkaa, joka perustuu useisiin antenneihin ja kanaviin samassa yhteydessä. (IEEE 802.11 2009.)

Standardi tukee teoriassa enintään 600 Mbit/s nopeutta, mutta käytännössä 100-200 Mbit/s nopeutta. Kantomatka on standardissa huomattavasti pidempi, koska signaalin käsittelynopeus on parantunut MIMO:n myötä. 802.11n on yhteensopiva 802.11g standardin kanssa. (IEEE 802.11 2009.)

- Hyvät puolet ovat: tiedonsiirtokyky, kantomatka, signaalin häiriönsietokyky.
- Huonot puolet ovat: kustannukset suuremmat kuin 802.11g, useamman antennin käyttö voi häiritä läheisiä 802.11b/g -standardiin pohjautuvia yhteyksiä.

(Wireless standards by Mitchell, Bradley 2007.)

## 5.3 WLAN-antennit

Antennit on suunniteltu toimimaan muuntajina elektromagneettisen- ja sähköisen signaalin välillä. Wlan-signaalin taajuusalue on 2,4-5,7 GHz riippuen maiden julkisista ja ennalta määrätyistä taajuusalueista. Yleisesti antenni sijaitsee valmiiksi Wlan-laitteessa, mutta signaalin kantomatkan pidentämiseksi tarvitaan erillinen käyttötarkoitukseen sopiva antenni. Antennimalleja on monenlaisia ja näistä yleisin on 360 astetta säteilevä antenni (Kuvio 4). Ympärille säteilevät antennit toimivat laitteissa, jotka tuottavat matalaa radiosignaalia (2,4 GHz). (Harte ym. 2005, 407–408.)

Kuvio 4. Ympärisäteilevä antenni (Videovalvontaopas 2004).

Korkeaa radiosignaalia tuottavat antennit ovat paneeli- tai paraboolianteneja (Kuvio 5). Näiden antennien tuottama radiosignaali voidaan kohdistaa haluttuun kohteeseen. Paneeliantennin suuntakulma signaalille on 65–70 astetta ja paraboolianteennin 13–20 astetta. Sopiva käyttökohde on esimerkiksi toimistorakennuksien välinen yhteys.
(Videovalvontaopas 2004; Harte ym. 2005, 407–408.)

Kuvio 5. yleiset mallit suunnattavista antenneista (Videovalvontaopas 2004).

Antennin signaali tasoa voidaan parantaa käyttämällä WLAN laitetta kahdella antennilla, joka tarkoittaa signaalin jakautumista kahteen eri antenniin ja näistä WLAN laite valitsee signaalilaadun perusteella paremman yhteyden. , joka vaikuttaa tiedonsiirron nopeuteen ja peittoalueeseen. (Harte ym. 2005, 407–408.)

## 5.4 Verkkorakenteet

Wlan-verkko toimii ilman tukiasemaa tai tukiasemalla. Ilman tukiasemaa verkkoa kutsutaan Ad-hoc–verkoksi. (Kuvio 6.) Ad-hoc–verkkorakennetta käytetään ympäristöissä, jossa tiedonsiirto vaatii nopeutta kuten moninpelaamisessa. Yhteyden nopeus verkkomallissa johtuu P2P-yhteydenottotavasta, mutta ad-hoc -yhteyksiä ei suositella pysyviin asennuksiin käyttäjä skaalautuvuuden ja yhteyden peittoalueen vuoksi. (Wireless LAN 2009.)


Kuvio 6. Ad-Hoc-verkkotopologia (WLAN 2003).

Infrastruktuuriverkko jaetaan kahdeksi eri malliksi BSS (Basic Service Set) ja ESS (Extended Service set). BSS-malli on yleisin verkon muodostustapa ja siihen kuuluu vain yksi tukiasema. (Kuvio 7.) BSS-verkko muuttuu ESS-verkoksi, kun ympäristön verkkoon lisätään toinen tukiasema. (Kuvio 8.) Tällä tavalla langattoman verkon peittoaluetta ja käyttäjäskaalautuvuutta saadaan laajennettua ympäristön vaatimusten mukaan. (Wireless LAN 2009.)


Kuvio 7. BSS-verkkotopologia (WLAN 2003).


Kuvio 8. ESS-verkkotopologia (WLAN 2003).

## 5.5 Wlan-tietoturvallisuus

Tietoturvallisuus on tärkeää Wlan-yhteyksissä, koska yhteyden tuottamalla peittoalueella yhteyden fyysinen taso on kaikkien saatavilla ilman tietoturvaa. Tietoturvalla on tarkoitus suojata yhteys luvattomilta käyttäjiltä. Yhteyden tietoturvallisuus heikkenee, jos salasanan yhdistelmä koostuu esimerkiksi pelkistä kirjaimista. Salasanassa suositellaan sisältävän kirjaimia, numeroita ja merkkejä sekä merkkijonon tulisi olla vähintään 8-merkkiä pitkä. Wlan-tietoturvallisuus on jaettu kolmeen luokkaan: yhteyden luonti, käyttäjän varmistustapa ja informaation salausavaimen käyttö. (IEEE 802.11i 2009.)

Wlan-laitteen lähettämän signaalin tieto voidaan salata erikseen salausavaimella. Informaation salausavain voi olla esimerkiksi AES (Advanced Encryption Standard). AES-standardista on kolmea eri versiota, jotka ovat AES-128 bittiä, AES-192 bittiä ja AES-256 bittiä. Wlan-yhteyden tunnistautumisen sekä salasanan varmennuksen ja salauksen käytännöt vaihtelevat laitteen ominaisuuksien mukaan. Wlan-verkon SSID-tunnuksen(Service Set IDentifier) voi myös piilottaa näkyvistä toisille käyttäjille. Tunnuksen piilottamista kutsutaan ESSID-metodiksi (Extended Service Set Identifier).
(Wireless LAN security 2009; Harte ym. 2005, 381–384.)

Luvattomat käyttäjät voivat käyttää monia erilaisia tapoja kaapata yhteys tai vakoilla tietoja yhteydestä luvattomasti. Esimerkiksi salasanan voi purkaa tavalla, joka kokeilee salasanaa vaihtamalla merkkejä systemaattisesti. Sanakirja-hyökkäys perustuu sanakirjaan, josta hakkerien ohjelma kokeilee yhteyden salasanaa sanakirjasta haetuilla sanoilla.
(Harte ym. 2005, 381–384.)

## 5.6 802.11i

802.11i-standardi on turvallisuusstandardi 802.11 luokkaan. I-standardi sisältää WEP- (Wired Equivalent Protection), WPA- (WiFi Protected Access) ja WPA2-salaukset (kehittyneempi malli WPA:sta).

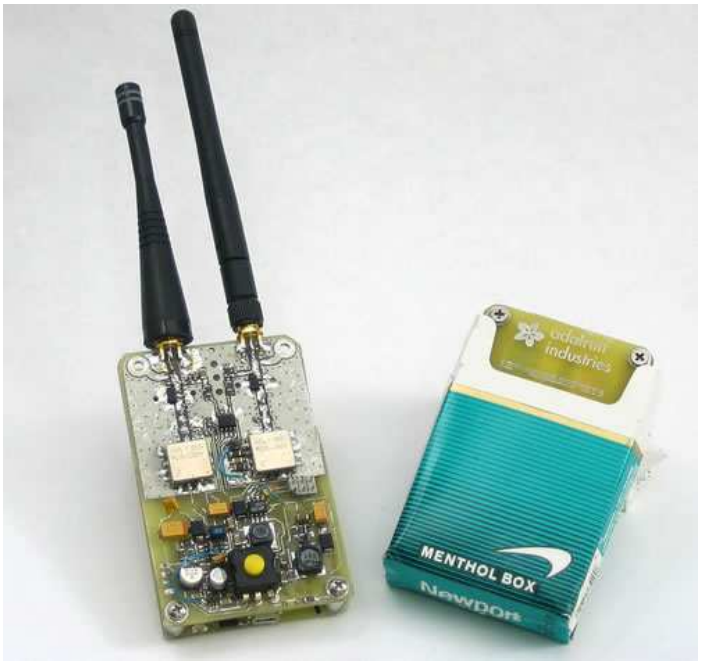
Salausavaimissa käytetään algoritmia salauksen purkuun ja salaukseen. Tiedon vastaanottamiseksi ja lähettämiseksi osapuolet varmentavat tiedon salausavaimilla. Salauksen purkuun tarvitaan salausavain. Salausavaimen salasana voi olla 8- merkkinen sisältäen numeroita tai kirjaimia tai 63-merkkinen heksadesimaaliavain.
(Harte ym. 2005, 385–387.)

WEP-salaus käyttää 40-, 64- tai 128-bittistä avainta yhteyden varmentamiseen. WPA-salaus käytti alun perin TKIP- protokollaa (Temporal Key integrity protocol) yhteyden salasanan salaukseen. TKIP:n huonona puolena oli yhteensopivuus vanhempien tukiasemien kanssa. TKIP-protokollan lisäksi WPA-protokollassa käytetään PSK-metodia (Pre-Shared Key), joka suojaa WEP-salauksen tavoin salasanan. Erona WEP-salauksen tapaan PSK vaihtaa avainta jokaisen yhteydenoton aikana yhteyspisteeseen. WPA2 eroaa WPA:sta käyttämällä hyväkseen AES-salaukseen pohjautuvaa CCMP-protokollaa (Counter Mode with Cipher Block Chaining Message Authentication Code Protocol) (Wi-Fi Protected Access 2009). WPA2-metodin avaimen tunnistukseen käytetään WPA:n tapaan PSK-metodia. PSK-metodi on suunnattu kotikäyttäjille, jotta tietoturvallisuus olisi helposti käytettävissä eikä tarvitsisi käyttää erikseen tunnistautumispalvelimia järjestelmissä. Nykypäivänä tämä tietoturvaominaisuus esiintyy yleisesti langattomissa laitteissa ja tietokoneiden käyttöjärjestelmät tukevat sitä.
(IEEE 802.11i 2009; Harte ym. 2005, 385-387.)

# 6 Radiosignaalien häirintä

Radiosignaaleilla toimivien laitteiden häirintä perustuu tekniikkaan, jolla häiritään fyysisen tason signaalin lähettämistä ja vastaanottoa signaalin kanavan kautta. (Kuvio 9.) Signaalin häirintä onnistuu hankkimalla radiosignaalilähteen, jolla voi lähettää radiosignaalia laajalla taajuusalueella. MAC-osoitetta (Medium Access Control) voidaan käyttää siirtotason häiritsemiseksi. Tällä tavalla pystytään estämään laitteiden toiminta tietyllä kanavalla. (Anti-jamming timing channels for wireless networks 2008.) Fyysisen tason häirintään voidaan käyttää esimerkiksi suorahajotushajaspektriä. Tällä tarkoitetaan radiosignaalin lähettämistä laajalla kaistalla vaihtamalla taajuutta kymmenestä satoihin kertoihin sekunnissa ennalta määritellyn kaavan mukaan näennäisen satunnaisesti tai lisäämällä lähetettävään signaaliin näennäisesti satunnaista kohinaa. (Mikroaallot vs. infrapuna langattomassa tiedonsiirrossa 1999.) Suorahajotushajaspektritekniikkaa käytetään myös tiedonlähettämiseen, jotta signaalin häiritseminen olisi mahdollisimman hankalaa. Suorahajotushajaspektritekniikalla toimiva häirinnän estäminen on kuitenkin erittäin kallista ja sen takia ei ole kuluttajalaitteiden käytössä. (Anti-jamming timing channels for wireless networks 2008.)

Kuluttajaverkkojen häirinnän estämiseksi on useampi ratkaisu. Yhdeksi ratkaisuksi on ehdotettu automaattinen kanavan vaihto protkollassa häirinnän alkaessa. Tämä ratkaisu auttaisi vain estämään häirintälaitteet, jotka toimivat muutamalla kanavalla. Taajuushyppelytekniikka on myös yksi tapa vaikeuttaa häirintää, mutta se ei toimi toisen laajakaistan peittoalueen läheisyydessä mahdollisen kanavoiden päällekkäisyyden vuoksi. (Anti-jamming timing channels for wireless networks 2008.)

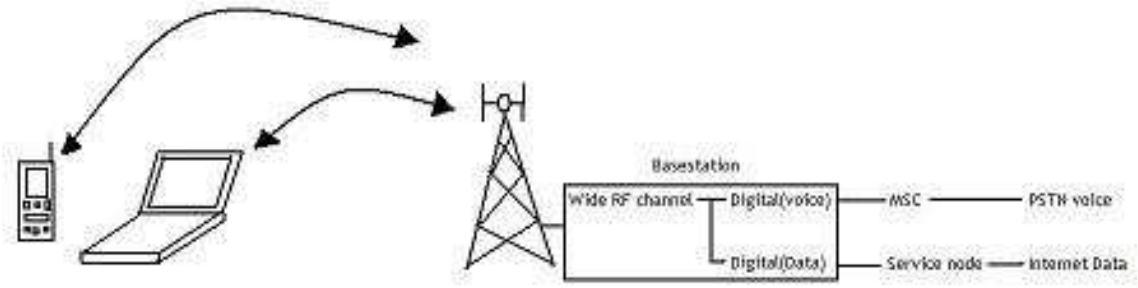



Kuvio 9. Radiosignaalien häirintälaite (GPS jammer 2007).

# 7 3G

3G (3rd generation) toiselta nimeltään UMTS (Universal mobile telecommunications system) on tietoliikenneyhteys, jota tukiaseman omistaja käyttää internetliikenteeseen. Euroopassa UMTS toimii 2100 MHz:n ja 900 MHz:n taajudella. 900 MHz:n taajuus on otettu käyttöön, koska taajuus sopii haja-asutus alueelle pidemmän kantomatkan takia. 3G-yhteyttä ei voida rakentaa LAN- (Local Area Network) tai WAN-verkon (Wide Area Network) malliin toisin kuin Wlan- tai Ethernet-verkkoa, koska tietoliikenne kulkee aina palveluntarjoajan palvelimien kautta. 3G on kehitetty kasvattamaan matkapuhelinten ja PDA-tietokoneiden (Personal Digital Assistance) dataliikennettä. Nykyisin 3G-yhteyden voi hankkia tietokoneisiin, jossa on USB-, PCMCIA- tai Express card -liitäntäpaikka. (UMTS 2004; Penttinen 2006, 64–67.)

3G käyttää 2G:n kapeakaistaisen aaltosignaalin sijaan leveäkaistaista, joka mahdollistaa suuremman dataliikenteen. 3G käyttää tiedon siirtämiseen internetliikenteen mahdollistamiseksi IP-protokollaa, joka myös mahdollistaa yhteensopivuuden runkoverkon liikenteen kanssa. 3G-tukiasemat koostuvat erilaisista moduuleista. Ensimmäisenä tukiaseman liikenteen erottelusta vastaa basestation, joka erottelee tukiasemalta tulevan liikenteen digitaaliseksi informaatioksi ja puheeksi. Basestation sisältää RNC-moduulin (Radio network controller), joka vastaa dataliikenteen salauksen purusta ja muista dataliikenteen hallintatehtävistä. Digitaalisesta tiedosta basestationin jälkeen vastaa SGSN (service node). (Kuvio 10.) (UMTS 2004; Penttinen 2006, 64–67)




Kuvio 10. Esimerkki 3G-tukiaseman tietoliikenteestä.

## 7.1 UMTS-tietoturvallisuus

UMTS-tietoturvallisuutta kehitettäessä pyritään löytämään ratkaisuita, jotka ovat GSM-verkon kanssa yhteensopiva. UMTS-tietoturvallisuuden kehitys seuraa kolmea kohtaa:

- Kehityksessä otetaan huomioon yhteensopivuus GSM-verkon kanssa jos vain mahdollista.
- Pyritään pitämään GSM-verkon ominaisuudet, jotka on todettu toimiviksi ja tehokkaiksi sekä käyttökelpoisiksi verkon käyttäjille.
- Kehityksessä pyritään parantamaan nykyisiä ominaisuuksia, jotta GSM-järjestelmien mukana tulleet heikkoudet tulisivat korjatuiksi.

(Security for the Third Generation (3G) Mobile System 2000.)

### 7.1.1 UICC-kortti

USIM-ohjelma (Universal Subscriber Identity Module) on ensimmäinen autentikointiväline käyttäjän ja palveluntarjoajan välillä. USIM sijaitsee UICC-kortilla (Universal Integrated Circuit Card), joka yhteyden ottaessa varmentaa PSK-avaimella 3G-verkkoon. UICC-korttia käytetään 3G-verkossa ja kortti on samanlainen kuin GSM-verkossa käytetty SIM-kortti (Subscriber Identity Module). UICC-korttiin voi turvallisuuden vuoksi lisätä PIN-koodin (Personal Identification Number), joka on neljästä kahdeksaan numeroa. Kortissa on myös PUC-koodi (Personal Unlocking Code), jolla kortin saa lukituksesta avattua. PUC-koodin saa vain yhteyden tarjoajalta.
(Subscriber Identity Module 2009; Security for the Third Generation (3G) Mobile System 2000.)

### 7.1.2 Autentikointi ja salausavain

Käyttäjän yhdistäessä tukiasemaan tapahtuu molemminpuolinen autentikointi ja salausavaimen luonti. Autentikointi ja salausavaimen luonti tapahtuu SGSN-moduulin kautta, johon käyttäjä on yhteydessä. Autentikointi toimii challenge/response -protokollan avulla, jolloin SGSN ehdottaa modeemille jotain johon modeemi vastaa.
(Security in third Generation Mobile Networks 2004.)

### 7.1.3 Tietoliikenteen pakettieheys ja alkuperän autentikointi

Pakettieheys varmistetaan, jotta signaalin sisältämää dataa ei ole muutettu laittomin keinoin. Alkuperän autentikoinnilla varmistetaan, että paketti on tullut juuri sieltä mistä on tarkoitus. Huonona puolena varmistuksessa on, että se laskee yhteyden nopeutta.
(Security in third Generation Mobile Networks 2004.)

### 7.1.4 KASUMI

KASUMI-salaustapa on integroitu suoraan UMTS-modeemin siruun. KASUMI on toiselta nimeltään A5/3, joka on paranneltu malli 2G-modeemien salausmallista A5/1. Salaustavan rakenteena on käytetty Feistel-tekniikkaa, joka on symmetrinen salausmalli. Kyseistä salausta ja salauksen purkua käytetään kaikessa UMTS-dataliikenteessä. Salaustavan kehitti SAGE (Security Algorithms Group of Experts). (KASUMI (block cipher) 2004.)

### 7.1.5 NDS

NDS:lle (Network domain security) kuuluvat ominaisuudet varmistavat, että UMTS- ytimen ja runkoverkon välinen tietoliikenne on suojattu. Päämäärän tavoittamiseksi käytetään apuna erilaisia protokollia ja rajapintoja. Protokollista tärkeimmät ovat MAP (Mobile application part) ja GPRS-tunnelointi -protokollat. Protokollia taas suojaavat jo käsitellyt salaustekniikat. IP-protokollaa tietoliikenneyhteydessä suojaavat IPsec-tekniikka ja SS7-protokollaan kuuluva MAPSEC-tekniikka. Lisäksi UMTS-liikennettä voidaan suojata Ethernet-verkkoihin suunnitelluilla ominaisuuksilla kuten palomuurit ja staattiset VPN-yhteydet (Virtual Private Network). (Security in third Generation Mobile Networks 2004.)

## 7.2 UMTS-yhteystyypit

UMTS-verkolla on tällä hetkellä (03/2009) kolme yhteystyyppiä toiminnassa. Yhteystyypit ovat HSDPA (High speed Downlink packet access) ja HSUPA (High speed Uplink packet access) sekä Evolved HSPA. Kahden ensimmäisen ero on, että HSDPA pystyy suureen kapasiteettiin dataliikenteessä käyttäjälle päin ja HSUPA ulkoverkon suuntaan (Esimerkiksi palvelimen toiminnalle sopisi paremmin HSUPA). Evolved HSPA (Evolved High speed packet access) on näistä yhteystyypeistä kehittynein kaistan kapasiteetin huomioon ottaen, mutta evolved HSPA-yhteys ei ole käytössä Suomessa. (UMTS 2004.)

Yhteystyyppien tiedonsiirtonopeudet:

- HSDPA:n teoreettinen enimmäiskapasiteetti on 14,4 Mbit/s päätelaitteen suuntaan ja ulkoverkkoon päin 384 kbit/s (HSPA 2004).
- HSUPA:n teoreettinen enimmäiskapasiteetti on ulkoverkon suuntaan 5,76 Mbit/s (HSPA 2004).
- Evolved HSPA-yhteyden teoreettinen enimmäiskapasiteetti on 42 Mbit/s päätelaitteen suuntaan ja ulkoverkon suuntaan 11 Mbit/s (Evolved HSPA 2007).

3G-tietoliikenneyhteyksien nopeudet ovat modeemien enimmäisnopeuksia. Suomessa enimmäisnopeus on HSDPA-yhteydellä 5 Mbit/s. Yhteyksien nopeudet käytännössä riippuvat yhteyden tarjoajan tukiasemien laitteista ja tukiaseman peittoalueen vahvuudesta. HSDPA- ja HSUPA-ominaisuuksia voidaan käyttää yhdellä modeemilla yhteyden aikana. (HSPA 2004.)

# 8 Digitaalinen tallennus

Ennen digitaalista tallennusta tallennus toteutettiin analogisesti. Analogisten kameroiden tuottama kuva tallennettiin videonauhureilla eikä tapa ollut kovin käytännöllistä, koska videokasettien kapasiteetti on hyvin rajallista. DVR-laitteiden (Digital Video Recorder) markkinoille tulon jälkeen videotallennus muuttui, koska pinta-alaa tallennuslaitteille tarvittiin vähemmän. Tallennuksen/tallenteiden säilytys tuli mahdolliseksi uusissa ympäristöissä. NVR (Network Video Recorder) tarkoittaa videokuvan tallennusta, mutta tallennus/kamerajärjestelmä on osa tietoverkkoa. NVR-järjestelmä voi toimia missä tahansa kohtaa sisäverkkoa. Kaapeloinnin takia DVR-järjestelmän pitää sijaita analogikameroiden läheisyydessä. (Storage Solutions Move to the Forefront of the Network 2008.)

Megapikselikameroiden markkinoille tulon jälkeen ongelmaksi tuli tallennuskapasiteetin riittämättömyys. Ongelmat johtuivat megapikselikameroiden korkeiden tarkkuuksien ja suurien kuvatahti per sekunti –vaatimusten takia. Eri ympäristöissä käytettävillä tallenteilla on erilaisia säilytysvaatimuksia. Esimerkiksi nauhoitettaessa yhdellä megapikselikameralla 24 tuntia päivässä neljän kuvantahdin vauhdilla tallennuskapasiteettia kuluu tallennusmedialta noin 100Kbit/kuva. Tallennustilaa tarvitaan koko vuoden säilytystä varten noin 12Tbit. (Storage Solutions Move to the Forefront of the Network 2008.)

Tallennusjärjestelmät sekä -mediat ovat kehittyneet vuosi vuodelta. Esimerkiksi RAID-ominaisuus (Redundant Array of Independent Disks) nopeuttaa tallennuslaitteiden luku- ja kirjoitusaikoja sekä parantaa tietoturvallisuutta. Muita verkkojen tekniikoita ovat SAN (Storage Area Network), NAS (Network Attached Storage) ja iSCSI-protokolla (Internet Small Computer System Interface). (Storage Solutions Move to the Forefront of the Network 2008.)

IV-ominaisuus (Intelligent Video) on kasvattanut paljon suosiotaan kamerajärjestelmien käyttöliittymissä, koska ominaisuudella voidaan tehokkaasti vähentää henkilöstökuluja sekä tehostaa tallennuksen tarkoituksenmukaisuutta. Tallennuksen tehostaminen tapahtuu käyttämällä IV-ominaisuuksia esim. tallennuksen kohdistamiseen tietylle alueelle ja/tai tiettyyn esineeseen. IV-ominaisuus pudottaa henkilöstökuluja, koska videotarkkailuun tarvitaan vähemmän henkilöstöä järjestelmän automaattisen hälytysilmoituksen vuoksi. (Trends in Security Surveillance 2009.)

## 8.1 Tallentimet

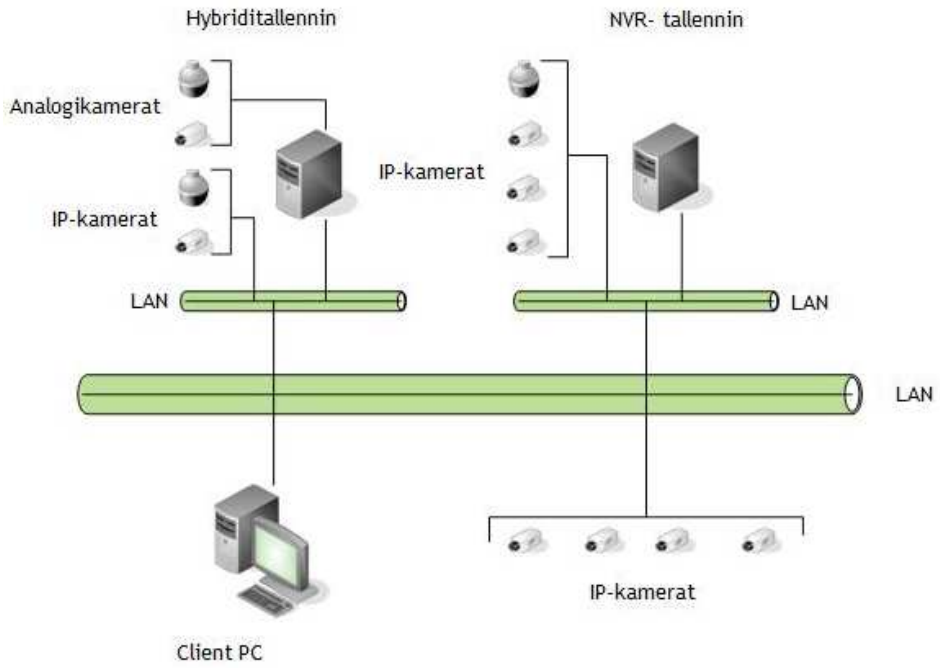
DVR-laite voi olla esimerkiksi tallentava digiboksi. DVR-laite on monikanavainen analogisisääntuloilla varustettu laite, jonka ominaisuuksiin kuuluuvat komposiittivideokuvan tallennus, tallennus toiselle digitaaliselle medialle, videon analysointi yhdelle tai yhtäaikaisesti monille eri käyttäjille. DVR-tallennin on yhden laitteen kokonaisuus, joka pakkaa tulevan analogikuvan digitaaliseksi esimerkiksi Mpeg-2 -(Moving Picture Experts Group) tai H.264/AVC –formaatiksi (Advanced Video Coding). DVR tallentaa videokuvan kovalevylle tai muulle digitaaliselle tallennusmedialle, josta informaatio voidaan siirtää esimerkiksi DVD-levyille pitkäaikaiseen säilytykseen. DVR-tallennin pystyy nauhoittamaan uutta videokuvaa kameroilta samaan aikaan, kun vanhaa videokuvaa analysoidaan. Lisäksi videokuvaa voidaan hallita DVR-järjestelmän kautta noutamalla esimerkiksi hälytysilmoituksia ja erilaisia raportteja kameroiden/järjestelmän toiminnasta. (Suddenly more storage options 2008.)

NVR-tallennin on käytännössä tietokone, jossa on verkkokortti. Suurin ero DVR-laitteeseen on siinä, että NVR tukee IP-pohjaisia laitteita ja ominaisuuksia. NVR-tallentimessa ei kuitenkaan ole käyttöliittymää verrattuna DVR-tallentimeen, jolla voi esimerkiksi katsella tallennettua kuvaa. NVR-tallennin ei ota vastaan analogisignaalia vaan Encoder:n kautta digitaalisesti pakattua videokuvaa, jossa Encoder pakkaa analogikuvan digitaaliseksi formaatiksi. Encoder-laite voi myös sijaita NVR-laitteen yhteydessä. NVR-tallennuslaite kehitettiin IP-pohjaisten megapikselikameroiden ja muiden IP-pohjaisten järjestelmien yleistymisen takia.
(Suddenly more storage options 2008.)

Kamerajärjestelmän uudistuksen tai uuden rakentamisen yhteydessä tulee ottaa huomioon seuraavat asiat:

- Käytössä olevien analogikameroiden määrä ja nykyisen tai tulevan kaapeloinnin hyötykäyttö
- Nykyisen tai tulevan verkon nopeuden määrittely vastaamaan tallennuksen asettamien resurssivaatimusten vuoksi
- Kohteen oman henkilökunnan osaaminen tietoliikenneverkoissa
- Nykyisen tai tulevan järjestelmän tallennuskapasiteetti vastaamaan tallennuksen vaatimuksiin
- Suunnittelu vaiheessa tulevaisuuden tarpeet huomioon tallennuksessa tai laitteiston skaalautuvuudessa

Hybrid DVR on yhdistelmä DVR:stä ja NVR:stä NVR:n IP-pohjaisilla ominaisuuksilla ja DVR:n käyttöliittymän ominaisuuksilla. Hybrid-tallennin on kehitetty väliaikaiseksi ratkaisuksi teknologiseen muutokseen analogikameroista IP-kameroihin. Hybrid-tallennin on kuitenkin riippuvainen analogikameroiden sijainnista kaapeloinnin takia. (Kuvio 11.)
(Suddenly more storage options 2008; Clusters, Clouds and the Future of Storage 2009.)




Kuvio 11. NVR:n ja hybridin erot (Mirasys, tuotteet ja palvelut 2009).

## 8.2 LuxRiot-käyttöliittymä

LuxRiot-ohjelmisto on suunniteltu videokuvan tallennukseen ja valvontaan Windows-käyttöjärjestelmässä. Ohjelmisto tukee erilaisia videokaapparikortteja, IP-kameroita, IP-videopalvelimia sekä kaikkia DirectShow-yhteensopivia laitteita. LuxRiot-ohjelmiston ominaisuuksia ovat muun muassa etävalvonta, liiketunnistus ja vähäinen tietokoneen resurssien kulutus. LuxRiot-ohjelmistosta saa ladattua internetistä ilmaisen version, johon saa yhden IP-kameran kytkettyä karsituilla ominaisuuksilla. Ohjelmistosta on myös enterprise-versio loputtomalla kameralisenssillä sekä muita erilaisia versioita.
(Luxriot from A & H review 2008.)

Ohjelmiston etävalvonta on rakennettu asiakas-isäntä arkkitehtuurin pohjalle. Ohjelmiston kokonaisuus käsittää asiakasohjelmiston (client) ja isäntäohjelmiston (server). Asiakasohjelmisto ottaa yhteyden IP-pohjaisten tietoliikenneyhteyksien kautta isäntäohjelmistoon. Isäntäohjelmisto varmentaa tunnuksien avulla profiilin käyttöoikeudet ja ominaisuudet. Ohjelmiston käyttöoikeuksia ja ominaisuuksia voi muokata profiilien kautta.

Käyttöoikeuksien ja ominaisuuksien profilointi yksittäiseen käyttäjään parantavat järjestelmän tietoturvallisuutta. (Luxriot from A & H review 2008.)

Liiketunnistus kuuluu IV-ominaisuuksiin ja tehostaa videokuvan tallennusta. Liiketunnistuksella voidaan ohjata kameroita seuraamaan liikettä tietyllä alueella. Liiketunnistusta ohjelmistossa voidaan rajata maalaamalla kamerakuvan alueet joilta ei haluta tallentaa kuvaa liikkeestä. Myös liiketunnistuksen herkkyyttä voidaan säätää. Herkkyyttä säätämällä on tarkoitus saada rajattua pienimmät liikkeet pois. Esimerkiksi voidaan rajata pois kuvasta puiden oksien tai lehtien pienimmät liikkeet. Ohjelmistossa on soitin, jolla voidaan katsella, analysoida sekä leikata videokuvaa .avi-tiedostomuotoon. (Luxriot from A & H review 2008.)

Ohjelmisto kuluttaa vähän tietokoneen resursseja. Suorittimen kulutus kuudella erilaisella IP-kameralla isäntämallissa on 11 % kameraresoluutiolla 640x480 ja asiakas-isäntä mallissa 30 %. Lisättäessä kolmen megapikselin kamera kulutus nousi isäntämallissa 23 %:iin ja asiakas-isäntämallissa 50 %:iin. Seitsemällä kameralla keskusmuistin käyttö oli 80–160 Mt. (Luxriot from A&H review 2008.)

Lux Riot-ohjelmiston suoritintehon kulutus:

- Intel Core 2 Duo 2,6 GHz (Kaksiytiminen suoritin) – 11 % kulutus isäntämallissa, 30 % kulutus asiakas-isäntämallissa.
- Intel Core Quad 2,5 GHz (Neliytiminen suoritin) – 4 % isäntämallissa, 11 % asiakas-isäntämallissa.

(Luxriot from A&H review 2008.)

## 8.3 Mirasys-käyttöliittymä

Mirasys-ohjelmistosta on olemassa Windows-käyttöjärjestelmälle kaksi versiota, jotka ovat pienille yrityksille tarkoitettu NVR Pro- ja isommille yrityksille tarkoitettu NVR Enterprise -versio. NVR Pro on karsitumpi versio verrattuna NVR Enterprise -versioon. NVR Pro -versio on rakennettu yhden käyttäjän tarpeisiin ja siihen ei ole mahdollisuutta rakentaa isäntä-asiakas-verkkoa. NVR Pro -versiossa isäntätallennin hallitsee kaikkia kameroita. Mirasys-ohjelmiston ominaisuuksia ovat esimerkiksi oppiva liiketunnistus, ohjelmistovahti, tuki H.264/AVC -videopakkaukselle ja kovalevyjen vikaantumista ehkäisevä järjestelmä. (Mirasys, tuotteet ja palvelut 2009; Mirasys, NVR Pro 2009; Mirasys, NVR Enterprise 2009.)

NVR Pro -versio sopii ympäristöihin, jossa on enintään 32 IP-kameraa kytkettynä tallentimeen. NVR Pro -ohjelmisto tue analogikameroita muuta kuin encoder:n kautta. NVR Enterprise -versiolla on mahdollista yhteensä 50 kameran, 16 äänikanavan ja 32 tekstikanavan tallennus yhdellä tallentimella. Lisäksi NVR Enterprise -version isäntä-asiakas -mallin takia on mahdollista käyttää 100 tallenninta yhdessä järjestelmässä, kun taas NVR Pro tukee yhden tallentimen järjestelmää. (Mirasys, NVR Pro 2009; Mirasys, NVR Enterprise 2009.)

Oppiva liikkeentunnistus on kehittyneempi versio liiketunnistuksesta, jossa ohjelmiston koodi oppii suodattamaan esimerkiksi heiluvat puiden oksat, sateen ja lumisateen tunnistettavasta liikkeestä. Liiketunnistuksessa taas säädetään kuvan liikkeen viivettä, jotta voidaan tunnistaa ja tallentaa haluttu liike kamerakuvasta. (Mirasys, NVR Enterprise 2009.)

Ohjelmistovahtia voidaan käyttää ohjelmistossa sattuviin tapahtumiin. Esimerkiksi kovalevyn vikaantuessa ohjelmisto lähettää sähköpostin ennalta määritettyyn osoitteeseen. Digitaalisia lähtöjä voidaan myös ohjata suorittamaan toiminto tapahtuman sattuessa. Digitaalinen lähtö tarkoittaa ohjelmoitua kytkintä, jolla voidaan ohjata erilaisia käskyjä ominaisuuksille. Ohjelmistot tukevat myös muokattua RAID 0 -tallennustapaa. Muokattu RAID 0 -tallennus tarkoittaa, että kovalevyn vikaantuessa tallenteet säilyvät. RAID 0 -tallennuksen myötä myös yleinen kovalevylle kirjoittaminen nopeutuu.
(Mirasys, tuotteet ja palvelut 2009; Mirasys, NVR Enterprise 2009.)

Ohjelmistot tukevat H.264/AVC -pakkausta tallennuksessa. Videokuvan H.264 -pakkausmuoto käyttää tehokkaasti kovalevytilaa ja säilyttää paremmin materiaalin kuvanlaadun kuin MPEG-2 -pakkaus. Huonona puolena H.264/AVC -pakkaus vaatii enemmän suoritintehoa kuin MPEG-2. Pakkaustavat käsitellään tarkemmin seuraavassa luvussa.
(Mirasys, NVR Enterprise 2009; Low-complexity video content adaptation for legacy user equipment 2007.)

Ohjelmisto sisältää työkalut videon osiointiin, analysointiin ja autentikointiin. Autentikoinnilla tarkoitetaan videokuvan aitouden varmistamista Mirasys-ohjelmiston omalla videosoittimella, jotta väärennetty videokuva tunnistettaisiin. Tallennetun videokuvan voi toistaa myös Windows-käyttöjärjestelmän mukana tulevalla Windows Media Player -nimisellä ohjelmalla. (Mirasys, tuotteet ja palvelut 2009.)

### 8.4 Videokuvan pakkausformaatit H.264/AVC ja MPEG-2

H.264/AVC -formaatti on tämän hetkisistä pakkausformaateista tehokkain ja säilyttää parhaiten myös kuvanlaadun pakkauksen yhteydessä. H.264/AVC -formaatti saavuttaa

kahdesta kolmeen kertaa pienemmän bittimäärän kuin tällä hetkellä yleisin formaatti MPEG-2. Pakkauksen tehokkuuden ja kuvanlaadun ansiosta palveluntuottajat suosivat formaattia. (Low-complexity video content adaptation for legacy user equipment 2007.)

H.264/AVC -pakkauksen hyödyt:

- Tallennustilan tarpeen pienentyminen
- Tietoliikenneyhteyden kaistan tarve pienenee, kun käytetään langattomia yhteyksiä.
- Parempi kuvalaatu kuin perinteisessä MPEG-2 -formaatissa

Kauan markkinoilla ollut MPEG-2 –formaatti on halpaa teknologiaa ja siksi yleinen kuluttajien suosimissa laitteissa. Videon pakkaus ja purkaminen järjestelmässä vaatii laitteilta erityisesti prosessointikykyä, koska H.264/AVC käyttää enemmän suoritintehoa ja muistiresursseja kuin MPEG-2 formaatti.
(Low-complexity video content adaptation for legacy user equipment 2007.)

## 8.5 SSD-kovalevy

SSD (Solid state drive) perustuu Flash-muistitekniikkaan, jota esimerkiksi käytetään tavallisten taskukameroiden muistikorteissa. SSD-tekniikan parhaita ominaisuuksia ovat vähäinen energian kulutus, nopeat I/O –toiminnot (input/output) ja vähäinen lämmöntuotto. HDD-kovalevyyn verrattuna SSD-kovalevyn hankintahinta on korkea. SSD-tekniikan energian kulutus riippuu tallennukseen käytettävien muistipiirien laadusta. SSD-tekniikoita on kahta erilaista arkkitehtuurityyppiä MLC- (Multi level cell) ja SLC-rakenne (Single level cell). (Kuvio 12.) (The SSD Anthology: Understanding SSDs and New Drives from OCZ 2009.)

SSD-tekniikan ominaisuudet:

- MLC-rakenteella saadaan aikaan nopeat lukuajat kovalevyltä, mutta hitaat kirjoitusajat ja etenkin kirjoitettaessa kovalevylle satunnaisesti. MLC-rakenteen huonona puolena pidetään vähäisiä kirjoituskertoja kovalevyn soluille, vain 1000 – 10000 kertaa.
- SLC-rakenteella kovalevy lukee ja kirjoittaa nopeammin kuin MLC-rakenteella, mutta SLC:n hankintahinta on huomattavasti kalliimpi. SLC-rakenteella kirjoituskerrat kovalevyn soluille on enintään 100000 kertaa.
  (Accelerate Your Hard Drive By Short Stroking 2009.)
- SSD-kovalevyn fyysinen koko vaihtelee 1,8”-, 2,5”- ja 3,5” tuuman välillä.
- Nopeimmat SSD-kovalevyt pystyvät 250 Mbit/s luku ja kirjoitusaikoihin riippuen tiedostojen koosta.

- SSD-kovalevyt ovat tärinälle vastustuskykyisiä, koska kovalevyjen tekniikka ei perustu liikkuviin osiin.

(The SSD Anthology: Understanding SSDs and New Drives from OCZ 2009.)


Kuvio 12. 2,5” SSD-kovalevy ATA-liitännällä (Solid state drive 2009).

## 8.6 HDD-kovalevy

HDD-tekniikka (Hard disk drive) perustuu magnetisoituihin levyihin, joihin tieto kirjoitetaan jonoihin bitti kerrallaan. Tämä kovalevytyyppi käyttää mekaanisia osia, jossa lukupää liikkuu levyillä eri kerroksissa lukemassa informaatiota. HDD-kovalevyjä on käytetty jo vuosien ajan erilaisissa käyttöympäristöissä ja todettu luotettaviksi etenkin yrityskäyttöön suunnatuilla malleilla. HDD-kovalevyn parhaina ominaisuuksina pidetään suurta tallennuskapasiteettia, halpaa hankintahintaa verrattuna tallennuskapasiteetin kokoon ja hyvää saatavuutta markkinoilla. (Kuvio 13.) (Accelerate Your Hard Drive By Short Stroking 2009.)

HDD-tekniikan ominaisuudet:

- Kovalevyllä on monta eri liitäntätapaa kuten IDE/ATA (Integrated Drive Electronics), SCSI, SATA (Serial ATA) ja SATA2. Näistä yleisimmät ovat IDE/ATA, SATA ja SATA2. SATA2-liitännällä on mahdollisuus saavuttaa 300Gbit/s tiedonsiirtonopeus.
- Kovalevyjen koot vaihtelevat 1,8”-5,25” välillä, mutta 5,25” koko ei ole enää käytössä.
- HDD-kovalevyn levyjen kierrosnopeus vaikuttaa tiedon hakuaikaan ja kirjoitukseen. Kierrosnopeudet vaihtelevat 5400- 15000 rpm (kierros per minuutti). Kannettavissa tietokoneissa käytetään 1,8” ja 2,5” levyjä joiden kierrosnopeudet vaihtelevat 5400 ja 7200 rpm välillä energian säästämiseksi.
- HDD-kovalevyjen keskimääräinen elinikä on 3-5 vuotta.
- HDD-kovalevyjen kirjoitusnopeus on enintään 125 Mt/s riippuen tiedon sijoittumisesta levylle.

(Hard drive 2009.)

Kuvio 13. 2,5” HDD kovalevy (Solid state drive 2009).

## 8.7 NAS- ja DAS-tallennusjärjestelmät

Kolmannen osapuolen palvelinhalleja käytetään tallennuksen ylläpitoon, mutta nykyään enenemässä määrin tallennus integroidaan yrityksen laitteisiin omia verkkoja hyväksikäyttäen. Tallennusjärjestelmät tukevat NAS (Network attached storage)- tai DAS-kokonaisuutta (Direct attached storage), jotta tallennus olisi mahdollisimman tietoturvallista ja tiedonjakeluverkoston kokonaisuuden ylläpito helppoa. NAS soveltuu parhaiten suurten yritysten tietojärjestelmien tarpeisiin. NAS (Network attached storage) on verkkotallennusjärjestelmä, joka jakaa tiedostoja verkossa yhteiskäyttöön. Järjestelmän palvelin on kytketty suoraan tietoverkkoon. Sisäisesti NAS sisältää sulautetun palvelimen ja kiintolevyjä käyttäen RAID-tekniikkaa. Ohjainkortit ovat RAID-toimintoja sisältäviä kortteja, jotka hallitsevat kovalevyjen I/O- toimintoja.
(Deng, Y. Deconstructing network attached storage 2009.)

NAS-verkkojakeluympäristön hyödyt:

- Ympäristön hallinnan yksinkertaisuus
- I/O- toimintojen yhdenmukaisuus
- Suuri skaalautuvuus
- Vähentää hallintakustannuksia tiedoston jaon keskittämisen ansiosta
- Virtuaaliympäristön käyttöönoton mahdollisuus jo kehitetyn X-NAS tekniikan ansiosta

Tallennusjärjestelmä ei ole sidoksissa yhteen käyttöjärjestelmään vaan se tukee eri käyttöjärjestelmiä. Lisäksi tallennusjärjestelmä on rakennettu toimintojen pohjalle, jotka koostuvat tunnetuista tietoliikenne- ja verkkoprotokollista. Yhdenmukaisen I/O –toiminnoista tekee NAS-järjestelmän verkon ja tiedoston I/O –toiminnot. Lisäksi Gigabit Ethernet –

tekniikan tiedonsiirtokyky mahdollistaa I/O -toimintojen yhdenmukaisuuden ylläpitämisen eri verkkojen välillä suuren tiedonsiirtokapasiteetin vuoksi.
(Deng, Y. Deconstructing network attached storage 2009.)

DAS on yksinkertaisempi tallennusratkaisu kuin NAS ja on tarkoitettu pienempien verkkoympäristöjen käyttöön. Ero NAS-ympäristöön on, että NAS on tarkoitettu toimimaan verkossa itsenäisenä laitteena monelle eri tietokoneelle, kun taas DAS on tarkoitettu ainoastaan isäntäkoneelle. DAS-ympäristössä tallennus tapahtuu isäntäkoneessa oleviin kovalevyihin ja sieltä DAS tallentaa tiedot omiin laitteisiin. DAS-järjestelmässä voi käyttää RAID-tallennusta tai tallennusmedia-asemaa esim. DAT-asema (Digital Audio Tape). DAS sopii hyvin ympäristöihin, jossa on enintään yksi tai kaksi palvelinta ja tiedonsiirto tapahtuu rakennuksen sisällä. (NAS, DAS or SAN? 2004.)

DAS-järjestelmän hyödyt ovat:

- Tallennusjärjestelmän rakennuskustannukset ovat pienemmät verrattuna NAS-järjestelmään.
- Hallinta isäntätietokoneen käyttöjärjestelmällä
- Yksinkertainen arkkitehtuuri

(NAS, DAS or SAN? 2004.)

DAS-järjestelmän heikkoudet:

- Skaalautuvuus, koska useamman palvelimen hankkiminen verkkoon käyttäjiä varten vaikeuttaa tiedostojen hallintaa
- Mahdollisten välissä olevien verkkolaitteiden vikaantuessa tallennusjärjestelmä ei toimi, koska se on suorassa yhteydessä isäntätietokoneeseen.
- Tallennusjärjestelmä ei sovi keskitettyyn tiedostonjakomalliin.

(NAS, DAS or SAN? 2004.)

## 8.8 RAID

RAID-tekniikasta on 7 eri variaatiota eri ominaisuuksilla ja lisäksi yhdistelmätekniikat. Eri versioiden tarkoitus on nopeuttaa kovalevyjen hakuaikoja levyltä sekä pienentää virhemarginaalia käyttämällä useaa eri levyä yhtäaikaisesti. RAID-tekniikan virhemarginaalit pienentyvät kirjoittamalla usealle kovalevylle tulevan tietovirran. Kyseistä menetelmää kutsutaan pariteettilevyksi. Pariteettilevymenetelmää käytettäessä tiedon menettämistä ei tapahdu, vaikka yksi kovalevyistä vikaantuu. RAID-ominaisuutta tukeva käyttöjärjestelmä on esimerkiksi Linux, joka tukee kaikkia RAID tasoja. Lisäksi Mac OS X -server ja Windows-server

sekä Xp Pro tukevat RAID 0,1 ja 5 -ominaisuuksia. RAID-ohjainkortit mahdollistavat tuen kasvattamisen. (RAID: high-performance, reliable secondary storage 1994.)

Käytetyin RAID-versio videotallennuksessa on RAID 5, joka yhdistää virhemarginaalien pienentämisen ja nopeat hakuajat. RAID 5:n heikkous on levylle kirjoittamisaikojen pidentyminen, koska RAID 5 kirjoittaa datan vähintään kahdelle eri levylle samaan aikaan. Lisäksi heikkoutena voidaan pitää I/O -toimintojen yhteneväisyyden epävarmuus levyillä mahdollisen järjestelmän kaatumisen aikana.
(RAID: high-performance, reliable secondary storage 1994.)

Videokuvan tallennus rasittaa kovalevyjä paljon, koska usein tallennus on päällä 24 tuntia vuorokaudessa. Kovan käytön vuoksi kovalevyjen käyttöikä pienenee ja tästä seuraa kovalevyn vikaantumisia useammin. RAID-ominaisuudesta on tässä tapauksessa hyötyä, koska tekniikan voi konfiguroida käyttämään ominaisuutta, joka sallii kovalevyn vaihdon kesken kirjoituksen ilman keskeytyksiä tai virheitä järjestelmän toiminnassa. Tekniikan ominaisuutta kutsutaan Hot-Swap- toiminnoksi. (RAID: high-performance, reliable secondary storage 1994.)

### 8.8.1 RAID 0

RAID 0- tekniikka on ei-vikasietoinen -tekniikka. Tekniikka mahdollistaa nopeat tiedon haku- ja kirjoitusajat levyllä, koska ominaisuus kirjoittaa paloja tiedoista molemmille levyille samaan aikaan. Hakuajat tekniikalla eivät ole yhtä nopeat kuin levylle kirjoitusajat verrattuna esim. RAID 1-tekniikkaan. Tekniikan heikkous on, että kovalevyn vikaantuessa järjestelmässä menetetään kaikki tieto. Ominaisuutta käytetään ympäristöissä, joissa tarvitaan suurta suorituskykyä eikä luotettavuutta. (RAID: high-performance, reliable secondary storage 1994.)

### 8.8.2 RAID 1

Vikasietoinen tekniikka käyttää kaksi kertaa enemmän kovalevyjen tallennuskapsiteetista kuin ei-vikasietoinen, mutta tarjoaa enemmän luotettavuutta. Tekniikassa kirjoitetaan samaan aikaan kummallekin levylle sama informaatio. Tekniikalla saavutetaan paremmat hakuajat kuin RAID 0:lla, koska tieto haetaan yhdeltä levyltä ainoastaan. Heikkoutena tekniikalla kirjoitusajat levylle kasvavat, koska tieto joudutaan kirjoittamaan kahteen kertaan. Tekniikan hyötynä on luotettavuus, koska toisen levyistä hajotessa tieto on tallessa toisella.
(RAID: high-performance, reliable secondary storage 1994.)

### 8.8.3 RAID 2

Ominaisuus hallitsee useamman kovalevyjen avulla vikaantuneiden kovalevy komponenttien aiheuttamia virheitä tietovirrassa, mutta korjaa tietovirran lukemalla toimivaa kovalevyä. Vikaantuneen komponentin aiheuttama virhe luetaan toimivan peili-kovalevyn komponentista ja viallinen tieto eheyden säilyttämiseksi tietovirrassa. Tallennuksen tehokkuus tekniikassa kasvaa mitä enemmän kovalevyjä on sidottu järjestelmään.
(RAID: high-performance, reliable secondary storage 1994.)

### 8.8.4 RAID 3

RAID 3 on rakennettu RAID 2:n pohjalta. Ero RAID 3:ssa on, että tekniikka tarvitsee vain yhden ylimääräisen pariteettilevyn riippumatta levyjen määrästä. RAID 3 tarjoaa samanaikaisen saannin, koska tiedostot on hajautettu pieniin juoviin eri kovalevyihin. Levyvirheen tapahtuessa pariteettilevyyn viitataan ja tiedostorakenteet muodostetaan uudelleen jäljelle jääneistä levyistä, kun hajonnut levy on korvattu.

Korkea tiedonsiirtokyky on mahdollinen, koska data on pilkottu palasiin eri levyille ja saanti on samanaikainen. Tiedon haku käyttää kaikkia levyjä rinnakkain ja siksi saavuttaa pienet hakajat. Heikkoutena tiedon hakemisessa voidaan suorittaa vain yksi pyynti kerrallaan, jolloin suorituskyky laskee samanaikaisten hakujen määrän noustessa.
(RAID: high-performance, reliable secondary storage 1994.)

### 8.8.5 RAID 4

RAID 4-tekniikka kuuluu riippumattomaan RAID-tekniikkaan, jossa jokainen kovalevy toimii itsenäisenä ja siksi erillisiä I/O -hakuja voidaan palvella samanaikaisesti. Tästä syystä riippumaton tekniikka sopii paremmin tiedonsiirtoympäristöön, joka vaatii pieniä hakuaikoja. Tekniikka ei palvele hyvin ympäristössä, jossa tarvitaan suurta kirjoitusnopeutta. Kirjoitusnopeuden hitauden syy on, että tekniikassa on ainoastaan yksi pariteettilevy. Jokainen itsenäinen levy käyttää pariteettilevyä turvatakseen kovalevyn tiedot. Levylle kirjoittaminen itsenäiselle levylle vaatii joka kerran tekniikan hallintajärjestelmältä käyttäjän datan päivittämisen ja vastaavat pariteettitiedot pariteettilevylle.
(RAID: high-performance, reliable secondary storage 1994.)

### 8.8.6 RAID 5

RAID 5 on rakennettu RAID 4:n kaltaisesti. Erona RAID 4:een RAID 5 jakaa pariteettiosiot jokaiselle levylle eikä yhdelle pariteettilevylle. RAID 5 on suosituin RAID-taso, koska se vaatii vain yhden ylimääräisen levyn, eikä siinä ole RAID 4:n kaltaista heikkoutta

kirjoitusnopeudessa. Pariteetin kirjoitus eheästi vaatii paljon prosessointikykyä ja sen takia RAID 5 toteutetaan aina erillisellä ohjainkortilla.

RAID 5 -tekniikka on nopein pienten- ja isojen tiedostojen lukemisessa kovalevyltä. Lisäksi suurten tiedostojen kirjoituskyky on tehokkainta RAID-järjestelmissä. RAID 5:n heikkous on pienten tiedostojen kirjoituksessa, koska tekniikalla joudutaan suorittamaan RAID 4:n tavoin luku-muokkaus-kirjoitus -toiminto pariteetin päivittämiseen.
(RAID: high-performance, reliable secondary storage 1994.)

### 8.8.7 RAID 6

RAID 6-tekniikka pohjautuu vikaantuneiden levyjen palautukseen ja on toteutettu RAID 5-tekniikan pohjalta. Vian sattuessa palautus tapahtuu kovalevylle pariteetin palautusalgoritmin avulla. Verrattuna RAID 5-tekniikkaan kovalevyn vikaantuessa palautukseen tarvitaan kaikki eheät levyt luettaviksi ja hakuvirheen mahdollisuus on suuri kesken pariteetin palautuksen levyissä.

RAID 6 on toiselta nimeltään vikasietoinen P+Q -tekniikka, jolla voidaan palauttaa kahden vikaantuneen kovalevyn tiedot. Suojaus tapahtuu käyttämällä vähitään kahta levyä palautukseen. Tekniikan erona RAID 5 -tekniikkaan on kirjoittaessa kovalevylle. RAID 5 käyttää kirjoitukseen neljää levyä ja RAID 6 käyttää kuutta levyä, koska tekniikka joutuu päivittämään myös P+Q -levyt. (RAID: high-performance, reliable secondary storage 1994.)

### 8.8.8 RAID 10- ja 0+1 -yhdistelmätekniikat

RAID 10 toteutetaan RAID 0:na, jonka levyt ovat RAID 1 -tekniikan tapaisia peilejä. Tekniikalla saavutetaan sama virhemarginaali kuin RAID 1 –tekniikalla. Järjestelmän I/O -toiminnot käyttävät RAID 0 –tekniikkaa paremman suorituskyvyn vuoksi. (RAID 2009.)

RAID-taso 0+1 toteutetaan RAID 1:nä, jonka levyt ovat RAID 0 ositettuja pariteetteja. RAID 0+1 tarjoaa saman virhetoleranssin kuin RAID 5, mutta järjestelmä rakennetaan RAID 10 tavoin. RAID 10 tavalla rakennettu järjestelmä tarkoittaa, että kuuden levyn järjestelmässä käytetään kolmea levyä kopiointiin. (RAID 2009.)

Vaikka turvallisuus ei ole yhtä hyvä kuin RAID 10:ssä, RAID 0+1 tarjoaa tehokkuutta ja tekniikkaa voidaan käyttää samoissa sovelluksissa kuin RAID 0. (RAID 2009.)

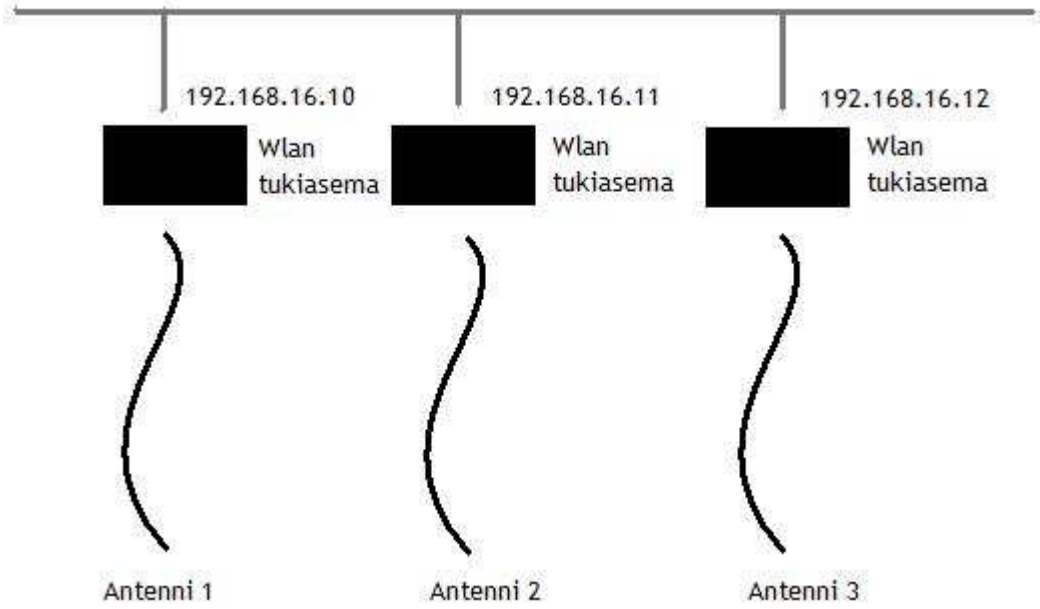
# 9 Yhteenveto tutkimuksesta

Tietoliikenneyhteyden täytyy olla turvallinen käyttää ja laitteiden tulee olla rakenteellisesti luotettavia sijoituskohteessa. Wlan-yhteys on tietoturvallisesti parempi ratkaisu kuin 3G-yhteys, koska 3G-yhteys käyttää palvelun tarjoajan erillisiä tai jossain tapauksessa vuokrattuja tukiasemia yhteyden muodostamiseen. Tietoliikenneyhteyden ylläpito on tärkeää tietoturvallisuuden kannalta pitää omissa käsissä joten ulkopuolisten tukiasemien käyttö yhteyden muodostamiseen ei ole suositeltavaa. Tietoturvallisuusvaatimuksen myötä tietoliikenneyhteyden ylläpito on vikatilanteissa reaktioherkempää ja verkkoyhteyden jatkokehitys on luontevampaa oppimisympäristössä.

Tietoturvallisuustekniikat ovat yhteensopivampia Wlan-yhteyksissä Ethernet-tekniikan kanssa kuin 3G-yhteyksien salausmenetelmien kanssa. 3G-yhteys on kuitenkin yhteensopiva käyttämänsä IP-protokollan vuoksi Ethernet-tekniikan kanssa. 3G-tekniikka on kehitetty vanhan 2G-tekniikan pohjalta yhteensopivuuden saavuttamiseksi. Wlan-tekniikalla verkon vasteajat ovat paljon pienemmät kuin 3G-tekniikalla, joka vaikuttaa reaaliaikaisen videon katseluun verkkoyhteyden yli. Internetpalveluntarjoajien 3G-yhteyden kautta kaistan nopeus ei ole suuri ja nopeus vaihtelee tukiaseman käyttäjien aiheuttaman ruuhkaisuuden mukaan. Tämä ei ole hyvä asia silloin, kun yhteys pitää olla vakaa ja luotettava tilanteesta riippumatta sekä oman valvonnan alla. 3G-yhteyden voi myös rakentaa oman tukiaseman varaan, jolloin tietoliikenneyhteyden kustannukset olisivat huomattavasti suuremmat kuin Wlan-tekniikkaa käytettäessä.

Wlan-laitteiden salaustekniikat ovat tehokkaita ja yleisesti käytössä olevia standardeja. Tietoliikenneyhteydessä tulisi käyttää standardia 802.11g, koska standardin nopeusluokka videon katseluun on tarpeeksi suuri ja standardi on nykyisten Wlan-tietoliikennekorttien kanssa tuettu. Toinen vaihtoehto siirtostandardiksi olisi 802.11a- ja 802.11n -standardi. 802.11a -standardi toimii noin 5,2 GHz alueella ja tämän takia kantomatka on standardilla pienempi kuin g-standardilla. Lisäksi 802.11a -standardin yhteensopivuus nykyisten tietoliikennekorttien kanssa on heikkoa, koska lähes kaikki tietoliikennekortit tukevat g-standardia. 802.11:n -standardi on nykyaikaisin ja nopein tiedonsiirtokyvyltään, mutta yhteensopivuus muiden standardiluokkien kanssa on osoittautunut hankalaksi yhteyshäiriöiden vuoksi. Wlan- ja 3G-yhteyksien häirintä ja häirintälaitteiden valmistus ovat kiellettyjä Suomessa, mutta monissa muissa maissa häirintälaitteiden valmistusta ei ole lailla kielletty. Häirintälaitteiden hankkiminen ei ole vaikeaa internetin kautta, mutta häirintälaitteilta suojautuminen on erittäin kallista eikä ole kannattavaa Laurean kaltaiselle ympäristölle.

Wlan-yhteyden käyttäminen Laurea Leppävaaran toimipisteen ympäristössä vaatii antenneja, jotka säteilevät peittolalueen lähiympäristöön. Tähän tarkoitukseen on saatavilla eri tavalla signaalin suuntaavia antenneja. Tutkimuksen perusteella käyttäisin Laurean ympäristöön paneeliantennin ja ympärisäteilevän antennin yhdistelmää, koska ympärisäteilevä peittää paremmin julkisivut ja paneeliantenni etupihan. Paneeliantennilla on säteilykulma 65–70 astetta ja kapean säteilykulman takia voisi käyttää myös kahta ympärisäteilevää antennia peittämään koko alueen, mutta silloin mahdollisuus signaalin säteilemisestä tarpeettoman kauas kasvaisi. Ympärisäteilevän antennin huono puoli on siinä, että signaali säteilee sellaisiin paikkoihin, mihin ei ole tarkoitus. Wlan-yhteyden muodostaminen Laurean ympäristöön vaatii 2-3 tukiasemaa, jotka ovat omassa aliverkossa reititettynä ainoastaan kamerajärjestelmän kirjautumisien hallintapalvelimelle. Fyysisen sabotoinnin estämiseksi antennit on mahdollista peittää pleksisuojakotelolla, jotta esimerkiksi kovilla esineillä ei pystyisi rikkomaan antennia maasta käsin. (Kuvio 14.)




Kuvio 14. Esimerkki reitityksestä tietoliikenneyhteyttä varten.

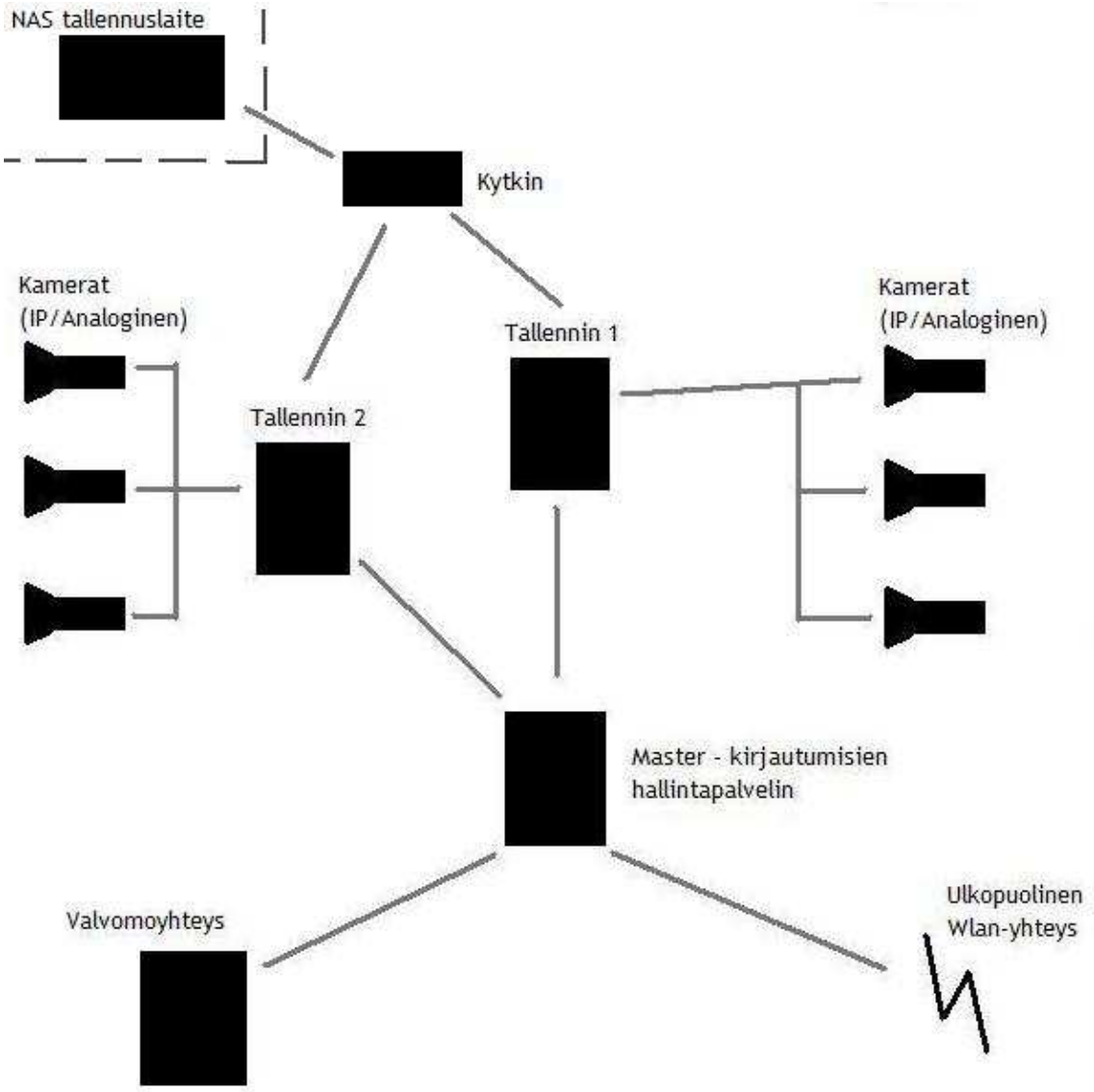
Laurean kamerajärjestelmä tällä hetkellä käyttää LuxRiot-käyttöliittymää kameroiden ja tallennuksen hallintaan. LuxRiot-käyttöliittymä on ominaisuuksiltaan riittävä, mutta siitä puuttuu uusimpia ominaisuuksia. Ohjelmistosta puuttuu videokuvan pakkausformaatti H.264/AVC:n tuki, jolla säästettäisiin tallennustilaa. Samalla tallennetun kuvan laatu paranisi. Lisäksi ohjelmistosta puuttuu ulkoympäristöön suunniteltu oppiva liiketunnistus, joka suodattaa sateen, lumen ja heiluvat puun oksat pois. Tosin LuxRiot-ohjelmistossa on liiketunnistus, jossa voi säätää liikkeen viivettä. Säätöominaisuudella pystytään karsimaan osa liikkeistä pois, mutta ei niin paljon kuin oppivalla liiketunnistuksella. Hyvät puolet ohjelmistossa ovat ohjelmiston suoritintehon ja keskusmuistin resurssien käyttö, joka on hyvin säästeliästä. Toinen hyvä puoli on ohjelmiston arkkitehtuuri, joka on isäntä-asiakas-mallinen.

Isäntä-asiakas-arkkitehtuuri mahdollistaa järjestelmän ulkopuolisien yhteyksien käytön asiakasohjelmistolla. Ohjelmiston kolmas hyvä puoli on ohjelmiston avoimuus shareware-versiona, jonka saa ladattua internetistä kokeiltavaksi. Toisaalta avoimuus turvallisuusohjelmistoissa ei välttämättä ole hyvä asia, koska väärissä käsissä heikkouksien löytäminen ohjelmistosta helpottuu.

Toinen tutkimani ohjelmisto Laurean kamerajärjestelmän hallintaan oli Mirasys NVR, josta oli kaksi eri versiota pienemmille ja isommille yrityksille. Pienemmille yrityksille tarkoitettu NVR Pro -versio riittäisi ominaisuuksien puolesta hyvin, mutta versiosta puuttuu isäntä-asiakas-arkkitehtuuri. Arkkitehtuurin puuttumisen takia kamerajärjestelmän skaalautuminen tulevaisuudessa ja hätätietoliikenneyhteyden muodostaminen ei onnistuisi. Tulevaisuudessa megapikselikamerat yleistyvät ja IP-tekniikka tulee kasvamaan markkinoita hallitsevaksi tekniikaksi. Siitä syystä tallennusjärjestelmän skaalautuvuus tallennuskapasiteetin suhteen on tärkeää tulevaisuudessa. NVR Enterprise -versio tukee Master-tyyppistä verkkotopologiaa, joka mahdollistaa yhdelle yhteyksien hallintapalvelimelle liitettävän enintään 100 tallenninta. Hallintapalvelin toimii ainoastaan kirjautumisien ja käyttöoikeuksien hallitsijana. Verkkotopologialla säästetään itse tallentimien kuormaa, jolloin tallennin ei itse toimi yhteyden tunnistautumisessa. Tietoturvallisuus Master-verkotuksella paranee, koska tallentimeen ei oteta yhteyttä vaan hallintapalvelimeen.

Kamerajärjestelmässä olisi hyvä ratkaisu käyttää hybridi-tallentimia, koska analogikameroita on Laurean järjestelmässä vielä jäljellä. Tulevaisuudessa järjestelmän skaalautuvuuden ansiosta voidaan lisätä IP-kameroiden määrää. Laurean järjestelmään tulisi kaksi hybriditallenninta, koska resurssien käyttö kovalevyiltä ja muilta komponenteilta on hyvä jakaa tallentimien kesken. Kummassakin hybriditallentimessa voisi olla 16 paikan analogikameroiden kaapparikortit. Koaksiaalimonitorilähtöjä ei tarvita, koska asiakas-ohjelmistolla voidaan luoda monitorinäkymiä.

Kamerajärjestelmän tallenteet voidaan varmuuskopioida NAS-järjestelmää käyttävän tallennuslaitteen kanssa. NAS-laite olisi hyvä vaihtoehto, koska laitteen voisi sijoittaa fyysisesti toiseen paikkaan kytkettynä lähiverkkoon. DAS-järjestelmä taas on tarkoitettu pienemmille ympäristöille, mutta laitetta ei saa kytkettyä lähiverkkoon. DAS-tallennuslaite pitää olla kytkettynä suoraan tallentimeen esimerkiksi USB- tai Firewire-portin kanssa. DAS-järjestelmää käytettäessä laitetta ei pystyisi sijoittamaan fyysisesti eri tilaan kuin videotallennin. Esimerkiksi tulipalon sattuessa tallentimen tilassa NAS-järjestelmän varmuuskopioinnilla pystyisi säilyttämään tallenteet. NAS-järjestelmä on tarkoitettu isommille ympäristöille, mutta suurta tallennuskapasiteettia tullaan tarvitsemaan tulevaisuudessa megapikselikameroiden kanssa. (Kuvio 15.)




Kuvio 15. Tutkimuksen perusteella toteutettu järjestelmäkaavio.

Lähteet

@450. 2009. Wikipedia. Viitattu 29.7.2009.
http://fi.wikipedia.org/wiki/@450

Accelerate Your Hard Drive By Short Stroking. 2009. Tom's Hardware US. Viitattu 9.4.2009.
http://www.tomshardware.com/reviews/short-stroking-hdd,2157.html

Anti-jamming timing channels for wireless networks. 2008. ACM. Viitattu 30.3.2009.
http://nelli.laurea.fi:2079/citation.cfm?id=1352533.1352567&_coll=GUIDE&_dl=GUIDE&_CFID=69873091&_CFTOKEN=26194609

Clusters, Clouds and the Future of Storage. 2009. ProQuest. Viitattu 8.4.2009.
http://nelli.laurea.fi:2107/pqdweb?did=1646098551&Fmt=3&VInst=PROD&VType=PQD&RQT=309&VName=PQD&

Deng, Y. Deconstructing network attached storage. 2009. Elsevier science direct.
Viitattu 15.4.2009.
http://nelli.laurea.fi:2075/science?_ob=ArticleURL&_udi=B6WKB-4VTCMD2-2&_user=953156&_rdoc=1&_fmt=&_orig=search&_sort=d&view=c&_acct=C000049240&_version=1&_urlVersion=0&_userid=953156&md5=90315c5ad767ca72331ae9eb3a8c4985

Evolved HSPA. 2007. Wikipedia. Viitattu 1.4.2009.
http://en.wikipedia.org/wiki/Evolved_HSPA

GPS jammer. 2007. Navigadget. Viitattu 14.4.2009.
http://www.navigadget.com/wp-content/postimages/2007/10/gps-jammer-01.jpg

Hard drive. 2009. Wikipedia. Viitattu 14.4.2009.
http://en.wikipedia.org/wiki/Hard_drive

Harte, L., Bowler, D., Ofrane, A. & Levitan, B. 2005. Wireless Systems. North Carolina, Fuquay-Varina: Althos Publishing.

HSPA. 2004. Wikipedia. Viitattu 1.4.2009.
http://fi.wikipedia.org/wiki/HSPA

IEEE 802.11. 2009. Wikipedia. Viitattu 11.3.2009.
http://fi.wikipedia.org/wiki/IEEE_802.11

IEEE 802.11i. 2009. AllExperts encyclopedia. Viitattu 17.3.2009.
http://en.allexperts.com/e/i/ie/ieee_802.11i.htm

Infrared networking. 2009. About. Viitattu 29.7.2009.
http://compnetworking.about.com/od/homenetworking/g/bldef_infrared.htm

Järvinen, P. & Järvinen, A. 2004. Tutkimustyön metodeista. Tampere: Tampereen Yliopistopaino, Juvenes-Print.

KASUMI(block cipher). 2004. Wikipedia. Viitattu 31.3.2009.
http://en.wikipedia.org/wiki/KASUMI_(block_cipher)

Korkeakoulujen turvallisuus posteri 2009. Laurea-ammattikorkeakoulu. Laurea Leppävaara. Espoo. Hankejulkaisu.

Langattomat lähiverkot. 2001. Joensuun yliopisto. Viitattu 9.3.2009.
http://cs.joensuu.fi/~mjaarane/laudaturseminaari/seminaari.html

Latenssi. 2009. Wikipedia. Viitattu 29.7.2009.
http://fi.wikipedia.org/wiki/Latenssi

Low-complexity video content adaptation for legacy user equipment. 2007. ACM.
Viitattu 20.4.2009.
http://nelli.laurea.fi:2079/citation.cfm?id=1385289.1385293&coll=GUIDE&dl=GUIDE&CFID=69873091&CFTOKEN=26194609

LuxRiot Features. 2009. LuxRiot. Viitattu 20.4.2009.
http://www.luxriot.com/features.html

LuxRiot from A&H review. 2008. Video Home Surveillance Guide. Viitattu 20.4.2009.
http://www.video-home-surveillance.com/software-reviews/luxriot

Mikroaallot vs. infrapuna langattomassa tiedonsiirrossa. 1999. Tietoliikenneohjelmistojen ja multimedian laboratorio. Viitattu 30.3.2009.
http://www.tml.tkk.fi/Studies/Tik-110.300/1999/Wireless/infrared_1.html

Mirasys, NVR Enterprise. 2009. Mirasys. Viitattu 14.4.2009.
http://www.mirasys.com/?q=fi/webfm_send/16

Mirasys, NVR Pro. 2009. Mirasys. Viitattu 14.4.2009.
http://www.mirasys.com/?q=fi/webfm_send/17

Mirasys, tuotteet ja palvelut. 2009. Mirasys. Viitattu 14.4.2009.
http://www.mirasys.com/?q=fi/webfm_send/22

NAS, DAS or SAN?. 2004. Storagesearch. Viitattu 15.4.2009.
http://www.storagesearch.com/xtore-art1.html

Nokia Siemens hautaa oman wimaxin. 2009. Digitoday. Viitattu 28.7.2009.
http://www.digitoday.fi/mobiili/2009/07/27/nokia-siemens-hautaa-oman-wimaxin/200917067/66?rss=6

Penttinen, J. 2006. Tietoliikennetekniikka – 3G ja erityisverkot. Porvoo: Werner Söderström.

Personal Cell Phone Signal Blocker Device. 2009. Dealextreme. Viitattu 28.7.2009.
http://www.dealextreme.com/details.dx/sku.4355

Subscriber Identity Module. 2009. Wikipedia. Viitattu 13.3.2009.
http://en.wikipedia.org/wiki/Subscriber_Identity_Module

RAID. 2009. Wikipedia. Viitattu 17.4.2009.
http://en.wikipedia.org/wiki/RAID#cite_note-9

RAID: high-performance, reliable secondary storage. 1994. ACM. Viitattu 16.4.2009.
http://nelli.laurea.fi:2079/citation.cfm?id=176979.176981&coll=GUIDE&dl=GUIDE&CFID=69873091&CFTOKEN=26194609

Security for the Third Generation (3G) Mobile System. 2000. Elsevier Science Direct.
Viitattu 31.3.2009.
http://nelli.laurea.fi:2075/science?_ob=ArticleURL&_udi=B6VJC-416C2C3-7&_user=953156&_rdoc=1&_fmt=&_orig=search&_sort=d&view=c&_acct=C000049240&_version=1&_urlVersion=0&_userid=953156&md5=c9aad4e4b2a32fcc141d91f502200b2d

Security in third Generation Mobile Networks. 2004. Elsevier Science Direct. Viitattu 1.4.2009.
http://nelli.laurea.fi:2075/science?_ob=ArticleURL&_udi=B6TYP-4B8X2JP-4&_user=953156&_rdoc=1&_fmt=&_orig=search&_sort=d&view=c&_acct=C000049240&_version=1&_urlVersion=0&_userid=953156&md5=eb42fb1817839b1ba60dffbc00e7f6a2

Solid state drive. 2009. Wikipedia. Viitattu 14.4.2009.
http://en.wikipedia.org/wiki/Solid-state_drive

Storage Solutions Move to the Forefront of the Network. 2008. ProQuest. Viitattu 2.4.2009.
http://nelli.laurea.fi:2107/pqdweb?did=1590057621&Fmt=3&VInst=PROD&VType=PQD&RQT=309&VName=PQD&

Suddenly more storage options. 2008. ProQuest. Viitattu 3.4.2009.
http://nelli.laurea.fi:2107/pqdweb?did=1480181411&Fmt=3&VInst=PROD&VType=PQD&RQT=309&VName=PQD&

The SSD Anthology: Understanding SSDs and New Drives from OCZ. 2009. Anandtech.
Viitattu 14.4.2009. http://www.anandtech.com/storage/showdoc.aspx?i=3531&p

Tetra: introduction to technology. 2004. etiworld. Viitattu 30.7.2009.
http://www.etiworld.com/tetra.pdf

Trends in Security Surveillance. 2009. ProQuest. Viitattu 20.4.2009.
http://nelli.laurea.fi:2107/pqdweb?did=1603358941&Fmt=3&VInst=PROD&VType=PQD&RQT=309&VName=PQD&

UMTS. 2004. Wikipedia. Viitattu 1.4.2009.
http://fi.wikipedia.org/wiki/UMTS

Videovalvontaopas. 2004. Turvakamera. Viitattu 16.3.2009
http://www.turvakamera.fi

VIRVE. 2009. Wikipedia. Viitattu 30.7.2009.
http://fi.wikipedia.org/wiki/VIRVE

What is a wireless LAN? – Knowledge Base. 2009. Indiana University. Viitattu 29.7.2009
http://kb.iu.edu/data/aick.html

What is UMTS?. 2009. TechFAQ. Viitattu 29.7.2009.
http://www.tech-faq.com/umts.shtml

WLAN. 2003. Muropaketti. Viitattu 9.3.2009.
http://plaza.fi/muropaketti/artikkelit/sekalaiset/wlan

Wimax-An-Introduction. 2005. Rfdesign. Viitattu 29.7.2009.
http://www.rfdesign.info/doc-desc/18/WiMAX-An-Introduction.html

Wireless LAN. 2009. Wikipedia. Viitattu 16.3.2009.
http://en.wikipedia.org/wiki/Wireless_LAN#Peer-to-peer

Wireless LAN security. 2009. Wikipedia. Viitattu 30.7.2009.
http://en.wikipedia.org/wiki/Wireless_LAN_security

Wireless standards by Mitchell, Bradley. 2007. About. Viitattu 11.3.2009.
http://compnetworking.about.com/cs/wireless80211/a/aa80211standard.htm

Wi-Fi Protected Access. 2009. Wikipedia. Viitattu 31.7.2009.
http://en.wikipedia.org/wiki/Wi-Fi_Protected_Access

Kuvioluettelo



Taulukkoluettelo