LAUREA

TETRA–radioverkkojärjestelmän turvallisuuden tutkimus teknisen vertailun ja riskianalyysin avulla

Jari Laakso

Hannu-Heikki Leino

2011 Leppävaara

Laurea-ammattikorkeakoulu
Laurea Leppävaara

TETRA–radioverkkojärjestelmän turvallisuuden tutkimus teknisen vertailun ja riskianalyysin avulla

Laakso, Jari; Leino, Hannu-Heikki
Tietojenkäsittelyn koulutusohjelma
Opinnäytetyö
Toukokuu, 2011

Laurea-ammattikorkeakoulu
Laurea Leppävaara
Tietojenkäsittelyn koulutusohjelma

Tiivistelmä

Laakso, Jari; Leino, Hannu-Heikki

TETRA–radioverkkojärjestelmän turvallisuuden tutkiminen teknisen vertailun ja riskianalyysin avulla

Vuosi 2011 Sivujen lukumäärä 81

Tämä opinnäytetyö tutkii TETRA (Terrestrial Trunked Radio) –radioverkkostandardin soveltuvuutta viranomaisten, kuten poliisin, palo- ja pelastuslaitosten sekä sosiaali- ja terveystoimen, viestinnälle asettamiin vaatimuksiin sekä langattoman viestintäteknologian kohtaamia moninaisia riskitekijöitä. Työssä käsitellään myös yleisimpiä radio- ja matkapuhelinjärjestelmiä ja verrataan niiden sisältämiä teknisiä ratkaisuja TETRA–verkon tarjoamiin ominaisuuksiin. Riskitekijöiden todennäköisyyttä ja vakavuutta sekä niiden seurauksia arvioidaan riskianalyysin avulla. Työn tilaajana on Laurea-ammattikorkeakoulu ja työ kuuluu osaltaan Saterisk–projektiin laadittujen viestintäteknologioiden riskitutkimuksiin.

Opinnäytetyössä TETRA ja muut käsitellyt radio- ja matkapuhelinjärjestelmät on selvitetty niitä käsittelevien kirjallisten julkaisujen ja sähköisten dokumentaatioiden avulla. Lähteiden sisältämä teoriatieto on esitetty johdonmukaisesti vertailun ja riskianalyysin toteutusta silmälläpitäen. Tekniikoiden vertailu on toteutettu laatimalla näistä lähteistä kerätyistä tiedoista yleistävä taulukko, jossa muiden tutkittujen järjestelmien toimintaominaisuuksia verrataan TETRA–järjestelmään.

Tekniikoiden vertailu tukee työssä laadittua riskianalyysia, jossa käsitellyt riskit on kerätty sekä kirjallisista että sähköisistä lähteistä, mukaan lukien monien uutislähteiden julkaisemat todelliset riskitapaukset. Riskianalyysin läpivienti toteutettiin laatimalla riskianalyysityökalu, johon tarvittavat riskien todennäköisyyden ja vakavuuden asteet hankittiin alan asiantuntijalle toimitetun lomakkeen avulla. Riskien asteet esitetään taulukossa numeerisesti ja näiden tietojen valossa on tehty johtopäätöksiä riskien esiintyvyydestä terveydenhuollon organisaation toiminnassa.

Tutkimustyön tulosten perusteella TETRA–standardi on ominaisuuksiltaan tällä hetkellä tarjolla olevista radio- ja matkapuhelinjärjestelmistä kokonaisuutena käyttökelpoisin ja turvallisin vaihtoehto viranomaistahojen käyttöön, erityisesti puhepalveluiden osalta. TETRA osoittautui toiminnaltaan varmaksi niin epävarmoissa tilanteissa kuin riskialttiissa toimintaympäristöissäkin, koska sitä voidaan rajoitetusti käyttää myös niissä olosuhteissa, joissa muut tutkitut järjestelmät olisivat käytännössä lähes tai jopa kokonaan toimintakyvyttömiä. Tämä opinnäytetyö voi toimia päätöksenteon tukena organisaatioille, jotka harkitsevat matkapuhelinjärjestelmänsä kehittämistä nykyisten teknologiavaihtoehtojen pohjalta tietoturvallisempaan ja toimintavarmempaan suuntaan.

Asiasanat Matkapuhelinjärjestelmä, radioverkko, riskianalyysi, TETRA, tietoturva

Laurea University of Applied Sciences
Laurea Leppävaara
Bachelor's Programme in Business Information Technology

Abstract

Jari Laakso, Hannu-Heikki Leino

Research of the security of the TETRA radio network system with the help of a technical comparison and a risk analysis

Year 2011 Pages 81

This thesis studies the suitability of the TETRA (Terrestrial Trunked Radio) radio network standard to the communicational requirements of authorities such as the police, fire brigades, rescue services, social and health care organisations. The many risks posed by wireless communication technology are also researched. Additionally the most commonly used radio and mobile phone systems are covered. Their technical aspects are compared with the properties offered by the TETRA network. A risk analysis is used to estimate the consequences of the probability and severity of the risk factors. This study is commissioned by Laurea University of Applied Sciences and is a part of the risk studies of communication technologies belonging to the Saterisk project.

In this thesis TETRA and the other radio and mobile phone systems have been examined according to the literary publications and online documentations concerning them. The theoretical knowledge included in the sources is presented coherently with the technical comparison and the risk analysis in mind. The technical comparison has been made by composing the literary sources into a generalised table in which the features of the systems studied are compared with the TETRA system.

The technical comparison supports the risk analysis for which the risks are collected from both literary and online sources, including many news articles reporting real life incidents. The implementation of the risk analysis was done by creating a risk analysis tool to which the required degrees of probability and severity were acquired with a form filled by an expert of the field. The risk degrees are presented numerically in the table and conclusions are drawn in light of their frequency in the activities of a health care organisation.

Based on the results of the research, the TETRA standard is the most secure and usable alternative as a whole out of the radio and mobile phone systems available today for the use of authorities, especially when services for voice calls were considered. The operation of TETRA proved to be reliable in both uncertain situations and in risk-prone operational environments as well, because it is available for limited usability in circumstances where the other researched systems would be practically almost or entirely inoperable. This thesis can assist decision making for organisations that consider improving their mobile communications system to a more secure and reliable direction based on the current technologies available.

Keywords Information security, mobile phone system, radio network, risk analysis, TETRA

Sisällys

1 Johdanto

Tämän opinnäytetyön tutkimuskohteena on viranomaiskäyttöön suunniteltu TETRA–radioverkkostandardi. Työssä tutkitaan TETRA-järjestelmän teknisiä ominaisuuksia yleisellä tasolla. Lisäksi selvitetään langattomaan viestintään liittyviä riskejä, joiden pohjalta laaditaan riskianalyysi TETRA-järjestelmän käytöstä suomalaisessa organisaatiossa, ja verrataan järjestelmää muihin yleisesti käytettyihin radio- ja matkapuhelinjärjestelmiin. Vertailun sekä riskianalyysin perusteella tehdään johtopäätöksiä siitä, miten TETRA soveltuu vaativaan ammattikäyttöön ja löytyykö vertailtavista verkkotekniikoista sille vaihtoehtoa kokonaisuutena tai jossakin viestinnän osa-alueessa.

TETRA (Terrestrial Trunked Radio) on ETSI (European Telecommunications Standards Institute) –instituutin kehittämä digitaalinen radioverkkostandardi. TETRA-standardin tarkoituksena on tarjota luotettava kommunikaatiojärjestelmä monien ammattialojen, kuten poliisin, palo- ja pelastuslaitosten, sosiaali- ja terveystoimen, vartijoiden, liikenteen, asevoimien ja teollisuuden käyttöön. Laajasta kohderyhmästä johtuen standardissa on mahdollistettu verkon räätälöinti käyttäjä- ja valmistajakohtaisesti. (TETRA Memorandum of Understanding 2011.)

TETRA-standardin pohjaksi luotu yhteistyöelin TETRA Memorandum of Understanding -yhdistys perustettiin vuonna 1994 ja siihen kuuluu nykyisin lukuisia edustajaorganisaatioita, kuten laitevalmistajia, operaattoreita, palveluntarjoajia ja muita järjestelmästä kiinnostuneita tahoja. TETRA on tarkoitettu maailmanlaajuiseksi järjestelmäksi, joten sen sisältämät standardit vaativat kansainvälisen hyväksynnän. Euroopassa TETRA-standardi on täysin hyväksytty ja siihen pohjautuvia verkkoja on ollut käytössä jo jonkin aikaa, mutta esimerkiksi Pohjois-Amerikassa TETRA-verkkoja ei ole vielä käytössä. TETRA on tarkkaan määritelty, koska eri laitevalmistajien laitteiden on oltava keskenään yhteensopivia ja verkon on muutenkin oltava kansainvälisesti yhteensopiva käytön laajentumista varten. TETRA:sta arvioidaan tulevan lähitulevaisuudessa laajimmalle levinnyt viranomaisverkkojen teknologia. (Penttinen 2006b, 39-40.)

Opinnäytetyön tilaajana on Laurea-ammattikorkeakoulu ja ohjaajana Laurean yliopettaja Jyri Rajamäki. Työ kuuluu osaltaan kansainväliseen, kahden suomalaisen korkeakoulun johtamaan Saterisk-projektiin. Opinnäytetyö tulee projektiin osallistuvien tahojen hyödynnettäväksi. Lisäksi Laurean turvallisuuslaboratorion yhteistyökumppanit ovat kiinnostuneita viranomaisverkkojen tarkemmasta selvityksestä, joten TETRA-tutkimus mahdollisesti palvelee laajaa joukkoa toimijoita.

Laurea-ammattikorkeakoulun ja Lapin yliopiston yhteinen Saterisk-projekti, jonka päärahoittajana on Tekes, selvittää satelliittipaikannukseen liittyviä teknisiä, juridisia ja käyttötapaan liittyviä riskejä. Lapin yliopisto oikeustieteellisen tiedekuntansa voimin on keskittynyt juridisen puolen tutkimiseen, joten Laurean vastuulla ovat tekniikkaan ja käyttötapoihin liittyvät riskiselvitykset. Projektissa on lisäksi mukana satelliittipaikantamiseen kytköksissä olevia yrityksiä sekä ulkomaisia korkeakouluja ja yhteistyökumppaneita. Projekti on alkanut vuonna 2008 ja jatkuu vuoden 2011 kesään saakka. Projektin lopullisena tavoitteena on tuottaa kattava kartoitus satelliittipaikannuksen riskeistä tällä hetkellä ja tulevaisuudessa sekä synnyttää uusia laite-, palvelu- ja koulutusinnovaatioita. (Saterisk 2011.)

1.1 Työn tarkoitus

Opinnäytetyön tarkoituksena on tutkia viranomaistahojen, kuten poliisin, palo- ja pelastuslaitosten sekä sosiaali- ja terveystoimen, viestintään suunniteltua eurooppalaisen standardin mukaista TETRA-radioverkkojärjestelmää. Tutkimus sisältää järjestelmän teknisten ominaisuuksien selvittämisen, TETRA:n ominaisuuksien vertailemisen muihin yleisiin langattomiin matkaviestintätekniikoihin, radio- ja matkapuhelinjärjestelmien yleisten riskien kartoittamisen ja TETRA-järjestelmän riskianalyysin. Tutkimustyötä tukee käytännön kokemusten hankkiminen asiantuntijalta, joka työskentelee järjestelmää hyödyntävässä organisaatiossa.

Viranomaistahojen työn arkaluontoisuus ja tärkeys asettaa omat vaatimuksensa viestinnälle nopeasti muuttuvassa yhteiskunnassa. Viranomaisten radiopuhelimilta odotetaankin nykyisin hyvin suojattua ja riittävän nopeaa tietoliikennettä, verkon, päätelaitteiden ja palvelusovellusten toimintavarmuutta hankalissakin oloissa, laitteiden fyysistä kestävyyttä, käyttäjien ja käyttäjäryhmien hallinnan vaivattomuutta turvallisuudesta tinkimättä sekä kustannustehokkuutta viestinnän laadun siitä kuitenkaan kärsimättä. Tästä johtuen viranomaisverkot ovat tälläkin hetkellä ajankohtainen aihe ja sen tutkimiselle on olemassa todellinen tarve.

TETRA:n ominaisuuksia verrataan analogiseen radiotekniikkaan, tuttuun toisen sukupolven GSM-verkkoon ja sen radioversioon GSM-R:ään sekä kolmannen sukupolven UMTS-verkkoon. Analoginen radio on poistunut viranomaiskäytöstä Suomessa, mutta on edelleen yleisessä käytössä mm. takseissa ja kuljetusalalla sekä TETRA-järjestelmä on nimenomaan suunniteltu analogisten radioverkkojen korvaajaksi. TETRA:n tavoin digitaaliset GSM- ja UMTS-verkot ovat kaupallisessa käytössä selvästi yleisimmät matkapuhelinjärjestelmät. Toisen sukupolven GSM on ollut lähes parikymmentä vuotta johtavassa asemassa matkaviestinnässä ja siitä on myös julkaistu aikanaan rautatiekäyttöön suunniteltu radioversio GSM-R; kymmenisen vuotta

markkinoilla ollut kolmannen sukupolven UMTS:n asema kuitenkin vahvistuu datasiirron tarpeiden kasvaessa ja UMTS-järjestelmään tulee saataville yhä enemmän erilaisia palveluita.

Riskianalyysin tarkoituksena on tutkia, millaisia riskejä TETRA-järjestelmän käytössä esiintyy suomalaisessa toimintaympäristössä ja miten todennäköisiksi ja vakaviksi ne koetaan. Analyysi on toteutettu sosiaali- ja terveystoimen näkökulmasta, koska TETRA-asiantuntija valikoitui kyseiseltä alalta. Riskianalyysissa käsitellyt riskitekijät on koottu sekä kirjallisista että sähköisistä lähteistä, jotka on selvitetty tarkemmin työn riskejä käsittelevässä osiossa. Analyysin toteutuksessa kartoitetut riskit lajitellaan niille lasketun riskiarvon mukaiseen järjestykseen, josta ilmenevät vakavimmiksi ja lievimmiksi koetut riskitekijät. Riskianalyysin avulla voidaan tehdä päätelmiä TETRA:n käytön turvallisuudesta sosiaali- ja terveystoimen osalta Suomessa.

Riskianalyysin toteutuksen apuna käytetään Saterisk-projektin puitteissa tehtyä Pasi Kämpin ja Robert Guinnessin laatimaa satelliittipaikannuksen riskianalyysia: Technical Risk Analysis for Satellite Based Tracking Systems. Opinnäytetyön rajauksen suunnittelussa konsultoitiin tarvittaessa työn ohjaajan lisäksi muutakin Laureassa Saterisk-projektin parissa työskentelevää henkilöstöä, jotta tutkimustyö palvelisi projektia mahdollisimman tarkoituksenmukaisella ja täysipainoisella tavalla. Työ ei kuitenkaan itsessään käsittele varsinaista satelliittiteknologiaa, vaan ainoastaan tutkittujen radio- ja matkapuhelinjärjestelmien paikannussovellusten osalta olennaisia asioita.

1.2 Työn tavoitteet

Opinnäytetyön päätavoitteena on tuottaa Saterisk-projektille selvitys TETRA–standardin soveltuvuudesta viranomaiskäyttöön. TETRA:n teknisten ominaisuuksien, teknisen vertailun, riskianalyysin sekä niistä muodostettavien tutkimustulosten perusteella määritellään, sopiiko TETRA siihen käyttötarkoitukseen, jota varten se on erityisesti kehitetty. Työtä voidaan myös käyttää apuna TETRA:n käyttöönottoa suunnitteleville tahoille, jotka harkitsevat matkaviestintänsä kehittämistä turvallisemmaksi ja toimintavarmemmaksi.

Teknisen vertailun tavoitteena on saada käsitys siitä, voiko jokin muu teknologia korvata TETRA:n sen nykyisessä käyttötarkoituksessa. Vertailussa muita vertailtavia tekniikoita rinnastetaan TETRA:n ominaisuuksiin, jotta saadaan selville, onko muissa tekniikoissa niitä ominaisuuksia, mitä viranomaiskäytössä välttämättä tarvitaan. Vertailun perusteella voidaan myös todeta TETRA:n mahdollisia puutteellisia osa-alueita, joissa jokin muu teknologia toimii paremmin tällä hetkellä.

Työhön saadaan käytännön kokemusta terveydenhuoltoalan organisaation valmiuspäällikön täyttämän riskiarviointilomakkeen avulla. Asiantuntijalta lomakkeeseen saatujen riskitekijöiden todennäköisyyden ja vakavuuden asteiden avulla laaditaan riskianalyysi, jonka pohjalta TETRA:n turvallisuudesta terveydenhuollon tehtävissä voidaan tehdä yleisluontoisia johtopäätöksiä. Lomakkeen lisäksi työssä hyödynnetään muita hänen huomioitaan ja hänen kauttaan saatuja tietoja TETRA-järjestelmän nykytilanteesta Suomessa.

Kämppi ja Guinness hyödyntävät tutkimuksessaan laatimaansa riskianalyysityökalua. Tavoitteena on luoda tämän työkalun kaltainen oma suppeampi sovellutus, jolla voidaan keskittyä tutkimaan matkapuhelinjärjestelmissä esiintyviä riskejä. Tämän itse laaditun taulukkotyökalun avulla tutkitaan opinnäytetyön puitteissa vain TETRA:n käytössä ilmeneviä riskejä, mutta sitä voidaan muissa tutkimuksissa hyödyntää myös muiden radio- ja matkapuhelintekniikoiden vastaaviin riskianalyyseihin. Työkaluun kootut riskitekijät ovat luonteeltaan matkapuhelinjärjestelmille yleispäteviä, koska ne perustuvat sekä alan yleiseen teoriaan että käytännön esimerkkitapauksiin.

2 Tutkimusmenetelmät

Tässä osiossa selvennetään tämän opinnäytetyön toteutuksen metodit eli käsitellään tutkimustyössä käytettyjä teorioita, menetelmiä ja työtapoja. Ensiksi selvennetään työssä käytetyt teoriat, joille tutkimustyö perustuu. Sen jälkeen käydään läpi tiedonkeruumenetelmiä käytettyjen lähteiden ja käyttäjälähtöisen kokemuspohjaisen tiedon hankinnan osalta.

2.1 Käytetyt teoriat

Tämän opinnäytetyön läpivientiin on käytetty toimivaksi todettuja teorioita, jotka tukevat tutkimuksen asettamia tavoitteita. Käytettäväksi valittiin kvalitatiivinen aineiston keräys- ja tutkimustapa. Tutkimusongelman kannalta kvantitatiivinen määrällinen menetelmä ja aineisto olisivat hyödyllisiä, mutta laajaa numeerista tietomäärää ei tämän työn läpiviennissä pystytty riskien kartoittamisen yhteydessä luomaan tai saamaan käsiteltäväksi. Tämän vuoksi laadullinen lähestymistapa osoittautui käyttökelpoisemmaksi vaihtoehdoksi tutkimuksen toteuttamiseen.

2.1.1 Kvalitatiivisen tutkimuksen teoria

Kvalitatiivinen tutkimusmenetelmä on olemukseltaan laadullinen eikä se perustu tilastollisiin aineistoihin. Laadullinen tutkimus menetelmänä ei vaadi tutkimusaineistoa toisin kuin määrällinen kvantitatiivinen tutkimus. Tutkimustulosten saamiseksi laadullista menetelmää

käyttävällä ei välttämättä ole mahdollisuutta satunnaisotantoihin tai matemaattisiin päätelmiin ja osoituksiin aineistostaan. Pääasiallinen ero laadullisen ja määrällisen tutkimuksen välillä on siis niiden kyvyssä perustella tieteellinen selitysvoimansa ja uskottavuutensa. Määrällinen tutkimus nojaa numeerisiin tilastoihin, joista pystytään johtamaan matemaattisia päätelmiä. Laadullinen tutkimus puolestaan perustelee tuloksiaan aineistonsa hankintamenetelmillä, jotka toteuttavat ratkaisun kyseessä olevan tutkimuksen esittämään tutkimusongelmaan. Vaikka tieteellinen lähestymistapa vaatii perusteltuja väittämiä ja ne todistavan aineiston olemassaolon saadakseen uskottavuutta, voi laadullinen tutkimus ilman määrällistä aineistoa tai sen mahdollisuutta silti olla suositeltava lähestymistapa tietynlaisia tutkimuskohteita käsiteltäessä sekä tietynlaisissa tutkimusolosuhteissa. Laadullinen tutkimus soveltuu erityisesti esimerkiksi sosiaalisten ja kulttuurillisten tutkimusten läpivientiin, joissa tutkimuskohteena ovat ihmisten käyttäytymiseen liittyvät ilmiöt sekä mahdollisesti muuttuvat olosuhteet. (Grönfors 1982.)

Kvalitatiivisessa tutkimuksessa tärkein tutkimusväline voidaan sanoa olevan tutkija itse. Tutkimusaineiston hankinnassa tutkijan on laadittava aineistonsa keräysmenetelmä, jonka avulla tutkimuksen tavoitteisiin päästään. Laadullinen tutkimus painottaa ihmisläheistä työskentelyä. Määrällinen tutkimus puolestaan voidaan toteuttaa valmiin aineiston pohjalta tai ihmiskosketus voi rajoittua vain kysely- tai haastattelulomakkeiden laadintaan ja niiden lähettämiseen otoksen edellyttämälle joukolle ihmisiä. Kvalitatiivinen tutkimus keskittyykin oikeastaan uuden teoriatiedon luomiseen ennemmin kuin hypoteesien todistamiseen. Tutkimuksia ei voida silti jakaa vain laadullisiin ja määrällisiin niiden läpiviennissä käytettyjen tutkimusmenetelmien perusteella, sillä kvalitatiivisia ja kvantitatiivisia menetelmiä voidaan käyttää saman tutkimuksen eri työvaiheiden aikana. Nämä tutkimusmenetelmät eivät ole aina toisensa poissulkevia vaan ne voivat myös täydentää toisiaan ja laajentaa saatavaa tutkimusaineistoa suuremman kokonaisuuden hahmottamiseksi. (Grönfors 1982.)

Riskianalyysin toteuttamiseksi tarvittava tietämys hankittiin tätä opinnäytetyötä varten toimittamalla tutkimuksessa havaittuja riskitekijöitä tiedusteleva arviointilomake aiheen asiantuntijan täytettäväksi. Asiantuntijaa pyydettiin arvioimaan lomakkeeseen siinä esitettyjen riskitekijöiden todennäköisyyttä ja vakavuutta. Vaikka tämä käytetty menetelmä on luonteeltaan määrällinen, ei vain yhdellä lomakkeella kerätystä tiedosta kuitenkaan voida muodostaa matemaattisia johtopäätöksiä, jollaisia suuremmalla otoksella olisi voitu laatia esimerkiksi tulosten keskiarvoja laskemalla. Riskitekijöitä pyydettiinkin siksi arvioimaan numeroarvoilla, jotka vastasivat laadullisia kuvailevia termejä: pieni, melko pieni, keskisuuri, melko suuri, suuri. Lomakkeella saatuja tietoja käytettiin siten suuntaa-antavina laadullisten päätelmien johtamiseksi riskianalyysistä.

Kvantitatiiviset tutkimukset pohjautuvat usein deduktiiviseen logiikkaan ja kvalitatiiviset puolestaan induktiiviseen logiikkaan. Deduktiivinen logiikka johtaa teoriatiedon ja tosiasioiden kautta yksityiskohtien muodostamiseen. Tällaista menetelmää tukevat laajat aineistot, joiden esittämiä tietoja voidaan pitää vallitsevana totuutena tutkitusta asiasta silloin kun niihin vaikuttavien tekijöiden kausaalinen suhde voidaan osoittaa. Induktiivinen logiikka on oikeastaan päinvastaista, jossa havaituista yksityiskohdista johdetaan teoriaa. Induktiivisessa ajattelussa tutkimusaineistosta pyritään löytämään vallitsevia yhteisiä piirteitä, jotka mahdollistavat selityksen ja johtopäätösten päättelemisen. Tutkimuksen kohteesta riippuu voidaanko induktiolla johdettua teoriaa pitää pätevänä vain tutkimuksen rajaamalla aineistolla vai voiko teoria olla pätevä myös muiden vastaavanlaisten aineistojen kohdalla. Tällainen jako määrällisessä ja laadullisessa tutkimuksessa käytettävien logiikoiden välillä ei kuitenkaan tarkoita ajattelutapojen olevan toisensa poissulkevia, vaan molempia voidaan soveltaa käytettäviksi tutkimuksen luonteesta riippuen. (Grönfors 1982.)

Kvalitatiivinen analyysi perustuu tutkimusaineistosta johdettuihin päätelmiin. Kvalitatiivisen aineiston kohdalla tutkijan on kiinnitettävä huomiota tapoihin, joilla teoria johdetaan aineistosta. Tutkimusraportissa johtopäätösten perustelujen ja niiden muodostamisen mahdollistanut päättely tulee yhdistää empiirisesti hankittuun aineistoon. Laadullinen tutkimus on hyvin riippuvainen tutkijan itsensä työskentelystä ja ajattelusta, jolloin analyysin voidaan sanoa osin tapahtuvan jo aineistoa kerätessä. Tutkimusaineiston muodostuessa tutkija johtaa jo päätelmiä itsekseen tutkittujen kohteiden esiintyvyydestä ja vaikutuksesta. Kvalitatiivinen tutkimus ei ole yksinomaan induktiivisen logiikan varassa, sillä myös deduktiota tarvitaan johtopäätösten kehittymiseen. Tutkimusongelman käsitteleminen vaatii käytettävien toimintatapojen pohtimista ennen tutkimuksen aloittamista, tutkimusaineiston järjestämistä ja tarkastelua sekä kokonaisuuden hahmottamista analyysin luomiseksi. Pelkkä induktiivinen logiikka ei yksinään riitä laadullisen tutkimuksen kokonaisvaltaiseen läpiviemiseen. (Grönfors 1982.)

Teknisessä vertailussa radio- ja matkapuhelintekniikoiden välillä tässä opinnäytetyössä nojaudutaan sekä induktiiviseen että deduktiiviseen loogiseen päättelyyn. Tietoa tekniikoista hankittiin pääasiassa niitä käsittelevistä kirjallisista julkaisuista. Matkapuhelinjärjestelmien ja radioverkkojen teknisistä tiedoista laadittiin niiden sisältämiä ominaisuuksia yleisluontoisesti listaava taulukko, jonka avulla tekniikoiden väliset erot olivat heti nähtävissä. Taulukon avulla tehtiin johtopäätöksiä vertaamalla muiden tekniikoiden sisältämiä ominaisuuksia TETRA–tekniikan ominaisuuksiin, jotta TETRA:n soveltuvuudesta viranomaiskäyttöön saataisiin konkreettista näyttöä.

2.1.2 Grounded Theory

Opinnäytetyössä käytetään riskianalyysin tukena Barney Glaserin ja Anselm Straussin kehittämää Grounded Theory -menetelmää, joka voidaan suomentaa vapaasti aineistopohjaiseksi teoriaksi. Menetelmää on alun perin käytetty ihmisiä tutkivan sosiologiatieteen piirissä, mutta sitä voidaan soveltaa muillakin aloilla. Käsitteellistämisen etenemistapa ei itsessään aseta rajoituksia itse tutkimuskohteelle tai –aineistolle. Grounded Theory -menetelmää on käytetty yleisimmin kvalitatiivisessa tutkimuksessa. (Koskennurmi-Sivonen 2007.)

Grounded Theory tarkoittaa systemaattista kvalitatiivista tutkimusmetodologiaa, joka painottaa uuden teorian luomista tutkimustulosten perusteella. (Martin & Turner 1986.) Se on tutkimusmenetelmä, joka toimii lähes päinvastaisella tavalla tavanomaiseen tutkimustyöhön nähden. Perinteisessä tieteellisessä tutkimuksessa tehdään ensin tutkimustyötä ja kehitetään jokin hypoteesi, kun taas Grounded Theory -menetelmässä kerätään ensin tietoa eri tavoin. Kerätyn tiedon avainkohdat merkitään koodein, jotka ryhmitellään konsepteihin. Konsepteista laaditaan sitten kategorioita, joiden perusteella voidaan kehittää jokin teoreettinen malli. (Allan 2003.)

Grounded Theory sopii tutkimuskohteisiin, joista tarvitaan teoreettista ja jäsentynyttä tietoa esimerkiksi päätöksenteon tueksi, mutta joista tätä tietoa ei vielä ole olemassa. Tutkimusaineisto voi olla missä muodossa tahansa; tavallisesti menetelmää on käytetty kvalitatiivisten aineistojen analysoinnissa, mutta kvantitatiivisten aineistojen käyttökään ei ole poissuljettu. Tärkeintä on, että aineistosta voidaan tehdä käsitteellistäviä tulkintoja, eikä esimerkiksi tilastollisia, sillä Grounded Theoryn tarkoituksena on paljastaa käsitteellisiä suhteita määrällisten kuvausten sijaan. (Koskennurmi-Sivonen 2007.)

Grounded Theory -menetelmässä koodaus on keskeisessä asemassa. Koodauksella tarkoitetaan merkkejä tai muilla keinoin aineistoon tehtyjä jäsenteleviä merkintöjä ja luokitteluja. Koodausmerkinnöillä on tarkoitus helpottaa aineiston käsittelyä, sillä merkitsemällä samoin koodein tekstikohdat, joissa puhutaan samoista tai samankaltaisista asioista, tiedon löytää nopeammin. Tutkija ei välttämättä koe harjoittavansa koodausta kirjaimellisesti edellä olevan kuvauksen mukaisesti, mutta hän tekee sitä kuitenkin enemmän tai vähemmän näkyvästi. Tutkimustyössä joutuu aina pohtimaan, mitä aineistossa on ja mitä siinä ei ole. Lisäksi aineistoa on jäsenneltävä, jotta sen sisältöä on helpompi havainnoida ja kartoittaa. (Saaranen-Kauppinen & Puusniekka 2006.)

Aineistosta tehdään kolmenlaista koodausta: avointa koodausta, aksiaalista tai akselikoodausta ja selektiivistä koodausta. Ensimmäisenä tehdään avointa koodausta, jossa

tutkija tekee tutkittavien alkuperäisten ilmausten perusteella sisällöllisiä koodeja. Tekstin koodauksen tarkkuus vaihtelee tutkijasta ja tutkimuksen tarkoituksesta riippuen; tekstiä voi koodata esimerkiksi rivi riviltä tai kappale kappaleelta. Toisessa vaiheessa luodaan avoimen koodauksen pohjalta tarkennettuja kategorioita, mikä toisin sanoen tarkoittaa koodaamista keskeisiksi valittujen elementtien (avainasioiden) eli akselien ympärillä. Kolmannessa vaiheessa kootaan koko aineisto teoriaksi eli etsitään aineistoista niiden ”punainen lanka”, josta tulee tutkimuksen ydinkategoria. (Saaranen-Kauppinen & Puusniekka 2006.)

Edellä olevan perusteella saattaisi luulla, että kyse on lineaarisesta etenemismallista tai toisistaan erillisistä vaiheista, mutta todellisuudessa ne ovat erilaisia tapoja käsitellä lähdemateriaalia ja tutkija liikkuukin vaiheiden välissä ja yhdistelee niitä tilanteen ja tarpeiden mukaan. Prosessi kuitenkin yleensä ottaen etenee tuossa järjestyksessä, eli työ aloitetaan avoimella koodauksella ja loppua kohden selektiivinen koodaus tulee tärkeämmäksi. Pienistä havainnoista kuljetaan kohti suurempaa kokonaisuutta eli teoriaa tutkittavasta aiheesta. (Saaranen-Kauppinen & Puusniekka 2006.)

Teorian muodostuksessa käytetään vertailevaa tapaa, jota voidaan nimittää analyyttiseksi vertailumetodiksi. Aineistosta tehdään käsitteitä sekä koodeja ja näiden välisiä suhteita analysoidaan ja vertaillaan. Vertailun edetessä mennään empiiriseltä tasolta kohti teoreettisempaa käsitteellistämistä. Prosessin aikana havainnoista, heränneistä kysymyksistä ja ideoista tehdään muistiinpanoja, jotka sitten omalta osaltaan selittävät muodostettuja koodeja. Kirjallisuus tulee mukaan yleensä vasta sitten, kun on päästy aineiston alustavaan jäsennykseen. (Saaranen-Kauppinen & Puusniekka 2006.)

2.2 Tiedonkeruumenetelmät

Opinnäytetyön toteutus on vahvasti riippuvainen sen aihetta käsittelevän lähdemateriaalin hyödyntämisestä. Pääasiallisina lähteinä tälle opinnäytetyölle on käytetty olemassa olevaa kirjallisuutta TETRA-, GSM- ja UMTS-tekniikoiden toiminnasta ja sovelluksista. Lisäksi lähdemateriaalina on käytetty yleisemmin tietoliikenteen toimintasovelluksia, laitteita ja tekniikan osa-alueita piinaavista riskitekijöistä löydettyä tietoa. Vaikka opinnäytetyö käsitteleekin pääpainoisesti aiheensa puolesta vain TETRA:n toiminnallisuutta, on silti olennaista selventää myös muita siihen verrattavia tekniikoita ja järjestelmiä sekä aihealueen yleistä teoriaa, jotta TETRA-tekniikan soveltuvuuden ja mahdollisuuksien kartoitus voidaan toteuttaa onnistuneesti ja siten myös analysoida siihen kohdistuvien riskien esiintyvyyttä ja vaikutuksia.

Tärkeitä lähteitä ovat tietoliikennealan ammattilaisten teettämät ja julkaisemat tutkimukset sekä TETRA-tekniikalla toteutettujen palveluiden toimintakuvaukset. Molempia on

hyödynnetty tiedonsaannissa mahdollisimman paljon, sillä ne laajentavat aiheen tietopohjaa tarjoten uusia näkemyksiä. Rajoittavaksi tekijäksi havaittiin kuitenkin TETRA:lla toteutettujen palveluiden tarkkojen toimintakuvausten verrattain vähäinen määrä, sillä tutkittu tekniikka on osin mahdollisten salassapitosopimusten piiriin rajoittuvien tahojen käytössä. Tekninen tieto TETRA:sta ja vertailuun valituista muista radio- ja matkapuhelinjärjestelmistä, analoginen radiotekniikka, GSM ja UMTS, on kuitenkin julkista.

Perustietoa TETRA:sta saatiin sen standardia ylläpitävän TETRA MoU –yhdistyksen Internet-sivustolta. Lisätietoa tarjosivat myös TETRA:n käyttäjätahojen muodostaman TETRA Industry Groupin Internet-sivut. Pääasiallisena lähteenä tämän opinnäytetyön TETRA–tekniikkaa käsittelevälle osuudelle palveli kuitenkin Kimmo Heikkosen, Tero Pesosen ja Tiina Saariston yhteistyönä kirjoittama kirja: You and Your TETRA Radio. Teos osoittautui pääpainoltaan käyttäjälähtöiseksi ja siten hieman vähemmän tekniseksi, mutta erinomaisesti TETRA:n käyttöä ja sen ominaisuuksia kuvaavaksi. Lisäksi ajankohtaista uutta näkemystä TETRA:n kehityksestä, mahdollisuuksista ja käytöstä Suomessa täydensi Markku Rantaman kirjoittama ja Pelastusopiston tänä vuonna julkaisema tutkimus: Pelastustoimen langattoman tiedonsiirron tarpeet ja toteutusmahdollisuudet tulevaisuudessa.

GSM- ja UMTS-kirjallisuutena, osin TETRA-teknikkaa täydentävänä sekä radio- ja matkapuhelinjärjestelmien riskien kartoittamisen apuna käytettiin pääasiassa Jyrki Penttisen kirjoittamia kahta kirjaa, jotka kuuluvat samaan kirjasarjaan, eli Tietoliikenne – Perusverkot ja GSM sekä Tietoliikenne – 3G ja erityisverkot. Molemmat soveltuvat selkeän ulkoasun ja jäsentelyn ansiosta hyödynnettäväksi opinnäytetyöhön. Lisäksi on käytetty Jochen Schillerin alun perin kirjoittamaa ja Erkki Hurun suomeksi kääntämää teosta Mobiilitietoliikenne, joka on sisällöltään hieman kahta ensiksi mainittua teknisempi. Täydentävää ja uudempaa tietoa saatiin myös useammasta verkkolähteestä.

Radio- ja matkapuhelinverkkojen yleisistä riskeistä ei löytynyt suoraan aihetta käsittelevää kirjallisuutta, joten riskit koottiin GSM- ja UMTS–kirjallisuudesta sekä monista sähköisistä lähteistä ja uutisista. Erityisesti sähköisistä uutisartikkeleista sai tiedoksi paljon todellisia riskejä langattoman matkaviestinnän arkikäytöstä. Kirjallisuudesta puolestaan löytyi enemmän tietoa teknisistä riskeistä. Kokonaisuutena riskien laaja-alainen kokoaminen oli työläs prosessi, mutta tarpeellinen työn tavoitteita ajatellen.

Tutkimustyössä käytetyt teoriat perustuvat myös luotettuun lähdemateriaaliin. Yleisen tutkimusmenetelmien teorian laadulliselle tutkimukselle tarjosi Martti Grönforsin aiheesta vuonna 1982 kirjoittaman teoksen uusintapainoksen sähköinen versio. Uusintapainoksen esipuheessa hän toteaa teoksensa sisällön olevan edelleen ajankohtaista ja toimivan korkeakouluopiskelijoiden tietolähteenä laadullisen tutkimuksen ymmärtämisessä ja

hyödyntämisessä. Tässä opinnäytetyössä käytettyjen tutkimusmenetelmien pääasiallisena lähdemateriaalina toimivat hänen ajatuksensa kvalitatiivisen tutkimuksen läpiviennistä.

Grounded Theory –tutkimusmenetelmän lähteinä käytettiin pääasiallisesti Anita Saaranen-Kauppisen ja Anna Puusniekan laatimia artikkeleita, jotka ovat Tampereen yliopiston yhteiskuntatieteellisen tietoarkiston verkkosivuilla. Lisäksi pienemmässä määrin käytettiin Helsingin yliopiston verkkosivuilla olevan Ritva Koskennurmi-Sivosen laatimaa Grounded Theory –tietoartikkelia sekä kahta amerikkalaista julkaisua. Lähteitä yhdistämällä saatiin kokonaiskäsitys siitä, millainen tutkimusmenetelmä Grounded Theory on ja kuinka sitä opinnäytetyön riskianalyysissa käytetään ja hyödynnetään.

Vaikka aiemmat tutkimustulokset ja niiden sovellukset muodostavat yhdessä käytettyjen tietolähteiden välityksellä tässä opinnäytetyössä esitetyn teoriatiedon ja siten myös radio- ja matkapuhelintekniikoiden vertailun rungon, riskianalyysin läpivieminen ja tutkimustulosten johtaminen on toteutettava erilaisia toimintatapoja noudattaen. Olennainen osa tutkimustyössä lähdeteosten ja -dokumentaatioiden sisältämän tiedon hyödyntämisen lisäksi on toiminta aihealueen mahdollisten käyttäjä-, kehittäjä- ja ylläpitäjätahojen kanssa. Radioverkkotekniikan tapauksessa tämä tarkoittaa kyseisen tekniikan parissa työskentelevien tahojen toimintatapojen ja tietämyksen keräämistä, hyödyntämistä ja eteenpäin viemistä. Teoreettisen tiedon lisäksi on tärkeää saada käytännöllistä tietoa tukemaan hahmottuvia tutkimustuloksia.

Käyttäjien kokemusten keräämiseen havaittiin tutkimusta suunniteltaessa olevan kaksi hyödyllistä toimintatapaa: henkilöhaastattelut ja kyselylomakkeiden käyttö. Lisätietojen keräämiseksi käyttäjälähtöisestä näkökulmasta tämän opinnäytetyön toteuttamisen aikana harkittiin TETRA-päätelaitteita käyttävän tahon edustajien haastattelua. Henkilöhaastatteluista kuitenkin luovuttiin runsaan tiedonsaannin todennäköisen vaikeuden vuoksi. Suomessa TETRA on pääasiallisesti viranomaistahojen käytössä, joten realistiset haastattelumahdollisuudet tutkimukselle arvioitiin kaiken kaikkiaan rajoitteellisiksi, sillä mahdolliset salassapitosopimukset suurella todennäköisyydellä rajoittavat tiedonsaantia ammattihenkilöiltä riskitekijöihin ja turvallisuusasioihin liittyen sekä näiden tietojen käyttöä opinnäytetyön yhteydessä.

Toinen havaittu menetelmä oli kyselylomakkeiden käyttö, johon tosin tämän opinnäytetyön näkökulmasta vaikuttivat samat ongelmatekijät kuin haastatteluiden järjestämisessäkin. Kyselylomakkeita voidaan käsitellä digitaalisesti ja lähettää sähköpostilla, joten niiden käyttö on huomattavasti tehokkaampaa kuin henkilökohtaiset käyttäjien tapaamiset ja paperiset lomakkeet. Tietoturvan näkökulmasta kohdistuu sähköiseen dataan kuitenkin enemmän uhkatekijöitä kuin haastattelutilanteissa käsiteltyyn suulliseen tietoon. Avoimen sähköpostin

käyttöä lomakkeiden yhteydessä olisi tarvittaessa vältetty tietoturvallisuuden säilyvyyden vuoksi, sillä kaikki TETRA:n käyttöön liittyvä tieto ei ehkä ole tarkoitettu julkiseksi ja saattaisi mahdollisesti kaapatuksi tullessaan aiheuttaa vahinkoa.

Alun perin tämän opinnäytetyön pääasialliseksi menetelmäksi kerätä käyttäjälähtöisiä tietoja suunniteltiinkin juuri kyselylomakkeiden käyttöä, joilla olisi voitu kerätä kohdeorganisaatiosta riskianalyysia varten määrällisen tutkimuksen mahdollistava aineisto. Tätä lähestymistapaa kuitenkin jouduttiin työn edetessä supistamaan jatkuvasti, jolloin lähestymistapa tutkimukselle muuttui lähtökohtaisesti laadulliseksi.

Tämän opinnäytetyön toteutuksen aikana päädyttiin lopulta toteuttamaan vain yksi sähköpostikysely TETRA–tekniikkaan enemmän perehtyneen henkilöstön ilmeisen vähäisen määrän vuoksi. Kyselyn kohdeorganisaatioksi saatiin Helsingin ja Uudenmaan Sairaanhoitopiiri (HUS), jonka TETRA-asiantuntija valmiuspäällikkö Pekka Koskinen täytti riskianalyysia varten laaditun lomakkeen. Lomakkeen ohessa toimitettiin sen täyttöä ja sisältöä tarkentava selvennysosa.

Lisäksi varteenotettavana tutkimusvaihtoehtona olisi ollut TETRA–päätelaitteiden tai –verkon omatoiminen testaaminen, joka olisi tehokas ja varma tapa saada luotettavaa ensikäden tietoa tekniikan toimivuudesta. Mikäli käytettävissä olisi TETRA–päätelaite sekä jonkin muun verkkotekniikan päätelaite (esim. tavallinen GSM-matkapuhelin) olisi radio- ja matkapuhelintekniikoiden vertailu voitu toteuttaa käytännössä ennalta päätettyjen ja suunniteltujen simuloitujen käyttötapausten avulla. Käyttötapauksista kerättäisiin tilastoitu aineisto, jonka analyysi antaisi keskenään verrattavia tuloksia kunkin tekniikan toiminnasta ja mahdollisesti esiintyvistä riskitekijöistä.

Tätä opinnäytetyötä toteutettaessa kuvatunlainen testausmenetelmä jäi kuitenkin vain ajatuksen asteelle ja vertailun toteutus jäi niin ikään vain teoriatietoon pohjautuvaksi. TETRA-päätelaitteita ei monien riskitekijöiden sanelemista syistä luovuteta muiden kuin ammattihenkilöiden käyttöön. Tästä syystä testauksen mahdollisuudesta luovuttiin jo alkuunsa, mutta se on kuitenkin oleellinen ja huomionarvoinen menetelmä muiden tutkimuksien laadintaan alan ammattilaisten toimesta tulevaisuudessa.

3 TETRA

Tämä osio sisältää kuvauksen TETRA–tekniikasta ja sen ominaisuuksista. TETRA–standardin esittely antaa kuvan siitä, mikä TETRA oikeastaan on, miksi se on kehitetty ja mihin tarkoituksiin sitä käytetään. Standardin esittelyä seuraa TETRA-tekniikan sisältämien ominaisuuksien selvitykset osa-alueittain jaettuna: ensiksi käsitellään puhelutekniikkaa ja

puhelunmuodostamistapoja, sitten tekstimuotoista viestintää, tiedonsiirtomenetelmiä ja siihen liittyviä tekniikoita, Direct Mode Operation (DMO) –teknologiaa sekä lopuksi perehdytään turvallisuuskysymyksiin ja tekniikan mahdollistamiin ratkaisuihin. Viimeisenä esitetään kaksi yleisluontoista esimerkkikäyttötapausta TETRA–verkon ja –päätelaitteiden hyödyntämisestä arkitehtävissä.

3.1 Standardin esittely

TETRA (Terrestrial Trunked Radio) on digitaalinen puheen ja datan siirtoon sekä salaukseen käytetty tietoliikennejärjestelmä. Vastaavanlaisia järjestelmiä on maailmalla käytössä useita ja yleisemmin voidaankin puhua matkapuhelinjärjestelmien standardeista. TETRA on Eurooppalainen standardi, jonka kehittäjätaho on ETSI (European Telecommunications Standards Institute). TETRA on myös avoin standardi, joka mahdollistaa eri tuottajatahojen kehittää päätelaitteitaan ja ohjelmistojaan yhteensopiviksi TETRA–tekniikan kanssa. TETRA–standardi on kokoelma pienempiä tietoliikenteen tiettyihin osa-alueisiin kehitettyjä standardeja ja teknologioita. (TETRA Memorandum of Understanding 2011.)

TETRA on kuitenkin erityisesti suunniteltu suojatun tiedonvälityksen tarpeisiin ja siksi sen käyttö onkin pääasiassa suuntautunut valtiollisille viranomaistahoille, joista erityisesti julkisille pelastuspalveluille. TETRA:n käyttö ei kuitenkaan ole rajattu vain viranomaisille, sillä se on myös kasvavassa määrin mm. kuljetusalojen käytössä. (TETRA Industry Group 2011.) Vaikka valtaosa TETRA:n käyttäjätahoista onkin Euroopassa, TETRA–standardin käyttö on leviämässä osiin Aasiaa, Lähi-itää ja Etelä-Amerikkaa. Matkapuhelinjärjestelmän standardina TETRA on teknologialtaan alati kehittyvä ja se on saanut osakseen kasvavat markkinat sekä ohjelmistokehittäjien tuen. TETRA–standardin käyttö tulee siis todennäköisesi yleistymään tulevaisuudessa. (TETRA Memorandum of Understanding 2011.)

TETRA–standardia käytetään maailmalla julkisen turvallisuuden, kuljetusalan, kunnallistekniikan, valtion, asevoimien, lentoliikenteen sekä kaupan ja tekniikan alojen radioliikenteen toimintatarpeisiin. Suurimmat käyttäjätahot ovat julkisen turvallisuuden alaisuuteen kuuluvia organisaatioita. Ensimmäinen TETRA–verkko otettiin käyttöön vuonna 1997 ja uusien verkkojen määrä on kasvava. (TETRA Memorandum of Understanding 2011.) TETRA:n tarkoituksena on ollut ja on maailmalla paikoin edelleenkin vanhempien analogisten radiojärjestelmien korvaaminen tarjoamalla niiden tilalle uusi turvallisempi ja tehokkaampi ratkaisu kaikille käyttäjätahoille.

Suomessa viranomaisten käyttämää TETRA-verkkoa kutsutaan nimellä VIRVE, joka tarkoittaa viranomaisradioverkkoa. VIRVE-verkon rakentaminen aloitettiin vuonna 1998 ja työ saatiin päätökseen vuonna 2002. Liittymien laskuttaminen alkoi vuonna 2004, jolloin VIRVE:n käytön

voidaan sanoa todella alkaneen. VIRVE:n suurimmat käyttäjätahot ovat pelastustoimi, poliisi, puolustusvoimat, rajavartiolaitos sekä sosiaali- ja terveystoimi. (Rantama 2011.)

Yleisesti esimerkiksi pelastustoimi, joka on TETRA:n suurin käyttäjäryhmä Suomessa, perustaa toimintansa nopealle ja luotettavalle kommunikaatiolle. Tapaturmatilanteessa tilanteeseen osallisten henkilöiden, sivustakatsojien ja pelastustyöntekijöiden itsensäkin turvallisuus riippuu paljolti paikalla olevan henkilökunnan ja toimintaa ohjaavan komentokeskuksen välisen viestinnän tehokkuudesta. Käskyjen ja tilanneraporttien on kuljettava esteettä ja välittömästi tilanteen eri toimijoiden välillä.

Tapaturman laajuudesta riippuen julkiset viestintäverkot (esim. tavanomainen matkapuhelinverkko) voivat olla osin tai kokonaan poissa käytöstä tai pahoin ruuhkautuneet, jolloin ne ovat välittömään viestintään kelpaamattomia. Siksi viranomaistahojen tehtävät vaativat toimiakseen esteettä erillisen paikallisista tekijöistä mahdollisimman riippumattoman kommunikaatioväylänsä. Viestinnän suhteen nykyaikainen toiminta on täysin riippuvainen käytettävissä olevasta teknologiasta ja sen päätelaitteiden ominaisuuksista. Tähän on käytetty aiempina vuosikymmeninä lähinnä analogista radioverkkoa, jonka ominaisuudet ovat lopulta varsin rajalliset. TETRA–standardi kehitettiinkin korjaamaan puutteita ja korvaamaan aiemmat teknologiat. (Heikkonen ym. 2004, 2.)

TETRA mahdollistaa suojatun salatun viestinnän, joka estää tietoon oikeuttamatonta osapuolta salakuuntelemasta radioliikennettä. Tämä ominaisuus tekee TETRA:sta erittäin käyttökelpoisen sellaisille toimijoille, jotka käsittelevät arkaluontoisia ja mahdollisesti väärissä käsissä vaarallisia tietoja. Tällaisia tietoja voisivat olla esimerkiksi puheviestinnän osalta poliisipartioiden ja johdon välinen radioliikenne, ja dataliikenteen osalta vaikkapa ensihoidon operaatiossaan käsittelemät potilastiedot.

Viestinnän salauksen lisäksi TETRA on myös taloudellinen standardi. Esimerkiksi valtion ja sen alaisten tahojen kaikki radioliikenne voidaan hoitaa TETRA:lla, jolloin valtion ei tarvitse ylläpitää erillisiä perinteisiä analogisia radioverkkoja eri käyttötarkoituksia varten. Koska TETRA–verkon käyttäjät voidaan myös jakaa rajattuihin puheryhmiin, joita voidaan muokata tarvittaessa tilanteen mukaan, voivat esimerkiksi poliisi ja pelastuslaitos olla yhteydessä toisiinsa omien puheryhmiensä ulkopuolelle samoilla TETRA–päätelaitteilla kuin omassa puheryhmässään. TETRA–verkossa viestintä on myös välitöntä eli yhteyden muodostus päätelaitteiden välillä tapahtuu ilman odotusaikoja. Etenkin pelastustöissä välitön viestin välittyminen on ensisijaisen tärkeää. Julkiset matkapuhelinverkot, kuten GSM, tarvitsevat muutaman sekunnin aikaa yhteyden muodostamiseen, joka on jo tapaturmatilanteessa kohtuuttoman pitkä aika vain odottaa. Matkapuhelinverkot ovat myös usein ruuhkautuneita ja siksi toiminnaltaan hitaita. Ne tarvitsevat myös tukiasemia yhteyksien luomiseen, mutta

TETRA voi muodostaa yhteyden päätelaitteiden välille tarvittaessa ilman tukiverkkoa DMO (Direct Mode Operation) -tekniikalla. (Heikkonen ym. 2004, 9-10.)

Avoimena standardina TETRA:n päätelaitteiden tuotantoa ja kehittelyä ei ole rajattu vain yhdelle valmistajalle. TETRA:n käyttäjätahoilla onkin mahdollisuus valita monien eri valmistajien tuotteita, jotka ovat kuitenkin yhteensopivia keskenään, sillä ETSI ja TETRA MoU –yhdistys huolehtivat standardin määrittämisestä sopivuuden ylläpitämiseksi. Toisaalta avoin standardi johtaa myös siihen, että yhden valmistajan TETRA–päätelaitteissa saattaa olla toimintoja, joita toisen valmistajan laitteissa ei puolestaan ole. Ennalta määritettyjä ovat vain standardin käyttämät rajapinnat laitteiden ja verkkojen välillä. Avoimuus takaa TETRA–standardin teknologian vapaan kehityksen ja markkinoiden kasvun valmistajien välisen kilpailun johdosta. (Heikkonen ym. 2004, 10-11.)

TETRA:sta on olemassa kaksi julkaistua versiota: TETRA Release 1 ja 2. Ensimmäinen versio valmistui vuonna 1996 ja alkuperäistä järjestelmää täydennettiin uusilla standardeilla vuosien varrella. Toinen versio saatiin valmiiksi vuonna 2005 ja sen pääasiallinen tehtävä oli vastata ilmenneisiin uusiin käyttötarpeisiin sekä lisätä TETRA:n kilpailukykyä. TETRA Release 3 ei ole vielä kehitteillä, mutta ETSI:n sisällä TETRA:n tulevasta kehityssuunnasta on alettu käydä keskustelua. (Rantama 2011.)

3.2 Puhelutekniikka

TETRA–päätelaitteet voivat olla käsiradioita tai toimistoihin, ajoneuvoihin ja muihin kulkuneuvoihin asennettavia radiolaitteita. Päätelaitteiden ulkomuoto voi vaihdella eri valmistajien tuotteiden välillä, mutta tavallisesti ne muistuttavat nykypäivänä tavanomaisia matkapuhelimia. TETRA–puhelimet ovat käytännössä sekoitus perinteistä radiopuhelinta ja nykyaikaista matkapuhelinta. TETRA–puhelimella voi siksi puhua pitämällä sitä korvalla samoin kuin matkapuhelinta tai pitämällä laitetta suun edessä kuin radiopuhelinta.

TETRA:lla on paljon yhtäläisyyksiä GSM-järjestelmän kanssa. Molemmat järjestelmät käyttävät taajuuksien jakamiseen Time Division Multiple Access (TDMA) -tekniikkaa. TETRA:n käyttämät taajuudet on jaettu neljän aikavälin kehyksiin ja alin vaadittu taajuusjako on 25 kHz. Puheen koodauksen nopeus TETRA:ssa on 7,2 kb/s virheenkorjauksineen. (Penttinen 2006b, 41.) TETRA:n kehitykseen on käytetty elementtejä olemassa olleesta GSM-tekniikasta, johon on yhdistetty radiopuhelimien toimintaperiaatteita. TETRA-puhelimet ovat niin tekniikaltaan kuin tavallisesti ulkomuodoltaankin radio- ja matkapuhelinten yhdistelmiä. Kehitystyöstä johtuen TETRA on samankaltaisilta ominaisuuksiltaan kuitenkin toiminnaltaan GSM-järjestelmää huomattavasti tehokkaampi.

TETRA–puhelimella voi soittaa yksilöpuheluita päätelaitteesta toiseen aivan kuin matkapuhelimellakin. Tekniikka mahdollistaa myös puhelun TETRA–verkosta muihin matkapuhelinverkkoihin, mutta tällainen toiminnallisuus on yleensä rajoitettua. TETRA–puhelimella voi myös lähettää tekstiviestejä toisiin päätelaitteisiin. Joistakin päätelaitteista voi myös olla mahdollista lähettää tekstiviestejä GSM–verkkoon. Merkittävin ero TETRA–puhelimen ja tavallisen matkapuhelimen välillä on se, että TETRA–puhelimella voi myös tehdä ryhmäpuheluita samaan tapaan kuin radiopuhelimella. Ryhmäpuhelun vastaanottavat kaikki samaan puheryhmään liitetyt päätelaitteet. (Heikkonen ym. 2004, 14.)

Erillisten TETRA-verkkojen välillä voi olla myös määriteltynä yhteinen rajapinta. Tämä rajapinta eli Inter-System Interface (ISI) mahdollistaa toiseen verkkoon kuuluvan päätelaiteen vierailun (roaming) eri TETRA-verkon alueella. Vieraillessa käytettävissä voi olla vain osa kotiverkon palveluista. (Penttinen 2006b, 43.) Tällaisella toimintamahdollisuudella TETRA-verkkojen käytöstä voidaan tehdä hyvinkin kansainvälistä. Valtiollisten verkkojen välille voidaan halutessa luoda yhteinen rajapinta edistämään viranomaisten yhteistyötä.

Kuten perinteisissä radiopuhelimissakin, myös TETRA–puhelimissa on PTT (Push-to-talk) -painike. PTT–painike on yleensä radiopuhelimen kyljessä oleva painike, jota pohjaan painamalla päätelaite avaa puheyhteyden käytössä olevan radioverkon ylitse. Tällainen ryhmäpuhelu on yhdensuuntainen (half-duplex) eli vain PTT–painikkeen painaja voi tehdä puhelun kunnes tämä vapauttaa painikkeen. Järjestelmä sallii vain yhden päätelaitteen avaaman puheyhteyden kerrallaan, jolloin muut samaan puheryhmään kuuluvat päätelaitteet ainoastaan vastaanottavat puhelun. Tällainen vuorotteleva puhejärjestys on hyvin kontrolloitua ja soveltuu siksi mainiosti sellaisiin käyttöympäristöihin, joissa väärinkäsityksiin ei ole varaa ja tiedonkulun on oltava selkeää. TETRA mahdollistaa myös radioliikenteen järjestämisen ennalta määriteltyjen prioriteettien mukaan, jolloin esimerkiksi komento- tai hätäkeskuksen aloittamaa puhelua pidetään tärkeämpänä ja se muodostaa aina puheyhteyden muiden päätelaitteiden ylitse tavoittaen kaikki puheryhmän päätelaitteet välittömästi. (Heikkonen ym. 2004, 28-29.)

3.2.1 Yksilöpuhelut

TETRA–päätelaitteella tehtävät yksilöpuhelut (individual call) voidaan jakaa kolmeen lajiin: yksilöpuhelut TETRA–verkon sisällä, yksilöpuhelut TETRA–verkon ulkopuoliseen matkapuhelinverkkoon ja suorat puhelut PTT–painiketta käyttäen. TETRA–verkon sisäinen yksilöpuhelu on samankaltainen kuin tavanomainen puhelu lanka- tai matkapuhelimella. Jokaisella TETRA–päätelaitteella on oma tunnistenumeronsa, johon toisesta päätelaitteesta voi soittaa näppäilemällä vastaanottajan numeron ja painamalla puhelun yhdistävää näppäintä. Tällainen puhelu on TETRA:ssa mahdollista toteuttaa kahdensuuntaisena (full-

duplex) tai yhdensuuntaisena (half-duplex). Kahdensuuntaisessa puhelussa molemmat osapuolet voivat puhua samanaikaisesti, kun taas yhdensuuntaisessa puhelussa osapuolet puhuvat vuorotellen. (Heikkonen ym. 2004, 41.)

Puhelut TETRA–verkosta sen ulkopuolelle tapahtuvat samoin kuin verkon sisäisetkin puhelut. Soittaja näppäilee vastaanottajan puhelinnumeron ja painaa puhelun yhdistävää näppäintä. TETRA–verkosta on mahdollista soittaa julkisiin puhelimiin, matkapuhelinverkkoon tai yksityisiin puhelinvaihteisiin. TETRA–puhelin voi myös vastaanottaa puheluita ulkopuolisista verkoista, jos tätä ominaisuutta ei ole rajoitettu. (Heikkonen ym. 2004, 42.) Puheluiden tekeminen verkosta toiseen on tehty helpoksi ja tekniikaltaan käyttäjille huomaamattomaksi sen ollessa rajoittamatonta. Useimmiten kuitenkin eri verkkojen välisiä puheluita on rajoitettu TETRA:n käyttäjäorganisaation toimesta.

Suora puhelu (direct call) on nopea tapa välittää viesti päätelaitteelta toiselle. Suora puhelu aloitetaan näppäilemällä vastaanottajan tunnistenumero ja painamalla PTT–painike pohjaan. Tämä toiminto avaa välittömästi yhteyden vastaanottavaan päätelaiteeseen. Suora puhelu on aina yhdensuuntainen ja soveltuu pikaisten viestien ja ohjeiden välitykseen. (Heikkonen ym. 2004, 41-42.)

TETRA–verkko mahdollistaa puhelun soittamisen kolmella eri tavalla. Tavallisin on Individual TETRA Subscriber Identity (ITSI), joka tarkoittaa TETRA–päätelaitteisiin ohjelmoidun tunnistenumeron käyttöä. Toinen tapa on verkkoon määritettyjen lyhennettyjen numeroiden käyttö eli Fleet Specific Short Number (FSSN). FSSN–numeroa ei tarvitse ohjelmoida päätelaitteisiin, vaan se voi olla käyttäjäkohtainen. FSSN on erityisen käyttökelpoinen suoria puheluja tehtäessä. Kolmas tapa on käyttää Mobile Subscriber Integrated Services Digital Network (MS-ISDN) –numeroa, joka on päätelaitteesta riippumaton ja perustuu ITSI:n tunnistenumeroon. Tätä MS-ISDN–numeroa voidaan käyttää myös TETRA–verkon ulkopuolisten puheluiden vastaanottamiseen. Tämä sama toiminto voi olla TETRA:ssa käytössä myös nimellä Radio User Number (RUN). (Heikkonen ym. 2004, 43.)

3.2.2 Puheryhmät

Ryhmäpuhelu (group call) on radioverkon peruspuhelu, jolla tavoitetaan joukko kuulijoita. TETRA:ssa ryhmäpuhelun vastaanottaa päätelaitteeseen määritelty puheryhmä. Puheryhmä (talk group) tarkoittaa joukkoa TETRA–päätelaitteita, jotka ovat määritetty viestimään keskenään. Puheryhmät ovat yleensä määritelty tietyn organisaation, toimenkuvan, tai alueen mukaan. Esimerkiksi saman kaupungin, pelastus- ja poliisilaitoksilla voi kaikilla olla käytössään sama TETRA–verkko, jolloin verkko on todennäköisesti jaettu puheryhmiin näiden mukaan. Puheryhmät selkeyttävät kommunikaatiota kun esimerkiksi palolaitoksen viestintä ei

ole kuultavissa myös poliisin päätelaitteista. Puheryhmät voivat olla myös alueellisesti rajattuja esimerkiksi eteläiseen ja pohjoiseen poliisipiiriin. TETRA–tekniikka ei kuitenkaan rajoita puheryhmiä maantieteellisille alueille, vaan saman puheryhmän jäsenet voivat olla hyvinkin kaukana toisistaan kunhan vain verkon infrastruktuuri kattaa kyseisen alueen. TETRA–järjestelmä määrittää automaattisesti puheryhmän käyttämät tukiasemat ja taajuudet, jolloin päätelaitteen käyttäjän ei tarvitse itse vaihtaa taajuuksia tai huolehtia etäisyyksistä. (Heikkonen ym. 2004, 17.)

TETRA–päätelaite voi myös seurata useita puheryhmiä samanaikaisesti. Päätelaite näyttää listan mahdollisesti käytettävistä puheryhmistä. Puheryhmät voivat myös olla listattu kategorioittain esimerkiksi tietyn alueen mukaan. Kaikki TETRA–verkon sisältämät puheryhmät eivät välttämättä kuitenkaan ole valittavissa yksittäisestä päätelaitteesta, sillä verkon käyttöoikeuksia voidaan rajoittaa siten, että vain tietyt sallitut käyttäjät voivat seurata tiettyjä puheryhmiä. Uusia puheryhmiä voidaan myös joissakin laitemalleissa aktivoida päätelaiteeseen oikeilla koodiavaimilla, mikäli siihen sallittu käyttäjä näkee sen tarpeelliseksi. (Heikkonen ym. 2004, 11-12.)

Puheryhmät ovat yleensä määritelty päätelaitteisiin valmiiksi jo ennalta. Tavallisesti käyttäjät tarvitsevat vain omaa puheryhmäänsä, mutta voi ilmetä tilanteita, joissa viestiyhteys olisi tarpeen myös jonkin toisen puheryhmän kanssa. TETRA mahdollistaakin puheryhmien suunnittelun ja määrittämisen päätelaitteisiin siten, että käytettäviä puheryhmiä voidaan muuttaa tilanteen mukaan välittömästi. Katastrofitilanteessa voidaan esimerkiksi ottaa käyttöön valmis puheryhmä, jossa pelastus- ja poliisilaitoksen kenttähenkilöstö ovat kaikki mukana ja voivat kommunikoida keskenään. Huolellisen suunnittelun tärkeys korostuu kun puheryhmiä määritellään. Tilanteeseen nähden liian laaja puheryhmä saattaa haitata viestintää radioliikenteen yhdensuuntaisen luonteen vuoksi vain yhden käyttäjän voidessa puhua kerrallaan. Tärkeä viesti voi olla tarpeen saada välitettyä heti, mikä ei onnistu, jos puheyhteys on jo varattu. (Heikkonen ym. 2004, 12.)

Yksittäinen käyttäjä ei voi omalta päätelaitteeltaan luoda uusia puheryhmiä tai muokata jo olemassa olevia. Puheryhmiä voi hallinnoida vain verkon komentokeskus, joka pystyy luomaan ennalta laitteisiin määrittelemättömiä väliaikaisia puheryhmiä tilanteen vaatiessa ja välittämään ne viipymättä langattomasti verkon käyttäjille. (Heikkonen ym. 2004, 28.) Rajoittamalla yksittäisten päätelaitteiden kykyä vaikuttaa käytettyihin puheryhmiin, verkon turvallisuutta saadaan lisättyä ja salakuuntelun riskiä pienennettyä. HUS-organisaation valmiuspäällikön kautta tiedoksi kuitenkin tuli, että Suomessa tämä kyseinen väliaikaisten puheryhmien luominen on määritelty organisaatioiden vastuuhenkilöille eli pääkäyttäjille toimintaa ohjaavan komentokeskuksen sijaan.

Ominaisuus, joka mahdollistaa puheryhmien muokkaamisen on nimeltään Dynamic Group Number Assignment (DGNA). Komentokeskus voi lähettää väliaikaisen puheryhmämääritelmän käyttäjille yksitellen (Individually Addressed DGNA) tai ryhmälle käyttäjiä (Group Addressed DGNA). Kun puheryhmä lähetetään yksittäisille päätelaitteille, komentokeskus ja verkon arkkitehtuuri tietävät mitkä kaikki päätelaitteet ovat jo saaneet määrityksen, jolloin signaali jatkaa ainoastaan niille päätelaitteille, joilta se vielä puuttuu. Puheryhmämäärityksen lähettäminen ryhmälle päätelaitteita samalla kertaa on nopeaa, mutta päätelaitteet eivät vahvista saaneensa määrityksen. Yksittäinen lähettäminen on siis varmempaa ja säästää verkon resursseja. (Heikkonen ym. 2004, 31-32.)

TETRA-päätelaite voidaan asettaa etsimään sille sallittuja puheryhmiä kuuloalueelta (scanning), jolloin se valitsee ensimmäisen löytämänsä aktiivisen puheryhmän. Käyttäjä voi osallistua löytämänsä puheryhmän viestintään normaalisti PTT-painikkeella. Puheryhmien etsintä on hyödyllistä silloin kun samalle käyttäjäjoukolle on määritetty useita puheryhmiä. Esimerkiksi poliisilla voi olla samalla kaupunkialueella useita puheryhmiä henkilöstön toimenkuvan mukaan jaettuna. Puheryhmien etsinnän voi toteuttaa myös tärkeysmäärityksen mukaan (priority scanning). Käyttäjä voi itse määrittää päätelaitteensa löytämille puheryhmille tärkeysjärjestyksen ja seurata niiden viestintää kyseisessä järjestyksessä. Käyttäjä seuraa ja voi osallistua aina tärkeysjärjestyksessä korkeimmalla olevaan puheryhmää. Kun viestintä seuratussa puheryhmässä lakkaa, vaihtuu se automaattisesti seuraavaksi tärkeimmäksi aktiiviseksi puheryhmäksi, jonka päätelaite löytää. Näin käyttäjä pysyy aina ajan tasalla tärkeimmistä tiedoista. (Heikkonen ym. 2004, 34-35.)

Vaikka tekniikka tekeekin käyttäjille mahdolliseksi puheryhmien tärkeysjärjestyksen asettamisen itse, on se kuitenkin usein ohjelmoitu päätelaitteisiin jo valmiiksi. Tärkeysjärjestyksen mukaisen puheryhmien seurannan voi myös kytkeä pois päältä kokonaan. Tärkeysmääritelmät ovat yleensä asteikolla: pieni, keskisuuri, suuri. (Heikkonen ym. 2004, 37.) Tärkeysjärjestysten ja puheryhmien jäsenten suunnittelun huolellisuus korostuu organisaatioissa, sillä liian suuri määrä puheryhmiä ja väärät määritykset niiden tärkeydelle voivat johtaa monenlaisiin ongelmiin. Esimerkiksi oleellisia tietoja voi jäädä kuulematta, jos tärkeysjärjestys on määritetty heikosti ja tärkeimpiä tietoja ei siten kyetä välittämään niitä tarvitseville. Turhan monijäseniset puheryhmät voivat myös aiheuttaa sekaannusta, kun seuratun viestinnän määrä on liian suuri.

TETRA:ssa voi luoda myös taustaryhmän (background group), joka on tavanomaisesta poikkeava puheryhmä. Taustaryhmään ei varsinaisesti kuulu jäseniä vaan kaikki päätelaitteiden käyttäjät voidaan asettaa seuraamaan tätä puheryhmää muun viestinnän taustalla. Taustaryhmän puhelut korvaavat muun viestiliikenteen ja siihen viestittää yleensä vain komentokeskus, jolloin kaikki saavat tietoonsa tärkeimmät koko toimintaa koskevat

tiedotukset ja varoitukset. Taustaryhmiä voi olla useita ja ne voivat olla rajoitettuja alueellisesti tai vain tiettyjen puheryhmien jäsenille. (Heikkonen ym. 2004, 39-40.)

3.2.3 Ryhmäpuhelut

TETRA–verkon toimintaidea on sama kuin perinteisessä analogisessa radioverkossakin. Radiopuhelimella yksittäinen käyttäjä voi tavoittaa nopeasti yhden napin painalluksella suuren joukon muita käyttäjiä. TETRA:ssa tällaisen puhelun vastaanottaa päätelaitteeseen ohjelmoidun puheryhmän mukainen joukko muita päätelaitteita. Ryhmäpuhelu aloitetaan painamalla TETRA–puhelimen sivulla olevaa PTT (Push-to-talk) -painiketta. Tämä avaa välittömästi puheyhteyden muihin saman puheryhmän päätelaitteisiin. Ryhmäpuhelu on yhdensuuntainen (half-duplex) eli vain yksi käyttäjä voi puhua kerrallaan. Puhelinjan ollessa jo käytössä voi seuraava puhuja painaa jo valmiiksi päätelaitteensa PTT–painikkeen pohjaan, jolloin linjan vapautuessa järjestelmä antaa puhevuoron seuraavalle jonossa olevalle. Jonotuskäytäntö voi perustua PTT-painikkeen painamisjärjestykseen tai yksittäisille käyttäjille määritettyyn tärkeysjärjestykseen. (Heikkonen ym. 2004, 27-29.)

Kuten analoginen radioverkkokin, myös TETRA mahdollistaa liittymisen ryhmäpuheluun ja puheryhmään kesken käyttäjien välisen kommunikaation. Analogisessa radioverkossa radiopuhelimen kanava vaihdettiin samaksi kuin muillakin osallistujilla, mutta TETRA:ssa kanavien vaihto tapahtuu automaattisesti. Puheryhmään liittyvä vain valitsee kyseisen ryhmän päätelaitteestaan. TETRA:ssa tällainen puheryhmään liittyminen voidaan myös tarvittaessa estää. (Heikkonen ym. 2004, 29.)

TETRA–verkon toiminta on suunniteltu siten, että käyttäjien ei tarvitse huolehtia verkon infrastruktuurista. Käyttäjät voivat siirtyä tukiaseman vaikutuspiiristä toiselle huomaamattaan ja ilman taukoja viestinnässä. TETRA–tekniikka mahdollistaa siirtymisen myös TETRA–verkosta toiseen. Tämä on kuitenkin mahdollista vain jos päätelaitteelle on annettu toimintaoikeudet molemmissa verkoissa niiden ylläpitäjien tahoilta. Kaikki mahdolliset palvelut ja ominaisuudet eivät välttämättä kuitenkaan ole käytössä kaikissa TETRA-verkoissa. Jos alueella olevat TETRA–verkot ovat suunniteltu niiden käyttäjätahojen välistä yhteistyötä tukeviksi ja päätelaitteille on annettu toimintaoikeudet niihin, voi käyttäjä siirtyä verkosta toiseen valitsemalla päätelaitteestaan verkon, johon haluaa siirtyä. (Heikkonen ym. 2004, 29-30.)

Ryhmäpuhelun toimintaetäisyys riippuu käytetyn verkon laajuudesta. TETRA–verkon koolle ei ole rajoitetta ja yksi verkko voi kattaa vaikka kokonaisen valtion alueen. Saman puheryhmän jäsenet voivat olla satojen kilometrien etäisyydellä toisistaan ja osallistua silti samaan reaaliaikaiseen keskusteluun. Vaikka itse tekniikka ei rajoitakaan puheluiden etäisyyksiä,

voivat määritellyt käyttöoikeudet ja mahdolliset muut TETRA–verkot rajata viestintäetäisyyksiä. Usein puheryhmän käyttämät puhe-etäisyydet ovat rajattu tietylle alueelle, jolla puheryhmän jäsenet työskentelevät. Tämä alue voidaan määrittää joko mahdollistamalla ensin niin suuri puhealue kuin mahdollista ja rajoittamalla sitä käytön perusteella sille alueelle, jolta puheluja tehdään, tai sitten puhealue voidaan määrittää ennalta käyttämään vain tiettyjä verkon tukiasemia. Puhealueen huolellisella määrittelyllä voidaan säästää verkon resursseja. (Heikkonen ym. 2004, 30-31.)

Ryhmäpuheluissa puheoikeus on tavallisesti PTT–painikkeen painamisjärjestyksen mukainen. Tärkeällä käyttäjällä voi kuitenkin olla käytössään Voice Override –toiminto, jota käyttämällä tämä saa aina keskeytettyä puheryhmän muun viestinnän ja välitettyä oman viestinsä. Tämä on erityisen hyödyllistä silloin kun tilanteeseen nähden tärkeä viesti on välittömästi saatava välitettyä kaikille puheryhmän jäsenille. Verkon käyttäjien tekemille puheluille on myös voitu määritellä tärkeysjärjestys (call priority), jolloin tarpeeksi korkean tärkeyden tason omaavan käyttäjän tekemä puhelu voi verkon kapasiteetin ollessa täynnä korvata vähemmän tärkeän puhelun kokonaan (pre-emptive call rights). Tämä vaikuttaa myös TETRA-verkossa tehtyihin yksilöpuheluihin. Tällainen puhelu ei kuitenkaan korvaa muita, jos verkon kapasiteettia on vapaana. (Heikkonen ym. 2004, 33-34.)

Päätelaitteille määriteltäviä puheoikeuksia on TETRA:ssa kaiken kaikkiaan 15 tasoa. Ensimmäiset 11 tasoa vaikuttavat vain puheluiden jonotusjärjestykseen verkossa. Tasot 12, 13 ja 14 myös korvaavat alemman tärkeyden puheluja verkon ollessa tukkeutunut. Taso 15 on varattu ainoastaan hätäpuheluille, jotka ylittävät tärkeydessään kaiken muun viestinnän. TETRA:ssa jokaiselle päätelaitteen käyttäjälle on määritetty jokin puheoikeuden taso, jolla ryhmäpuheluiden jonotusjärjestystä ylläpidetään. (Heikkonen ym. 2004, 38.)

TETRA-päätelaitteella voi myös tehdä ryhmäpuhelun, johon muut puheryhmän jäsenet eivät voi vastata (Supplementary Service Broadcast Call). Tällainen puhelu on yleensä rajoitettu vain johtohenkilöille tai komentokeskukselle, ja puhelu tehdään ennalta määriteltyyn taustaryhmään. (Heikkonen ym. 2004, 39.)

3.2.4 Hätäpuhelu

Hätäpuhelu (emergency call) on TETRA:ssa automaattisesti yhdellä painikkeella tehtävä käyttäjän henkilökohtaisen turvallisuuden takaava ominaisuus. TETRA–puhelimessa on yleensä erillinen helposti havaittava punasävyinen painike, jolla hätäpuhelu aloitetaan. Hätäpuhelun vastaanottaa jokin ennalta määritetty taho, joka voi olla esimerkiksi organisaation komentokeskus, tietty puheryhmä tai yleinen hätäkeskus. Jos hätäpuhelu ei tavoita sille määritettyä vastaanottajaa, on se voitu määritellä jatkamaan yhteydenottoa johonkin toiseen

tahoon. Joissakin tapauksissa hätäpuhelun aloittamiseen on voitu liittää automaattisen tilaviestin lähettäminen komentokeskukselle. Hätäpuhelun vastaanottoa varten on myös voitu perustaa aivan oma puheryhmänsä, johon kuuluu esimerkiksi lääkäri. Hätäpuheluilla on korkein mahdollinen tärkeys kaikista TETRA–verkon puheluista, joten niille on aina taattu yhteys ylitse muun verkkoliikenteen. Hätäpuhelun vastaanottavat päätelaitteet myös ilmoittavat saapuvasta hätäpuhelusta huomiota herättävästi näytöllään sekä hälytysäänellä. (Heikkonen ym. 2004, 77-78.)

Päätelaitteiden ollessa TETRA–verkon ulkopuolella ja niiden siten käyttäessä kommunikaatioon DMO (Direct Mode Operation) –toimintatilaa, hätäpuhelu voi yrittää saada yhteyden verkkoon ja toimittaa sen määritellylle vastaanottajalle samoin kuin tavallisesti verkon alueellakin. Toinen menettelytapa on se, että päätelaite tekee hätäpuhelun vain DMO:n käyttämässä puheryhmässä, jolloin se toimii samalla tavalla kuin tavallinenkin ryhmäpuhelu, paitsi suurimmalla tärkeystasolla. Tällaisessa hätäpuhelussa sen tekijä ei kuitenkaan voi tietää saavuttiko puhelu kuulijoita, sillä DMO:ssa ainoa tapa saada vahvistus puhelun vastaanottamisesta on vastapuhelu. (Heikkonen ym. 2004, 78.)

Hätäpuhelun katkaiseminen tapahtuu yleensä vain erityismenettelyillä, jotta yhteys avuntarvitsijaan ei keskeydy. Hätäpuhelun katkaisee yleensä komentokeskus, mutta jos se on nähty tarpeelliseksi, myös käyttäjälle itselleen on voitu antaa oikeudet katkaista hätäpuhelunsa. Hätäpuheluihin on myös voitu asettaa ajastus, jotta mahdollinen vahingossa tehty hätäpuhelu ei estä muuta verkkoliikennettä loputtomiin. (Heikkonen ym. 2004, 79.)

3.2.5 Komentokeskuksen erillispalvelut

Osa TETRA–verkon mahdollistamista puhelutekniikkaan liittyvistä palveluista on rajoitettu verkon käyttäjätahon komentokeskukselle (dispatcher) tai johdolle. Esimerkiksi pelastustoimessa toimintaa ohjaava komentokeskus kontrolloi muiden päätelaitteiden käyttöä ja voi siten käyttää näitä rajattuja palveluja. Tällainen toiminnallisuuden rajoittaminen lisää TETRA–verkon turvallisuutta estämällä yksittäisten päätelaitteiden mahdollisuutta haitata verkon toimintaa. (Heikkonen ym. 2004, 43-44.)

Puhelun aloittavan TETRA–päätelaitteen tunnistenumero näkyy puhelun vastaanottajalle. Tämä tunniste eli Calling Line Identification (CLI) voidaan myös kytkeä pois päältä komentokeskuksen taholta, jotta soittajan identiteetti pysyy piilotettuna. Yksittäinen käyttäjä ei voi itse aktivoida tätä Calling Line Identification Restriction (CLIR) –toimintoa päätelaitteeltaan käsin. Tärkeimmillä toimijoilla, kuten esimerkiksi hätäkeskuksella, voi olla käytössään CLIR Override, jolla soittajan identiteetti on aina nähtävissä siitä huolimatta, että puhelun tekijän verkossa CLIR on toiminnassa. (Heikkonen ym. 2004, 43-44.)

Saapuvia puheluita voidaan TETRA:ssa siirtää ennalta määritettyyn numeroon samoin kuin esimerkiksi GSM–verkossa, jos puhelun vastaanottaja ei ole tavoitettavissa. Erona GSM:n toimintaan TETRA:ssa puhelun siirron määrittelee verkon komentokeskus, jolloin puhelun vastaanottajan voidaan varmistaa olevan oikeutettu käyttäjä. Lisäksi Komentokeskus voi estää puheluja ja hallita käyttöoikeuksia. Komentokeskus voi myös sallia tai olla sallimatta puheluja TETRA–verkon ja julkisten verkkojen välillä. Joissakin tapauksissa TETRA–verkkoa ylläpitävä taho on kuitenkin voinut rajoittaa tai estää tällaisen toiminnallisuuden. (Heikkonen ym. 2004, 44-45.)

3.3 Teksti- ja statusviestit

Vaikka ääni onkin pääasiallinen viestintäkeino radioverkoissa, voidaan tekstimuotoisilla viesteillä tukea kommunikaatiota. Puhelut eivät tavallisesti tallennu laitteiden muistiin myöhempää tarkastelua varten ja ihmiset voivat helposti myös kuulla annetun viestin väärin etenkin hektisissä tilanteissa. Tekstimuotoinen viesti tallentuu päätelaitteen muistiin ja siten viestin voi tarvittaessa lukea uudelleen. Tekstiviesti (text message) soveltuu erityisen hyvin esimerkiksi nimien ja osoitetietojen välittämiseen. Tekstiviestitys myös kuluttaa vähemmän verkon kapasiteettia kuin puheen välittäminen. Tekstiviestin voi lähettää TETRA:ssa joko yksittäiselle päätelaitteelle tai valitun puheryhmän kaikkiin laitteisiin. (Heikkonen ym. 2004, 47.)

TETRA:ssa on käytettävissä kahdenlaisia tekstimuotoisia viestejä: teksti- ja statusviestejä (status message). Tekstiviestillä välitetään vapaamuotoinen viesti päätelaitteelta toiselle samoin kuin matkapuhelinjärjestelmissäkin. TETRA–puhelimen muisti täyttyy tallennetuista tekstiviesteistä ja vanhimpia viestejä täytyy poistaa ajoittain muistin vapauttamiseksi. Statusviesti puolestaan on ennalta laadittu yksinkertainen ilmoitus, jonka kirjoittamiseen käyttäjän ei tarvitse kuluttaa aikaa. Statusviesteillä voidaan ilmoittaa esimerkiksi sijainnin muutoksesta, työvuoron alkamisesta, tehtävän suorittamisesta tai hätätapauksesta. TETRA–verkko voi sisältää valmiita statusviestejä jopa tuhansia kappaleita kaikenlaisiin ennakkotilanteisiin sopien. (Heikkonen ym. 2004, 47-48.)

Tekstiviestipalvelua kutsutaan TETRA:ssa myös nimellä Short Data Service (SDS), joka vastaa GSM:n käyttämää Short Message Service (SMS) -palvelua. TETRA–tekniikka mahdollistaa tekstiviestin lähettämisen GSM–verkkoon, jos käytetyt päätelaitteet tukevat tätä toimintoa. (Heikkonen ym. 2004, 50.) TETRA:ssa tekstiviestien pituus tosin ei määrity merkkimäärän perusteella, vaan viestin kokoluokan mukaan. Luokkia on 1-4 ja niiden maksimaaliset datamäärät ovat 16, 32, 64 ja 2047 bittiä. (Penttinen 2006b, 47.)

TETRA–päätelaite voi toimia myös hakulaitteen tavoin. TETRA–verkot ja päätelaitteet voivat vaihdella hakulaitetoimintojen suhteen ylläpitäjän tai valmistajan mukaan, mutta nämä ovat kuitenkin yleensä yhteensopivia keskenään. Komentokeskus saa aina ilmoituksen lähetetystä hakuviestistä, sen vastaanottavista käyttäjistä sekä vahvistuksen niistä käyttäjistä, jotka vastaamalla viestiin varmistavat vastaanottaneensa sen. Hakuviesti voidaan lähettää myös tarvittaessa vain tietyllä alueella oleville käyttäjille. Hyödyllinen käyttötapa tällaiselle hakulaitetoiminnolle on yksikköhälytyksen (unit alert) lähettäminen. Yksikköhälytys sisältää statusviestin hälytettävästä asiasta, jonka käyttäjätaho voi laatia itse. Yksikköhälytys myös laukaisee päätelaitteessa hälytystoiminnon, jolloin laite välkyttää valojaan ja toistaa hälytysääntä. Hälytysääni kuuluu laitteesta siitä huolimatta onko käyttäjällä puheryhmiä valittuna, puhuuko tämä puhelua, tai onko päätelaite kytketty äänettömään toimintatilaan. Erilliseen hakulaitteeseen verrattuna TETRA:ssa etuna on, että käyttäjä voi heti hälytyksen saatuaan aloittaa puhelun ja osallistua viestintään samalla laiteella. (Heikkonen ym. 2004, 51-52.)

3.4 Tiedonsiirto

TETRA mahdollistaa käyttäjien pääsyn käsiksi tietokantojen sisältämiin tietoihin myös heidän ollessaan liikkeellä kenttätehtävissä. Tietokantojen käsittely tarvitsee tehtävään sopivan laitteen kuten kannettavan tietokoneen, kämmentietokoneen, tai siihen soveltuvan TETRA-puhelimen. TETRA–puhelimissa mallista riippuen voi olla mahdollisuus käyttää sisäänrakennettua WAP (Wireless Application Protocol) –selainta tietojen käsittelemiseen, jolloin erillislaitteita ei tarvita. (Heikkonen ym. 2004, 55.)

TETRA on suunniteltu suojatun tietoliikenteen tarpeisiin kaikissa olosuhteissa. Kriisitilanteissa, joissa TETRA–verkon toiminta on vilkasta tai kapasiteettia on rajallisesti, voidaan vähemmän kriittisiä sovelluksia käyttää myös vaihtoehtoisesti muiden verkkotekniikoiden kautta. Korvaaviksi tiedonsiirtotekniikoiksi soveltuvat myös GSM tai UMTS. (Heikkonen ym. 2004, 55.) Turvallisuuden osalta GSM ei sovellu nykyisellään enää kovinkaan hyvin minkäänlaiseen salattavaan tietoliikenteeseen. Uudempi UMTS on huomattavasti vahvempi salausmenetelmiltään.

TETRA:n yhteydessä käytetyt sovellukset on usein räätälöity käyttäjätahon tarpeisiin sopiviksi. Sovellukset ovat voitu kehitellä käyttämään aina tilanteessa sopivinta tiedonsiirtotekniikkaa, jolloin käyttäjän itsensä ei välttämättä tarvitse tietää sovelluksen ja käytetyn verkon tekniikasta paljoakaan toimiakseen tehokkaasti työtehtävissään. Usein tietyt sovellukset kuitenkin vaativat toimiakseen juuri tietyn verkkotekniikan, joka rajoittaa niiden käyttöä. (Heikkonen ym. 2004, 55.)

Data kulkee TETRA–verkossa pakettimuotoisena. Tähän käytetty toimintaprotokolla on tietotekniikassa yleisesti käytetty Internet Protocol (IP). TETRA tukee sekä edelleen vallitsevaa IPv4- että käyttöön hiljalleen ilmaantuvaa IPv6-protokollaa. Pakettimuotoisen datan vahvuus on se, että sitä tukevat verkot näkyvät ulkopuolisille verkoille samoin kuin mitkä tahansa muutkin pakettikytkentäiset verkkoratkaisut. (Penttinen 2006b, 47.) IP-osoitteiden perusteella toimiva datan välitys tekee laitteiden keskinäisestä paketinvaihdosta käytännöllistä ja lisää niiden yhteensopivuutta keskenään, sillä lähes kaikki nykyaikaiset yhteydelliset laitteet toimivat IP:n ehdoilla. Matkaviestimien on kyettävä vaihtamaan dataa langallisten tietoverkkojen kanssa tarvittaessa.

Pakettimuotoisuus tarkoittaa sitä, että tieto eli data kulkee verkon halki pilkottuna pieniin osiin; datapaketteihin. Paketit säästävät verkon kapasiteettia kun kaikkea dataa ei siirretä samalla kertaa. Pakettimuotoisessa tiedonsiirrossa yhteys lähettävän ja vastaanottavan laitteen välillä säilyy kunnes kaikki paketit ovat vastaanotettuja. Tämä mahdollistaa datapakettien siirron hetkellisen katkaisemisen esimerkiksi puhelun välittämiseksi. (Heikkonen ym. 2004, 56.) Pakettimuotoista tiedonvälitystä käytetäänkin valtaosin tietokoneiden välityksellä kulkevan datan käsittelemiseen. Tällaista dataa ovat esimerkiksi tekstidokumentit ja kuvatiedostot, jotka ovat usein tiedostokooltaan suuria. Nykyaikaiset palvelut ja sovellukset vaativatkin yhä enemmän tiedonsiirron kapasiteettia osakseen myös langattomissa verkoissa.

TETRA–verkko käyttää myös toisenlaista tiedonsiirtomenetelmää; piirikytkentäinen data (circuit switched data). Piirikytkentäinen data on pääosin puheen siirtoon käytetty menetelmä. Erona pakettimuotoisen ja piirikytkentäisen datan välillä on se, että pakettimuotoisen datan käyttäessä yhteyttä vain sen aikaa kun dataa siirretään, piirikytkentäinen data käyttää aina tiettyä kanavaa yhteyden ylläpitämiseen. Piirikytkentäinen tiedonsiirto on ollut olennainen osa verkkotekniikoita niiden kehittämisestä lähtien, mutta nykyisin kaiken datan on käytännössä oltava pakettimuotoista, jotta käytetyt laitteet, sovellukset ja teknologiat ovat helposti yhteensopivia keskenään. (Heikkonen ym. 2004, 56.) Piirikytkentäisen datan bittinopeuden kokonaismäärä TETRA:ssa on 36 kb/s. Käytännössä suurin vapaa siirtonopeus on kuitenkin 28,8 kb/s. Käytetyt aikavälit ja suojauksen tasot saattavat kutistaa nopeutta vielä huomattavastikin lisää. (Penttinen 2006b, 45.) Turvallisen puheenvälityksen osalta TETRA on tällä hetkellä vallitsevassa asemassa siihen käytetyistä tekniikoista ainakin Euroopan oloissa. Piirikytkentäisen puhedatan kaappaaminen ja salakuuntelu on TETRA:n avulla tehty käytännössä mahdottomiksi vahvoilla salausmenetelmillä.

TETRA:ssa saattaa esiintyä datanvälityksen yhteydessä siirtoaikojen kasvua. Kantoaallon sisältäessä jo puhe- tai dataliikenteen välitykseen käytetyn nopean kanavan, joudutaan uusi

data siirtämään hitaalla kanavalla. Siirtonopeus voi tällöin pudota jopa 1/18-osaan siitä, mitä se nopealla kanavalla olisi. Tämä voi aikaansaada sen, että tukiasemien käyttämät sanomapuskurit täyttyvät liikenteen määrästä. (Rantama 2011.) Verkon kapasiteetin ollessa kovassa käytössä TETRA ei enää välttämättä välitä dataa kovinkaan nopeasti. TETRA:ssa tietynlaiset puhelut kuitenkin ohittavat kaiken muun liikenteen, jolloin tärkeille puhepalveluille riittää aina kapasiteettia. Tilanteesta riippuen myös datan nopea vastaanotto voi olla ensisijaisen tärkeää.

3.4.1 WAP -palvelut

Wireless Application Protocol (WAP) on langattomia verkkoja varten kehitetty sovellusprotokolla. WAP–selain mahdollistaa Internetin käytön päätelaitteella langattomasti ja WAP tuo käytettäviksi erilaiset WAP–palvelusovellukset. TETRA:ssa WAP mahdollistaa lähes välittömän tietokantojen käsittelyn verkon päätelaitteilla. Tämä on esimerkiksi poliisille ja pelastuspalveluille tärkeä ominaisuus, jonka avulla päästään sopivalla sovelluksella käsiksi vaikkapa potilastietoihin tai ajoneuvorekistereihin niitä tarvittaessa. WAP–sovellukset asennetaan niitä ylläpitävälle palvelimelle, johon päätelaitteet ottavat yhteyttä sovelluksia käytettäessä. Ilman WAP:ia kaikki käytettävät sovellukset täytyy asentaa päätelaitteille erikseen, mutta WAP:in avulla halutut sovellukset saadaan käyttöön halutuille päätelaitteille ilman asennuksia. WAP–palvelimelle voidaan sijoittaa myös tarpeellisia tietoja, jotka palvelun käyttäjä voi ladata tarvittaessa myös vaikkapa tietokoneelleen. WAP voi käyttää tiedonsiirtoon myös tekstiviestejä. Viestin lähettäjänä voi olla palvelun ylläpitäjä tai organisaation komentokeskus, joka välittää käyttäjille esimerkiksi tekstilinkin tärkeää tietoa sisältävälle WAP-sivulle. (Heikkonen ym. 2004, 57-58.)

3.4.2 Muut datapalvelut

TETRA–verkossa on mahdollista käyttää monenlaisia eri sovellusvalmistajien tiedonsiirtoon kehittelemiä palveluita. Yksi tärkeä palveluominaisuus on pakettimuotoisen datan mahdollistama kuva- ja videotiedostojen siirtäminen. Kuvan välittäminen esimerkiksi onnettomuuspaikalta komentokeskukselle tai johdolle voi olla äärimmäisen tärkeää koko toiminnan kannalta. Tietynlaiset kameralaitteet voidaan ohjelmoida lähettämään niillä otetuista kuvista automaattisesti kopiot ennalta määritetyille tietokoneille. Kuvien lähettäminen toimii tietysti myös vastavuoroisesti komentokeskukselta kentällä olevalle henkilöstölle. (Heikkonen ym. 2004, 59-60.) Tällaisia tärkeitä tilanteen aikana välitettäviä kuvatiedostoja voisivat olla esimerkiksi alueiden kartat, kuvat onnettomuusalueelta ja rakennusten pohjakaaviot.

Reaaliaikaisen videon välittäminen on myös mahdollista, mutta sen kuluttaman verkkokapasiteetin suuren määrän vuoksi käyttö on todennäköisesti vähäistä. Kapasiteettia voidaan kuitenkin lisätä väliaikaisesti yksittäisen päätelaitteen käytettäväksi, jolloin videokuvaa voidaan välittää päätelaitteelta komentokeskukselle tai toisinkin päin päätelaitteelle komentokeskukselta riittävällä nopeudella. Hidas videokuva ei välttämättä vaadi kovin suurta tiedonsiirtonopeutta. (Penttinen 2006b, 46.)

TETRA:an on olemassa myös automaattisia paikannussovelluksia. Yksinkertainen jako voidaan tehdä kulkuneuvojen paikantamisen; AVL:n (Automatic Vehicle Location) ja henkilöiden paikantamisen; APL:n (Automatic Person Location) välille. Paikannuksen kohde on molemmissa TETRA-päätelaite. Komentokeskus seuraa paikannussignaaleja digitaalisten karttojen avulla. Paikannuksessa käytetään pääasiassa GPS (Global Positioning Satellite) –satelliittijärjestelmää sijaintitietojen saamiseksi, mutta kohteen ollessa TETRA–verkon toiminta-alueella voidaan kohde määrittää myös verkkopohjaisen paikannuspalvelimen avulla. TETRA–päätelaite voidaan liittää ulkoiseen GPS–paikannuslaitteeseen, jos päätelaitteessa ei ole sellaista valmiiksi sisäänrakennettuna. Päätelaitteet kommunikoivat paikannukseen käytetyn järjestelmän kanssa teksti- ja statusviestein. Tietynlaisella palvelusovelluksella teksti- ja statusviesteillä voidaan TETRA:ssa myös lähettää kontrollidataa sähkölaitteille; kuten valaisimille, lukituslaitteille ja turvakameroille. (Heikkonen ym. 2004, 60-61.)

Erilaisten viestien ja raporttien lähettämiseen on myös olemassa hyödyllisiä palveluita. TETRA–päätelaitteeseen voi yhdistää kannettavia tietokonelaitteita tiedostojen käsittelyä varten, jolloin tilanneraporttien laatiminen ja lähettäminen on nopeaa. TETRA–verkkoon on myös voitu liittää mahdollisuus käyttää Internetin välityksellä kulkevaa sähköpostia. Tämä on yleensä toteutettu käyttämällä erillisiä sähköpostipalvelimia ja palomuureja turvallisuuden vuoksi. Lisäksi käytössä voi olla palvelu potilastietojen turvalliseen ja nopeaan lähettämiseen sairaaloille kentältä. Tietojen raportointi tekstimuotoisina voi olla tarkempaa ja säästää enemmän aikaa kuin samojen tietojen välittäminen puheen avulla. (Heikkonen ym. 2004, 62.)

3.5 Direct Mode Operation

Tavallisesti kommunikaatio TETRA–verkossa tapahtuu käyttäen useita kanavia vaihtelevaa tekniikkaa Trunked Mode Operation (TMO), mutta TETRA:ssa on myös mahdollista käyttää verkon ulottuvuuden ulkopuolella toimivaa yhden puhekanavan Direct Mode Operation (DMO) -tekniikkaa. DMO mahdollistaa päätelaitteiden välisen viestinnän alueella, jossa verkon tukiasemien toiminta on heikkoa tai sitä ei ole laisinkaan. Käytännössä DMO:n avulla voidaan siis jatkaa kommunikaatiota asuttujen alueiden ulkopuolella, rakennusten sisällä ja vaikkapa tunneleissa. DMO:lla on kuitenkin rajoitettu toiminta-alue, joka vaihtelee noin kuudesta tai

useammasta kilometristä esteettömillä ulkoalueilla vain muutamiin metreihin paksujen betoniseinien sisäpuolella. (Heikkonen ym. 2004, 63-64.)

DMO on tarkoitettu väliaikaiseen vallitsevan tilanteen sanelemaan käyttöön. Silloin kun DMO:ta käytetään TETRA–verkon ulkopuolella, verkon tarjoamat palvelut eivät ole käytettävissä. Koska kaikki päätelaitteiden välinen viestintä tapahtuu DMO:ta käytettäessä vain yhtä kanavaa pitkin, voi kanava suuren käyttäjämäärän vuoksi ruuhkautua nopeasti. Tämä yksi kanava on kaiken tiedonsiirron käytössä, joten tukkeutumisen estämiseksi monia päätelaitteiden toimintoja ei voida tehokkaasti käyttää. Verkon infrastruktuurin ollessa poissa käytöstä päätelaitteet eivät voi ilmoittaa käyttäjälleen kuuluvuusaluetta ja signaalin voimakkuutta, jolloin DMO:n ollessa toiminnassa viestinnän perille pääsystä ei voida olla varmoja ennen kuin vastaanottaja viestittää takaisin. Käyttäjät eivät siis yhteyttä testaamatta tiedä ovatko he kuuluvuusalueella vai sen ulkopuolella. DMO:n käyttäjä ei myöskään kuule tavanomaisesti TMO:lla käytyä kommunikaatiota, kuten ei TMO:n käyttäjäkään kuule DMO:lla käytyä viestintää, vaikka TETRA–verkko yltäisikin alueelle. (Heikkonen ym. 2004, 64.)

DMO:ssa on mahdollista käyttää osaa TETRA–teknologian sisältämistä palveluista. Palvelut, jotka vaativat yhteyden TETRA–verkkoon tai sen ulkopuolelle, ovat käyttökelvottomia DMO:n aikana. DMO:ssa käytettävissä ovat samat puhelumuodot; yksilöpuhelut ja ryhmäpuhelut puheryhmineen kuin tavallisestikin verkon alueella TMO:ssa. Puheryhmät toimivat DMO:ssa kuitenkin vain ennalta määritettyä kanavaa pitkin, jolloin kyseinen kanava ei ole enää TMO:n käytettävissä rajoittaen osaltaan sen toimintamahdollisuuksia. Teksti- ja statusviestit ovat myös DMO:n käytettävissä, mutta ne käyttävät tiedonsiirtoon samaa kanavaa kuin puheliikennekin. (Heikkonen ym. 2004, 65-67.) TETRA:ssa on kuitenkin lisäksi käytössä taajuustehokas toimintamuoto (frequency efficient mode), jonka avulla käytettävänä kapasiteettina on neljä aikaväliä samalla kanavalla. Yksittäinen siirtosuunta käyttää vain yhtä aikaväliä. Esimerkiksi kahdensuuntaisia puheluita voi DMO:n aikana olla käynnissä kaksikin samanaikaisesti, sillä jokainen päätelaite tarvitsee vain yhden aikavälin. (Penttinen 2006b, 44.)

DMO:n toimintamahdollisuuksia voidaan laajentaa erikoislaitteilla. Tällaisia ovat DMO–toistimet (repeater) ja DMO–portit (gateway). Molemmat ovat TETRA–päätelaitteita, jotka asennetaan kulkuneuvoihin tai muihin liikuteltaviin kohteisiin. Toistimet ja portit toimivat vain päätelaitteiden kohdalla, jotka tukevat tekniikaltaan niiden käyttöä. DMO–toistin laajentaa DMO:n kuuluvuusaluetta. Toistin ei välttämättä tue kaikkia TETRA:n toimintoja ja on siksi yleensä varattu vain puheviestinnän välittämiseen. DMO–portti puolestaan yhdistää DMO:n ja TMO:n siten, että DMO:ta käyttävät päätelaitteet voivat vastaanottaa viestejä TETRA-verkosta. Tämän ongelmana on turvallisuuden vaarantuminen, sillä DMO–portin avulla

TETRA–verkkoon liitetyn päätelaitteen todennus on vaikeaa. Tämän vuoksi portti rajataan yleensä vain yhden helpommin hallittavan puheryhmän käyttöön. (Heikkonen ym. 2004, 67-68.)

3.6 Turvallisuus

TETRA–standardin kaikki ominaisuudet ja palvelut ovat kehitetty suojattua ja turvallista tiedonsiirtoa silmälläpitäen. TETRA ei ainoastaan tehosta sen käyttäjätahon turvallisuutta vaan myös toiminnan kohteen turvallisuutta. Esimerkiksi tapaturman uhrien selviytyminen on varmempaa ja nopeampaa, kun pelastajat voivat koordinoida keskinäisen toimintansa onnistuneella kommunikaatiolla. Valtaosa TETRA:n turvaratkaisuista on kuitenkin teknisiä ja vaikuttavat itse verkon tai päätelaitteen toiminnassa ilmenemättä yksittäisille käyttäjille millään tavoin. Käyttäjiltä ei siten myöskään vaadita tietoa järjestelmän toiminnasta päätelaitteita käytettäessä turvallisesti. TETRA-järjestelmän tärkeimmät turvaominaisuudet ovat verkon ja laitteiden todennus sekä tietoliikenteen salaus.

Todennuksen ollessa käytössä jokaisen TETRA–päätelaitteen on todennettava itsensä aina rekisteröityessään verkkoon eli kun laitteeseen kytketään virta ja silloin, kun laite vaihtaa tukiasemaa tai TETRA-verkkoa. Tämä ominaisuus tekee TETRA–päätelaitteiden väärentämisen mahdottomaksi. TETRA–verkossa kulkeva data on myös aina salattua kaikissa yhteyden vaiheissa. Tämä puolestaan tekee TETRA–verkon salakuuntelun ja siirretyn datan kaappaamisen käytännössä mahdottomaksi. TETRA:n toiminta on siis tavallisesti täysin suojattua tietoihin oikeuttamattomilta käyttäjiltä. (Heikkonen ym. 2004, 71.)

3.6.1 Todennus

Todennuksella tarkoitetaan sitä, että vain TETRA–verkkoon rekisteröidyt oikeutetut päätelaitteet voivat saada yhteyden verkkoon sekä lähettää ja vastaanottaa siellä kulkevia signaaleja. Todennuksella varmistetaan sekä käytetyn verkon että päätelaitteen aitous.

Jokaiseen päätelaitteeseen on ohjelmoitu jo niiden tuotantolaitoksessa yksilöllinen todennusavaimensa (authentication key), jonka pituus on 128 bittiä. TETRA–verkkoon on jokaista siihen liitettyä päätelaitetta varten luotu ensin yksilöllinen tunnistenumeronsa (ITSI), joka ohjelmoidaan päätelaiteeseen. Verkkoon liitetään tämän tunnistenumeron yhteyteen vastaavasti oma viiteavaimensa (reference key). Itse todennusprosessi toimii ETSI:n määrittelemän algoritmin avulla luodun numeron (seed number) mukaisesti. Päätelaitteen ottaessa yhteyttä verkkoon verkko lähettää algoritmilla luomansa numeron päätelaitteelle, johon laite vastaa verkon luoman numeron, oman todennusavaimensa ja tunnistenumeronsa avulla määrittämällään numerosarjalla. Verkko määrittää vastaavanlaisesti algoritmilla

luomansa numeron, laitteen viiteavaimen sekä sen tunnistenumeron avulla numerosarjan, johon päätelaitteen määrittämän numerosarjan täytyy täsmätä. Molempien numerosarjojen ollessa samanlaiset todennus on onnistunut. Lisäksi päätelaite on voitu määritellä vaatimaan verkolta todennus sen aitoudesta, jolloin sama prosessi käydään läpi uudelleen päinvastaisena. (Heikkonen ym. 2004, 72-73.)

3.6.2 Salaus

TETRA–verkon tietoliikenteensä salaukseen, tulkintaan ja purkamiseen käytettävissä on kaksi menetelmää, jotka ovat Air Interface Encryption (AIE) sekä niin kutsuttu päästä päähän salaus (end-to-end encryption). Molemmissa menetelmissä salauksen vahvuuteen vaikuttavat kolme avaintekijää, jotka ovat TETRA–tekniikassa taattuja: vahva salausalgoritmi, pitkä salausvain ja käytettyjen salausavainten säännöllinen vaihtuvuus. (Heikkonen ym. 2004, 73.)

AIE salaa kaiken tietoliikenteen päätelaitteelta tukiasemalle ja sisältää kolme eri salauksen tasoa. Ensimmäinen taso käyttää TETRA:n sisäänrakennettua tavanomaista digitaalista salausta ilman erillisiä salausavaimia. Toinen taso käyttää vahvaa ETSI:n määrittämää salausalgoritmia sekä päätelaitteisiin ohjelmoitua muuttumatonta salausavainta (static cipher key). Kolmas taso käyttää myös vahvaa ETSI:n määrittämää salausalgoritmia, mutta lisäksi todennuksen yhteydessä luotua salausavainta (derived cipher key). Kolmannen tason salauksessa käytetyt salausavaimet siis vaihtuvat joka kerta kun todennus tapahtuu uudelleen luoden todella voimakkaan salauksen tason. Salauksen kohdistuessa tukiasemalta joukolle päätelaitteita siihen käytetään yleistä salausavainta (common cipher key), joka on yksilöllinen jokaista tukiasemaa kohtaan, mutta sitä vaihdetaan usein salauksen vahvistamiseksi. (Heikkonen ym. 2004, 73.)

Päästä päähän salaus puolestaan salaa vain puhemuotoisen tietoliikenteen päätelaitteelta toiselle koko TETRA–verkon läpi. Päästä päähän salauksen yhteydessä on siten silti käytettävä AIE–salausta muun tiedon salaamiseen. Verkon sovellukset kuitenkin käyttävät päästä päähän salausta myös oman datansa salaamiseen. Päästä päähän salaus ei ole myöskään määritelty käyttämään tiettyä salausalgoritmia kuten AIE on, joten käyttäjätahot voivat kehittää omansa tai käyttää tarjolla olevia valmiita vaihtoehtoisia algoritmeja. Toisin kuin AIE päästä päähän salaus estää salatun tiedon purkamisen verkon sisältä käsin, sillä liikenne pysyy saman salauksen alla koko verkon lävitse. Päästä päähän salauksella voidaankin torjua lisäksi hypoteettisia sisäisiä uhkia; esimerkiksi tietovuotoja tai verkon langallisiin osiin kytkettyjä dataa kaappaavia laitteita. Päästä päähän salauksen käyttöä kuitenkin rajoittaa sen käyttämien salausavainten hallinnan työläys ja sen toimintaa tukevien laitteiden korkeampi hintataso. (Heikkonen ym. 2004, 74.)

3.6.3 Verkon muut turvaominaisuudet

TETRA–verkko on suunniteltu säilyttämään toimintakuntonsa kaikissa olosuhteissa. Jos TETRA-päätelaiteen yhteys verkkoon katkeaa jonkinlaisen verkon infrastruktuurisen vian tai häiriön vuoksi, aktivoituu erityistoiminto, jolla päätelaite säilyttää yhteyden sillä hetkellä käyttämäänsä tukiasemaan (base station fallback). Tällaisessa tilanteessa päätelaite on yhteydessä vain yhteen tukiasemaan ja siksi kuuluvuusalue on rajallinen. Käytetyt puheryhmät säilyvät yhteydenpitoon ja osa muistakin verkon palveluista voi pysyä käytettävissä. Ongelmalliseksi koituu kuitenkin se, ettei yksittäinen päätelaitteen käyttäjä voi tietää kuinka suuri osa verkosta on poissa käytöstä ja ovatko puheryhmän muut jäsenet saman tukiaseman alueella. (Heikkonen ym. 2004, 76.)

Edellä kuvattua TETRA:n ominaisuutta, joka takaa päätelaitteiden välisten viestiyhteyksien toiminnan vain yhden tukiaseman varassa yhteyden katketessa muuhun verkkoon, ei kuitenkaan ole Suomessa vielä tällä hetkellä käytössä. Tämä tieto saatiin HUS-organisaation valmiuspäällikön kautta. Base station fallback -ominaisuuden voi kuitenkin korvata rajoitetusti käyttäen DMO–toimintatilaa menetettäessä yhteys TETRA-verkkoon, jolloin kuuluvuusalue on kuitenkin DMO:n mukainen ja siten vieläkin pienempi kuin yhdellä tukiasemalla.

Yksittäisiä TETRA–päätelaitteita voidaan myös kytkeä väliaikaisesti tai jopa pysyvästi pois verkosta. Päätelaite voidaan kytkeä pois verkosta esimerkiksi huollon ajaksi, katoamisen tai varkauden vuoksi. Väliaikainen poiskytkentä (stun) voidaan tehdä langattomasti ja se estää päätelaitteen yksilöllisen tunnistenumeron käytön verkon laitteissa, jolloin kyseisellä päätelaiteella ei voida tehdä minkäänlaisia puheluja tai käyttää verkon palveluja. Lievempi versio väliaikaisesta poiskytkennästä voi jättää DMO:n käyttökelpoiseksi. Päätelaite pysyy kuitenkin rekisteröitynä verkkoon ja se voidaan halutessa palauttaa käyttökelpoiseksi (enable). Päätelaitteen pysyvä poiskytkentä (kill) voidaan myös tehdä langattomasti verkon kautta ja se tekee koko laitteen pysyvästi toimintakyvyttömäksi. Ainoa keino palauttaa pysyvästi poiskytketty päätelaite on toimittaa se laitevalmistajalle uudelleenkytkentää varten. Nämä voimakkaat TETRA–verkon turvaominaisuudet ovat yleensä rajoitettu vain organisaation komentokeskukselle ja mahdollisesti jopa sitäkin korkeammille päätäntätahoille. (Heikkonen ym. 2004, 76-77.)

3.6.4 Päätelaitteiden turvaominaisuudet

TETRA–päätelaitteet muistuttavat yleensä perusominaisuuksiltaan paljon tavanomaisia matkapuhelimia. Vahingossa tehtyjä puheluita ja muita näppäinkomentoja estetään näppäinlukolla. Näppäinlukko estää näppäinten toiminnan kunnes se aukaistaan yleensä kahta

ennalta määritettyä laitteen näppäintä peräjälkeen painamalla. Näppäinlukko voi olla määritelty siten, että se ei estä PTT–näppäimen käyttöä, jolloin ryhmäpuheluihin on mahdollista osallistua näppäinlukituksesta huolimatta. (Heikkonen ym. 2004, 79.)

TETRA–päätelaitteissa on myös useimmiten käytössä matkapuhelimista tutut PIN (Personal Identification Numbers) ja PUK (Personal Unblocking Keys) -koodit. Päätelaite kysyy PIN-koodia kun siihen kytketään virta. PIN–koodin ollessa oikein laite käynnistyy normaalisti, mutta koodin ollessa väärin laite kysyy sitä uudelleen muutaman kerran, jonka jälkeen se lukitsee itsensä syötettyjen koodien ollessa edelleen vääriä. Tämän jälkeen laitteen saa päälle ainoastaan syöttämällä siihen oikean PUK–koodin. Päätelaitteet on myös voitu määrittää kysymään erillisiä koodeja tiettyjen toimintojen tai asetusten yhteydessä, jos niiden käyttöä on haluttu lisätyn turvallisuuden vuoksi rajoittaa. (Heikkonen ym. 2004, 79.)

Sähkölaitteiden käyttöön sisältyy aina hyvin pieni kipinöinnin tai virtalähteen räjähtämisen riski. Teoriassa tämä aiheuttaa aina vaaratilanteen mahdollisuuden räjähdysherkkien tai tulenarkojen materiaalien läheisyydessä. Valmistajasta riippuen TETRA–päätelaite voi olla määritetty räjähdyssuojatuksi (explosion proof). Räjähdyssuojatun puhelimen osat ja akku voivat olla erikoisvalmisteisia ja sen virtapiirit päällystetty suojamateriaalilla. (Heikkonen ym. 2004, 81.) TETRA:n käyttäjätahoista erityisesti palokunnilla on tarve käyttää vain räjähdyssuojattuja radiolaitteita työskentelyolosuhteiden usein erittäin korkeista lämpötiloista johtuen. Liian korkea lämpötila voi aiheuttaa sähkölaitteissa kipinöintiä, jolloin räjähdysvaara kasvaa huomattavasti.

Radioaaltoja lähettävät laitteet saattavat myös häiritä joitakin toisia niille herkkiä sähkölaitteita. Tällaisia laitteita voi olla käytössä esimerkiksi sairaaloissa ja muissa terveydenhuollon laitoksissa. Tavallisesti radiopuhelimet on määrätty suljettaviksi sairaala-alueilla. TETRA–päätelaitteissa on kuitenkin tästä syystä erillinen toimintatila (transmission inhibit), jota käytettäessä niiden tuottama sähkömagneettinen säteily on minimoitua. (TETRA Industry Group 2011.)

Säteilysuojatussa tilassa päätelaite ei voi lähettää signaaleja, vaan voi ainoastaan vastaanottaa niitä. Poikkeuksen tähän tekee hätäpuhelu, jonka tekeminen on turvallisuussyistä aina mahdollista. Säteilysuojatussa tilassa päätelaite siis voi vain vastaanottaa puheluita ja viestejä, mutta käyttäjä ei voi vastata niihin tai aloittaa omia puheluitaan suojauksen ollessa käytössä. Koska päätelaite ei säteilysuojatussa tilassa lähetä signaaleja, voi se menettää yhteyden TETRA–verkkoon käytetyn tukiaseman vaihtuessa kunnes normaali toimintatila palautetaan. Säteilysuojattua tilaa kuitenkin harvoin käytetään niin pitkillä välimatkoilla. Kulkuneuvoihin asennetut TETRA–päätelaitteet käyttävät useimmiten

ulkoista antennia, jolloin esimerkiksi ambulansseissa olevat mahdollisesti häiriötä saavat laitteet ovat säteilyltä turvassa ilman erillistä suojaustakin. (Heikkonen ym. 2004, 82.)

3.6.5 Terveyshaitat

Eräs käyttäjien henkilökohtaisen turvallisuuden ongelma on sähkömagneettiselle säteilylle altistuminen. Nykyisin sähkömagneettiselle säteilylle altistumista on kuitenkin lähes mahdoton välttää. Kaikki arkisetkin sähkölaitteet luovat ympärilleen heikon säteilykentän. Kansainvälisillä sopimuksilla on luotu rajoitteita sallituille säteilymäärille terveyshaittojen välttämiseksi.

Lukuisia tieteellisiä tutkimuksia on laadittu radiolaitteiden ja matkapuhelinten aiheuttamista säteilyhaitoista, mutta niiden tulokset ovat olleet ristiriitaisia, ja selviä yhteyksiä kudosvaurioiden ja testeissä olleiden laitteiden välillä ei ole voitu varmuudella osoittaa. Laitteet eivät saa ylittää asetettuja säteilymääriä, jotka ilmaistaan SAR (Specific Absorbation Rate) -arvolla. TETRA–päätelaitteet noudattavat samoja säteilyarvojen säädöksiä kuin tavanomaiset matkapuhelimetkin. (Heikkonen ym. 2004, 83.)

TETRA-tekniikan mahdollisista terveyshaitoista tehtyjen tutkimusten perusteella ei ole syytä olettaa TETRA-laitteiden aiheuttavan sen enempää säteilyä kuin tavallisten matkapuhelintenkaan. Terveyshaittoja ei ole kyetty osoittamaan todeksi mm. aivotoimintaa, verenkiertoelinten toimintaa ja syöpäkasvainten kehittymistä mittaavissa tutkimuksissa. (TETRA Industry Group 2011.) Tieteellisesti ei voida kuitenkaan sanoa täysin varmasti, ettei terveyshaittojen mahdollisuutta olisi laisinkaan. Tutkimusten avulla voidaan vain todeta, että kyseisessä kokeessa ei havaittu yhteyksiä TETRA:n ja tutkitun terveyshaitan välillä.

3.7 Esimerkkikäyttötapaukset

Esimerkkinä TETRA:n tavanomaisesta arkikäytöstä ja sen toimintamahdollisuuksista esitetään kaksi käyttötapauskuvausta. Kuvaukset perustuvat tämän opinnäytetyön pääasiallisena TETRA–lähteenä käytettyyn kirjaan You and Your TETRA Radio. Kirja sisältää muutamia fiktiivisiä, mutta todellisiin kommunikaatiomalleihin perustuvia esimerkkejä TETRA:n käytöstä ja päätelaitteiden sisältämistä toiminnoista vaihtelevissa tilanteissa eri organisaatioiden toimesta. Tässä osiossa esitetyt kaksi käyttötapausta pohjautuvat kirjassa olleiden esimerkkien sisältämien tietojen yhdistelmiin, mutta ne ovat tämän opinnäytetyön edetessä itse laadittuja ja siten myös fiktiivisiä. Käyttötapauksien kulkua selvennetään niin ikään itse laadituin kaaviokuvin (kuviot 1 ja 2), joilla havainnollistetaan tilanteissa vallitsevien TETRA–puheryhmien jakoa. Tehokas ja rajoittamaton puheryhmien hallinta on yksi TETRA:n

käyttökelpoisimmista ominaisuuksista seuraavia kahta esimerkkitapausta vastaavissa todellisissa tilanteissa.

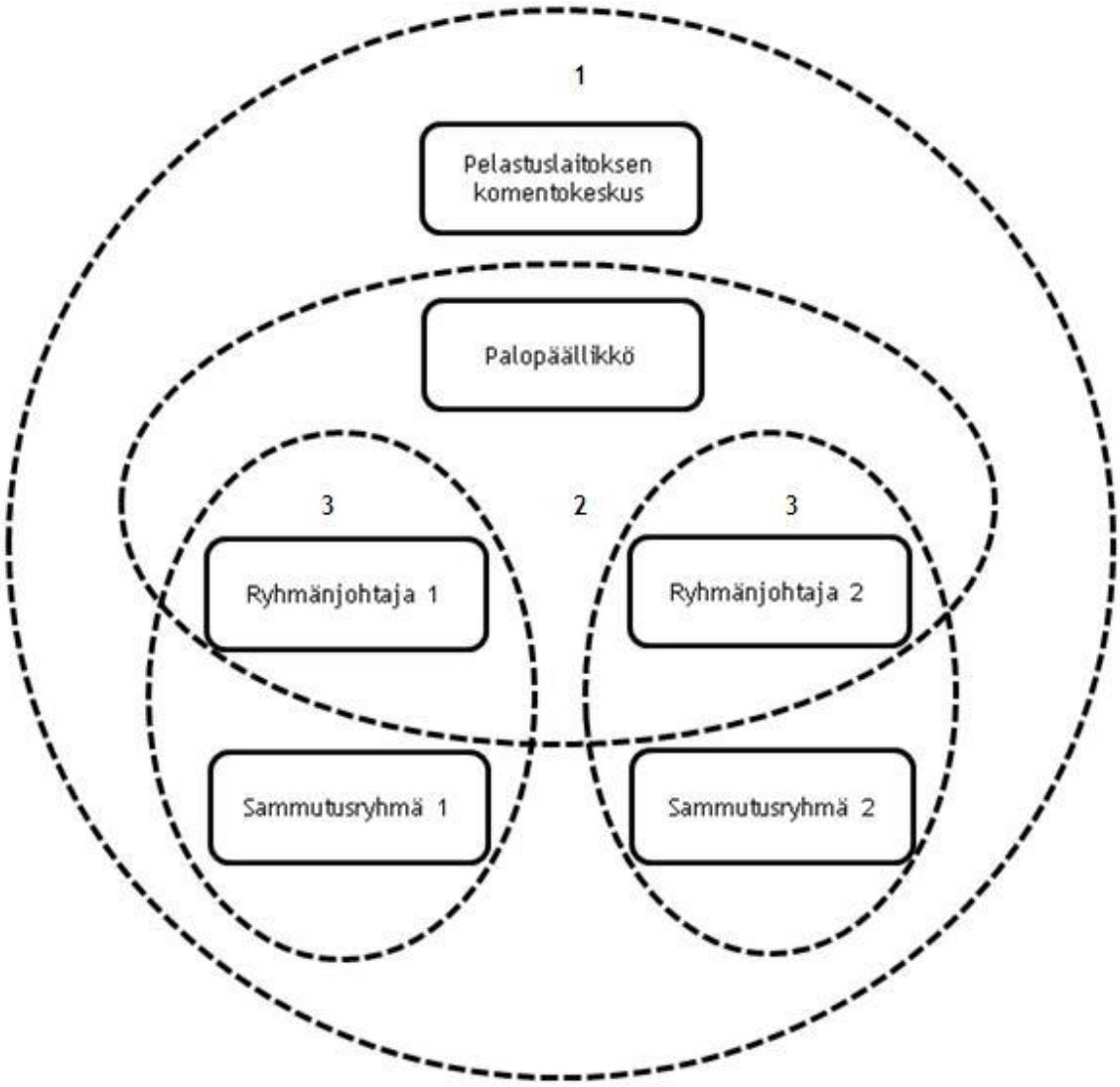
3.7.1 Tapaus 1: Sammutustehtävä

Työpäivän päätyttyä ja työntekijöiden poistuttua esikaupunkialueella sijaitsevan teollisuuslaitoksen varastorakennuksesta odottamattoman sähkövian aiheuttama kipinöinti sytyttää varaston nurkassa sijaitsevat puulavat tuleen. Ohikulkija huomaa varastorakennuksesta nousevan savun ja soittaa matkapuhelimellaan hätäkeskukseen. Hätäkeskuksesta välitetään hälytys pelastuslaitoksen alueelliseen yksikköön vastaavanlaisen tilanteen varalta ennalta laaditun toimintasuunnitelman mukaisesti. Pelastuslaitokselta matkaan lähetetään pikaisesti kaksi valmiudessa ollutta sammutusajoneuvoa. Palopäällikkö saa myös tiedon tapahtuneesta ja päättää saapua paikalle, mutta on kyseisellä hetkellä liikenteessä kaupungin ruuhkaisessa keskustassa.

Pelastuslaitoksen yksiköiden toimintaa ohjaa alueellinen komentokeskus, joka saa tietojärjestelmiensä kautta tulipalotilanteeseen ja palon kohteeseen liittyvät uusimmat tiedot. Jokaisella palomiehellä sammutusajoneuvoissa on oma TETRA–radiopuhelimensa, joiden lähettämää sijaintisignaalia komentokeskus seuraa jatkuvasti digitaaliselta kartalta. Matkalla olevat palomiehet ovat jaettuna kahteen ryhmään, joista kummallakin on oma ryhmänjohtajansa. Kun sammutusajoneuvot saapuvat palopaikalle, ryhmänjohtajat varmentavat saapuneensa kohteelle lähettämällä statusviestin päätelaitteellaan komentokeskukselle ja palopäällikölle. Palopäällikkö vastaa ryhmänjohtajille ryhmäpuhelulla ja kertoo saapuvansa paikalle myöhässä.

Palopäällikkö ja ryhmänjohtajat kuuluvat samaan puheryhmään keskenään. Myös komentokeskus seuraa palopäällikön ja ryhmänjohtajien puheryhmää. Palomiehet kuuluvat omiin ryhmäkohtaisiin puheryhmiinsä ryhmänjohtajineen. Ryhmänjohtajat seuraavat siis päätelaitteillaan kahta puheryhmää samanaikaisesti, mutta palopäällikön sisältävälle puheryhmälle on määritetty suurempi tärkeys, jolloin siellä tapahtuva viestintä on aina kuultavissa. Operaatiolle on myös määritetty taustaryhmä, jota kaikki päätelaitteet seuraavat, mutta johon vain komentokeskus voi tehdä kaiken muun viestinnän tärkeydessään ylittäviä ilmoituksia. Puheryhmien jakoa havainnollistaa tarkemmin kuvio 1.

Tulipalo ei ole palokunnan nopean toiminnan vuoksi ehtinyt vielä levitä laajalti ja palo saadaan hallintaan tehokkaasti. Kun palopäällikkö vihdoin saapuu paikalle, palo on jo saatu sammutettua, jolloin tämä ilmoittaa komentokeskukselle tilanteen olevan ohi.



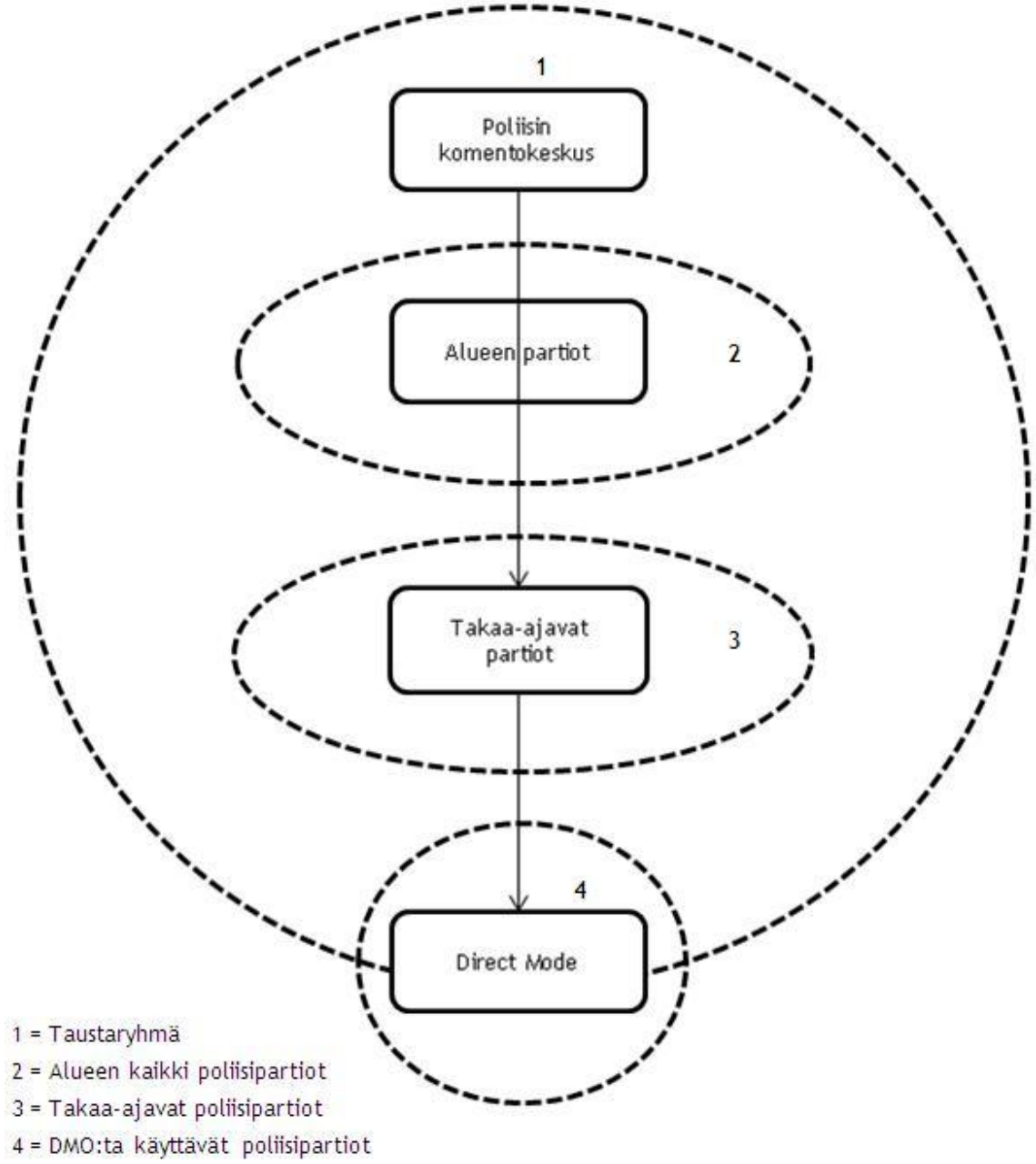
Kuvio 1: Kaaviokuva sammutustehtävässä käytetyistä puheryhmistä

3.7.2 Tapaus 2: Takaa-ajotilanne

Poliisipartio mittaa nopeuksia maantien laidalla ja havaitsee henkilöauton, jonka vauhti ylittää reilusti tiellä sallitun nopeuden. Jonkin matkan päässä maantietä eteenpäin odottelee toinen partio, jolle nopeuksia mittaavat poliisit ilmoittavat partioautonsa TETRA–radiolaitteella lähestyvästä ylinopeutta ajavasta henkilöautosta. Pian toinenkin poliisipartio huomaa kaaharin ja lähtee takaa-ajoon. Kaahari ei tottele pysäytyskäskyä vaan päinvastoin lisää vaarallisesti nopeuttaan.

Jahtaava poliisipartio ilmoittaa tilanteesta komentokeskukselle, joka seuraa kaikkia alueen poliisipartioita päätelaitteiden lähettämien sijaintitietojen perusteella. Kaikki alueen poliisipartiot seuraavat päätelaitteillaan viestinnälle määritettyä taustaryhmää ja saavat komentokeskukselta sen kautta tiedon ylinopeutta ajavasta henkilöautosta sekä sen sijainnista. Komentokeskus lähettää ilmoituksen myös tekstimuodossa partioille. Lähimmät kaksi partioautoa lähtevätkin tilannetta kohti ja ilmoittavat siitä ryhmäpuhelulla kaikkien alueen partioiden käyttämään yhteiseen puheryhmään, jonka viestintää myös komentokeskus seuraa. Komentokeskus luo takaa-ajoon osallistuville kolmelle partiolle oman väliaikaisen puheryhmänsä viestinnän selkeyttämiseksi. Puheryhmien kehityskulkua tilanteessa havainnollistaa kuvio 2.

Takaa-ajo kestää pitkään ja johtaa pois TETRA–verkon kattamalta alueelta, jolloin kaaharia seuraavat poliisipartiot siirtyvät käyttämään DMO:ta. Yhdessä partioautoista on asennettuna DMO–portti, ja se pysähtyy verkon laitamille säilyttämään yhteyden TETRA–verkkoon niin pitkään kuin vain mahdollista. Läheisessä jyrkässä mutkassa kaahari ei hidasta vauhtiaan tarpeeksi vaan suistuu tien viereiseen ojaan. Poliisipartiot pysähtyvät nopeasti ja lähestyvät jalkaisin tieltä suistunutta kaaharia, joka kömpii itse ulos ajoneuvostaan ilmeisesti lievin vahingoin. Poliisit pidättävät kaaharin, joka osoittautuu vahvasti päihtyneeksi. DMO–portin avulla yhteys verkkoon on säilynyt ja tilanteen ratkeamisesta voidaan ilmoittaa komentokeskukselle.



Kuvio 2: Kaaviokuva takaa-ajotilanteessa käytetyistä puheryhmistä

4 Radio- ja matkapuhelintekniikoiden vertailu

Tämä osio sisältää radio- ja matkapuhelintekniikoiden keskinäisen vertailun. Tarkoituksena on selvittää tekniikoiden sisältämiä ominaisuuksia, verrata niitä keskenään ja siten arvioida niiden soveltuvuutta viranomaistahojen vaativaan käyttöön. TETRA:n lisäksi vertailukohteiksi valittiin jo väistyvä analoginen radiotekniikka, yleisesti matkapuhelimien käyttämä GSM ja se radioversio GSM-R sekä uudempi, käytössä yleistyvä UMTS. Vertailu on suoritettu

taulukoimalla näiden tekniikoiden sisältämiä ominaisuuksia niitä käsittelevästä kirjallisuudesta. Vertailutaulukossa GSM-R käsitellään GSM:n alaisuudessa samassa sarakkeessa. GSM- ja UMTS-palveluihin sisältyvät myös faksitoiminnot, mutta niitä ei mainintaa laajemmin käsitellä tässä työssä faksin merkityksen vähennyttyä viestiliikenteessä. Varsinaista vertailua edeltää vertailukohteiden tiivistetyt kuvaukset, joissa on kyseisen tekniikan yleisten pääpiirteiden lisäksi pyritty löytämään niiden sisältämät keskeiset vertailun läpivientiin vaikuttavat seikat. Tekniikoiden vertailu täydentää tässä opinnäytetyössä laadittua TETRA-standardin riskianalyysiä osoittamalla konkreettisesti TETRA:n sisältämät käytön turvallisuutta edistävät ominaisuudet ja palvelut, joita muissa vastaavissa verkkotekniikoissa ei välttämättä ole käytettävissä laisinkaan.

4.1 Analoginen radio

Analoginen radiotekniikka on ollut olemassa ja sovellettuna monenlaisiin käyttötarkoituksiin jo kauan. Vielä nykyisinkin perinteisiä analogisia radiolaitteita käytetään monilla aloilla tekniikan iästä huolimatta.Radiotekniikasta käytetään myös nimityksiä Professional Mobile Radio ja Private Mobile Radio (PMR).

Ennen uudempia digitaalisia tekniikoita analoginen PMR-tekniikka oli TETRA:n nykyisten pääasiallisten käyttäjätahojen käytössä. Analogiset radioverkot olivat kuitenkin huomattavasti vähemmän käyttökelpoisia näiden alojen toiminnalle nykyisiin ratkaisuihin verrattuina, sillä analoginen radioverkko on sidonnainen tiettyyn toiminta-alueeseen, sillä on käytettävissään vain vähän kanavia puheen välitykseen ja kanavien vaihto tapahtuu manuaalisesti päätelaitteen käyttäjän toimesta. Tämän rajoitteellisuuden vuoksi yhdellä organisaatiolla saattoi olla käytössään useita analogisia radioverkkoja eri alueita ja käyttötarkoituksia varten. Kommunikaatio eri verkkojen käyttäjien välillä oli hankalaa ja käyttäjän ollessa oman radioverkkonsa toiminta-alueen ulkopuolella tavanomainen viestintä ei ollut mahdollista ilman erityisjärjestelyjä. (Heikkonen ym. 2004, 3.)

Teknisiltä ominaisuuksiltaan analoginen PMR–teknologia on uudempiin ratkaisuihin verrattuna yksinkertaista. Analogiset radiolaitteet on suunniteltu pääasiassa vain äänen välittämiseen, mutta jotkin kehittyneemmät analogiset päätelaitteet voivat myös tukea statusviestien lähettämistä TETRA:n tavoin. Kaikki samaa kanavaa käyttävät päätelaitteet muodostavat yhdessä puheryhmän eli ne vastaanottavat muilla päätelaitteilla kanavalle lähetettyjä signaaleja ja voivat itse lähettää signaaleja muille samaa kanavaa seuraaville päätelaitteille. Käytössä on siis yksi kanava yhdelle joukolle käyttäjiä, jotka viestivät keskenään. Vain yksi käyttäjä kerrallaan voi puhua analogiseen radiopuhelimeensa, jolloin muut joutuvat odottamaan kanavan vapautumista ennen kuin voivat itse lähettää signaalia. Viestintä on siis

yhdensuuntaista (half-duplex). Analoginen PMR–tekniikka ei mahdollista TETRA:n kaltaisia käyttäjien tärkeysjärjestyksiä, joilla puheoikeuksia hallitaan. (Heikkonen ym. 2004, 3-4.)

Analogisella radioverkolla ei ole tavallisesti minkäänlaista suojausta, joka tekee siitä erittäin haavoittuvaisen. Radioliikenne on kuitenkin mahdollista salata kalliilla erikoisratkaisuilla, mutta käytännössä suuri osa radioliikennettä on tästä mahdollisuudesta huolimatta suojaamatonta. Varastetulla päätelaitteella esimerkiksi rikolliset ovat voineet salakuunnella viranomaisten radioliikennettä ja häiritä sen kulkua. Analoginen radioverkko ei sisällä ominaisuuksia, joilla päätelaitteita voitaisiin kytkeä pois verkon yhteydestä niiden joutuessa vääriin käsiin. Analoginen radiotekniikka ei myöskään ole laajalti standardisoitua, joka on osaltaan johtanut yhteensopivuusongelmiin erilaisten verkkojen ja päätelaitteiden välillä. (Heikkonen ym. 2004, 3-4.)

4.2 GSM

GSM (Global Systems for Mobile Communications) on toisen sukupolven langaton digitaaliseen tiedonsiirtoon perustuva viestinjärjestelmä, jonka käyttöönotosta on kulunut jo parisenkymmentä vuotta. GSM oli alun perin tarkoitettu eurooppalaiseksi järjestelmäksi, mutta se kuitenkin levisi maailmanlaajuiseen käyttöön. (Elers 2011.) Niinpä GSM onkin yksi käytetyimmistä matkaviestinjärjestelmistä ja se tulee olemaan laajassa käytössä ainakin lähitulevaisuudessa. Uudet järjestelmät toimivatkin yhdessä GSM-verkon kanssa eivätkä korvaa sitä. (Penttinen 2006 1, 121.) Toisaalta operaattoreille usean rinnakkaisen matkapuhelinverkon ylläpitäminen on kallista ja uudemmat järjestelmäsukupuolvet tuovat kustannussäästöjä niiden paremman kapasiteetin ansiosta, joten GSM-verkon valta-aseman säilyminen ei ole taattua pidemmällä tähtäimellä. (Sajari 2008.)

GSM-matkaviestimeen (MS, Mobile Sation) kuuluu itse viestilaite (ME, Mobile Equipment) ja siihen kytketty SIM-kortti (Subscriber Identity Module). Puhelimeen on oltava mahdollistaa syöttää numerot 0-9 sekä erikoismerkit * ja #, mutta syöttäminen voi tapahtua näppäimistön lisäksi puheentunnistuksella tai ohjelmallisella syötöllä. SIM–kortti on luonteeltaan älykortti, joka toimii tilaajan tunnisteena GSM-verkossa. Kortti mahdollistaa minkä tahansa GSM-puhelimen käytön lukuun ottamatta eräitä operaattoreiden tarjoamia SIM-lukollisia laitteita. SIM-kortilla on pysyvästi tallennettuna tilaajan tunnistetietoja sekä tunnistusalgoritmit A3 ja A8. (Penttinen 2006a, 132-136.)

4.2.1 Tekniikka

GSM-verkko koostuu monista alijärjestelmistä, joiden väliset rajapinnat on standardoitu yksiselitteisesti eri laitevalmistajien elementtien liittämisen mahdollistamiseksi samaan

verkkoon. Nämä alijärjestelmät ovat keskusjärjestelmä (NSS, Network and Switching Sub-System), tukiasema- eli radiojärjestelmä (BSS, Base Station Sub-System) sekä niitä ohjaava käytönhallintajärjestelmä (OSS, Operations Sub-System). GSM-verkon käytön mahdollistava GSM-palvelualue koostuu suurimmillaan kaikista toiminnassa olevista GSM-verkoista, joita voidaan käyttää verkkovierailuun. Radioverkon liikennettä välittää tukiasemajärjestelmä, joka käsittää tukiasemat (BTS, Base Transceiver Station) ja niitä hallitsevat tukiasemaohjaimet (BSC, Base Station Controller). Lisäksi järjestelmään kuuluu myös transkooderi- ja nopeudensovituslaitteisto (TC, Transcoder tai TRAU, Transcoder/Rate Adapter). Solu on puolestaan samaa aluetta palvelevien lähetin-vastaanottimien (TRX, Transceiver) peittoalue, jossa on aina vähintään yksi TRX. Yksittäinen tukiasema välittää tilanteesta riippuen yhden tai useamman solun liikennettä. (Penttinen 2006a, 122-123.)

Yksittäinen TRX välittää radioliikennettä yhdellä taajuudella, jos sitä ei ole erikseen määritetty toimimaan eri taajuusalueilla. GSM-taajuus on jaettu kahdeksaan aikaväliin (TS, time slot), joten yhdellä taajuudella voi olla parhaimmillaan kahdeksan piirikytkentäisen puhe- tai datapalvelun käyttäjää; kaksi puhekäyttäjää voi myös vuorottelemalla jakaa saman aikavälin käyttämällä puolen nopeuden puhekoodekkeja (HR, Half Rate), jolloin taajuudella voi olla 16 käyttäjää. Pakettikytkentäisiä GPRS- ja EGPRS-käyttäjiä on mahdollista vuorotella (multipleksaus) vielä piirikytkentäisiä käyttäjiä huomattavasti enemmän. Osa resursseista kuluu joka tapauksessa merkinantoon, joten jokaista aikaväliä ei voida välttämättä hyödyntää. (Penttinen 2006a, 123.)

Tukiasemaohjain eli BSC hallinnoi oman alueensa radioresursseja. Matkapuhelinkeskus kytkee sen kautta puhelut päätelaitteelle samalla kun tukiasemaohjain huolehtii yhteyden radiorajapinnan tapahtumista. Yleensä yhden BSC:n alueella on useita tukiasemia, joista muodostetaan sijaintialueita niitä ryhmittelemällä. Päällä oleva päätelaite eli matkapuhelin ilmoittaa BSC:lle sen siirtymisestä sijaintialueelta toiselle, jotta verkko pystyy reitittämään puhelimeen saapuvan liikenteen oikean sijaintialueen kautta. Puhelun tullessa asiakkaan puhelimeen BSC lähettää kutsun kaikille sijaintialueella oleville soluille; puhelimen vastattua kutsuun parhaan solun kautta BSC antaa kanavamäärityksen, samoin jos puhelin pyytää itse kanavaa lähtevän puhelun vuoksi. (Penttinen 2006a, 128.)

GSM-verkossa voi tapahtua kanavanvaihtoa, jos kentän voimakkuus tai yhteyden laatutaso vaihtelee. BSC tietää aina alueellaan olevien solujen tilanteen sekä yhteyksien laatutason valvomalla radioresursseja; viestinjärjestelmän mittaustulosten keskiarvojen perusteella päätellään, milloin kanavanvaihto on tarpeellinen. Transkooderi- ja nopeudensovitusyksikkö TRAU puolestaan huolehtii puheen koodauksesta ja dekoodauksesta sekä datan nopeussovittamisesta GSM-verkon ja muiden verkkojen välillä. (Penttinen 2006a, 128.)

Keskusjärjestelmä eli NSS kytkee GSM-verkon sisäisten puhelujen ohella myös GSM-puhelinten ja muiden verkkojen väliset puhe- ja datayhteydet. Myös siinä tapauksessa, että yhteys muodostetaan saman solun sisällä olevien GSM-puhelinten välille, yhteys reitittyy vähintään yhden matkapuhelinkeskuksen eli MSC:n kautta. MSC:n tehtäviin kuuluvat puhelujen kytkeminen, ylläpito ja kytkeminen omalla alueellaan. Jos vastaanottava puhelin ei ole MSC:n alueella, kauttakulkukeskus (GMSC, Gateway MSC) välittää puhelun oikealle matkapuhelinkeskukselle. (Penttinen 2006a, 129-130.)

Kotirekisterissä (HRL, Home Location Register) on tallennettuna tilaaja- ja laskutustietoja sekä numeroon liittyviä lisäpalveluita. Pysyviä tietoja ovat mm. kansainvälinen ISDN- tai MSISDN-numero (Mobile Subscriber ISDN number), tilaajan tunnus (IMSI, International Mobile Subscriber Identity), tilaajan salausparametrit sekä liittymän tyyppi. Sen sijaan tavoitettavuustiedot, kuten tieto tilaajan liittymisestä verkkoon, reititystiedot ja puhelun siirrot yms. muut palvelut ovat muuttuvia tietoja. MSC:n vierailijarekisteri (VLR, Visitor Location Register) pyytää HRL:stä uudelle alueelle siirtyvän puhelimen tilaajatiedot, jotka myös pysyvät muistissa sen aikaa, kun puhelin on tämän alueella. Puhelimen siirtyessä toiselle alueelle sen tiedot siirtyvät kyseisen alueen VLR:ään. (Penttinen 2006a, 130-131.)

Jokaisessa GSM-puhelimessa on yksilöllinen laitetunnus, joka löytyy myös operaattorilla mahdollisesti olevasta laiterekisteristä (EIR, Equipment Identity Register). Verkko voi tarvittaessa tarkastaa puhelimen tiedot ja puhelimen käyttö voidaan myös estää operaattorin tai kansainvälisen rekisterin (CEIR, Central EIR) avulla. Tunnistuskeskus (AuC, Authentication Centre) säilyttää tilaajille verkkoon liittyessä määritettyjä tunnistenumeroita. Puhelunmuodostuksessa AuC:n vierailijarekisterille antamia tunnistenumeroita verrataan tilaajalaitteen lähettämiin numeroihin. Jos soittajalla ei ole oikeutta verkkoon, puhelu estetään. Ryhmäpuhelurekisteri (GCR, Group Call Register) vaaditaan verkkoon, jos halutaan käyttää esimerkiksi konferenssipuheluita ja muita ryhmäpuhelupalveluita. (Penttinen 2006a, 131.)

Käytönhallintajärjestelmä (OSS, Operations Sub-System) useimmiten vaatii yhteyden BSS:n tai NSS:n kanssa. OSS:n ja muiden GSM-järjestelmän osien välinen Q3-rajapinta periaatteessa mahdollistaa yhteensopivuuden kaikkien valmistajien laitteiden kautta, mutta yleensä helpointa on kytkeytyä saman laitevalmistajan OSS:n kautta, jotta palveluvalikoima on täysin yhteensopiva. OSS huolehtii verkon käytöstä ja kunnossapidosta sekä tilaajatietojen ja päätelaitteiden hallinnasta. Järjestelmässä olevan käyttö- ja kunnossapitokeskuksen avulla asennetaan GSM-elementtien ohjelmistoja, syötetään ja muutetaan parametreja sekä tehdään verkon valvontaa; keskuksia voi OSS-järjestelmässä olla yksi tai useampi. (Penttinen 2006a, 132.)

GSM–järjestelmää on laajennettu kattamaan myös radiopuhelinmaisia toimintoja rautatiekäyttöä varten. Tätä laajennusta kutsutaan siksi nimellä GSM-Railway (GSM-R). Perinteisten radiopuhelinten tavoin GSM-R mahdollistaa yhdensuuntaisen viestinnän käytettyyn radioliikenteen puhekanavaan tai -ryhmään. Tavalliset kahdensuuntaiset GSM-puhelut ovat silti myös mahdollisia. GSM-R sisältää lisäksi osittain TETRA:n vastaavien ominaisuuksien kaltaiset puheryhmien muokkauksen, hätäpuhelun soittamisen ja puheluiden tärkeysjärjestyksen määrittämisen toiminnot. Puheyhteyksien muodostus on kuitenkin huomattavasti hitaampaa kuin esimerkiksi TETRA:ssa. (Heikkonen ym. 2004, 5.) GSM-R ei radiopuhelinominaisuuksistaan huolimatta pysty kilpailemaan TETRA:n kanssa, koska siitä puuttuu viranomaiskäytölle keskeisiä ominaisuuksia. Mm. Direct Modea ei ole, puheryhmiä ei voida muokata dynaamisesti, päästä päähän-salausta ei ole ja palveluita ei pystytä ylläpitämään ilman verkkoa. Lisäksi GSM-R:n laajempi käyttö todennäköisesti vaatisi paljon lisää verkkokapasiteettia. (TETRA Memorandum of Understanding 2004.)

4.2.2 Tietoturva

Digitaalisen GSM-järjestelmän turvallisuustoiminnot ovat analogisia edeltäjiään huomattavasti paremmat. Jo puhelun alkaessa GSM-verkko tarkistaa SIM-kortin oikeuden verkon käyttöön ja tarvittaessa katkaisee puhelun, jos lupaa ei ole. Varmennuksen jälkeen luodaan uusi salausavain, jonka jälkeen viestiliikenne puhelimen ja tukiaseman välillä on suojattu; tähän kuuluvat numerotiedot, sijaintialuepäivitykset, kanavanvaihdot, tekstiviestit ja puhe- sekä datalähetteet. Salaukseen käytettävästä A5-algoritmista on kaksi toteutusta, joista A5/1 antaa paremman ja A5/2 heikomman suojan. Yleisesti käytetään ensin mainittua. (Penttinen 2006a, 148-150.)

GSM-verkon A5/1-algoritmikaan ei kuitenkaan enää takaa turvallista viestintää, sillä se pystytään nykyisin murtamaan tarkoitukseen suunnitellulla laitteistolla ja ohjelmistolla hyvinkin nopeasti, jopa alle minuutissa: viestinnän luottamuksellisuus on siten hyvin kyseenalaista. Viestintävirasto suositteleekin suojautumaan salakuuntelulta käyttämällä uudempia verkkoja, kuten kolmannen sukupolven järjestelmiä. (Kirkkonummen Sanomat 2011, 6.) Viestintävirasto ei kevyin perustein tällaista suosittelisi, joten GSM-verkon tietoturva ei ole enää kovin hyvällä tasolla, ellei ole jopa vaarallisen heikko.

4.2.3 Palvelut

GSM-verkon keskeisiin palveluihin kuuluvat tekstiviestit. Maksimissaan 160 merkin pituisia viestejä lähetetään tekstiviestipalvelun (SMS, Short Message Service) kautta. Viestejä voidaan lähettää ja vastaanottaa sekä valmiustilassa että puhelimen ollessa käytössä, koska ne välitetään merkinantokanavilla. Viestissä oleva sanomakeskuksen numero ohjaa sen HLR-

tiedon perusteella oikean MSC/VLR:n alueelle ja sitten SIM-kortille tai puhelimen muistiin. Vastaanottavan puhelimen ollessa suljettuna lähete jää tekstiviestikeskukseen odottamaan puhelimen palaamista verkkoon, jolloin viestin lähetystä yritetään uudelleen. (Penttinen 2006a, 150-151.)

Viestien määrä ei rajoitu yhteen, vaan 160 merkin pituisia viestejä voidaan lähettää maksimissaan 255 kappaletta, jotka lähetetään siis erillään mutta käsitellään loogisena kokonaisuutena. Yleensä operaattori kuitenkin rajoittaa yhdistettävien viestien määrää, joka on yleensä 3-4. Tiettyjen solujen alueella voidaan käyttää myös solulähetyksiä (CB, Cell Broadcast), jotka ilmoittavat esimerkiksi onnettomuuksista tietyllä maantieteellisellä alueella puhelimiin automaattisesti lähetettävillä viesteillä. (Penttinen 2006a, 151-152.)

GSM-verkon data toimii molempiin suuntiin, eli on lähtevää (MO, Mobile Originated) ja saapuvaa (MT, Mobile Terminating) dataa. GSM-datapalvelu toimii kahdella tavalla: 1) virheenkorjaavasti (NT, Non-Transparent), jolloin verkko havaitsee virheitä, korjaa niitä sekä lähettää purskeita uudelleen tai 2) vakionopeudella (T, Transparent), jolloin siirrettävään dataan ei oteta kantaa, eli huolellisempi virheenkorjaus jää toteutettavaksi erillisillä protokollilla. Vakionopeuksisessa datansiirrossa käytetään FEC- eli Forward Error Correction -virheenkorjausta perusvirheiden havainnointiin ja korjaamiseen. Virheenkorjaavassa datansiirrossa käytetään lisäksi RLP-protokollan (Radio Link Protocol) mukaista virheenkorjausta. (Penttinen 2006a, 152-153.)

Perus-GSM:n datanopeus on maksimissaan 9,6 kb/s ja radiorajapinnan yli siirrettävä perusnopeus on 12 kb/s. FEC:n jälkeen nopeus on 22,8 kb/s. Vastaavasti puolen nopeuden kanavalla maksiminopeus on 4,8 kb/s. Nopea piirikytkentäinen datapalvelu HSCSD (High Speed Circuit Switched Data) kasvattaa nopeustasoa, koska sen avulla verkko ja päätelaite voivat käyttää useampaa kuin yhtä aikaväliä per käyttäjä. Lisäksi on mahdollista käyttää kevennettyä kanavakoodausta ja V.42bis-kompressiota toisistaan riippumatta. Useiden aikavälien käytöllä voidaan päästä nopeuteen 64 kb/s vakionopeuksisessa datasiirrossa ja virheenkorjaavassa datasiirrossa nopeuteen 38,4 kb/s. Kevennetyllä kanavakoodauksella käyttäjänopeudet ovat vastaavasti 64 kb/s ja 57,6 kb/s. (Penttinen 2006a, 152-155.)

Kuten Internet-yhteyksissä, myös HSCSD-palvelussa on symmetrinen ja asymmetrinen palvelu. Ensin mainitussa sekä uplink- että downlink-suunnassa on yhtä paljon aikavälejä käytössä, kun taas jälkimmäisessä käytetään eri suuntiin eri määrää aikavälejä. Symmetrisessä palvelussa kapasiteetti lähettää ja vastaanottaa on siis yhtäläinen, kun asymmetrisessä esimerkiksi lähetyskapasiteetti on pienempi kuin vastaanottokapasiteetti (vrt. ADSL-yhteys). HSCSD osaa käyttää myös joustavasti radiokanavaresursseja; datanopeus voi muuttua joko nopeammaksi tai hitaammaksi, jos vapaiden kanavien lukumäärää muuttuu. Virheenkorjaavassa yhteydessä

verkko pystyy jakamaan dynaamisesti HSCSD-resursseja, mikä onnistuu myös vakionopeuksisessa yhteydessä, mutta käyttäjän datanopeus on oltava vakio. Konfiguraation muutos tehdään puhelun aikana kanavien lukumäärän kasvattamisella ja vähentämisellä. (Penttinen 2006a, 156-157.)

4.3 UMTS

UMTS (Universal Mobile Telecommunications System) on kolmannen sukupolven (3G) matkaviestinteknologia, joka mahdollistaa GSM-verkkoa nopeammat datayhteydet. Perustekniikka ei pysty vastaamaan vaativampien sovellusten käyttöön, joten nopeampien verkkojen käyttöönotto on järkevää. Radioverkko on täysin erilainen verrattuna GSM-järjestelmään, mutta runkoverkossa resursseja voidaan silti jakaa GSM- ja GPRS-järjestelmien kesken. UMTS-järjestelmällä on paljon teknisiä yhteneväisyyksiä GSM-järjestelmän kanssa, mutta myös huomattavia eroja, erityisesti radioverkossa. (Penttinen 2006b, 64-73.)

Yhteensopivuus GSM-järjestelmän kanssa on tarkoin harkittua, koska pitkässä siirtymävaiheessa toisen sukupolven matkaviestinnästä kolmannen sukupolven matkaviestintään on tärkeää pystyä käyttämään 3G-puhelinta myös GSM-verkossa. UMTS käyttää kuitenkin eri taajuuksia kuin GSM ja hyödyntää uutta tekniikkaa datasiirrossa puhelimen ja tukiaseman välillä. UMTS-järjestelmä mahdollistaakin maksimissaan nopeuden 2 Mbit/s pakettipohjaisessa dataliikenteessä, joten se on merkittävästi GSM-verkkoa nopeampi. (Brewer ym.)

4.3.1 Tekniikka

UMTS-verkossa on radiojärjestelmä (RNS, Radio Network System) ja runkoverkko (CN, Core Network). Päätelaitteet ovat radiorajapinnan kautta yhteydessä radiojärjestelmään. Lisäksi päätelaitteen ja GSM–järjestelmän SIM–korttia vastaavan USIM-kortin välillä on oma rajapintansa. GSM-verkon tapaan käytönhallintajärjestelmän avulla ohjataan ja valvotaan UMTS-verkon osia. UMTS:n radioliityntäverkkoon (UTRAN, Universal Terrestrial Radio Access Network) kuuluvat tukiasemat ja niitä ohjaavat radioverkko-ohjaimet (RNC, Radio Network Controller), jotka vastaavat GSM:n tukiasemaohjaimia. UMTS-verkossa on mahdollisuus liittää radioverkko-ohjaimet suoraan toisiinsa, jolloin päätelaitteen radioverkko-ohjainten välinen kanavanvaihto vie vain vähän runkoverkon keskuskapasiteetista; GSM-verkossa tämä ei ole mahdollista. Runkoverkossa on yksinkertaisimmassa toteutuksessa UMTS-matkapuhelinkeskuksia (MSC, Mobile Services Switching Centre) ja/tai GPRS-verkko. (Penttinen 2006b, 64-65.)

Jo UMTS-runkoverkon ensimmäisessä vaiheessa vaatimuksina olivat GSM-release 99:n mukaisten verkkomääritysten lisäksi tuki vähintään 64 kb/s piirikytkentäiselle ja vähintään 2 Mb/s pakettikytkentäiselle tiedonsiirrolle. (Penttinen 2006b, 65-66.) Tämä omalta osaltaan korostaa sitä, että UMTS on suunniteltu erityisesti datasiirron vaatimuksia silmälläpitäen ja siten se soveltuu suurempien datamäärien nopeaan siirtämiseen päätelaitteiden välillä. Uusia palveluita kehitetään jatkuvasti ja uudet datapalvelut mahdollistavat moninkertaisesti nopeamman tiedonsiirron ainakin optimaalisilla kuuluvuusalueilla ja hyvissä olosuhteissa.

Matkaviestinverkon (PLMN, Public Land Mobile Network) määrittäminen tapahtuu samalla tavoin kuin GSM-järjestelmässä. Verkko tarvittaessa tarjoaa palveluita yhdellä tai useammalla taajuudella. Verkon käyttäjien ja verkon ulkopuolisten verkon käyttäjien yhteydenmuodostukseen käytetään yhteensovitusta. Matkaviestinverkko toimii yleensä yhden maan rajojen sisäpuolella, mutta päällekkäisyyksiä palvelualueissa voi olla silti, jos maassa on useampi kuin yksi PLMN. Häiriöiden minimoimiseksi päällekkäisyyksiä on kuitenkin hyvä olla vähän. Järjestelmäalue on alue, jolle voi muodostaa yhteyden tarvitsematta tietää alueella olevan matkaviestintilaajan sijaintia. Alueellinen palvelu puolestaan toimii vain tietyllä, pienemmällä osalla koko viestinverkon toiminta-aluetta. Lisäksi on paikkapalvelualue, joka voi tarjota paikkatietopalveluita, jolloin puhelun hinta on mahdollista riippua käyttäjän paikan mukaan. (Penttinen 2006b, 73-74.)

UMTS-järjestelmässä loogiset kanavat vastaavat siitä, mitä siirretään, fyysinen kanava siitä, minne dataa ollaan siirtämässä ja siirtokanava puolestaan siitä, miten data siirretään. Erona GSM-järjestelmään on se, että UMTS-järjestelmässä voidaan kuljettaa usealla erityyppisellä fyysisellä kanavalla yhtä tai useampaa siirtokanavaa, kun taas GSM-järjestelmässä fyysinen kanava on yksittäinen aikaväli, jolla on yksi tai tarvittaessa useampi looginen kanava. (Penttinen 2006b, 74.)

Toisin kuin GSM-järjestelmässä, UMTS-järjestelmässä päätelaitteen on mahdollista olla yhtä aikaa yhteydessä verkkoon useamman solun kautta. Tällä saavutetaan parempi yhteyden laatu, mutta kokonaiskapasiteetti on pienempi monen solun kautta. Kanavanvaihtoa on kahdenlaista: solunvaihdon tapahtuessa kahden järjestelmän tai taajuuden välillä sitä kutsutaan hard-handoveriksi eli ”kovaksi” kanavanvaihdoksi ja vastaavasti solunvaihdon tapahtuessa saman järjestelmän eri solun välillä sitä nimitetään soft-handoveriksi eli ”pehmeäksi” kanavanvaihdoksi. Mikäli kanavaa vaihdetaan saman solun sisällä, puhutaan softer-handoverista eli ”pehmeämmästä” kanavanvaihdosta. GSM-järjestelmässä merkinanto kulkee kahden tukiasemaohjaimen välisen keskuksen kautta, mutta UMTS-järjestelmässä merkinanto voidaan lähettää suoraan keskenään kanavanvaihdon tapahtuessa kahden eri radioverkko-ohjaimen välillä. (Penttinen 2006b, 81-82.)

4.3.2 Tietoturva

UMTS-verkon tietoturvatoiminnot pohjautuvat paljolti GSM-verkon tietoturvaratkaisuihin, mutta toimintoja on lisätty ja jo olemassa olevia on valtaosin paranneltu. GSM-verkosta perityt merkittävimmät tietoturvaelementit ovat käyttäjän todentaminen, päätelaitteesta erillinen identiteettimoduuli eli SIM-kortti ja radiorajapinnan salaus. UMTS-järjestelmässä on kuitenkin GSM-järjestelmää vahvempi salausalgoritmi, tietoturvatoiminnot ovat päivitettävissä ja autentikointi on toteutettu paremmin. UMTS-verkossa salaus tehdään radioverkko-ohjaimessa, kun GSM-verkossa se tehdään tukiasemalla. (Brewer ym.)

UMTS-matkapuhelin voidaan määritellä pysymään aina omassa verkossaan, jolloin salakuuntelu ei Viestintäviraston tiedossa olevilla menetelmillä ole mahdollista. (Kirkkonummen Sanomat 2011, 6.) UMTS-verkon tietoturvallisuus vaikuttaakin olevan GSM-verkkoa huomattavasti paremmalla tolalla ja erityisesti viranomaiskäytön turvallisuusvaatimuksia ajatellen UMTS on näistä kahdesta ainoa järkevä vaihtoehto.

UMTS:ssa käytetään molemminpuolista autentikointia, eli sekä käyttäjä että verkko todentavat toisensa. Ne pystyvät keskenään neuvottelemaan siitä, mitä eheysalgoritmeja, salausalgoritmeja ja salausavaimia käytetään. Nämä ominaisuudet omalta osaltaan eliminoivat väärien tukiasemien käyttämisen vakoilutarkoitukseen ja vaikeuttavat hyökkäysten tekemistä radiorajapinnan kautta. Radioyhteyden kautta ei ole myöskään mahdollista kaapata käyttäjä- tai merkinantotietoja eikä selvittää käyttäjän liikkumista ja sijaintia. (Brewer ym.)

4.3.3 Palvelut

GSM-verkkoon verrattuna UMTS-verkon palvelu- sekä sovellustarjonta ovat kattavampia. UMTS-verkon palvelut voidaan jakaa informaatiosovelluksiin (Internet), koulutussovelluksiin, viihdesovelluksiin (pelit ja audio/video), kunnallispalveluihin (hälytyspalvelut), liikesovelluksiin (liikkuvat toimistopalvelut), tietoliikennesovelluksiin (videopalvelut, äänitunnisteet), kaupallis- ja rahoitussovelluksiin (maksu-, pankki- ja laskutuspalvelut) sekä liikenne- ja telematiikkasovelluksiin (liikennetiedot, turvallisuussovellukset). Palveluiden kattavuus tekee UMTS-verkosta multimediajärjestelmän, mutta pelkän puheen välitys ja muut perinteisemmät palvelut ovat edelleen käytettävissä. UMTS-järjestelmässä on eri palvelutasoluokkia, jotka määritellään mm. liikenneluokan, prioriteetin, luotettavuuden ja nopeuden mukaan. Esimerkiksi puheyhteydessä viivettä ei juuri ole, mutta ”virtaavassa” dataliikenteessä, kuten audio ja video, viivettä voi olla lähes 10 sekuntiakin. Lisäksi osa palveluista on virheensietoisia, toiset eivät: puheyhteydet ja -viestit ovat virheensietoisia,

kun taas interaktiiviset palvelut ja Internetin selaaminen eivät ole virheensietoisia. (Penttinen 2006b, 70-73.)

UMTS-järjestelmän telepalvelut ovat pitkälti yhteneväiset GSM-verkon kanssa, eli niihin kuuluvat puhe, hätäpuhelu ja tekstiviestit. Puhepalvelun puhekoodekki toimii sekä UTRAN- että GSM-verkossa niin, että toimivuus säilyy myös päätelaitteen tehdessä kanavanvaihtoa UTRAN:n ja GSM:n välillä. Tekstiviestipalvelu, johon kuuluvat sekä kaksipisteyhteydellinen viesti SMS-PP että solulähete SMS-CB, toimii sekä GSM- että UMTS-verkoissa. UMTS-järjestelmästä löytyy myös kaksi erilaista faksipalvelua, joista store-and-forward –palvelussa vastaanottaja hakee faksin muodostamalla yhteyden faksin varastointielementtiin; end-to-end–palvelussa puolestaan muodostetaan suora yhteys UMTS-päätelaitteen ja ulkopuolisessa verkossa olevan faksilaitteen välille. (Penttinen 2006b, 70-71.)

Telepalveluiden mukaisesti myös verkkopalveluissa on otettu huomioon yhteensopivuus GSM-verkon kanssa; UMTS-järjestelmä tukee piiri- ja pakettikytkentäistä dataa. Käyttäjä ei myöskään huomaa eroa siinä, onko yhteys muodostettu UMTS- vai GSM-verkon kautta. Palvelu tukee sekä vakionopeuksista että virheenkorjaavaa versiota. Molemmissa palveluissa menetetään mahdollisimman vähän dataa kanavanvaihdossa GSM:n ja UMTS:n välillä. Pakettikytkentäinen data on yhteensopiva ulkopuolisten verkkojen, kuten IP:n ja LAN:n kanssa. Verkkopalveluihin kuuluvat piirikytkentäiset puhelut, LCD (Long Constrained Delay Data) -palvelut reaaliaikaisille yhteyksille ja UDD (Unconstrained Delay Data) –palvelut ei-reaaliaikaisille yhteyksille. LCD on mahdollista toteuttaa joko piiri- tai pakettikytkentäisenä, mutta UDD on aina pakettikytkentäinen. (Penttinen 2006b, 70-72.)

4.4 Vertailun läpivienti

Radio- ja matkapuhelintekniikoiden vertailun toteuttamiseksi mahdollisimman selkeästi ja johdonmukaisesti tiedot tekniikoiden sisältämistä ominaisuuksista esitetään taulukoituna (kuvio 3). Vertailutaulukossa esitetyt ominaisuudet perustuvat tämän opinnäytetyön TETRA–tekniikkaa käsittelevässä osiossa selvennettyihin TETRA:n sisältämiin ominaisuuksiin. TETRA on suunniteltu tarkoituksella viranomaistahojen vaativaan käyttöön, joten vertailun pohjustaminen TETRA:n sisältämien ominaisuuksien etsimiseen myös muista yleisesti tarjolla olevista radio- ja matkapuhelintekniikoista antaa kokonaisvaltaisen yleiskuvan niiden soveltuvuudesta vastaavanlaiseen käyttöympäristöön ja -tarkoitukseen. Tiedot kunkin tekniikan sisältämistä ja niille tarjolla olevista ominaisuuksista perustuvat tämän opinnäytetyön lähteinä käytettyihin niitä käsitteleviin kirjallisiin teoksiin. Seuraavalla sivulla olevaa vertailutaulukkoa seuraa vielä sen esittämien tietojen selvennykset sekä niiden nojalla esitettyjä päätelmiä tekniikoiden soveltuvuudesta suhteessa TETRA:an.

OMINAISUUS	TETRA	A. PMR	GSM	UMTS
Käyttövalmiita verkkoja	x	x	x	x
Lähes välitön puheyhteyden muodostus	x			x
Kahdensuuntaiset puhelut (full-duplex)	x		x	x
Yhdensuuntaiset puhelut (half-duplex)	x	x	x*	
Mahdollisuus tehdä puheluja toisiin verkkoihin	x		x	x
Suorat half-duplex puhelut (direct call)	x			
Ryhmäpuhelut (group call)	x	x	x*	
Puheryhmät (talk group)	x		x*	
Dynamic Group Number Assignment (DGNA)	x			
Puheryhmien etsintä (scanning)	x			
Puheluiden tärkeysjärjestys (priority call)	x		x*	
Hätäpuhelut	x		x	x
Tekstiviestit	x		x	x
Statusviestit	x	x*		
Pakettimuotoinen tiedonsiirto	x		x	x
Piirikytkentäinen tiedonsiirto	x	x	x	x
Internet-yhteys ja monipuolisia datapalveluja	x		x	x
GPS-paikannussovelluksia	x		x	x
Direct Mode Operation (DMO)	x	x*		
Päätelaitteen todennus	x		x	x
Verkon todennus	x			x
Tietoliikenteen salausmenetelmiä	x		x	x
Toimintakykyisyys yhden tukiaseman varassa	x			
Päätelaitteiden kytkeminen pois verkosta	x		x	x
Näppäinlukitus	x	x*	x	x
PIN- ja PUK-koodit	x	x*	x	x
Päätelaitteen räjähdyssuojaus	x*	x*	x*	x*
Transmission inhibit -toimintatila	x			
* Ominaisuus voi sisältyä joidenkin valmistajien laitteisiin tai ohjelmistoihin.				

Kuvio 3: Radio- ja matkapuhelintekniikoiden vertailutaulukko

Kaikissa vertailuun osallistuvissa järjestelmissä on tällä hetkellä käyttövalmiita verkkoja, eli kukin järjestelmä on organisaatioiden käytettävissä. Viranomaiset ovat Suomessa TETRA:n pääasiallinen käyttäjäryhmä, mutta mikään ei tiettävästi rajoita sen hyödyntämistä myös muilla aloilla, kuten esimerkiksi teollisuudessa ja kuljetusalalla. Analogisten radiopuhelinten käyttö on jatkuvasti vähenemässä, mutta tekniikan lopullinen poistuminen käytöstä tulee todennäköisesti kestämään vielä pitkän aikaa. GSM on ollut yleisin matkapuhelinjärjestelmä jo 90-luvulta lähtien ja sen valta-asema tavanomaisissa matkapuhelimissa tulee säilynemään vielä useampia vuosia, vaikka kolmannen sukupolven verkot, kuten UMTS, tulevat varmasti kasvattamaan markkinaosuuttaan lähitulevaisuudessa. Matkapuhelinpalveluiden tarjonta ja kysyntä kasvaa, nopeampien datayhteyksien tarve lisääntyy sekä operaattorit pyrkivät toimintoja tehostaessaan vähitellen luopumaan rinnakkaisten verkkojen ylläpitämisestä.

TETRA ja UMTS kykenevät muodostamaan puheyhteyden nopeudella, jonka voidaan sanoa olevan lähes välitön. Vertailutaulukossa lähes välittömän puhelunmuodostuksen viiveen ajatellaan olevan alle sekunnin luokkaa. UMTS kykenee muodostamaan puheyhteyden noin alle sekunnin viiveellä TETRA:n ollessa tätäkin nopeampi alle puolen sekunnin viiveellä. Perinteinen radiotekniikka tai GSM eivät pysty vastaaviin nopeuksiin.

TETRA:ssa on kattavat puheluominaisuudet, joihin sisältyy sekä kahdensuuntainen (full-duplex) että yhdensuuntainen (half-duplex) viestintä. Analogiset radiot kykenevät vain yhdensuuntaiseen viestintään, jossa kaikki samaa kanavaa kuuntelevat henkilöt muodostavat käytetyn puheryhmän. GSM ja UMTS muodostavat tavallisesti kahdensuuntaisia puheluita, mutta GSM:n laajennus GSM-R lisää radiopuhelimen kaltaisen toiminnallisuuden, kuten yhdensuuntaiset ryhmäpuhelut, puheryhmien käytön sekä TETRA:n vastaavia toimintoja rajoitteellisemmat hätäpuhelut ja puheluiden tärkeysjärjestyksen määritykset. TETRA, GSM ja UMTS pystyvät muodostamaan puheluita omasta verkostaan myös muilla tekniikoilla toteutettuihin verkkoihin. GSM:n ja UMTS:n kohdalla yhteensopivuus on erityisen tärkeää, koska verkkoja käytetään vielä useampia vuosia rinnakkain.

GSM- ja UMTS–puhelimilla hätäpuhelulla tarkoitetaan mahdollisuutta soittaa yleiseen hätänumeroon ilman käyttäjän tunnistusta PIN–koodilla. TETRA:ssa sekä osin GSM-R:ssä hätäpuhelun vastaanottaja ei ole rajoitettu vain yleiseen hätänumeroon, vaan puhelu voidaan olla määritetty vastaanotettavaksi verkon komentokeskukselle tai johonkin tiettyyn puheryhmään.

Puhepalveluidensa monipuolisuuden ja puhedatan välittämisen osalta TETRA vaikuttaa olevan muita vertailukohteita huomattavastikin parempi. TETRA on ainoa järjestelmä, jossa voidaan käyttää suoria puheyhteyksiä, luoda väliaikaisia tilannekohtaisia puheryhmiä sekä seurata

monia puheryhmiä samanaikaisesti. Puheluiden tärkeysjärjestyksen määritykset ja puheryhmien muodostus sisältyvät samankaltaisina myös GSM-R:n ominaisuuksiin.

Tekstiviestipalvelu on olemassa käytännössä samanlaisena sekä TETRA, GSM- että UMTS–järjestelmissä. TETRA:ssa tekstiviestipalvelua käytetään kuitenkin myös useissa muissa palveluissa tiedonsiirron jatkeena. Esimerkiksi paikannuspalvelujen käsittelemän datan siirto voi tapahtua dataviesteillä. Statusviestit eroavat tekstiviesteistä siten, että niillä on tarkoitus välittää vain lyhyitä sanomia, joita käyttäjien ei itse tarvitse kirjoittaa. Statusviestit toimivat usein automaattisesti tietyissä tilanteissa ja siksi statusviestipalvelu ei ole välttämätön erillisenä, mikäli tavalliset tekstiviestit ovat käytettävissä. Statusviestejä käytetään tavallisesti vain radioverkoissa, kuten TETRA:ssa ja joissakin tietyissä analogisissa radiopuhelinmalleissa.

Piirikytkentäinen tiedonsiirto on osana kaikkia radio- ja matkapuhelinjärjestelmiä, mutta nykyisin käytännössä kaikkien verkkotekniikoiden on tuettava pakettimuotoista tiedonsiirtoa, jotta laitteet ja palvelut olisivat keskenään yhteensopivia. Esimerkiksi Internet–yhteydet ja suurin osa nykyisin tarjotuista datapalveluista perustavat toimintansa pakettimuotoiselle tiedonsiirrolle. Pakettimuotoisen datan tukeminen mahdollistaa puhelimen kytkemisen esimerkiksi tietokoneeseen, jolloin niiden välillä voidaan siirtää tiedostoja.

Tiedonsiirron nopeuden osalta UMTS on vertailtavista tekniikoista kapasiteetiltaan selkeästi suurin. Lisäksi 3G:n datasiirto kehittyy yhä edelleen nopeammaksi kolmannen sukupolven laitteiden yleistyessä ja alan kilpailun edetessä. TETRA alkaa olla nykyajan mittapuun mukaan datasiirron kapasiteetiltaan pieni: mitä vahvempaa salauksen tasoa käytetään, sitä hitaammaksi siirtonopeus laskee. Turvallisuusominaisuudet kuluttavat kapasiteettia muulta liikenteeltä. Puhepalveluiltaan TETRA on ylivoimainen, mutta datasiirron puolesta 3G on verratuista vaihtoehdoista paras.

GPS–paikannuspalvelu on erityisen käyttökelpoinen TETRA–verkon toiminnassa, sillä se mahdollistaa päätelaitteiden reaaliaikaisen seurannan etäisyyksistä riippumatta. Myös GSM- ja UMTS–puhelimiin on tarjolla monia palvelusovelluksia, jotka ovat toteutettu GPS:n avulla. Yhdysvaltalainen GPS on toistaiseksi käytännössä vallitsevassa asemassa satelliittipaikannusjärjestelmissä, mutta venäläinen GLONASS, eurooppalainen Galileo ja kiinalainen COMPASS tulevat suurella todennäköisyydellä nousemaan kilpailevaan asemaan tulevaisuudessa.

Direct Mode Operation –toimintatilaa on mahdollista käyttää ainoastaan TETRA:ssa sekä joidenkin valmistajien analogisilla radiolaitteilla. GSM ja UMTS eivät sisällä DMO–ominaisuutta. DMO:n tekee erittäin hyödylliseksi se, että sen avulla viestiliikennettä voi

jatkaa rajoitetusti myös verkon toiminta-alueen ulkopuolella ilman tukiasemia. Lisäksi TETRA kykenee ylläpitämään päätelaitteiden toiminnan jopa verkkoyhteyden katketessa vain lähimmän toimintakykyisen tukiaseman varassa. Verkon kautta toimivat palvelut eivät kuitenkaan ole käytettävissä. Muissa radio- ja matkapuhelinjärjestelmissä vastaavaa ominaisuutta ei ole.

Matkapuhelinjärjestelmälle keskeisiä turvaominaisuuksia ovat kyky salata verkkoliikenne sekä todentaa verkossa käytettävien päätelaitteiden ja itse käytettävän verkon oikeellisuus. Kaikkiin, paitsi analogiseen radiotekniikkaan, sisältyy salausmenetelmiä tietoliikenteen turvaamiseksi. GSM:ssä on nykytarpeisiin nähden verrattain hyvinkin heikko salaus, koska salaukseen käytetyt algoritmit alkavat olla jo vanhentuneita. UMTS on kehitetty käytännössä GSM:n verkon korvaajaksi, joten sen käyttämät salausmenetelmät ovat vahvempia. TETRA:ssa kaikki liikenne on salattua kaikissa yhteyden vaiheissa ja käytettävissä voi olla kaksikin salausmenetelmää samanaikaisesti.

Perinteiseen radiotekniikkaan ei sisälly päätelaitteiden tai verkon todennusta. GSM:ssä todennetaan päätelaite, mutta käytössä olevan verkon aitoutta ei vahvenneta. UMTS ja TETRA sisältävät molemmansuuntaisen todennuksen, jolloin sekä päätelaite että verkko varmennetaan salausavaimin. Tämä tekee päätelaitteiden sekä verkon väärentämisen mahdottomaksi. Operaattori tai muu verkon ylläpitäjä voi estää väärennettyjen, hukattujen, varastettujen tai käytöstä poistettavien päätelaitteiden käytön verkon yhteydessä. TETRA:ssa tämä toiminnallisuus on laajempi: päätelaitteen väliaikaisen käytöstä poistamisen lisäksi se voidaan myös verkon välityksellä tehdä kokonaan toimintakyvyttömäksi, jolloin ainoastaan laitevalmistaja voi avata laitteen uudelleenkäytettäväksi. Tällaisilla ominaisuuksilla estetään tehokkaasti päätelaitteiden käyttö verkkoa hyödyntävää organisaatiota vastaan.

Matkapuhelimiin sisältyy tavallisesti näppäimien vahingollisten painallusten estävä lukitusominaisuus eli näppäinlukitus, käyttäjän todentava PIN–koodi sekä päätelaitteen tarvittaessa todentava PUK-koodi. Nämä ominaisuudet sisältyvät sellaisinaan tavallisesti myös TETRA-puhelimiin ja ne voivat sisältyä myös analogisiin radiopuhelimiin valmistajasta riippuen. Matka- ja radiopuhelimia on mahdollista saada myös räjähdyssuojattuina, mutta tätä vaativien käyttäjätahojen ulkopuolella räjähdyssuojattuja laitteita käytetään harvoin. Päätelaitteen aiheuttaman sähkömagneettisen säteilyn minimoimisen mahdollistava toimintatila (transmission inhibit) sisältyy ainoastaan TETRA-puhelimiin. Tämä ominaisuus on erityisen käyttökelpoinen sairaalaympäristössä, jossa on paljon radioaalloille herkkiä laitteita.

5 Radio- ja matkapuhelinverkkojen riskit

Riski voidaan ymmärtää monella tavalla. Ei-teknisissä yhteyksissä sillä usein viitataan tilanteisiin, joissa on mahdollista tapahtua jotakin, mitä ei haluta tapahtuvan. Teknisissä yhteyksissä riskillä on puolestaan useita merkityksiä. Riski voi olla jokin tietty epätoivottu tapahtuma, joka voi tapahtua tai ei välttämättä tapahdu; riski voi olla myös tämän tapahtuman syy tai todennäköisyys sen tapahtumiselle. Jotkut riskianalyytikot puolestaan pitävät nykyisin ainoana oikeana käyttötarkoituksena riskin ymmärtämistä epätoivotun tapahtuman tilastollisena odotusarvona, joka lasketaan tapahtuman todennäköisyydestä ja sen vakavuuden asteesta. Riski voi olla myös jonkin päätöksen tekeminen tiedostaen siihen liittyvät epävarmuudet. (Hansson 2007.)

Matkapuhelinverkon langattomuus on mullistanut tietoliikenteen viimeisten kahden vuosikymmenen aikana. Langattomien tietoverkkojen ja päätelaitteiden yleistyminen kuitenkin lisää niiden haavoittuvuutta väärinkäytöksille ja vahingoille. Verkon suunnittelijoiden, laitevalmistajien, palveluntarjoajien ja loppukäyttäjien aktiivisuus ja yhteistyö on tärkeää turvallisuuden parantamiseksi ja turvallisuusriskien minimoimiseksi. Käytettävyys kärsii, jos kaikkiin mahdollisiin uhkakuviin halutaan varautua tehokkaasti, mutta liian heikosti suojattu järjestelmä voi toisaalta mahdollistaa väärinkäytön. (Penttinen 2006b, 183-186.)

Seuraavassa käydään läpi matkapuhelinverkkojen keskeisiä riskejä, jotka voivat johtua verkkotekniikasta, päätelaitteesta tai käyttäjästä itsestään. Lisäksi on olemassa myös moninaisia verkkojen infrastruktuureihin ja toiminnallisuuteen vaikuttavia luonnonriskejä, mutta työn rajauksen vuoksi niitä ei tässä opinnäytetyössä käsitellä tarkemmin.

5.1 Verkkotekniikan riskit

Matkapuhelinverkon tekniikka sisältää monenlaisia riskejä ja uhkakuvia. Verkko ei aina välitä liikennettä riittävän nopeasti tai oikein tai verkko voi kaatua kokonaan. Verkkoa uhkaavat myös hyökkääjät, jotka tekijästä riippuen voivat aiheuttaa suurtakin vahinkoa. Langaton verkko on lisäksi altis erilaisille häiriöille eikä sitä voida suojata samoin keinoin kuin perinteistä langallista verkkoa. Tekniikan yleistyessä voi ilmetä myös yhteensopivuusongelmia.

5.1.1 Radiosignaalin ongelmat

Tyhjiössä radiosignaalit kulkevat valonnopeudella taajuudesta riippumatta, eli ne noudattavat suoraa linjaa, jos ei oteta huomioon painovoiman vaikutuksia. Mikäli tällainen linja on

olemassa lähettäjän ja vastaanottajan välillä, sitä kutsutaan näkölinjaksi. Kuitenkin jopa tyhjiössä signaaliin tulee hävikkiä. Vastaanotettu teho riippuu signaalin aallonpituudesta sekä vastaanottimen herkkyydestä ja lähettimen antenneista. Tilanne mutkistuu välittömästi, jos mitä tahansa ainetta ilmestyy lähettäjän ja vastaanottajan välille. Useimmiten signaalit matkaavat ilmakehän kautta ilman, sateen, lumen, sumun, pölyhiukkasten tai savusumun läpi. Hävikki ei aiheuta suuria ongelmia lyhyillä etäisyyksillä, mutta ilmakehä vaikuttaa merkittävästi pitkien matkojen lähetyksiin. Sääolot, kuten rankkasade, vaikuttavat matkapuhelinjärjestelmiin, koska sade voi imeä huomattavan määrän antennin säteilemää energiaa. Tästä syystä tietoliikenneyhteydet voivat sateen alkaessa romahtaa välittömästi. (Schiller 2001, 30-31.)

Paitsi sääolot, myös ympäristö vaikuttaa signaalin kulkuun. Matkapuhelimia käytetään paljon kaupungeissa ja rakennusten sisällä sekä myös haastavissa maasto-olosuhteissa, kuten vuoristoissa ja laaksoissa. Suuret kohteet, kuten rakennukset, voivat aiheuttaa radiosignaalien täydellistä tukkeutumista tai varjostumista. Signaalin taajuudesta riippuen myös pienemmät kohteet, kuten puut tai autot, voivat estää sen kulun. Signaali voi myös heijastua, jos sen kohde on suuri verrattuna signaalin aallonpituuteen, esimerkiksi iso rakennus. Esteet imevät signaalin tehoa, joten heijastunut, vastaanotettu signaali ei ole yhtä voimakas kuin alun perin lähetetty signaali. Mitä useammin signaali heijastuu eli ”pomppii” kohteesta toiseen, sitä heikommaksi se tulee. (Schiller 2001, 31.)

Radiosignaalin aallot voivat myös sirota. Jos signaalin reitillä olevan esteen koko on yhtä suuri tai pienempi kuin sen aallonpituus, tuleva signaali sirottuu useiksi heikommiksi signaaleiksi. Merkillepantavaa on se, että radiolähetyksen tyypillinen aallonpituus on muutaman kymmenen senttimetrin suuruusluokkaa, joten monet ympäristön esteet voivat aiheuttaa sirontaefektiä. Diffraktio on toinen radiosignaalin aalto-ominaisuuksiin liittyvä riski; siinä radioaallot poikkeavat suunnastaan esimerkiksi mäenkukkulan huipulla ja leviävät eri suuntiin. (Schiller 2001, 32.)

Edellä mainituista ilmiöistä seuraa yksi vakavammista radiokanavan toimintaan heikentävästi vaikuttavista ilmiöistä, joka on monitie-eteneminen. Lähettäjältä lähteneet signaalit voivat joko mennä esteettömästi suoraan vastaanottajalle, ne voivat heijastua suuresta esteestä tai sirota pienemmistä esteistä. Valonnopeuden äärellisyydestä johtuen signaaleilla on lukuisia eri teitä lähettäjältä vastaanottajalle, joten ne saapuvat perille eri aikoihin; tämä ilmiö tunnetaan hajaviiveenä. Alkuperäinen signaali on hajonnut ja jotkin osat viivästyvät. Langallisissa verkoissa tätä ei esiinny, koska kaapeli ohjaa aallot yhtä reittiä perille; optisissa siirroissa monitoimikuiduissa voi kuitenkin esiintyä hajontaa suurten bittimäärien osalta. Hajaviiveellä ei ole kuitenkaan mitään tekemistä lähettäjän tai vastaanottajan mahdollisen

liikkumisen kanssa, koska esimerkiksi GSM sietää 16 ms hajaviivettä eli yli kolmea kilometriä matkassa, kun viiveen tyypillinen arvo kaupungeissa on 3 ms. (Schiller 2001, 32.)

Hajaviiveen vaikutukset tietoa sisältäville signaaleille voivat olla jopa ratkaisevia. Todellisessa tilanteessa, joissa mahdollisia reittejä on satoja, yksi impulssi johtaa moniin heikompiin impulsseihin vastaanottajan päätelaitteessa. Vastaanotetuilla impulsseilla on eri tehoja, koska jokaisella reitillä on erilainen vaimennus. Liian heikot impulssit ilmenevät taustakohinana, eli niitä ei pystytä havaitsemaan. Lähetysvirheitä ja väärinymmärryksiä vastaanottajapuolella voi aiheutua, jos impulssit häiritsevät toisiaan eli menevät ajallisesti toistensa päälle. Impulssit edustavat jotakin tiettyä symbolia, joten energia, joka on tarkoitettu yhdelle symbolille, pilaa nyt viereisen symbolin. Symbolien välinen häiriö eli ISI (InterSymbol Interference) rajoittaa radiokanavien kaistanleveyttä, koska suurempi lähetettävän symbolin arvo pahentaa ISI:n vaikutuksia; alkuperäiset symbolit siirtyvät yhä lähemmäksi toisiaan. Riskiä voi pienentää, jos lähettäjä lähettää kokeilujakson, jonka vastaanottaja tuntee. Sitten vastaanottaja vertailee vastaanotettua signaalia kokeilujaksoon ja ohjelmoi tämän perusteella taajuusvasteen korjaajan eli ekvalisaattorin, joka kompensoi vääristymän. (Schiller 2001, 32-33.)

Hajaviivettä ilmenee jo kiinteissä radiolaitteissa, joten lähettäjän, vastaanottajan tai molempien mahdollinen liikkuminen lisäävät riskiä. Lähettäjän ja/tai vastaanottajan liikkuminen aiheuttaa sen, että radiokanavan ominaisuudet ja signaalin kulkureitit voivat muuttua, jolloin vastaanotetun signaalin teho voi vaihdella huomattavasti. Nopeita muutoksia vastaanotetussa signaalissa kutsutaan hetkelliseksi häipymiseksi. Kulkureiteistä riippuen signaalit voivat olla eri vaiheessa ja kumota toisiaan, joten vastaanottajan pitää yhä uudelleen ja uudelleen sopeutua kanavan vaihteleviin ominaisuuksiin muuttamalla ekvalisaattorin parametreja. Jos muutokset ovat liian nopeita, esimerkiksi ajettaessa moottoritiellä, vastaanottaja ei kykene sopeutumaan riittävän nopeasti, joten lähetyksen virheiden määrä kasvaa merkittävästi. Hiljalleen häipyminen on lisäefekti, jonka voi aiheuttaa esimerkiksi vaihteleva etäisyys lähettäjään tai useampi etäinen este. Lähettäjä voi kompensoida pitkällä aikavälillä tapahtuvaa häipymistä muuttamalla lähetystehoa tilanteen mukaan suuremmaksi tai pienemmäksi niin, että vastaanotettu signaali pysyy tiettyjen rajojen sisällä. Doppler-ilmiö eli aaltoliikkeen taajuudessa, vaiheessa tai aallonpituudessa tapahtuva muutos on myös lähettäjän ja vastaanottajan liikkumisesta johtuva efekti. (Schiller 2001, 33-34.)

5.1.2 Verkon kaatuminen

Matkapuhelinverkon kaatuminen voi tapahtua tahattomasti tai tahallisesti. Suomessa ja ulkomailla on tapahtunut verkkovikoja, jotka ovat mykistäneet jopa miljoonien käyttäjien

puhelimia. Tahattomat viat voivat johtua esimerkiksi virransyötön katkeamisesta operaattorin laitteisiin tai operaattorin ohjelmistoihin liittyvistä ongelmista. Verkko voidaan myös kaataa tahallisesti palvelunestohyökkäyksellä; hyökkäyksellä pyritään aiheuttamaan ruuhkaa verkkoon niin, että kapasiteettia kuluu turhaan tai koko palvelut hidastuvat ja sitten kaatuvat. Palvelunestohyökkäyksestä kerrotaan enemmän tietoturvauhkat-osiossa.

Suomessa tämän vuoden helmikuussa mykistyi noin miljoona Elisan, Saunalahden ja Kolumbuksen liittymää Vaasa-Mikkeli -linjan pohjoispuolella. Vika sai alkunsa Elisan laitetilassa tapahtuneen sähkönsyötön katkeamisesta. Huomioitavaa on kuitenkin, että verkkokatkos ei estänyt hätäpuheluiden soittamista, sillä Suomessa hätäpuhelut ohjautuvat katkosten aikana keskuksiin muiden operaattoreiden kautta. Vuonna 2007 Elisan verkossa oli vielä suurempi häiriö, joka koski noin kahta miljoona matkapuhelinliittymää. (Iltalehti 2011.)

Saksassa puolestaan kaatui vuonna 2009 maan suurimman operaattorin T-Mobilen verkko. Operaattorilla oli silloin noin 40 miljoonaa käyttäjää Saksassa. Deutsche Telekomin mukaan verkon kaatuminen johtui ohjelmistovirheestä. Vika esti kokonaan puheluiden ja tekstiviestien menemisen läpi. Varsinainen toimintahäiriö kesti noin kolme tuntia, jonka jälkeen ongelmat jatkuivat yhä, joskin lievemmässä muodossa. (Tietokone 2009.)

5.1.3 Verkon ruuhkautuminen

Matkapuhelinverkot rakennetaan normaalikäytön tarpeisiin. Tyypillisesti tukiasemat sijoitetaan mahdollisimman korkeille paikoille niin maaseudulla kuin kaupungeissa, jotta maastolliset esteet haittaavat mahdollisimman vähän radiosignaalin kulkua. Normaali tukiasema kykenee välittämään noin 15-40 käyttäjän puhelut ja viestit samanaikaisesti. Kapasiteetti voi kuitenkin ylittyä, jos verkkoon tulee nopeasti paljon samanaikaista liikennettä. (Elers 2011.)

5.1.4 Tietoturvauhkat

Verkkohyökkäykset ovat merkittävä riskitekijä, koska niitä ei voida ennakoida ja seuraukset voivat olla hyvin vakavia. Pakettipohjaisessa televerkossa ulkoiset rajapinnat kytkeytyvät IP-verkkoon GGSN:n (Gateway GPRS Support Node) välityksellä ja tähän kokonaisuuteen sisältyy palomuuritoiminnot, mutta palomuurin suojaus voidaan kumota riittävän suurella signalointikuormalla. Kaiken lisäksi verkosta tullutta hyökkäystä ei välttämättä huomata heti, vaan seuraukset voivat ilmetä vasta myöhemmin verkon ja palvelujen epämääräisenä toimintana. Matkapuhelinverkoissa on kolme pääaluetta, joita voidaan käyttää väärinkäytöksiin: radiorajapinta, muu verkon osa sekä päätelaite tilaajakortteineen. Kaikkien

tiedonsiirtoketjun osien tehokas suojaaminen on ainoa keino suojata verkko aukottomasti. (Penttinen 2006b, 185-192.)

Tietoverkkoihin kohdistuvista hyökkäyksistä puhutaan yleensä hakkerointina tai krakkerointina. Hakkeroinnilla tarkoitetaan yleisesti tunkeutumista verkkoon luvattomasti, kun taas krakkerointi on suojausten murtamista. Hyökkäysten vaikutus riippuu suuresti tunkeutujan motivaatiosta tuottaa vahinkoa. Tunkeutuja voi saada verkko-oikeudet tunnuksineen, mutta ei välttämättä halua tehdä enempää vahinkoa; toisaalta joku toinen haluaa samassa tilanteessa tuhota, vahingoittaa ja muuttaa tietoa. Jos tunkeutuja on tarpeeksi pahantahtoinen, hän voi myös muuttaa käyttöoikeuksia ja estää oikeutettujen käyttäjien pääsyn järjestelmään. Ilman käyttöoikeuksiakin tunkeutuja voi esimerkiksi lähettää väärennettyjä viestejä ja saada verkon toimimaan virheellisesti palvelunestohyökkäysten kautta. (Penttinen 2006b, 185-186.)

Tietoyhteiskunta on niin riippuvainen tietoliikenneyhteyksistä, että tietoverkon lamauttaminen voi aiheuttaa ennalta arvaamattomia, jopa katastrofaalisia kerrannaisvaikutuksia. Matkapuhelinverkkojen radiorajapinta on monimutkainen, joten tietomurron tekeminen ei ole yksiselitteistä. Alun perin salaiset algoritmit on mahdollista löytää nykyisin Internetistä, mutta yhteyksien purkaminen radiorajapinnalla ei kuitenkaan onnistu suoraan. Asiansa tunteva tunkeutuja voi kuitenkin löytää algoritmeista mahdollisia aukkoja ja siten purkaa yhteyksien suojauksen taltioimalla radiorajapinnan yhteyden. (Penttinen 2006b, 187.)

Palomuurin horjuttaminen on hyökkääjän ensisijainen tavoite, koska järjestelmään on sen jälkeen helpompi päästä. Palomuurin toimintaa voidaan heikentää monella tavalla. Palvelimelle voidaan lähettää niin paljon datapaketteja, että kevyesti suojattu palomuuri ylikuormittuu liian suuresta tietoliikenteestä. Palomuurin kuormittumisen jälkeen ohjelmistoon ja käyttöjärjestelmään voidaan yrittää hyökätä. Palomuurin hallintaohjelmistoon voi päästä lähettämällä liian isoja paketteja, jolloin hyökkääjä pystyy tekemään esimerkiksi omia virtual server -määrityksiään. (Penttinen 2006b, 188-189.)

Päätelaitteille voidaan ajaa viruksia Javaa tai vastaavia ympäristöjä käyttämällä; ne voivat esimerkiksi ottaa puhelimen toiminnot hallintaansa käynnistämällä puheluja. OTA-menetelmä (over the air) on hyvä keino SIM-kortin tietojen automaattiseen päivittämiseen, mutta samalla sitä voidaan käyttää verkkohyökkäykseen. Ensimmäiset matkapuhelimiin tarttuvat virukset tulivat vuonna 2004; kyseessä oli Bluetooth-yhteyden kautta siirtyvä koodi, josta ei sinällään ollut suurta harmia, mutta oli kuitenkin varoitus siitä, mitä on mahdollista tehdä. Haittakoodeja voidaan yrittää lähettää puhelimen omien tietoyhteyksien kautta tai verkosta käsin esimerkiksi merkinantoyhteyden avulla. Matkapuhelimien käyttöjärjestelmäalustojen

kehitystyöstä on paljolti kiinni, miten riittävät suojaukset otetaan huomioon eri matkapuhelinversioissa. (Penttinen 2006b, 187-188.)

Palveluntarjoajan palvelimet voivat olla heikko lenkki teleinfrastruktuurissa, sillä ne eivät suojaukseltaan ole välttämättä verkko-operaattorin suojausten tasoisia. Siten hyökkääjä voi aiheuttaa operaattorille paljon harmia. Hyökkääjä voi lähettää roskapostin tyylisiä viestejä suoraan päätelaitteisiin, jotka voivat pahimmassa tapauksessa estää koko tekstiviestipalvelun. Näitä niin sanottuja palvelunestohyökkäyksiä tehdään hyödyntämällä ohjelmistojen virheitä tai puutteita. Hyökkäyksellä pyritään aiheuttamaan verkon kapasiteetin ja resurssien ylimääräinen kulutus, järjestelmien tai sovelluksien hidastuminen tai jopa koko järjestelmän ja palvelujen kaatuminen. (Penttinen 2006b, 188.)

Dataa ja erilaisia tekijänoikeuksilla suojattuja palveluita on mahdollista varastaa. Tiedon sisältöä on myös mahdollista manipuloida muokkaamalla, lisäämällä, toistamalla tai poistamalla viestejä. Lisäksi tunkeutuja voi pyrkiä hankkimaan itselleen rahallista hyötyä esimerkiksi järjestämällä ilmaista puheaikaa, vaikeuttamalla laskutusta tuhoamalla laskutuslippuvaraston tai vaihtamalla omia tilaajapalveluitaan. Dataliikennettä seuraamalla voi myös selvittää käyttäjän sijainnin tai syyn jonkin viestin lähettämiseen, vaikka itse viestin sisältöä tunkeutuja ei saisikaan selville. Tämä onnistuu tutkimalla viestin ominaisuuksia, joita ovat mm. viestin pituus, lähettäjän ja vastaanottajan osoite ja viestittelytiheys. (Penttinen 2006b, 189-191.)

Toisen sukupolven matkaviestinverkkoja vaivaavat monet puutteet, jotka mahdollistavat verkkohyökkäyksiä. Valetukiaseman avulla voidaan tehdä aktiivisia hyökkäyksiä huomaamattomasti. Lisäksi käyttäjien tunnistukseen ja radiorajapinnan salaukseen tarkoitetut tiedot liikkuvat suojaamattomina verkossa. GSM:n salaus toimii myös ainoastaan päätelaitteen ja tukiaseman välillä. (Penttinen 2006b, 190.)

Kolmannen sukupolven verkoissa tietoturvapuutteet on pyritty ottamaan huomioon esimerkiksi molemminpuolisella tunnistuksella, mutta verkkojen kehittyessä on ilmennyt uusia riskejä. Verkko-operaattorien määrä kasvaa jatkuvasti langattomien verkkojen käytön kasvaessa ja käyttäjän mahdollisuudet oman liittymänsä palvelujen hallintaan lisääntyvät. Datapalveluiden merkitys kasvaa, kuten myös päätelaitteen merkitys sähköisen kaupankäynnin välineenä.

5.1.5 Yhteensopivuusongelmat

Televerkkojen kehityksestä saatujen kokemusten pohjalta voidaan päätellä, että verkkotekniikan yhteensopivuuden hallinta on haasteellista. Ongelmia voi ajoittain esiintyä

siitäkin huolimatta, että järjestelmät ja palvelut pyritään kehittämään avointen rajapintojen periaatteiden mukaisiksi, valmistajasta riippumattomiksi standardeiksi. Matkapuhelinverkkojen yhteensopivuusongelmia aiheuttavat uudet järjestelmät ja toteutukset sekä eri aikoina suoritetut ohjelmisto- ja laitteistoversioiden päivitykset. Uudet versiot ja toteutukset eivät aina ole spesifikaatioiden mukaisia, joten operaattoreiden, laitevalmistajien ja palveluntarjoajien voi olla haasteellista saada järjestelmät ja palvelut toimivaksi ja luotettavaksi kokonaisuudeksi. (Penttinen 2006b, 183-185.)

5.2 Laiteriskit

Myös puhelimessa tai päätelaitteessa on riskejä. Laite voi hajota teknisestä syystä tai käyttäjän vahingon seurauksena. Sääolot vaikuttavat myös puhelimen kestävyyteen. Lisäksi puhelimen käyttö synnyttää säteilyä, joten pitkäaikainen altistuminen sähkömagneettisuudelle voi muodostaa terveysriskin. Puhelimet ovat myös herkkiä häiriöille, joita muodostavat muut läheisyydessä olevat sähkölaitteet. Häiriöriskiä lisää myös puhelinten tyyppihyväksyntävaatimusten keventäminen.

5.2.1 Puhelimen hajoaminen

Puhelin voi hajota monella tavalla. Se voi pudota käyttäjältään ja hajota maahan osumisen seurauksena, yksittäinen komponentti voi pettää (esimerkiksi näyttö tai akku) tai koko laite voi jopa räjähtää. Lisäksi kosteus on tunnetusti sähkölaitteille suuri riski, joten veteen joutuessaan puhelin menee todennäköisesti epäkuntoon varsin nopeasti. Myös äärimmäiset lämpötilat ovat puhelimen kestävyydelle riski.

Nykyisten matkapuhelimien ominaisuudet ovat monipuolisuudessaan 90-luvun puhelimiin verrattuna aivan eri tasolla. Viat ovat kuitenkin samalla lisääntyneet ja puhelinten yleinen luotettavuus on heikentynyt. Puhelimissa on jopa rakenteellisia ongelmia, jotka voivat vahingoittaa sitä normaalissakin käytössä. Ohjelmistojen osuus luotettavuusongelmiin on myös merkittävä, jos sitä mitataan puhelimiin tehtävillä huoltotoimenpiteillä; huollossa tehdään yhä useammin ohjelmistopäivitys ainoana toimenpiteenä. Ohjelmistot tulevat markkinoille keskeneräisinä, mistä seuraa pikkuvikaisuutta ja jatkuvaa päivittämistarvetta. (It-viikko 2010.)

Puhelin voi myös hajota vakavin seurauksin; puhelimen räjähtämisestä on paljon esimerkkejä maailmalta. Vuonna 2009 Intiassa oli kaksi tapausta, joista ensimmäinen tapahtui tammikuussa: nainen kuoli puhuessaan ladattavana olleeseen kiinalaisvalmisteiseen puhelimeen, kun se räjähti. Elokuussa puolestaan nuori mies kuoli Nokia 1209 -puhelimen

räjähdyksen aiheuttamien vammojen vuoksi. Miehen ruumiin vierestä löydettiin puhelimen ja akun sirpaleita. (Digitoday 2010.)

Kiinassa on tapahtunut useita kuolintapauksia. Vuonna 2007 22-vuotias kiinalaismies menehtyi hänen rintataskussaan olleen Motorola-puhelimen räjähdettyä. Valmistaja ei kuitenkaan ollut välttämättä syyllinen vaan puhelimen altistuminen korkeille lämpötiloille, sillä uhri työskenteli rautamalmin käsittelylaitoksella. Korvaukset jäivätkin työnantajan eikä Motorolan maksettaviksi. (Digitoday 2007.) Vuonna 2009 kaupassa työskennellyt nuori mies laittoi puhelimeensa täyteen ladatun uuden akun, jonka jälkeen se räjähti ja tappoi miehen. Kaupassa ollut toinen työntekijä kuuli kovan pamauksen, jonka jälkeen hän löysi uhrin maasta. Puhelinvalmistajien mukaan onnettomuuksia aiheuttavat erityisesti halvat väärennetyt akut, joissa ei ole riittäviä suojauksia. (Tietokone 2009.)

Viime vuoden joulukuussa Apple iPhone 4 -puhelimen takalasi räjähti Norjassa, kun eräs norjalaisnainen oli pakkasilmalla matkalla autolla töihin. Nainen yritti saada Applea korjaamaan puhelimen, mutta valmistaja kieltäytyi sääoloihin vedoten; puhelinta voi säilyttää pakkasessa 20 asteeseen asti, mutta sen käyttäminen joko alle 0 tai yli 35 asteessa ei kuulu takuun piirin. (Digitoday 2011.)

Vuonna 2009 helsinkiläinen nainen sai lieviä vammoja, kun hänen Nokia-työpuhelimensa akku räjähti työpaikalla. Myös tässä tapauksessa akku oli ollut latautumassa; puhelin oli lentänyt ilmaan pöydältä ja syössyt liekkejä ympärilleen. Nokia myönsi, että osa kyseisen mallin akuista voi ylikuumentua. (Taloussanomat 2009.) Vuonna 2008 tamperelaisen miehen Nokia N70-puhelin lämpeni tulikuumaksi kesken puhelun. Mies laittoi puhelimen parvekkeelle ja jäi seuraamaan tilannetta ikkunan taakse. Puhelimesta nousi ensin sininen liekki, jonka jälkeen akku pullistui ja puhelin räjähti. Akku oli samanmallinen kuin helsinkiläisnaisen tapauksessa. (Kokkonen 2008.)

5.2.2 Sähkömagneettisuus

Sähkömagneettisuus on hyvin yleinen ilmiö. Sitä esiintyy jo luonnossa Maan ja Auringon aiheuttamien magneettikenttien muodossa, mutta myös ihmisen luomana. Kun mikä tahansa sähkölaite on kytkettynä pistorasiaan eli laitteessa on jännite, on laitteessa ja sen lähiympäristössä sähkökenttä. Laitteen käynnistäminen tuo siihen sähkövirtaa, jolloin muodostuu myös magneettikenttä. Molempien kenttien voimakkuus pienenee nopeasti laitteen pinnan ulkopuolella. Sähkökentän voimakkuus on suurta suurjännitteisten sähkönsiirtolaitteistojen ja suuritehoisten teollisuuslaitteiden läheisyydessä, mutta kodinkoneissa se on hyvin pieni. Magneettikentän lähteet ovatkin yleensä terveydelle merkityksellisempiä kuin sähkökentän lähteet. (Säteilyturvakeskus 2009.)

Matkapuhelimen käyttö muodostaa sähkömagneettisen kentän, jonka avulla puhelin voi muodostaa yhteyden tukiasemaan. Tekniikan kehittyminen on laskenut selvästi puhelimen tehoa ja kentän voimakkuutta, mutta puhelinten käytön yleistyessä kentälle ollaan yhä enemmän ja pidempiä aikoja alttiita. Puhelimeen puhutaan kauemmin ja sitä käytetään yhä monipuolisemmin esimerkiksi Internetin selailun, pelaamisen ja musiikin kuuntelun muodossa. (Cosmos 2010.)

5.2.3 Terveysriskit

Matkapuhelinten käytön on esitetty aiheuttavan hermoston sairauksia, pään alueen kasvaimia tai erilaisia oireita, kuten päänsärkyä. Aiemmin on tutkittu etupäässä aivokasvaimia, mutta kiistatonta yhteyttä matkapuhelimen käytön ja aivokasvaimien välillä ei ole todettu. Terveyshaittojen mahdollisuutta ei ole voitu myöskään sulkea pois. (Pelastustoimi 2009.)

Itävallassa viime vuonna julkaistun tutkimuksen mukaan riski sairastua tinnitukseen on keskimäärin kymmenen minuuttia päivässä puhuvalla henkilöllä merkittävästi suurempi kuin henkilöllä, joka ei juuri matkapuhelinta käytä. Neljän vuoden käyttö puolestaan tuplaa kroonisen tinnituksen riskin. Varmoja yhdistäviä tekijöitä matkapuhelimen käytön ja tinnituksen välillä ei kuitenkaan löydetty, vaan puhelinten säteilyn epäiltiin vaikuttavan haitallisesti korvan sisäosiin ja siten lisäävän kuulovaivojen todennäköisyyttä. (Turun Sanomat 2010.)

Viime vuosikymmenen puolivälissä tehtiin laaja kansallinen HERMO (Health Risk Assessment of Mobile Communications) -tutkimusohjelma, jossa tutkittiin matkapuhelinten lähettämien sähkömagneettisten kenttien vaikutuksia soluviljelmiin, koe-eläimiin ja koehenkilöitä. Syksyllä 2007 julkaistujen tutkimustulosten perusteella tässäkään tutkimuksessa ei löytynyt yksiselitteistä näyttöä terveydelle haitallisista vaikutuksista. (Säteilyturvakeskus 2007.) Vuonna 2006 Säteilyturvakeskus aloitti uuden seurantatutkimuksen, jossa tutkitaan matkapuhelinten käytön mahdollista yhteyttä päänsärkyyn, unihäiriöihin, korvien soimiseen ja masentuneisuuteen sekä neurologisiin sairauksiin. Tuloksia on odotettavissa vuoden 2011 ja 2012 vaihteessa. (Pelastustoimi 2009.)

Koska terveysvaikutusten tutkiminen jatkuu yhä ja jo julkistetut tutkimustulokset ovat keskenään ristiriitaisia, ei lopullista vastausta matkapuhelinten käytön terveysriskikysymykseen voida vielä antaa.

5.2.4 Häiriöt

Toisin kuin perinteisissä langallisissa tiedonsiirtojärjestelmissä, joissa voidaan käyttää suojattua kaapelia, langatonta radiolähetystä ei voida suojata häiriöitä vastaan. Muut sähkölaitteet puhelimen läheisyydessä voivat aiheuttaa vakavia häiriöitä, joiden seurauksena tiedonsiirron hävikki ja bittivirhemäärät kasvavat. (Schiller 2001, 12.)

Taajuudet ovat myös ongelma, koska radiotaajuuksia on rajallisesti ja laitteiden määrä kasvaa jatkuvasti. Kansainvälinen taajuustaulukko määrittelee erityisehtoja, jotka rajoittavat tiettyjen taajuuksien käyttöä; rajoituksia on esimerkiksi langattomille lähiverkoille. Eri maissa on kuitenkin yhä kansallisia säännöksiä, joten Suomeenkin voi tulla laitteita, joita ei tulisi käyttää kyseisellä taajuusalueella. Viestintävirasto pyrkiikin seuraamaan laitteiden markkinointia, jotta tällaisia radiolaitteita ei pääse käyttöön maahan. (Penttinen 2006b, 175.)

Uusien laitteiden ja järjestelmien tullessa markkinoille yhä kasvavassa määrin myös häiriöiden riski radiotaajuuksilla kasvaa. Lisäksi laitteiden luonne nykyisin kulutustavaroina, jotka kestävät vain joitakin vuosia, pahentaa ongelmaa, sillä ne voivat vioittuessaan pahimmillaan estää toisten lähellä olevien radiolaitteiden toiminnan. Esimerkiksi GSM:n päätelaitteiden tyyppihyväksyntävaatimuksia on kevennetty aikaisemmasta merkittävästi: aiemmin puhelimet voitiin hyväksyä vain valtuutetuissa tyyppihyväksyntälaboratorioissa, mutta nykyisin riittää valmistajan vakuutus, että laite täyttää vaatimukset. Ennen käyttäjien oli anottava erillinen taajuuslupa radiolaitteen käyttämiseksi, mutta odotetusti käytännöstä luovuttiin langattomien laitteiden käytön kasvaessa ja nykyisin esimerkiksi puhelinten käyttö on vapaata. (Penttinen 2006b, 175-176.)

5.3 Käyttäjästä johtuvat riskit

Käyttäjä voi omalla toiminnallaan luoda riskejä. Puhelin on vaarassa joutua varastetuksi tai se yksinkertaisesti voi kadota vahingossa. Käyttäjän hyväuskoisuus voi myös johtaa hankaluuksiin, jos puhelimen lainaa edes hetkeksi ulkopuoliselle henkilölle. Puhelimen käyttäjältä edellytetään siis tarkkuutta ja valppautta kaikkina aikoina, etenkin jos kyse on viranomaislaitteesta. Käyttäjä voi itse myös syyllistyä väärinkäytöksiin, jos hänellä on täysin luvalliset laajat oikeudet.

5.3.1 Puhelimen kadottaminen tai joutuminen varastetuksi

Käyttäjä voi kadottaa puhelimensa helposti liikkuessaan. Puhelin voi unohtua autoon, junaan, bussiin tai mihin tahansa kulkuvälineeseen. Puhelin voi jäädä myös jonnekin julkiselle paikalle, jossa on paljon ihmisiä, esimerkiksi ravintolaan, rautatieasemalle, kadulle tai

kauppakeskukseen. Käyttäjä ei välttämättä tajua vahinkoaan kuin vasta myöhemmin, jolloin puhelimen löytäminen on erittäin vaikeaa, ellei mahdotonta. Puhelimen voi myös pudottaa veteen, mikä on vaarana erityisesti kesäisin. Katoamisesta on seurauksena taloudelliset menetykset joko tuhoutuneena laitteena tai laitteen mahdollinen käyttäminen organisaatiota tai yksittäistä henkilöä vastaan tai niiden laskuun.

Puhelin voi tulla myös varastetuksi käyttäjältään, jolloin seuraukset ovat täysin ennalta arvaamattomia. Teini-ikäiseltä pojalta varastettiin Torniossa puhelin tämän vuoden tammikuussa. Liittymä suljettiin vasta noin viikko varkauden jälkeen, jolloin liittymän saldo oli ehtinyt nousta yli 3000 euroon. (Pohjolan Sanomat 2011.) Esimerkkitapauksesta käy hyvin ilmi se, että mikäli puhelimen varastamiseen ei reagoida tarpeeksi nopeasti, seuraukset voivat tulla käyttäjälle hyvin kalliiksi.

5.3.2 Käyttäjän hyväuskoisuus

Puheluita on mahdollista uudelleenreitittää yksinkertaisesti lainaamalla puhelinta hetkeksi. Tällöin voidaan luoda kolmansien osapuolten neuvottelupuhe, jossa lainaaja poistuu ohjausten teon jälkeen itse neuvottelusta. Lainaaja ei välttämättä tapahtunutta huomaa ennen kuin lasku tulee hänen maksettavakseen. (Penttinen 2006b, 189.)

Väärinkäyttäjä voi myös naamioida oman identiteettinsä ja uskotella käyttäjille olevansa verkon laillinen operaattori, vaikka hän on itse asiassa linkitetty väärennetyn verkon kautta. Näin väärinkäyttäjä voi saada käsiinsä luottamuksellista tietoa. Väärinkäyttäjä voi myös käyttää päätelaitetta tietoturva-aukkojen löytämiseksi ja hyväksikäyttämiseksi (Penttinen 2006b, 191.)

6 Riskianalyysi

TETRA–järjestelmän turvallisuutta tutkittiin riskianalyysin avulla. Riskianalyysi perustui Pasi Kämpin ja Robert Guinnessin laatimaan satelliittipaikannusjärjestelmien tekniseen riskianalyysiin, jota varten tehtyä riskianalyysityökalua oli tarkoitus käyttää mallina oman suppeamman analyysityökalun luomiseksi. Työkalua oli sitten hyödynnettävä TETRA–järjestelmän turvallisuuden tutkimiseen. Tämä ei kuitenkaan sulje pois riskianalyysityökalun käyttämistä myös muiden radio- ja matkapuhelinjärjestelmien riskitutkimuksissa, koska työkalun sisältämät riskitekijät ovat kaikkia työssä tutkittuja järjestelmiä yleisesti koskevia. Järjestelmät ovat teknisiltä ominaisuuksiltaan eritasoisia, mutta kuitenkin pohjautuvat samalle radiotekniikan toimintaperiaatteelle ja toisiaan muistuttaville laitteistoille.

Riskianalyysityökalu (kuvio 4) koostuu kuudesta sarakkeesta, jotka ovat riskitekijän kategoria, itse riskitekijät, riskin toteutumisen todennäköisyys, riskin toteutumisen vakavuus, riskitekijän toteutumisen seuraukset ja riskiarvo. Kategorioita on kolme: 1) verkkotekniikan riskit, 2) laiteriskit ja 3) käyttäjästä johtuvat riskit. Kategoriat ovat suoraan opinnäytetyön radio- ja matkapuhelinjärjestelmien riskejä käsittelevästä osiosta, jossa riskit jaettiin samalla tavalla kolmeen alakategoriaan. Riskitekijät–sarakkeessa on esitetty 16 riskitekijää, jotka pohjautuvat riskit-osion sisältämiin riskeihin. Teknisemmät riskitekijät koottiin radio- ja matkapuhelintekniikoita käsittelevistä kirjallisista ja sähköisistä lähteistä ja käytännönläheisemmät riskitekijät kerättiin moninaisista uutislähteistä. Teknisiin riskitekijöihin kuuluivat mm. signaalin kulkua ja verkon toimintaa uhkaavat riskit, kun taas käytännönläheisempiä riskitekijöitä olivat päätelaitteiden käyttöön liittyvät riskit. Viimeksi mainitut riskit eivät ole ainoastaan teoreettisia, vaan ne ovat myös todistettavasti tapahtuneet järjestelmien ja laitteiden arkikäytössä.

Riskin toteutumisen seuraukset–sarakkeen tiedot pohjautuvat sekä tutkittujen tekniikoiden teoriatietoon että riskit–osion sisältämiin tietoihin. Riskin tapahtumisen todennäköisyyden ja tapahtuman vakavuuden asteiden avulla lasketaan yhteenlaskuna riskiarvo, jonka avulla riskitekijät voidaan luetella järjestyksessä pahimmasta riskistä lievimpään riskiin. Tarvitut todennäköisyyden ja vakavuuden asteen arvot hankittiin lähettämällä alan asiantuntijalle riskiarviointilomake. Asiantuntijaksi saatiin Helsingin ja Uudenmaan sairaanhoitopiirin (HUS) valmiuspäällikkö Pekka Koskinen, joten riskianalyysin lähtökohtaiseksi näkökulmaksi valikoitui TETRA:n käyttö sosiaali- ja terveystoimen työtehtävissä.

Riskiarviointilomake (liite 1) on ulkoasultaan muuten sama kuin riskianalyysityökalu, mutta siitä on karsittu sarakkeet riskin kategorialle ja riskiarvolle selkeyden vuoksi. Riskiarviointilomakkeen lisäksi asiantuntijalle toimitettiin myös erillinen lomakkeen täyttöä ja siinä esitettyjä riskitekijöitä tarkemmin selventävä asiakirja. Riskiarviointilomakkeen selvennysosa (liite 2) sisältää opastuksen lomakkeen täyttämiselle ja riskitekijöiden kuvaukset tiivistetyssä muodossa. Lomakkeessa kysyttiin riskien todennäköisyydelle ja vakavuudelle arvoja asteikolla 1-5: 1 on pieni, 2 melko pieni, 3 keskisuuri, 4 melko suuri ja 5 suuri. Arvot siirrettiin työkaluun, jonka jälkeen voitiin laskea jokaiselle riskitekijälle yksilöllinen riskiarvo ja laittaa riskitekijät järjestykseen riskiarvon perusteella suurimmasta pienimpään. Riskiarvot jakautuvat asteikolla 2-10 todennäköisyyden ja vakavuuden asteiden summan mukaisesti.

KATEG.	RISKITEKIJÄT	TODENN.	VAKAVUUS	RISKIN TOTEUTUMISEN SEURAUKSET	RISKIARVO
1	Signaalin estyminen tai pirstoutuminen	3	5	Lähetetty signaali ei tavoita vastaanottajaa.	8
2	Päätelaitteen hajoaminen tai vioittuminen	3	4	Laitteen toimimattomuus.	7
2	Ohjelmistoviat	3	4	Ohjelmiston toimimattomuus.	7
2	Virtalähteen tai virtapiirien kipinöinti	2	5	Räjähdysvaara, henkilövahingot.	7
3	Päätelaitteen hukkaaminen tai katoaminen	3	4	Henkilöstön varomattomuus aiheuttaa tietoturvariskin.	7
3	Päätelaitteen joutuminen varastetuksi	3	4	Päätelaite väärissä käsissä; tietomurrot, salakuuntelu.	7
3	Käyttäjän hyväuskoisuus/päätelaitteen lainaaminen	3	4	Mahdollinen salakuuntelu, huijaukset, identiteettivarkaudet.	7
1	Verkon kaatuminen tai palvelun esto	1	5	Koko verkko tai sen osia ovat poissa käytöstä.	6
1	Verkkohyökkäykset: hakkerointi ja krakkerointi	1	5	Verkon toiminnan häiriöt tai estymiset. Tietomurrot: tiedon kaappaminen, väärentäminen tai tuhoaminen.	6
1	Tietoliikenteen salakuuntelu	1	5	Tiedon kerääminen ja väärinkäyttö, verkon vakoilu.	6
2	Päätelaitteen aiheuttamat sähkömagneettiset häiriöt	1	5	Mahdollisia häiriöitä lähistöllä olevin herkkiin laitteisiin.	6
2	Sähkömagnetismin mahdolliset terveyshaitat	1	5	Henkilöstön pitkäaikaisen altistumisen aiheuttamat vaivat.	6
1	Signaalin saapumisessa esiintyvä hajaviive	1	4	Signaalin havaitseminen vaikeutuu; viestin sisältö muuttuu epäselväksi tai pahimmillaan pelkäksi taustakohinaksi.	5
1	Verkon ruuhkautuminen/kapasiteetin ylittyminen	2	3	Tiedonsiirto katkonaista ja viivästynyttä.	5
2	Laitteistojen ja ohjelmistojen yhteensopimattomuus	2	3	Ongelmat toiminnassa ja luotettavuudessa.	5
2	Päätelaitteeseen vaikuttavat sähkömagneettiset häiriöt	1	3	Signaalin lähettämisen ja vastaanottamisen häiriintyminen.	4

Kuvio 4: Riskianalyysityökalu

Valmiuspäällikkö Pekka Koskiselta saatujen riskiarvioiden pohjalta (liite 3) voidaan havaita, että HUS–organisaatiossa esitettyjen riskien toteutumisen todennäköisyydet koetaan pääsääntöisesti pieniksi ja vakavuudet suuriksi. Kaikki todennäköisyyden asteet ovat korkeintaan keskisuuria tai matalampia: pieniä (1) on seitsemän, melko pieniä (2) kolme ja keskisuuria (3) kuusi. Kaikki vakavuuden asteet ovat puolestaan lievimmillään keskisuuria tai sitäkin korkeampia: keskisuuria (3) on kolme, melko suuria (4) kuusi ja suuria (5) seitsemän. Tästä voidaan päätellä, että TETRA ei ole turvallinen vain dokumentoituna vaan myös käytännössä. Asteista päätellen TETRA:a käytetään vaativassa toimintaympäristössä ja järjestelmässä käsitellään arkaluontoista tietoa, mikä selittää vakavuuden asteiden jakautumisen keskisuureksi ja sitä korkeammaksi. TETRA:n turvallisuus ja luotettavuus ovat kuitenkin niin korkealla tasolla, että todennäköisyyden asteet pysyvät verrattain matalina.

Kuudesta todennäköisyydeltään keskisuuren asteen riskitekijöistä puolet on käyttäjästä johtuvia riskejä, kaksi laiteriskejä ja vain yksi on verkkotekniikan riski. Päätelaitteen käyttäjän toimintaa on vaikea ennakoida, joten inhimillisten virheiden tai laiminlyöntien tapahtumista ei voida olla huomioimatta, vaikka organisaatio luottaakin henkilöstönsä ammattitaitoon ja harkintakykyyn. Melko pieniä tai pieniä todennäköisyyden asteita on viisi sekä verkkotekniikasta että laitteesta johtuvien riskitekijöiden osalta ja asteiden jakauma on hyvin tasainen niiden välillä. Kaiken kaikkiaan verkkotekniikan ja laitteiden riskien toteutumisen todennäköisyyksiä ei pidetä merkittävinä HUS–organisaatiossa.

Seitsemän kuudestatoista vakavuuden asteesta eli lähes puolet on luokitukseltaan suuria, kuusi melko suuria ja keskisuuria on vain kolme. Tämä havainto osoittaa, kuinka tärkeää on ylläpitää TETRA–järjestelmän turvallisuustaso korkealla. Riskien toteutumisen todennäköisyydet eivät saa nousta jatkossakaan suuremmiksi, koska vakavuuden asteiden voidaan olettaa pysyvän samalla tasolla niin kauan kuin organisaation toiminta pysyy samankaltaisena. Esimerkiksi riskin toteutumisen todennäköisyyteen voidaan vaikuttaa omalla toiminnalla, mutta riskin vakavuus muuttuu ainoastaan subjektiivisen näkemyksen perusteella.

Riskiarvot jakautuvat niin, että suurin arvo on kahdeksan ja pienin neljä: molempia ääriarvoja on vain yksi ja loput arvot asettuvat niiden välille. Suurin uhka analyysin mukaan vaikuttaa olevan signaalien estyminen tai pirstoutuminen. TETRA–järjestelmän turvallisuuden etevyydestä huolimatta radioaaltojen kulkuun voivat vaikuttaa sääolot, pinnanmuodot, rakennukset jne., joten urbaanin ympäristön tukiasemien välimatkojen lyhyydestä ja signaalin voimakkuudesta huolimatta signaalin kulkemista lähettäjältä vastaanottajalle asti ei voida taata täydellisesti. Lievimmäksi uhkaksi osoittautui päätelaitteeseen vaikuttavat sähkömagneettiset häiriöt, joita voivat aiheuttaa muut vahvat sähkömagnetismin lähteet tai suuri määrä pienempiä lähteitä. Sähkölaitteille on kuitenkin asetettu säädöksiä, jotka

rajoittavat laitteiden aiheuttamia häiriöitä muille laitteille. Radio- ja matkapuhelinten on toimittava myös silloin, kun ne ovat alttiina arkipäiväisille sähkömagneettisille häiriöille.

7 Johtopäätökset

TETRA on viranomaiskäytön vaatimuksia ajatellen ominaisuuksiltaan erittäin monipuolinen ja kattava matkaviestintäjärjestelmä. TETRA-puhelimet yhdistävät radio- ja matkapuhelimien toimintoja. TETRA:ssa on laajat puhepalvelut, joihin kuuluvat mm. yhden- ja kahdensuuntaiset puhelut, automaattinen hätäpuhelu, puheryhmien etsintä kuuluvuusalueelta, useamman puheryhmän samanaikainen seuranta, puheryhmien tärkeysjärjestyksen määrittäminen, väliaikaisten puheryhmien luominen, suorat puheyhteydet, puheluiden tärkeysjärjestyksen määritykset ja DMO-toimintatila. Lisäksi turvallisuuden ja toimintakyvyn säilyttävät ominaisuudet ovat kattavat: salauksen taso on vahva, järjestelmä voi käyttää kahdensuuntaista todennusta, päätelaitteita voidaan tarvittaessa poistaa väliaikaisesti tai jopa pysyvästi verkon yhteydestä ja verkolla on toimintakuntoisuutensa takaavia varmuustekijöitä. Edellä mainituista syistä johtuen TETRA on valta-asemassa viranomaisverkkojen eurooppalaisissa toteutuksissa.

Radio- ja matkapuhelintekniikoiden ominaisuuksien vertailu osoittaa, että TETRA on muihin vertailtuihin järjestelmiin nähden selkeästi paras puhepalveluiden ja turvallisuuden osalta. UMTS on turvallisuusominaisuuksiltaan myös hyvin kehittynyt, mutta ei yllä TETRA:n tasolle. GSM, kuten sen laajennus GSM-R, alkavat olla ajastaan jälkeenjääneitä järjestelmiä eivätkä enää pysty oikein vastaamaan nykyisiinkään tarpeisiin, tulevaisuudesta puhumattakaan. GSM-verkko ajetaan alas Suomessa todennäköisesti jo lähivuosina, joten 3G- ja 4G-verkot tulevat sen vähitellen korvaamaan.

TETRA:ssa puheyhteys muodostuu lähes välittömästi, kuten UMTS-järjestelmässäkin. TETRA on kuitenkin nopeampi, vaikka molemmat yltävätkin alle sekunnin muodostusnopeuteen. GSM on verrattain auttamattoman hidas useamman sekunnin kestävällä muodostuksella. Lisäksi riskianalyysin yhteydessä asiantuntijuutta tuoneen valmiuspäällikkö Pekka Koskisen mukaan Suomessa on myös sattunut valitettavia onnettomuustilanteita, joissa on täytynyt testata TETRA–verkon käytettävyyttä ja jolloin on todettu, että GSM–verkot kaatuvat hetkessä vastaavissa tilanteessa. TETRA:n kuormituksen sietokyky säilyy erilaisten teknisten ratkaisujen ansiosta käytännössä kaikissa tilanteissa. UMTS tuskin kestäisi vastaavanlaisissa tilanteissa äkillistä verkon rasitusta merkittävästi paremmin kuin GSM.

Datasiirron kannalta UMTS on vertailluista teknologioista paras järjestelmä suuren tiedonvälityskapasiteettinsa ansiosta. Samoin kuin TETRA on kehitetty erityisesti puhepalveluita ajatellen, UMTS:n painopiste on ollut kehitystyön alusta alkaen juurikin

datasiirrossa. Maksiminopeudet ovat protokollasta riippuen teoriassa jopa useita kymmeniä megabittejä sekunnissa eikä kehitys ole päättymässä siihenkään, vaan yhä nopeampia verkkoja odotetaan tulevan markkinoille ennen pitkää. TETRA ei nykyisellään kykene kilpailemaan UMTS-järjestelmän kanssa tiedonsiirron nopeuden osalta. TETRA:ssa nopeutta rajoittavat puheviestinnän ensisijaisuus sekä käytetty salauksen taso.

Riskianalyysin perusteella ainakin Helsingin ja Uudenmaan sairaanhoitopiirissä riskien toteutumista ei pidetä kovin todennäköisenä eli TETRA–verkon ja –päätelaitteiden toimintavarmuuteen ja turvallisuuden tasoon luotetaan. Riskien toteutumisen vakavuuksia ja seurauksia pidetään toisaalta pääpainoisesti suurehkoina, mutta todennäköisyyksien ollessa pieniä vakavilta riskeiltä ilmeisesti vältytään. Suomen oloissa ainakin sosiaali- ja terveysviranomaisten TETRA-laitteiden käyttöympäristön voidaan olettaa olevan keskenään hyvin samankaltainen, jolloin riskianalyysin avulla tehdyt päätelmät ovat todennäköisesti päteviä myös muiden sairaanhoitopiirien toiminnan kannalta. Kattavampien tulosten saamiseksi tutkimuksen tulisi olla laajempi ja käsittää esimerkiksi kaikki Suomen sairaanhoitopiirit. Muiden viranomaistahojen toiminnassa vallitsee toki omia erityispiirteitään, mutta yleistävästi Suomen oloissa TETRA:n luotettavuuden kannalta suurta varianssia tuskin esiintyisi.

TETRA-standardilla on alun perin ollut paljon yhteneväisyyksiä GSM:n kanssa. Standardia on kuitenkin kehitystyön myötä laajennettu käyttäjien vaatimusten asettamin ehdoin. GSM-järjestelmää on aikanaan laajennettu käsittämään myös radiopuhelinmaisia ominaisuuksia (GSM-R), mutta viranomaiskäyttöön sen kyvyt eivät riittäneet. Entä jos kolmannen tai neljännen sukupolven matkapuhelinverkkoratkaisuihin kehitetään soveltuvia radiopuhelimen kaltaisia ominaisuuksia? Tällainen uusi järjestelmä voisi parhaimmillaan kilpailla TETRA:n kanssa, jos sen puhepalvelut ja turvallisuusominaisuudet niin verkon kuin päätelaitteiden osalta olisivat yhtä korkeatasoisia. Viime vuosien nopean langattoman teknologian kehityksen perusteella voi ennustaa, että Internet-yhteyksien merkitys kasvaa myös viranomaisten viestinnässä, joten nykyisten TETRA-puhelinten toimivuus viestinnän pääasiallisena välineenä ei ole tulevaisuudessa itsestään selvää. TETRA-puhelinten kehitykseen vaikuttaa kuitenkin huomattavasti niiden käyttöympäristö, joka asettaa omia rajoituksiaan laitteiden rakenteelle.

Tutkimustyön avulla on selvitetty, että TETRA on edelleen ilmeisen soveltuva viranomaistahojen käyttöön ominaisuuksiensa puolesta, ja vaikka radioverkkotekniikkaa koskevat monenlaiset riskitekijät, riskien toteutuminen ei ole yleinen tapahtuma. TETRA–järjestelmään sisäänrakennetut turvallisuuden takaavat ominaisuudet ovat pääteltävästi riittäviä torjumaan tämän hetkiset järjestelmän käytössä ilmenevät uhkat.

Lähteet

Allan, G. 2003. A critique of using grounded theory as a research method. Electronic Journal of Business Research Methods. Viitattu 25.2.2011. citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.129.9102.pdf

Brewer, C., Carter, J., McKeon, D., McTaggart, M. GSM and UMTS Security. Viitattu 8.4.2011. http://ntrg.cs.tcd.ie/undergrad/4ba2.05/group7/index.html

Cosmos. STUKin tiedote 8.11.2010. Viitattu 13.3.2011. http://www.cosmostutkimus.fi/20

Digitoday. 2007. Räjähtävä Motorola tappoi miehen. Viitattu 13.3.2011. http://www.digitoday.fi/mobiili/2007/07/06/rajahtava-motorola-tappoi-miehen/200716611/66

Digitoday. 2010. Nokia-puhelin räjähti – mies kuoli. Viitattu 13.3.2011. http://www.digitoday.fi/yhteiskunta/2010/08/20/nokia-puhelin-rajahti-mies-kuoli/201011504/66

Digitoday. 2011. iPhone 4 räjähti pakkasella. Viitattu 13.3.2011. http://www.digitoday.fi/vimpaimet/2011/01/10/iphone-4-rajahti-pakkasella/2011350/66

Elers, N. 2011. Matkaviestinverkot 1G, 2G ja 3G. Viitattu 21.3.2011. http://www.ficom.fi/tietoa/tietoa_4_1.html?Id=1034921940.html

Elers, N. 2011. Näin toimii gsm-matkapuhelinverkko. Viitattu 15.3.2011. http://www.ficom.fi/tietoa/tietoa_4_1.html?Id=1038221839.html

Grönfors, M. 1982. Laadullisen tutkimuksen kenttätyömenetelmät. Viitattu 10.1.2011. http://homepage.mac.com/vilkka/Kirjat/Laadullisen_tutkimuksen.pdf

Hansson, S. 2007. Risk (Stanford Encyclopedia of Philosophy). Viitattu 25.2.2011. http://plato.stanford.edu/entries/risk/

Heikkonen, K., Pesonen, T. & Saaristo, T. 2004. You and Your TETRA Radio. Second edition. Helsinki: Edita.

Iltalehti. 2011. Miljoona kännykkää mykistyi – Elisa korjannut vian. Viitattu 16.3.2011. http://www.iltalehti.fi/uutiset/2011020513135770_uu.shtml

It-viikko. 2010. Kas näin kännykkäsi hajoaa. Viitattu 16.3.2011. http://www.itviikko.fi/teknologia/2010/08/30/kas-nain-kannykkasi-hajoaa/201011920/7

Kirkkonummen Sanomat. N:o 36. 8.5.2011. GSM-puheluita voidaan salakuunnella.

Kokkonen, J. 2008. Nokian kännykkä räjähti Tampereella. Viitattu 13.3.2011. http://plaza.fi/muropaketti/taskumuro/nokian-kannykka-rajahti-tampereella

Koskenniemi-Sivonen, R. 2007. Grounded Theory. Viitattu 25.2.2011. http://www.helsinki.fi/~rkosken/gt

Kämppi, P. & Guinness, R. 2010. Technical Risk Analysis for Satellite Based Tracking Systems. Tulostettu 28.4.2010.

Martin, P. A., Turner, B. A. 1986. Grounded Theory and Organizational Research. The Journal of Applied Behavioral Science.

Pelastustoimi. 2009. Viitattu 25.2.2011.
http://www.pelastustoimi.fi/uutiset/4919

Penttinen, J. 2006a. Tietoliikennetekniikka – Perusverkot ja GSM. 1. Painos. Helsinki: Werner Söderström Osakeyhtiö.

Penttinen, J. 2006b. Tietoliikennetekniikka – 3G ja erityisverkot. 1. painos. Helsinki: Werner Söderström Osakeyhtiö.

Pohjolan Sanomat. 2011. Varastetulla puhelimella puhuttiin yli 3000 eurolla. Viitattu 16.3.2011.
http://www.pohjolansanomat.fi/cs/Satellite/PS-Uutiset/1194664942286/artikkeli/varastetulla+puhelimella+puhuttiin+yli+3000+eurolla.html

Rantama, M. 2011. Pelastustoimen langattoman tiedonsiirron tarpeet ja toteutusmahdollisuudet tulevaisuudessa. Pelastusopisto. Viitattu 6.5.2011.
http://www.pelastusopisto.fi/pelastus/images.nsf/files/A1933B8977CDAE26C22578570025B300/$file/Pelti%20loppuraportti%20liitteineen.pdf

Saaranen-Kauppinen, A., Puusniekka, A. 2006. KvaliMOTV - Menetelmäopetuksen tietovaranto. Tampere: Yhteiskuntatieteellinen tietoarkisto. Viitattu 25.2.2011.
http://www.fsd.uta.fi/menetelmaopetus/kvali/L5_2_1_1.html
http://www.fsd.uta.fi/menetelmaopetus/kvali/L7_2_2.html

Sajari, P. 2008. Teleoperaattorit valmistautuvat lopettamaan gsm-verkot. Viitattu 25.3.2011.
http://www.hs.fi/talous/artikkeli/Teleoperaattorit+valmistautuvat+lopettamaan+gsm-verkot/1135235364148

Saterisk. 2011. Viitattu 9.1.2011.
http://saterisk.com/

Schiller, J. 2001. Mobiilitietoliikenne. Helsinki: Edita Oyj.

Säteilyturvakeskus. 2007. Tiedotteet. Viitattu 25.2.2011.
http://www.stuk.fi/stuk/tiedotteet/2007/fi_FI/news_465/

Säteilyturvakeskus. 2009. Magneettikentät. Viitattu 13.3.2011.
http://www.stuk.fi/sateilytietoa/sateilevat_laitteet/magneettikentat/fi_FI/index/

Taloussanomat. 2009. Nokian kännykän akku räjähti. Viitattu 13.3.2011.
http://www.taloussanomat.fi/tekniikka/2009/09/05/nokian-kannykan-akku-rajahti/200919450/133

TETRA Industry Group. 2011. Viitattu 25.2.2011.
http://www.tetrahealth.info/aboutTIG.htm
http://www.tetrahealth.info/FAQsHealth.htm
http://www.tetrahealth.info/FAQsInterference.htm
http://www.tetrahealth.info/FAQsWhoUses.htm

TETRA Memorandum of Understanding. 2004. TETRA or GSM-ASCI network for Public Safety – Let the users decide. Viitattu 8.5.2011.
http://www.tetramou.com/uploadedFiles/Files/Documents/TETRAvsGSMASCIpaperv2.pdf

TETRA Memorandum of Understanding. 2011. Viitattu 9.1.2011.
http://www.tetra-association.com/tetramou.aspx?id=44&ekmensel=fb5d653b_102_0_44_1

Tietokone. 2009. 40 miljoonan käyttäjän kännykkäverkko pimeni Saksassa. Viitattu 16.3.2011.

http://www.tietokone.fi/uutiset/2009/40_miljoonan_kayttajan_kannykkaverkko_pimeni_saksassa

Tietokone. 2009. Räjähtävä kännykkä tappoi miehen. Viitattu 13.3.2011.
http://www.tietokone.fi/uutiset/2009/rajahtava_kannykka_tappoi_miehen?ref=lk_ts_dt_2

Turun Sanomat. 2010. Tutkimus löysi yhteyden runsaan kännykän käytön ja tinnituksen välillä. Viitattu 16.3.2011.
http://www.ts.fi/online/kotimaa/147440.html

Kuvat ja kuviot

Liitteet

Liite 1: Riskiarviointilomake

RISKITEKIJÄT	TODENN.	VAKAVUUS	RISKIN TOTEUTUMISEN SEURAUKSET
Signaalin estyminen tai pirstoutuminen			Lähetetty signaali ei tavoita vastaanottajaa.
Signaalin saapumisessa esiintyvä hajaviive			Signaalin havaitseminen vaikeutuu; viestin sisältö muuttuu epäselväksi tai pahimmillaan pelkäksi taustakohinaksi.
Verkon kaatuminen tai palvelun esto			Koko verkko tai sen osia ovat poissa käytöstä.
Verkon ruuhkautuminen/kapasiteetin ylittyminen			Tiedonsiirto katkonaista ja viivästynyttä.
Verkkohyökkäykset: hakkerointi ja krakkerointi			Verkon toiminnan häiriöt tai estymiset. Tietomurrot: tiedon kaappaminen, väärentäminen tai tuhoaminen.
Tietoliikenteen salakuuntelu			Tiedon kerääminen ja väärinkäyttö, verkon vakoilu.
Laitteistojen ja ohjelmistojen yhteensopimattomuus			Ongelmat toiminnassa ja luotettavuudessa.
Päätelaitteen hajoaminen tai vioittuminen			Laitteen toimimattomuus.
Ohjelmistoviat			Ohjelmiston toimimattomuus.
Virtalähteen tai virtapiirien kipinöinti			Räjähdysvaara, henkilövahingot.
Päätelaitteen aiheuttamat sähkömagneettiset häiriöt			Mahdollisia häiriöitä lähistöllä oleviin herkkiin laitteisiin.
Päätelaitteeseen vaikuttavat sähkömagneettiset häiriöt			Signaalin lähettämisen ja vastaanottamisen häiriintyminen.
Sähkömagnetismin mahdolliset terveyshaitat			Henkilöstön pitkäaikaisen altistumisen aiheuttamat vaivat.
Päätelaitteen hukkaaminen tai katoaminen			Henkilöstön varomattomuus aiheuttaa tietoturvariskin.
Päätelaitteen joutuminen varastetuksi			Päätelaite väärissä käsissä; tietomurrot, salakuuntelu.
Käyttäjän hyväuskoisuus/päätelaitteen lainaaminen			Mahdollinen salakuuntelu, huijaukset, identiteettivarkaudet.

Liite 2: Riskiarviointilomakkeen selvennysosa

Laakso, Jari; Leino, Hannu-Heikki
Riskiarviointilomakkeen selvennysosa

Tämän opinnäytetyön riskianalyysiin käytetään lomaketta, jossa arvioidaan erilaisten matkapuhelinjärjestelmien käyttöä koskevien riskien esiintyvyyttä TETRA:n näkökulmasta. Lomakkeessa esitetään 16 riskitekijää, joiden toteutumisen todennäköisyyden ja vakavuuden asteita tarvitaan riskianalyysin läpiviemiseksi ja opinnäytetyön lopullisten tulosten johtamiseksi. Lomakkeeseen syötetään arvoja asteikolla 1-5, pienimmän arvon (1) tarkoittaessa lievintä astetta ja suurimman arvon (5) tarkoittaessa vakavinta astetta:

1 = pieni,
2 = melko pieni,
3 = keskisuuri,
4 = melko suuri,
5 = suuri.

Riskitekijät -sarakkeessa esitetyn riskitekijän todennäköisyys arvioidaan syöttämällä arvo vieressä olevaan todennäköisyys -sarakkeeseen. Vakavuus -sarakkeeseen syötetään arvo sen mukaan, miten vakaviksi riskin toteutumisen seuraukset -sarakkeen kuvailemat uhkakuvat koetaan edustamassanne organisaatiossa.

Seuraavassa luettelossa selvennetään lyhyesti lomakkeessa esitetyistä riskitekijöistä niiden ydinasiat, jotta käytetyistä termeistä tai asiayhteyksistä jäisi mahdollisimman vähän epäselvyyksiä:

- **Signaalin estyminen tai pirstoutuminen:** osa signaalista tai koko signaali voivat jäädä vastaanottamatta mahdollisten hankalien sääolosuhteiden, maantieteellisten esteiden tai muiden kohteiden kuten suurten rakennusten häiritessä sen kulkua lähettäjältä vastaanottajalle.
- **Signaalin saapumisessa esiintyvä hajaviive:** hajaviive johtuu radiosignaalien etenemisestä monia eri reittejä pitkin vastaanottavaan päätelaitteeseen, jolloin signaalin eri osat voivat saapua eri aikoihin ja vastaanotettu viesti voi olla epäselvä tai jopa pelkkää kohinaa.
- **Verkon kaatuminen tai palvelun esto:** matkapuhelinverkko voi kaatua tahattomasti esimerkiksi verkon ylläpitäjästä johtuvan häiriön, kuten sähkökatkoksen tai ohjelmistovian, takia. Vaihtoehtoisesti hyökkääjät voivat häiritä tai estää kokonaan verkon tai sen palvelujen käytön esimerkiksi palvelunestohyökkäyksillä.
- **Verkon ruuhkautuminen/kapasiteetin ylittyminen:** matkapuhelinverkko on kapasiteetiltaan rajallinen, eli se ei kykene välittämään liian suurta signaalimäärää kerralla. Tästä voi seurata puheliniikenteen ruuhkautumista tai tukkeutumista.
- **Verkkohyökkäykset: hakkerointi ja krakkerointi:** hyökkääjät voivat aiheuttaa vahinkoa matkapuhelinverkon toimintaan. Hakkerointi tarkoittaa tunkeutumista

verkkoon kiertämällä sen suojaukset, kun taas krakkerointi tarkoittaa suojausten murtamista. Hyökkäys voi kohdistua verkkoon, jolloin sen toiminnassa ilmenee häiriöitä tai estymistä, tai tietoon, jolloin tietoa voidaan kaapata, väärentää tai tuhota.

- **Tietoliikenteen salakuuntelu:** verkon liikennettä voidaan seurata luvattomasti esimerkiksi väärennetyillä tai varastetuilla päätelaitteilla tai muilla verkkoon liitetyillä vakoilun mahdollistavilla laitteilla. Salakuuntelun avulla luvaton käyttäjä voi saada haltuunsa tietoa, johon tämä ei ole oikeutettu.
- **Laitteistojen ja ohjelmistojen yhteensopimattomuus:** matkapuhelinten ja palvelusovellusten käytön kasvaessa voi seurata yhteensopivuusongelmia, koska laite- ja ohjelmistovalmistajien tuotteet eivät aina ole yleisesti noudatettujen standardien mukaisia tai standardia ei välttämättä ole laadittu ollenkaan.
- **Päätelaitteen hajoaminen tai vioittuminen:** päätelaite voi hajota tai vahingoittua arkisessa käytössä lukemattomista syistä, jolloin laite ei välttämättä ole enää käyttökelpoinen.
- **Ohjelmistoviat:** palveluntuottajat saattavat julkaista ohjelmistojaan keskeneräisinä tai yhteensopimattomina versioina, mistä seuraa mahdollisesti toimintavikoja.
- **Virtalähteen tai virtapiirien kipinöinti:** sähkölaitteiden käyttöön sisältyy teoreettinen kipinöinnin riski, joka saattaa aiheuttaa räjähdysvaaran laitteen virtalähteen ylikuumetessa tai henkilöstön toimiessa ympäristössä, jossa käsitellään räjähdysherkkiä tai tulenarkoja materiaaleja.
- **Päätelaitteen aiheuttamat sähkömagneettiset häiriöt:** sähkölaitteet luovat ympärilleen heikon sähkömagneettisen kentän, joka voi häiritä toisia herkkiä sähkölaitteita. Matkapuhelinten kohdalla erityisesti signaalien lähettäminen voimistaa säteilykenttää.
- **Päätelaitteeseen vaikuttavat sähkömagneettiset häiriöt:** matkapuhelimen toimintaa voi häiritä vahvan sähkömagneettisen kentän muodostava kohde, jolloin puhelimen toiminta ei ole luotettavaa tai se on estynyttä.
- **Sähkömagnetismin mahdolliset terveyshaitat:** sähkölaitteiden muodostamat sähkömagneettiset kentät voivat mahdollisesti aiheuttaa pitkäaikaisen altistumisen seurauksena vaihtelevia terveyshaittoja käyttäjille.
- **Päätelaitteen hukkaaminen tai katoaminen:** käyttäjän varomattomuuden seurauksena päätelaite voi unohtua tai pudota sattumanvaraiseen paikkaan, jolloin laitetta ei välttämättä enää löydy myöhemmin.
- **Päätelaitteen joutuminen varastetuksi:** päätelaite voi tulla varastetuksi ja siten joutua vääriin käsiin jolloin sitä voidaan käyttää vahingollisiin tarkoituksiin.
- **Käyttäjän hyväuskoisuus/päätelaitteen lainaaminen:** liiallinen luottamus ulkopuolisiin henkilöihin voi johtaa esimerkiksi salakuunteluun, henkilöllisyyden varastamiseen tai taloudellisiin vahinkoihin.

Liite 3: Vastaanotettu asiantuntijan täyttämä riskiarviointilomake

RISKITEKIJÄT	TODENN.	VAKAVUUS	RISKIN TOTEUTUMISEN SEURAUKSET
Signaalin estyminen tai pirstoutuminen	3	5	Lähetetty signaali ei tavoita vastaanottajaa.
Signaalin saapumisessa esiintyvä hajaviive	1	4	Signaalin havaitseminen vaikeutuu; viestin sisältö muuttuu epäselväksi tai pahimmillaan pelkäksi taustakohinaksi.
Verkon kaatuminen tai palvelun esto	1	5	Koko verkko tai sen osia ovat poissa käytöstä.
Verkon ruuhkautuminen/kapasiteetin ylittyminen	2	3	Tiedonsiirto katkonaista ja viivästynyttä.
Verkkohyökkäykset: hakkerointi ja krakkerointi	1	5	Verkon toiminnan häiriöt tai estymiset. Tietomurrot: tiedon kaappaminen, väärentäminen tai tuhoaminen.
Tietoliikenteen salakuuntelu	1	5	Tiedon kerääminen ja väärinkäyttö, verkon vakoilu.
Laitteistojen ja ohjelmistojen yhteensopimattomuus	2	3	Ongelmat toiminnassa ja luotettavuudessa.
Päätelaitteen hajoaminen tai vioittuminen	3	4	Laitteen toimimattomuus.
Ohjelmistoviat	3	4	Ohjelmiston toimimattomuus.
Virtalähteen tai virtapiirien kipinöinti	2	5	Räjähdysvaara, henkilövahingot.
Päätelaitteen aiheuttamat sähkömagneettiset häiriöt	1	5	Mahdollisia häiriöitä lähistöllä oleviin herkkiin laitteisiin.
Päätelaitteeseen vaikuttavat sähkömagneettiset häiriöt	1	3	Signaalin lähettämisen ja vastaanottamisen häiriintyminen.
Sähkömagnetismin mahdolliset terveyshaitat	1	5	Henkilöstön pitkäaikaisen altistumisen aiheuttamat vaivat.
Päätelaitteen hukkaaminen tai katoaminen	3	4	Henkilöstön varomattomuus aiheuttaa tietoturvariskin.
Päätelaitteen joutuminen varastetuksi	3	4	Päätelaite väärissä käsissä; tietomurrot, salakuuntelu.
Käyttäjän hyväuskoisuus/päätelaitteen lainaaminen	3	4	Mahdollinen salakuuntelu, huijaukset, identiteettivarkaudet.