Tampereen yliopisto

Petteri Lehtonen

VIRANOMAISVERKKOJEN TOIMINTAVARMUUS JA TULEVAISUUS

Kandidaatintyö
Informaatioteknologian ja viestinnän tiedekunta
Tarkastajat: Prof. Jukka Lempiäinen, TkT Joonas Säe
Toukokuu 2021

TIIVISTELMÄ

Petteri Lehtonen: Viranomaisverkkojen toimintavarmuus ja tulevaisuus
Kandidaatintyö
Tampereen yliopisto
Tieto- ja sähkötekniikan tutkinto-ohjelma
Toukokuu 2021

Viranomaisverkkojen kehitys on saavuttanut taitekohdan, sillä TETRA (terrestrial trunked radio) -pohjaisten verkkojen tilalle ollaan monessa maassa ottamassa käyttöön LTE (long term evolution) -pohjaisia viranomaisverkkoja. Viranomaisverkkojen vaatimukset erityisesti datanopeuksille ovat kasvaneet niin paljon, ettei TETRA-teknologian kehittäminen ole enää kannattavaa. Myös Suomessa Virve 2.0 -projektin tavoite on korvata nykyinen viranomaisverkko LTE-verkkoon pohjautuvalla ratkaisulla. Tämän työn tarkoituksena on standardien sekä alan julkaisujen perusteella selvittää LTE-verkkojen viranomaisille tarjoamia mahdollisuuksia sekä mahdollisia uhkakuvia verkkojen toimintavarmuudelle. Lisäksi luodaan katsaus viranomaisverkkojen tulevaisuudennäkymiin. Työtä varten myös haastateltiin kehityspäällikkö Kari Junttilaa Suomen Erillisverkot Oy:stä.

Viranomaisverkkojen tavoitteet eroavat kuluttajaverkoista jonkin verran, joten aluksi käsitellään viranomaisverkkoja sekä niissä käytettyjä teknologioita yleisesti. Työn toinen osa, toimintavarmuus, on jaettu kolmeen osaan, jotka ovat kattavuus ja kapasiteetti, häiriöiden ja häirinnän sieto sekä tietoturva. Kattavuuden ja kapasiteetin osalta käydään läpi viranomaisverkkojen toimintaedellytyksiä verkkojen reuna- ja katvealueilla sekä ruuhkatilanteissa. Häiriöiden ja häirinnän sietoa käsitellään LTE-verkon fyysisen kerroksen ominaisuuksien kannalta. Tietoturvaa taas käsitellään tiedon eheyttä ja luottamuksellisuutta varmistavien ominaisuuksien kautta. Kolmannessa osassa käsitellään tulevaisuudennäkymiä, erityisesti 5G-verkkojen tarjoamia mahdollisuuksia sekä myös LTE-verkkoihin integroitavia teknologioita, kuten tekoälyä ja esineiden internetiä.

Työssä havaittiin, että viranomaisverkkojen kattavuutta pystytään lisäämään ja kapasiteettia vapauttamaan nopeasti ja helposti. Häiriöiden sieto LTE-verkoissa on luonnollisten häiriöiden osalta riittävää, mutta verkkoja pystytään häiritsemään paikallisesti melko helposti. Tietoturvaominaisuuksissa on tehty tehokkuuden nimissä kompromisseja, jotka johtavat huomiota vaativiin heikkouksiin. Kirjallisuusselvityksen perusteella todettiin siis, että vaikka LTE-verkkojen tilanne on suhteellisen hyvä, täytyy kehitystyötä jatkaa edelleen erityisesti viranomaisverkkojen tarpeet huomioon ottaen. Tulevaisuudennäkymät vaikuttavat lupaavilta, mutta 5G-verkkojen kehitystyö on vielä pahasti kesken, erityisesti viranomaisverkkojen kannalta kiinnostavissa ominaisuuksissa. Tulevaisuuden teknologiat voivat kuitenkin mahdollistaa viranomaisille uusia toimintatapoja sekä tehostaa työskentelyä.

Avainsanat: Viranomaisverkot, Virve 2.0, PS-LTE

SISÄLLYSLUETTELO

LYHENTEET JA MERKINNÄT

3GPP	Mobiiliverkkojen standardointiorganisaatio (engl. Third Generation Partnership Program)
5G	Viidennen sukupolven matkapuhelinverkko (engl. Fifth Generation)
ACB	Käyttöoikeusluokkaan perustuva pääsyn rajoittaminen (engl. Access Class Barring)
AES	Kehittynyt salausstandardi (engl. Advanced Encryption Standard)
AKA	Todennus- ja avainsopimus (engl. Authentication and Key Agreement)
AoA	Saapumiskulma (engl. Angle of Arrival)
ARP	Verkkokapasiteetin jakamisen ja säilyttämisen prioriteetti (engl. Allocation and Retention Priority)
BPSK	Binäärinen vaiheavainnus (engl. Binary Phase Shift Keying)
CA	Kantoaaltojen yhdistäminen (engl. Carrier Aggregation)
CTR	AES-salauksen toimintamuoto (engl. Counter)
D2D	Laitteesta laitteeseen (engl. Device to Device)
DDoS	Hajautettu palvelunestohyökkäys (engl. Distributed Denial of Service attack)
DNS	Nimipalvelujärjestelmä (engl. Domain Name System)
DoS	Palvelunestohyökkäys (engl. Denial of Service attack)
eMBB	Parannettu mobiililaajakaista (engl. Enchanced Mobile Broadband)
EMI	Sähkömagneettinen häiriö (engl. Electromagnetic Interference)
ESN	Isossa-Britanniassa käyttöönotettava LTE-pohjainen viranomaisverkko (engl. Emergency Services Network)
FD	Tiedostonjako (engl. File Distribution)
GBR	Taattu bittinopeus (engl. Guaranteed Bit Rate)
GPS	Maailmanlaajuinen satelliittipaikannusjärjestelmä (engl. Global Positioning System)
GUTI	Globaalisti ainutlaatuinen tilapäinen tunnus (engl. Globally Unique Temporary Identity)

IMSI	Kansainvälinen matkaviestintilaajan tunnus (engl. International Mobile Subscriber Identity)
ISI	Symbolien välinen häiriö (engl. Intersymbol Interference)
ITU	Kansainvälinen televiestintäliitto (engl. International Telecommunications Union)
LTE	Neljännen sukupolven matkapuhelinverkko (engl. Long Term Evolution)
MCX	Tehtäväkriittinen palvelu (engl. Mission Critical X)
MIMO	Moniantennitekniikka (engl. Multiple-Input Multiple-Output)
MITM	Väliintulohyökkäys (engl. Man-in-the-middle attack)
MME	Liikkuvuuden hallintayksikkö (engl. Mobility Management Entity)
mMTC	Massiivinen konetyypin kommunikaatio (engl. Massive Machine Type Communications)
MOCN	Mobiiliverkon jakamistekniikka, jossa useat operaattorit käyttävät samaa radioverkkoa ja taajuuskaistaa (engl. Multi-Operator Core Network)
MORAN	Mobiiliverkon jakamistekniikka, jossa useat operaattorit käyttävät samaa radioverkkoa (engl. Multi-Operator Radio Access Network)
MPS	Multimedian etuoikeuspalvelu (engl. Multimedia Priority Service)
MU-MIMO	Monen käyttäjän moniantennitekniikka (engl. Multi-User MIMO)
MVNO	Mobiiliverkon jakamistekniikka, jossa operaattori vuokraa sekä radio- että runkoverkon toiselta operaattorilta (engl. Mobile Virtual Network Operator)
PCEF	LTE-verkossa määrityksiä ja laskutusta toimeenpaneva laite (engl. Policy and Charging Enforcement Function)
PDB	Paketin viivebudjetti (engl. Packet Delay Budget)
PELR	Pakettien hävikkisuhde (engl. Packet Error Loss Rate)
ProSe	LTE-verkon läheisyyteen perustuvat palvelut (engl. Proximity-based services)
QAM	Kvadratuuriamplitudimodulaatio (engl. Quadrature Amplitude Modulation)
QCI	Palvelun laatuluokan tunniste (engl. QoS Class Identifier)
QoS	Palvelun laatu (engl. Quality of Service)
QPSK	Nelivaihesiirtoavainnus (engl. Quadrature Phase Shift Keying)

Rakel	Ruotsissa käytössä oleva TETRA-pohjainen viranomaisverkko (ruots. radiokommunikation för effektiv ledning)
RB	Resurssilohko (engl. Recource Block)
RIP	Vastaanotettu häiriöteho (engl. Received Interference Power)
RSRP	Vastaanotetun vertailusignaalin teho (engl. Reference Signal Received Power)
RSRQ	Vastaanotetun vertailusignaalin laatu (engl. Reference Signal Received Quality)
RSSI	Vastaanotetun signaalin voimakkuuden ilmaisin (engl. Received Signal Strength Indicator)
SDF	Palvelun dataliikenne (engl. Service Data Flow)
SDS	Lyhytviestipalvelu (engl. Short Data Service)
SIM	SIM-kortti, sisältää matkapuhelinliittymän tilaajan yksilöintitiedot (engl. Subscriber Identity Module)
SINR	Signaali-häiriö-kohinasuhde (engl. Signal to Noise and Interference Ratio)
SVPL	Laki sähköisen viestinnän palveluista
TETRA	Viranomaiskäyttöön suunniteltu radioverkkostandardi (engl. Terrestrial Trunked Radio)
TMSI	Tilapäinen matkaviestintilaajan tunnus (engl. Temporaty Mobile Subscriber Identity)
TUVE-laki	Laki julkisen hallinnon turvallisuusverkkotoiminnasta
URLLC	Erittäin luotettava matalan viiveen kommunikaatio (engl. Ultra Reliable Low Latency Communications)
USIM	Uudempi versio SIM-kortin toiminnallisuudesta (engl. Universal Subscriber Identity Module)
Virve	Suomessa käytössä oleva TETRA-pohjainen viranomaisverkko (suom. viranomaisverkko)
VPN	Virtuaalinen yksityisverkko (engl. Virtual Private Network)

1. JOHDANTO

Ihmisten välinen yhteistyö vaatii aina kommunikaatiota. Tämä pätee myös viranomaisiin, kuten poliisiin, pelastuslaitokseen tai asevoimiin. Erityisen tärkeää kommunikaatio on nopeaa toimintaa vaativissa tilanteissa, jolloin käskyt on saatava perille viivytyksettä ja ymmärrettävässä muodossa, jotta käsky voidaan suorittaa onnistuneesti. Esimerkiksi pakenevaa henkilöä takaa-ajavan poliisipartion täytyy jatkuvasti raportoida sijaintiaan, jotta muut partiot voidaan ohjata tueksi oikeisiin paikkoihin. Myös palavaa rakennusta sammutettaessa on tärkeää säilyttää puheyhteys savusukeltajiin, jotta heidät voidaan tarvittaessa kutsua nopeasti pois. Erityisesti suuronnettomuuksien aikana vaaditaan paljon kommunikaatiota eri viranomaisten toiminnan koordinointiin.

Kommunikaatiota helpottamaan on kehitetty erilaisia teknologioita, joista radioverkot ovat olleet tärkeässä asemassa liikkuvien viranomaisten työtä helpottamassa. Erityisesti viranomaisten tarpeeseen vastaavat viranomaisverkot, joilla tässä työssä tarkoitetaan viranomaisten käyttöön tarkoitettuja mobiiliverkkoja. Viranomaisten vaatimukset verkkojen ja niiden laitteiden toimintavarmuudelle ovat kuluttajia tiukemmat, joten on ollut tarkoituksenmukaista, että viranomaisia varten on rakennettu omat, erilliset verkot.

Kokonaan erillisten verkkojen rakentaminen on kuitenkin vähentynyt, kun viranomaisverkkoja on siirretty käyttämään samoja standardeja kuin kuluttajaverkot. Verkkoja on myös toteutettu kaupallisten toimijoiden avulla myös olemassa olevia kuluttajaverkkoja hyväksi käyttäen, mikä nostaa kysymyksiä viranomaisten vaatimusten täyttymisestä. Työn tavoitteena onkin kirjallisuuden perusteella koota kuva nykyaikaisten viranomaisverkkojen toimintavarmuudesta, lähinnä Suomen uuden viranomaisverkko Virve 2.0:n kautta.

Työtä varten on myös haastateltu Suomen Erillisverkot Oy:stä kehityspäällikkö Kari Junttilaa, jolla on pitkä kokemus sekä mobiili- että viranomaisverkoista. Toisessa luvussa käydään läpi viranomaisverkkoja ja niiden toimintaperiaatteita yleisesti. Mobiiliverkkojen toimintavarmuus, jota käsitellään kolmannessa luvussa, koostuu useasta osa-alueesta, kuten verkon kattavuudesta, radioliikenteen häiriönsiedosta ja tietoturvallisuudesta. Verkkojen kattavuuden ohella käsitellään myös siihen olennaisesti liittyvä verkkojen kapasiteetti. Neljännessä luvussa käydään läpi viidennen sukupolven matkapuhelinverkkojen vaikutusta sekä muiden uusien teknologioiden mahdollisia integraatioita. Johtopäätökset viranomaisverkkojen nykytilasta ja tulevaisuudesta esitellään luvussa viisi.

2. VIRANOMAISVERKOT YLEISESTI

Viranomaisverkkoja on monenlaisia, mutta tässä työssä keskitytään viranomaisten käyttämiin mobiiliverkkoihin. Suomessa tätä tehtävää on täyttänyt Terrestrial Trunked Radio (TETRA) -pohjainen viranomaisverkko Virve. TETRA on digitaalinen yhteiskäyttöinen radioverkko, jonka tarkoitus on täyttää viranomaisten ja ammattikäyttäjien vaatimukset [1]. TETRA-verkkoja on rakennettu ympäri maailmaa, lähimpänä Rakel Ruotsissa [2]. Pääosin TETRAn kehitys on keskittynyt puheen ja lyhyiden viestien välittämiseen, eivätkä sen tarjoamat datayhteydet siten ole laajakaistaisia.

Laajakaistaisten datayhteyksien tarve on kuitenkin kasvanut huomattavasti, eikä TETRA pysty tarjoamaan vaadittuja nopeuksia. Tämän vuoksi Virve siirtyy LTE-verkkoon (long term evolution) 2020-luvun alussa. Siirtymäprojekti on nimeltään Virve 2.0. [3][4] LTE-pohjaisia viranomaisverkkoja on rakennettu maailmalla useita, esimerkiksi FirstNet Yhdysvalloissa [5, 6203(c)(2)], Emergency Services Network (ESN) Isossa-Britanniassa [6] sekä myös Ruotsin Rakel [7, s. 23]. Siirtyminen LTE-verkkoihin on tapahtunut suurimmaksi osaksi laajakaistaisten datayhteyksien vuoksi. Lisäksi LTE-standardin mukaisia laitteita on markkinoilla paljon, mikä pienentää kustannuksia ja parantaa yhteensopivuutta muiden verkkojen kanssa. [8]

Viranomaisverkko, kuten mikä tahansa mobiiliverkko, voidaan toteuttaa täysin itsenäisenä kokonaisuutena, joka käsittää sekä radio- että runkoverkon. Tämä lähestymistapa vaatii kuitenkin paljon resursseja, joten pienemmille tai tiettyyn osa-alueeseen keskittyville operaattoreille täysin oman verkon rakentaminen ei välttämättä ole mahdollista. Siksi verkon osien jakamiseen on kehitetty erilaisia menetelmiä, kuten MORAN (multi-operator radio access network) ja MOCN (multi-operator core network). Näistä MORAN on lähimpänä itsenäistä mobiiliverkkoa. Siinä jaettua on ainoastaan tukiasemien laitteistot, jokaisella operaattorilla on oma runkoverkko sekä taajuuskaista. [9] MOCN-menetelmällä toteutetussa verkossa taas jaetaan myös taajuuskaista, mutta operaattoreilla on edelleen omat runkoverkkonsa. Lisäksi on myös operaattoreita, jotka toimivat MVNO (mobile virtual network operator) -periaatteella. Tämä tarkoittaa toisen operaattorin verkossa toimivaa palveluntarjoajaa. [10] Virve 2.0 toteutetaan MOCN-menetelmällä, mutta esimerkiksi Yhdysvalloissa käytetään dedikoitua taajuuskaistaa [4][5, 6201(a)]. Isossa-Britanniassa ja Ruotsissa on myös päädytty MOCN-ratkaisuun, joskin Ruotsissa joillekin alueille tullaan rakentamaan valtio-omisteisia tukiasemia [6][7].

Alun perin Virve 2.0:aa ei ollut tarkoitus toteuttaa jaetulla taajuuskaistalla, vaan tähän jouduttiin pakon edessä poliittisten päätösten vuoksi. Monissa maissa viranomaisverkkojen käyttöön varattu taajuuskaista 700 MHz alueelta päätettiin Suomessa huutokaupata kaupalliseen käyttöön, mikä johti suunnitelmien muuttumiseen. [4] 700 MHz taajuusalue on ainakin Euroopassa ja Pohjois-Amerikassa siirretty mobiiliverkkojen käyttöön digitaalisilta TV-lähetyksiltä, mutta esimerkiksi Venäjällä näin ei ole vielä tehty. Toimiakseen samalla taajuuskaistalla digitaaliset TV-lähetykset ja LTE tarvitsevat useiden satojen kilometrien fyysisen välimatkan [11]. Tämän vuoksi Venäjältä tulevat TV-lähetykset aiheuttavat Itä-Suomessa merkittävää haittaa tällä taajuusalueella, eikä se siten soveltuisi Itä-Suomessa viranomaiskäyttöön. MOCN-arkkitehtuuri kuitenkin mahdollistaa radioverkon laajentamisen uusille taajuusalueille tulevaisuudessa. [4]

Kari Junttilan mukaan [4] monista hyvistä puolistaan huolimatta kaupallinen LTE-verkko on huono alusta viranomaisverkolle, sillä yhteistyö monikansallisten ja voittoa tavoittelevien operaattorien kanssa on haastavaa. Esimerkiksi lainsäädännön vastustus voi tulla ongelmaksi. LTE:tä ei myöskään ole suunniteltu alusta alkaen viranomaiskäyttöön, toisin kuin TETRA. Tilanne Suomessa on kuitenkin suhteellisen hyvä, sillä Suomessa toimivien operaattorien mielestä viranomaisverkko ja sitä sääntelevä lainsäädäntö ovat tarpeellisia [4]. Lisäksi LTE:n standardit julkaiseva 3GPP (Third Generation Partnership Program) on sisällyttänyt standardeihin ominaisuuksia, jotka ovat tärkeitä viranomaisverkoille.

3GPP:n LTE-standardeihin kuuluvista viranomaisverkkojen palveluista käytetään joissakin yhteyksissä nimitystä MCX (mission critical X), jossa X kuvastaa eri palveluita. Tällaisia palveluita ovat esimerkiksi MCPTT (mission critical push to talk), MCData ja MCVideo. PTT-ominaisuus tarkoittaa käytännössä radiopuhelinmaista toimintaa, jossa tangenttia painamalla saa välitettyä puheen toiseen laitteeseen [12]. MCData mahdollistaa lyhyet dataviestit (short data service, SDS) ja tiedostojen jaon (file distribution, FD). SDS vastaa tekstiviestejä, mutta tukee esimerkiksi vastaanotto- ja lukukuittauksia. [13] MCVideo tarjoaa videopuhelupalvelun [14]. Yhteistä kaikille edellä mainituille on, että ne kaikki toimivat laitteesta laitteeseen (device to device, D2D) -periaatteella myös ilman yhteyttä tukiasemaan, lukuunottamatta FD:tä. D2D-toiminnallisuuteen käytetään LTE-standardin ProSe (proximity-based services) -ominaisuuksia. [12][13][14] Lisäksi standardeissa on määritelty erilaisia tietoturvaominaisuuksia, joita käsitellään myöhemmin.

Edellisessä kappalessa mainitut palvelut tuotetaan runkoverkon puolella. Vastaavia palveluita on jo tarjolla kuluttajille internetin kautta, mutta verkkostandardiin sisällytetyt palvelut takaavat kaikkien palveluntarjoajien sovellusten yhteensopivuuden. Lisäksi operaattorin omassa verkossa tuotetut palvelut mahdollistavat pienemmät viiveet, suuremmat nopeudet sekä tarkemman kontrollin tietoturvan kannalta.

3. TOIMINTAVARMUUS

Viranomaisten toiminnan kannalta on kriittistä, että viranomaisverkot ovat käytettävissä kaikissa mahdollisissa tilanteissa. Tämä toteutetaan yleensä niin, että laeissa asetetaan vähimmäisvaatimukset, jotka palveluntarjoajat teknisin ratkaisuin pyrkivät ttamaan. Suomessa mobiiliverkkojen palvelutasosta säädetään lain sähköisen viestinnän palveluista (SVPL) luvuissa 29 ja 29 a. Laissa säädetään, että palveluntarjoajan on taattava etuoikeus viranomaiskäytölle sekä palvelun saatavuuden mahdollistava altapurku. [15] Käytännössä etuoikeus tarkoittaa muiden käyttäjien liikenteen hidastamista ja altapurku muiden käyttäjien poistamista verkosta. 3GPP:n standardien mukaiset ominaisuudet näiden toimintojen tuottamiseen esitellään luvussa 3.1.

Laissa julkisen hallinnon turvallisuusverkkotoiminnasta (TUVE-laki) on määritelty Suomen Erillisverkot Oy:lle erityisasema valtionhallinnon verkkopalvelujen tuottajana. Tämä tarkoittaa, että Erillisverkot vastaa turvallisuusverkkojen runko- ja pääsyverkosta. [16] Häiriöiden ja häirinnän siedosta laeissa ei yksityiskohtaisesti säädetä, ainoastaan TUVE-laki velvoittaa tuottajan varautumaan häiriötilanteisiin [17]. Häiriöitä ja häirintää käsitelläänkin yleisellä tasolla 3GPP:n standardien pohjalta luvussa 3.2. Tietoturvasta määrätään Valtioneuvoston asetuksessa julkisen hallinnon turvallisuusverkkotoiminnassa, että turvallisuusverkkot tulee kehittää niin, että niiden on mahdollista täyttää käsiteltävän tiedon määräämät vaatimukset [18]. Tietoturvaa käsitellään luvussa 3.3 yleisellä tasolla LTE-verkkoihin kohdistuvien uhkien kautta.

3.1 Kattavuus ja kapasiteetti

Verkon kattavuudella tai kuuluvuudella tarkoitetaan sen maantieteellistä peittoa. Suomessa Elisan mukaan operaattorin LTE-verkko kattaa 99 % asukkaista, mutta katvealueita löytyy etenkin Itä- ja Pohjois-Suomesta [19]. Kattavuus ei Kari Junttilan mukaan [4] kuitenkaan kerro kaikkea, ja siksi hän käyttää myös palvelualueen käsitettä. Palvelualueella tarkoitetaan aluetta, jolla tietty palvelu on saatavilla. Esimerkiksi puheluiden palvelualue on suurempi kuin teräväpiirtovideon siirtämisen, sillä puhelut vaativat vähemmän datansiirtoa toimiakseen hyvin. Kattavuus ja palvelualue ovat kuitenkin vahvasti kytköksissä toisiinsa, sillä kattavuuden laajentaminen luonnollisesti kasvattaa palvelualueita. Kapasiteetti taas tarkoittaa suurinta liikennemäärää, jonka verkko kykenee välittämään tie-

tyllä ajan hetkellä. Virve 2.0:n radioverkon Erillisverkot hankkii palveluna Elisalta, mutta SVPL:n mukaisesti myös muiden operaattorien täytyy mahdollistaa viranomaisliikenne kansallisen verkkovierailun avulla. Osaltaan myös muiden operaattorien verkon käyttö parantaa kattavuutta.

Kattavuus on tärkeää sen vuoksi, että viranomaisten täytyy pystyä toimimaan missä tahansa valtion rajojen sisällä. Kattavuutta voidaan lisätä saarekekäyttöisillä tukiasemilla (isolated operation for public safety, IOPS), jotka ovat ainoastaan viranomaiskäytössä. IOPS on hyödyllinen huonon kattavuuden alueilla, sillä siirrettävillä tukiasemilla voidaan saada hyvinkin nopeasti lisää kattavuutta. Kari Junttilan mukaan [4] vaikkapa poliisin johtoautoissa voisi tulevaisuudessa olla tarvittava tukiasemalaitteisto kattavuuden lisäämiseen tehtäväalueelle. Lisäksi päätelaite voi välittää toisen päätelaitteen liikenteen tukiasemalle ProSe-toimintojen avulla, mikäli toisella laitteista ei ole yhteyttä tukiasemaan.

IOPS-tukiasemat ovat viranomaisverkolle kokonaan varattuja ja ne voivat olla sekä kiinteitä että siirrettäviä. Kattavuuden lisäämisen kannalta kiinnostavampia ovat siirrettävät tukiasemat, joihin tässä työssä keskitytään. 3GPP määrittelee neljä IOPS-skenaariota runkoverkkoyhteyden saatavuuden mukaan. Ensimmäisessä skenaariossa ei ole ollenkaan runkoverkkoyhteyttä, toisessa vain verkon kontrolliliikenne on mahdollista, kolmannessa käyttäjädatan rajoitettu siirtäminen on mahdollista ja neljännessä sekä kontrolliliikenne että käyttäjädata voidaan siirtää normaalisti. Kaikissa skenaarioissa on mahdollista tuoda internet-yhteys jotakin toista reittiä, mutta tämän onnistuminen erämaaolosuhteissa on epätodennäköistä. [20]

Ilman runkoverkkoyhteyttä saatavat palvelut rajautuvat niihin, jotka voidaan tuoda tehtäväalueelle tai vain paikallisesti toimiviin palveluihin. Esimerkiksi puhe- ja viestiyhteydet toimivat kaikissa IOPS-skenaarioissa, mutta MCPTT vaatii ryhmäjäsenyyksien määrittelemisen etukäteen. IOPS tukee myös päätelaitteiden sekä tukiasemien liittymistä IOPS-verkkoon ja poistumista siitä. Tämä mahdollistaa esimerkiksi tavallisen verkon reuna-alueella liikkuvan laitteen käyttävän ensin tavallista verkkoa, mutta siirtyvän IOPS-verkkoon myöhemmin. Lisäksi IOPS-verkkoa voidaan laajentaa tarpeen mukaan uusilla tukiasemilla, eikä tämän tai tukiasemien poistumisen tulisi 3GPP:n standardin mukaan aiheuttaa häiriöitä verkon toimivuuteen. [20]

IOPS-tukiasemilla voidaan myös parantaa kaupunkiolosuhteissa kuuluvuutta sisätiloissa. Esimerkiksi savusukeltajan turvallinen toiminta palavassa rakennuksessa vaatii jatkuvan yhteyden kenttäjohtoon sekä toisiin savusukeltajiin. Kanavaolosuhteet palavassa rakennuksessa ovat huomattavasti heikommat kuin ulkotiloissa tai rakennuksen sisällä normaalitilanteessa, joten olemassa oleva verkko ei välttämättä riitä. Häiriöitä aiheuttavat esimerkiksi kuumuus, savu ja muut kaasut sekä mahdolliset romahtaneet rakenteet. Tällaisessa tilanteessa voi olla tarpeen tuoda tukiasema hyvinkin lähelle rakennusta, jotta saavutetaan tarpeeksi hyvä signaalin laatu.

ProSe terminä tarkoittaa läheisyyteen perustuvia palveluita, joita voidaan käyttää laitteesta laitteeseen -periaatteella. Tällaisia palveluita ovat esimerkiksi aiemmin mainitut MCPTT, MCData ja MCVideo. ProSe on kuitenkin myös oma 3GPP-standardinsa, jossa määritellään palveluiden laitteesta laitteeseen -toiminnallisuuden mahdollistavat yhteiset osat. Nämä osat ovat runkoverkon puolella tapahtuva palveluiden havaitseminen (EPC-level ProSe Discovery), runkoverkon tuki suoralle langattoman lähiverkon (Wi-Fi direct) liikennöinnille, suora havaitseminen ja kommunikoiminen sekä käyttäjälaitteen toimiminen linkkinä tukiasemaverkkoon. [21] Kaksi ensin mainittua mahdollistavat ProSe-toiminnallisuuden runkoverkon avustamana, kun taas Wi-Fi direct -toiminnallisuutta voidaan käyttää vaihtoehtoisen radioyhteyden luomiseen. Suora havaitseminen ja kommunikointi taas mahdollistavat ProSe-toiminnallisuuden ilman runkoverkkoa, ja molemmat pystytään toteuttamaan myös Wi-Fi directin avulla. Käyttäjälaitteen toimiminen linkkinä tukiasemaverkkoon mahdollistaa tukiaseman kattavuuden laajentamisen paikallisesti muutamien laitteden kesken.

Kapasiteettia tarvitaan, jotta kaikki viranomaisten laitteet pystyvät toimimaan samanaikaisesti sekä käyttämään tarvittavia palveluita. Radioverkon kapasiteettiongelmat voivat johtua esimerkiksi kaupunki- tai festivaalialueella suuresta käyttäjämäärästä tai harvaan asutuilla alueilla tukiasemien vähyydestä. Suurta käyttäjämäärää pystytään hallitsemaan erilaisilla palvelun laadun (quality of service, QoS) parannusmenetelmillä, joita voidaan käyttää SVPL:n vaatiman etuoikeuden toteuttamiseen. Lisäksi SVPL:n vaatima altapurku toteutetaan käyttöoikeusluokkaan perustuvalla pääsyn rajoittamisella (access class barring, ACB). Lisäksi kapasiteettia voidaan kasvattaa aiemmin mainituilla IOPS-tukiasemilla.

LTE-verkoissa QoS-ominaisuuksia on useita ja niitä käytetään normaalioloissa. Jaetussa radioverkossa QoS-ominaisuuksilla pyritään siis takaamaan viranomaisille tarvittavat resurssit, mutta myös palvelemaan tavallisia käyttäjiä mahdollisuuksien mukaan. Tässä kontekstissa tärkeimpiä ominaisuuksia ovat kapasiteetin jakamisen ja säilyttämisen prioriteetti (allocation and retention priority, ARP), palvelun laatuluokan tunniste (QoS class identifier, QCI) sekä multimedian etuoikeuspalvelu (multimedia priority service, MPS).

ARP on bearerille asetettava prioriteettiarvo, jonka perusteella tarjotaan etuoikeus jollekin käyttäjäryhmälle. Bearer tarkoittaa käytännössä yhteyttä tukiasemalta runkoverkon yhdyskäytävälle. 3GPP:n standardissa bearerin prioriteettiarvoja on määritelty 1–15, suurempi luku tarkoittaa korkeampaa prioriteettia. [22] Korkeamman prioriteetin bearer voi saada käyttöönsä resursseja alemman prioriteetin bearerilta, eli käytännössä viranomaisen liikennöinti voi aiheuttaa joidenkin tavallisten käyttäjien liikenteen estymisen. Mikäli solussa on paljon korkean prioriteetin liikennettä, kaikki matalamman prioriteetin liikenne voi estyä kokonaan. Uusia korkean prioriteetin käyttäjiä pyritään kuitenkin palvelemaan myös ruuhkatilanteissa.

QCI asetetaan jokaisen palvelun datavuolle (service data flow, SDF) palvelun tyypin mu-

kaan. Jokainen QCI:n luokka määrittelee palvelutyypille prioriteettitason suhteessa muihin tyyppeihin, suurimman viiveen (packet delay budget, PDB) käyttäjälaitteelta verkon määrityksiä ja laskutusta toimeenpanevalle laitteelle (policy and charging enforcement function, PCEF) sekä suurimman ruuhkautumisesta johtumattoman pakettihävikin määrän (packet error loss rate, PELR). Lisäksi määritetään, saako palvelu taatun datanopeuden (guaranteed bit rate, GBR) vai ei. [23]

Viranomaisverkkoja varten on standardoitu QCI:t MCPTT:lle, ei-kriittiselle PTT:lle, MCVideolle, MCDatalle sekä MC-palveluiden verkon kontrolliliikenteelle. Kolme ensimmäistä kuuluvat taatun datanopeuden piiriin. Esimerkiksi MCPTT:lle on määritetty prioriteettitaso 0,7, PDB 75 ms ja PELR 10^{-2}, eli maksimissaan 1 paketti 100:sta voidaan menettää. Vertailukohtana voidaan käyttää tavallista puhetta, jonka prioriteettitaso on 2, PDB 100 ms ja PELR 10^{-2}. [23] MCPTT siis syrjäyttää tavallisen käyttäjän puhelun ja tarvitsee pienemmän viiveen. Pakettihävikki saa olla suhteellisen suuri, sillä pelkän puheen välittäminen onnistuu melko pienellä pakettimäärällä.

MPS pyrkii takaamaan, että käyttäjän äänen, videon ja datan lähettäminen ja vastaanottaminen onnistuvat. Tämä toteutetaan niin, että käyttäjälaite pyytää verkolta etuoikeutta, joka myönnetään käyttäjälaitteen tunnistamisen jälkeen. Oikeuden käyttää MPS:ää myöntää etukäteen paikallinen viranomainen, Suomessa todennäköisesti Liikenne- ja viestintävirasto. MPS toimii erillään MC-palveluista, ja se tukee myös päästä päähän -priorisointia, mikä mahdollistaa myös esimerkiksi viranomaisen puhelun tavalliselle käyttäjälle priorisoituna. [24]

Kun tietyn solun alueella on viranomaistoiminnan kannalta liikaa muita käyttäjiä, käytetään ACB:tä. ACB perustuu käyttöoikeusluokkiin, jotka tallennetaan SIM (subscriber identity module) -kortille sitä luotaessa. Käyttöoikeusluokat ovat tavallisille laitteille 0–9. Näistä luokista määritellään jokaiselle laitteelle satunnainen käyttöoikeusluokka. Hätäpuhelut kuuluvat luokkaan 10 ja luokat 11–15 on varattu erityiskäyttöön. Viranomaislaitteiden luokat ovat 12 ja 14, jotka standardissa on määritelty turvallisuuspalveluiden ja pelastustoimen käyttöön. Käyttöluokat eivät määrittele prioriteettia numerojärjestyksessä, vaan niiden avulla voidaan sallia tai estää laitteen liittyminen soluun luokkakohtaisesti. [25]

Kun laite yrittää liittyä verkkoon, sen ensin täytyy vastaanottaa radioverkon järjestelmätiedot. Tukiasemat lähettävät tietoja säännöllisin väliajoin, ja niiden avulla laitteet muun muassa valitsevat solun. Solunvalintaa varten laitteen täytyy tietää, onko tiettyyn soluun liittyminen kielletty. Solu voidaan varata vain tiettyjen käyttöoikeusluokkien käyttöön, jolloin liittyminen on kielletty kaikkien muiden luokkien laitteilta. Myös soluun liittyneet laitteet seuraavat järjestelmätietoja aktiivisesti. Tästä seuraa se, että sallittujen käyttöoikeusluokkien muuttuessa kaikki kiellettyihin luokkiin kuuluvat laitteet poistuvat solusta.

3.2 Häiriöiden ja häirinnän sieto

Häiriöllä voidaan tarkoittaa verkon toiminnan häiriintymistä jollakin tavalla, esimerkiksi sähkönsyötön häiriintyessä tukiasemien tai runkoverkon laitteiden toiminta häiriintyy. Tässä työssä keskitytään kuitenkin sähkömagneettisiin häiriöihin (electromagnetic interference, EMI) tai fyysisten esteiden aiheuttamiin häiriöihin radioliikenteessä. Häirinnällä taas tarkoitetaan tässä työssä tahallista häiriöiden aiheuttamista sähkömagneettisen säteilyn avulla.

Kansainvälisen televiestintäliiton (International Telecommunications Union, ITU) mukaan [26] EMI tarkoittaa ei-toivotun energian aiheuttamaa suorituskyvyn laskua, vääriä tulkintoja tai informaation menetystä. Nämä kaikki aiheuttavat palvelun tason laskua ja viranomaistoiminnassa pahimmillaan jopa henkilöstön tai materiaalin vaarantumista, minkä vuoksi häiriöiden ja häirinnän sieto on kriittistä viranomaisverkoissa. Viranomaisverkkojen käyttöön 3GPP ei kuitenkaan ole standardoinut erillisiä häiriönsietomenetelmiä, joten tältä osalta viranomaisverkot toimivat kuten kuluttajaverkotkin. Häiriöiden lisäksi vastaavia vaikutuksia voi aiheuttaa myös kohina, mutta kohina on yleensä melko hyvin ennustettavissa ja siten siihen varautuminen on helpompaa. Sähkömagneettisia häiriöitä voivat aiheuttaa esimerkiksi muut saman järjestelmän laitteet, korkeajännitelinjat sekä auringon säteilyssä tapahtuvat piikit.

Kanavaolosuhteiden vaihtelun vuoksi LTE:ssä on käytössä linkin mukautumistekniikka [27]. Käytännössä tämä tarkoittaa, että modulaatiomenetelmiä voidaan vaihdella kesken liikennöinnin. Alalinkki, eli yhteys tukiasemalta käyttäjälaitteelle, tukee QPSK (quadrature phase shift keying), 16QAM (quadrature amplitude modulation), 64QAM sekä 256QAM -modulaatioita. Ylälinkki, eli yhteys käyttäjälaitteelta tukiasemalle, tukee näiden lisäksi myös BPSK (binary phase shift keying) -modulaatiota. [28] Digitaalisilla modulaatiomenetelmillä muunnetaan bittisekvenssit symboleiksi, jotka voidaan lähettää radioteitse tehokkaammin kuin yksittäiset bitit. Edellä mainittujen modulaatiomenetelmien suurin ero on bittien määrä per symboli.

Mainituissa QAM-menetelmissä on nimiensä mukaisesti 16, 64 tai 256 erilaista symbolia, joilla voidaan lähettää 4, 6 tai 8 bittiä per symboli. QPSK:ssa taas on 2 bittiä per symboli ja BPSK:ssa 1 bitti per symboli. Suurempi bittien määrä symbolissa tarkoittaa suurempaa virhealttiutta, sillä ajassa yhtä pitkissä symboleissa suuremmalla bittimäärällä sekvenssit voivat sekoittua helpommin toisiinsa. Tämän vuoksi paremman bittivirhesuhteen saavuttamiseksi huonommissa kanavaolosuhteissa käytetään modulaatiomenetelmiä, joissa bittien määrä per symboli on pienempi. Vastaavasti paremmissa kanavaolosuhteissa voidaan saavuttaa parempia bittinopeuksia käyttämällä modulaatiomenetelmiä, joissa on enemmän bittejä per symboli. Tärkeä häiriölähde ulkopuolisten laitteiden tai ilmiöiden lisäksi on myös lähetetty signaali itse, jolloin on kyse symbolien välisestä häiriöstä (intersymbol interference, ISI).

Symbolien väliset häiriöt voivat aiheutua monitie-etenemisestä tai siitä, että signaali on kaistarajoitettu. Kaistarajoitettu signaali on nimensä mukaisesti signaali, jonka kaistanleveys on rajoitettu. Signaaleja äärettömällä kaistanleveydellä on käytännössä mahdotonta käyttää jo käytännön syistä, sillä se sallisi vain yhden radiotaajuisen järjestelmän käytön kerrallaan. Tämän vuoksi kaikilla käytössä olevilla radiojärjestelmillä on oma, rajattu taajuusalueensa. Monitie-eteneminen tarkoittaa saman signaalin päätymistä vastaanottajalle montaa eri reittiä pitkin. Eri reittejä saapuneita saman signaalin versioita kutsutaan monitiekomponenteiksi. Eri monitiekomponentit kokevat erilaiset kanavaolosuhteet, joihin vaikuttavat häiriöiden lisäksi fyysiset esteet, kuten maasto, rakennukset ja mahdollinen laitteen liike. Erityisen tärkeää monitiekomponenteissa on niiden vaihe-ero, eli kuinka paljon komponentit ovat viivästyneet toisiinsa nähden. Komponenttien viivästymisestä johtuen tietty symboli voi saapua samaan aikaan jonkin toisen symbolin kanssa ja aiheuttaa häiriötä.

Symbolien välisiä häiriöitä voidaan estää esimerkiksi käyttämällä suojajaksoa ja syklistä etuliitettä symbolien lähettämisen välillä ja taajuuskorjainta vastaanottavassa laitteessa. Suojajakso on symbolien lähettämisen välillä pidettävä ajanjakso, jolloin ei lähetetä mitään, ja syklinen etuliite on jokaiseen symboliin liitettävä ja molemmille osapuolille tunnettu etuliite. Näiden avulla pyritään varmistamaan, että symbolien alku ja loppu pystytään havaitsemaan luotettavasti. Taajuuskorjaimen avulla taas pyritään kumoamaan kanavan aiheuttamat vääristymät signaalissa. Tähän tarvitaan kuitenkin jonkinlainen arvio kanavasta, joka pystytään luomaan LTE:n vertailusignaalien avulla.

Vertailusignaaleja käytetään kanavan siirtofunktion arvioimiseen, jotta päätelaitteissa voidaan käyttää taajuuskorjaimia. Vertailusignaaleja on useita ja ne on määritelty 3GPP:n standardeissa [28]. Vertailusignaalien avulla lasketaan myös useita yhteyden laadun tunnuslukuja, kuten vastaanotetun signaalin voimakkuuden ilmaisin (reference signal strength indicator, RSSI), vastaanotetun vertailusignaalin teho (reference signal received power, RSRP), vastaanotetun vertailusignaalin laatu (reference signal received quality, RSRQ) ja signaali-häiriö-kohinasuhde (signal to interference and noise ratio, SINR). Nämä tunnusluvut liittyvät pääasiassa käyttäjälaitteen solunvalintaan, ja niiden laskenta käyttäjälaitteessa perustuukin tukiaseman lähettämään vertailusignaaliin. Myös joitakin päinvastaisesti toimivia tunnuslukuja on käytössä, esimerkiksi vastaanotettu häiriöteho (received interference power, RIP) sekä signaalin saapumiskulma (angle of arrival, AoA). [29]

RSSI saadaan laskemalla keskiarvo vastaanotettujen OFDM-symbolien tehoista. RSRP on saman tyyppinen luku, mutta siinä missä RSSI:n tehomittaukset tehdään käytössä olevan kaistanleveyden perusteella, RSRP:n mittaukset tehdään koko mahdollisen kaistanleveyden perusteella. [29] RSSI siis on sitä suurempi, mitä enemmän taajuuskaistaa on käytössä, vaikkei itse signaalin voimakkuus olisi parempi. RSRP taas voi menettää yksityiskohtaista tietoa jonkin tietyn taajuusalueen kanavaolosuhteista. Näiden ominaisuuksien vuoksi käytössä on myös RSRQ, joka ottaa huomioon RSSI:n ja RSRP:n suh-

teen, sekä käytössä olevien resurssilohkojen (resource block, RB) lukumäärän [29]. RB on pienin allokoitava resurssien määrä LTE-verkon fyysisellä kerroksella. SINR:n tarkoituksena on kertoa, kuinka hyvin lähetetty signaali kuuluu verrattuna häiriöihin ja kohinaan. SINR lasketaan jakamalla keskimääräinen signaaliteho yhteenlasketulla keskimääräisellä häiriö- ja kohinateholla [29].

Tukiaseman laskemia tunnuslukuja on vähemmän, sillä LTE-verkoissa päätös solunvalinnasta tehdään pääasiassa käyttäjälaitteen mittaamien tietojen perusteella [30]. Kuitenkin RIP mitataan yhden resurssilohkon taajuudelta, ja tuloksia saadaan yhtä monta kuin alikantoaaltoja on käytössä [29]. Näiden tulosten perusteella voidaan määrittää, mitä alikantoaaltoja kannattaa käyttää. AoA ei varsinaisesti liity solunvalintaan tai kanavaresurssien käyttöön, vaan se kertoo käyttäjälaitteen suunnan verrattuna karttapohjoiseen [29]. Tätä tietoa voidaan käyttää esimerkiksi keilanmuodostuksessa, joka on merkittävä tekniikka signaalin kuuluvuuden ja häiriönsiedon parantamiseksi.

Keilanmuodostus tarkoittaa signaalin lähettämistä niin, että pääosa signaalin energiasta suuntautuu haluttuun suuntaan. Kun suuri osa energiasta lähetetään tiettyyn suuntaan, saadaan vakiolähetysteholla ja samalla etäisyydellä parempi SINR verrattuna tilanteeseen, jossa ei käytetä keilanmuodostusta. Käytännössä tämä voidaan tehdä joko aikatasossa tai taajuustasossa ohjaamalla antenniryhmää analogisesti tai digitaalisesti. Aikatason keilanmuodostuksessa signaalikomponenttien vaihetta, eli viivettä, muokataan niin, että komponenttien summautuessa lähetettävä signaali muodostaa keilan haluttuun suuntaan. Taajuustason keilanmuodostus taas perustuu siihen, että viive aikatasossa vastaa muutosta taajuustasossa. Taajuustasossa keilat ovat painotettuja lineaarikombinaatioita signaalien Fourier-muunnosten kertoimista. Analogista keilanmuodostusta käyttävä järjestelmä on yksinkertaisempi toteuttaa ja vaatii vähemmän laskentatehoa, mutta digitaalinen keilanmuodostus mahdollistaa pienemmän näytteenottotaajuuden käytön. Lisäksi digitaalisen keilanmuodostuksen kanssa voidaan käyttää suurempaa määrää antennielementtejä. [31]

Aikatasossa käytetään ainoastaan analogista keilanmuodostusta. Siinä syötetään sama signaali kaikille antenneille, mutta signaalien vaiheita muokataan yksittäin ennen antennia. Digitaalisessa keilanmudostuksessa signaali muokataan etukäteen jokaiselle antennielementille erikseen. Tämä mahdollistaa Fourier-muunnosten tekemisen yksittäisille signaalikomponenteille ja siten taajuustason keilanmuodostuksen. Digitaalista keilanmuodostusta voidaan kuitenkin käyttää myös aikatasossa.

Keilanmuodostuksen mahdollistaa useiden antennien yhtäaikainen käyttö. Tämä tekniikka on nimeltään MIMO (multiple-input multiple-output), kun antenneja on useita sekä lähetykseen että vastaanottoon. Mobiiliverkoissa suuria antenniryhmiä mahtuu ainoastaan tukiasemiin, joiden täytyy palvella useita käyttäjälaitteita yhtä aikaa. Jokaiselle käyttäjälaitteelle ei kuitenkaan voi fyysisen tilan sekä kustannusten vuoksi olla omaa antenniryh-

määnsä, joten useiden laitteiden tulee käyttää samoja antenniryhmiä. Tällä lisäyksellä saadaan MU-MIMO (multi-user MIMO), joka käytännössä tarkoittaa samanaikaista lähettämistä monelle käyttäjälaitteelle. Monen antennin käyttäminen vaatii myös niiden sijoittamista erilleen toisistaan, joka parantaa toimintavarmuuden lisäksi myös spektraalista tehokkuutta. [32] Spektraalisesti tehokas järjestelmä saavuttaa samalla taajuuskaistalla paremman bittinopeuden kuin spektraalisesti tehoton järjestelmä. Näin voidaan palvella useampia käyttäjiä kapeammilla taajuuskaistoilla, jotka ovat vähemmän alttiita häiriöille. Toisaalta, kun käyttäjiä on vähemmän, voidaan suuremman bittinopeuden saavuttamiseksi yhdistää kantoaaltoja.

Kantoaaltojen yhdistäminen (carrier aggregation, CA) mahdollistaa usean kapean taajuusalueen yhtäaikaisen käytön. LTE:ssä yhdelle käyttäjälle varattava yhden kantoaallon taajuusalue voidaan valita 1,4 MHz ja 20 MHz väliltä, ja kantoaaltoja voidaan yhdistää niin, että kokonaistaajuus on maksimissaan 640 MHz. Kantoaaltojen ei tarvitse käyttää vierekkäisiä taajuusalueita, ja eri kantoaallot voidaan lähettää eri tukiasemille. [30] Yhteyden hajauttaminen usealle fyysisesti eri paikoissa vastaanotettavalle kapealle taajuuskaistalle vähentää yhteyden alttiutta satunnaisille häiriöille huomattavasti.

Satunnaisten häiriöiden lisäksi myös tarkoituksellinen häirintä on mahdollista. Radiotaajuushäirintää voidaan tehdä lähettämällä halutulla taajuusalueella esimerkiksi satunnaissignaalia suuremmalla teholla kuin häirittävä järjestelmä. Mikäli taajuusalueeksi valitaan järjestelmän taajuusalue kokonaan tai lähes kokonaan, on kyseessä raakaan voimaan perustuva hyökkäys (brute force jamming). Tämä tapa perustuu häirittävän järjestelmän signaalien peittämiseen, ja siten vaadittava lähetysteho voi olla hyvinkin suuri riippuen häirittävän alueen koosta. Esimerkiksi taajuusmoduloidun radiosignaalin häiritseminen vaatii 15 dB suuremman lähetystehon häiritsijän ollessa 2 kertaa kauempana vastaanottajasta kuin lähettäjä. Taajuusmoduloitu signaali vaatii tarpeeksi suuren SINR:n, jotta vastaanotetusta signaalista voidaan tulkita informaatiota onnistuneesti. [33] Tämän ominaisuuden vuoksi taajuusmodulaatiota voidaan käyttää vertailukohtana myös nykyaikaiselle LTE-verkolle.

Häirintäsignaalit voidaan kuitenkin kohdistaa tiettyihin kantoaaltoihin tai ne voidaan suunnitella estämään tietty osa verkon kontrolliliikenteestä, jolloin käytetään nimitystä älykäs häirintä (smart jamming). Erityisesti LTE-verkoissa häirinnän kohteeksi voidaan valita OFDM-modulaatioon upotetut vertailusignaalit, joita käytetään kanavan arvioimiseen. Nämä signaalit voidaan pyrkiä joko peittämään kohinasignaalin alle, tai nollaamaan vastakkaisen signaalin avulla. Vertailusignaalin peittäminen toimii samalla periaatteella kuin brute force -hyökkäys, mutta vain vertailusignaalin taajuudella. Nollaaminen taas perustuu siihen, että häiritsijä tietää vertailusignaalin muodon. Tällöin häiritsijä voi muodostaa signaalille vastakkaisen parin, joka destruktiivisen interferenssin kautta nollaa vertailusignaalin. Verrattuna brute force -hyökkäykseen vertailusignaalien häiritseminen on huomattavasti energiatehokkaampaa, ja vertailusignaalin nollaaminen on vielä tehokkaampaa

kuin sen peittäminen kohinasignaalilla. [34]

Vertailusignaalin onnistunut häiritseminen johtaa siihen, että järjestelmä tulkitsee kanavaolosuhteet väärin ja taajuuskorjaa signaalin väärin, mikä johtaa symbolien bittisekvenssien virhetulkintoihin. Häiritsijän on kuitenkin pystyttävä seuraamaan radioliikennettä ja tiedettävä vertailusignaalien muoto. LTE-verkkojen kanssa molemmat vaatimukset on suhteellisen helppo toteuttaa, sillä vertailusignaalit on määritelty avoimesti saatavilla olevissa standardeissa. Tämän heikkouden ratkaisu on haastavaa, sillä verkkoon liittyminen vaikeutuisi huomattavasti, mikäli vertailusignaaleja ei jaettaisi vapaasti. Eräs ratkaisu voisi olla julkisen avaimen kryptografiaan perustuva vertailusignaalien määrittely, mutta tällaista ei ole vielä kehitetty [34]. Ratkaisun löytämiseen saakka LTE-signaalien tehokas häirintä rajatulla alueella on suhteellisen helppoa, ja voi pahimmassa tapauksessa tehdä tiedonsiirron mahdottomaksi.

Kari Junttilan mukaan [4] viranomaisverkoissa nojataan mahdottomien kanavaolosuhteiden tapauksissa täysin erillisiin varajärjestelmiin. Tällaisia voivat olla esimerkiksi paikallisesti toimivat perinteiset radiopuhelimet tai viimeisenä vaihtoehtona kynä ja ruutupaperi. Lisäksi LTE-standardit määrittelevät, että huonoissa kanavaolosuhteissa tulee poistaa paljon dataa vieviä palveluita käytöstä, mikä osaltaan helpottaa tilannetta kaikkein kriittisimmille puheyhteyksille. Myös TETRA-pohjaiselta Virveltä vapautuvaa 380–400 MHz taajuusaluetta voi olla mahdollista käyttää Virve 2.0:n laajentamiseen. Tämä taajuusalue on huomattavasti Virve 2.0:n LTE-taajuuksia matalampi, mutta MOCN-arkkitehtuuri mahdollistaa lähes minkä tahansa radioverkon käytön. Kuitenkin tällä taajuusalueella datanopeudet tulisivat olemaan huomattavasti pienempiä, joten sekin soveltuisi nykyisen Virven tapaan lähinnä puheen välittämiseen.

3.3 Tietoturva

Tietoturva määritellään Sanastokeskus ry:n Kyberturvallisuuden sanastossa [35] seuraavasti: "järjestelyt, joilla pyritään varmistamaan tiedon saatavuus, eheys, ja luottamuksellisuus". Saatavuudella tarkoitetaan, että tietoa voi hyödyntää silloin kun se on tarpeen. Tämän luvun aiemmissa alaluvuissa käsitellyt osa-alueet ovat tärkeä osa saatavuutta, mutta tietoturvan kannalta tärkeää on pystyä minimoimaan saatavuutta heikentävien hyökkäysten vaikutus. Eheys ja luottamuksellisuus puolestaan viittaavat tiedon koskemattomuuteen. Tieto on ehyttä, kun se ei muutu lähetyksen ja vastaanoton välillä. Luottamuksellisuus tarkoittaa, että lähetetty tieto ei päädy kenenkään ulkopuolisen haltuun. Viranomaisviestinnässä nämä seikat ovat erittäin tärkeitä, sillä häiriöt verkkojen saatavuudessa tai tietojen eheydessä voivat johtaa vaaratilanteisiin tai vääriin toimenpiteisiin. Lisäksi luottamuksellisen tiedon joutuminen vääriin käsiin voi aiheuttaa merkittävää vahinkoa yksittäisille henkilöille tai valtion turvallisuudelle.

Saatavuutta voidaan heikentää aiemmin käsitellyn radiohäirinnän lisäksi erilaisilla palve-

lunestohyökkäyksillä (denial of service attack, DoS). Nimensä mukaisesti näissä hyökkäyksissä pyritään saamaan aikaan tilanne, jossa hyökkäyksen kohteena oleva palvelu ei pysty vastaamaan sille lähetettyihin pyyntöihin. Tällaisen tilanteen voi aiheuttaa joko brute force -hyökkäyksellä tai hyväksikäyttämällä haavoittuvuutta palvelussa. Brute force -hyökkäyksessä lähetetään palvelulle niin paljon pyyntöjä, että joko palvelun käytössä oleva verkkoyhteys tai laitteistoresurssit ylikuormittuvat. Tällaisissa hyökkäyksissä yleensä käytetään bottiverkkoja, jotka muodostetaan tietokoneista tai muista laitteista, joihin on saatu asennettua etäohjauksen mahdollistava haittaohjelma. Tällöin käytetään yleensä termiä hajautettu palvelunestohyökkäys (distributed denial of service attack, DDoS), sillä bottiverkkojen laitteet yleensä ovat tavallisten ihmisten laitteita ympäri maailmaa. Palvelunestohyökkäyksen mahdollistavat haavoittuvuudet toimivat niin, että palvelu saadaan virhetilaan, jossa se ei pysty palvelemaan käyttäjiä. Nämä haavoittuvuudet eivät yleensä mahdollista tietojen varastamista tai käyttöoikeuksien korottamista, mutta joitakin haavoittuvuuksia voidaan käyttää moniin tarkoituksiin.

Muuntyyppiset haavoittuvuudet voivat mahdollistaa esimerkiksi väliintulohyökkäyksen (man-in-the-middle attack, MITM), jolloin hyökkääjä voi kuunnella liikennettä tai muokata lähetettyjä viestejä. Lisäksi käyttöoikeuden korottamisen mahdollistavat haavoittuvuudet voivat avata hyökkääjälle mahdollisuuksia edetä pidemmälle ja mahdollisesti luoda takaportteja järjestelmään haavoittuvuuksien paikkaamisen varalta. Tällaisten riskien minimoimiseksi ennaltaehkäisevät toimet ovat ensisijaisen tärkeitä. Mikäli hyökkääjä saa jonkinlaisen jalansijan järjestelmään, tämä täytyy tietysti havaita ja eteneminen estää, mutta tiedon luottamuksellisuuden kannalta on parempi, ettei hyökkääjä saa tietoonsa mitään ulkopuolisille kuulumatonta.

LTE-verkko on jaettu hallinnollisiin kerroksiin, joiden tarkoituksena on auttaa tietoturvamääritysten kohdentamista oikein. Kerroksia ovat sovelluskerros, kotikerros ja siirtokerros. Sovelluskerros on kerroksista ylin, ja sillä toimivat normaalit käyttäjälle näkyvät palvelut. Kotikerroksella, tai palvelevalla kerroksella, toimivat operaattorin runkoverkon palvelut, kuten käyttäjän tunnistus ja laskutuksen hallinta. Siirtokerroksella taas tapahtuu radioliikenne ja sen hallinta. [36] Laitteen liittyessä verkkoon, siirtokerroksella on ensimmäisenä vuorossa käyttäjän ja tukiaseman tunnistus.

Käyttäjän ja tukiaseman tunnistusprosessi tapahtuu haaste-vaste protokollalla, joka on 3GPP:n standardissa määritelty authentication and key agreement (AKA). AKA-prosessin avulla määritellään myös salausavaimet käyttäjälaitteen ja tukiaseman välisen käyttäjä- ja kontrolliliikenteen salaamiseen, mikäli operaattori on nämä valinnaiset ominaisuudet ottanut käyttöön. Tämä prosessi alkaa käyttäjän pyytäessä lupaa liittyä verkkoon, jolloin verkon päätelaiteliikkuvuutta hallinnoiva laite (mobile management entity, MME) lähettää laitteelle satunnaisen haasteen. Vastaanotettuaan haasteen käyttäjälaite varmistaa sen aitouden, ja laskee vasteen USIM (universal subscriber identity module) -sovelluksella. USIM on SIM-kortin toiminnallisuudet toteuttava sovellus, jota käytetään tietoturvaomi-

naisuuksien tuottamiseen [37]. Lisäksi USIM:n avulla lasketaan salaus- ja eheysavaimet **CK** ja **IK**, jotka lähetetään MME:lle. Mikäli laitteelta saatu vaste oli oikea, MME laskee avaimen **K** saatujen avaimien perusteella ja lähettää **K**:n käyttäjälaitteelle verkon identiteetin kanssa. Käyttäjälaite tarkistaa, että avain on MME:n laitteen itsensä lähettämien tietojen perusteella laskema. Samalla todennetaan verkon identiteetti. Lopuksi molemmilla laitteilla on varmuus toisen laitteen identiteetistä sekä avain liikenteen salaamiseen. [36]

Identiteetin varmistukseen käytetään IMSI (international mobile subscriber identity) -numeroita, jotka koostuvat maa- ja operaattorikoodista sekä yksilöllisestä tunnisteesta [38]. Nämä numerot tallennetaan SIM-kortille, ja ne muuttuvat vain operaattoria vaihdettaessa. Tämän vuoksi IMSI-numeroita on mahdollista käyttää mobiililaitteiden seuraamiseen. Käytännössä mobiililaitteiden seuraaminen tarkoittaa henkilöiden seuraamista, joten tämä on viranomaisverkkojen kannalta suuri uhka henkilöstön turvallisuudelle. IMSI-numeroita pyritään kuitenkin LTE-verkoissa lähettämään ainoastaan laitteen liittyessä tiettyyn verkkoon ensimmäistä kertaa, joten standardeissa on määritelty tilapäisiä identiteettinumeroita, kuten TMSI (temporary mobile subscriber identity) ja GUTI (globally unique temporary identity). TMSI on käytössä vain yhden MME:n alueella, kun taas GUTI yhdistää TMSI:n sekä tiedon siitä, millä MME:llä on tieto TMSI–IMSI-yhteydestä. [39]

Vaikka edellä mainittujen TMSI:n ja GUTI:n tulisi olla väliaikaisia, ne eivät sitä aina välttämättä ole. Tämä johtuu suurelta osin siitä, että operaattorit voivat verkon toimintaa tehostaakseen olla vaihtamatta identiteettejä tarpeeksi usein. Identiteettien pysyminen samana johtaa niiden hyötyjen menettämiseen, eli käytännössä käyttäjiä voidaan seurata edelleen. Seuraamisessa käytetään hyväksi myös LTE-verkon älykästä hakua (smart paging) eli menetelmää, jolla verkko löytää laitteen käyttämän solun. Verkkojen toiminnan tehostamiseksi hakuviestit lähetetään vain tietyn solun alueelle koko hakualueen (tracking area, TA) sijasta. TA on alue, jonka yksi tukiasema kattaa, ja solu on osa tästä alueesta. [40]

Seurantahyökkäyksiä voi tehdä passiivisesti, puolipassiivisesti tai aktiivisesti. Passiivisessa hyökkäyksessä hyökkääjä vain kuuntelee liikennettä, ja puolipassiivisessa hyökkääjä voi aiheuttaa kuunneltavaa liikennettä. Aktiivisessa hyökkäyksessä taas käytetään valetukiasemaa. Passiivinen liikenteen kuuntelu ja väliaikaisten identiteettien seuranta on mahdollista, sillä näitä identiteettejä lähetetään yleislähetyksinä salaamattomana sekä ilman tunnistautumista. Koska nämä yleislähetykset lähetetään vain sille alueelle, jossa käyttäjälaite verkon tietojen mukaan on, voidaan niiden perusteella passiivisesti seurata laitteen liikkeitä alueelta toiselle tietyn aikavälin sisällä. Puolipassiivisen hyökkäyksen avulla voidaan saada selville laitteen karkea sijainti tietyllä ajanhetkellä. Aktiivista valetukiasemaa käyttämällä voidaan selvittää laitteen tarkka sijainti pyytämällä käyttäjälaitteelta raportti tukiasemien kuuluvuuksista. Nämä pyynnöt lähetetään myös suojaamattomina, joten käyttäjälaite ilmoittaa tukiasemien kuuluvuudet ja jopa GPS (global positioning system)

-koordinaatit, mikäli laite tukee niiden lähettämistä. Ilman GPS-koordinaattejakin laite voidaan paikantaa kolmiomittauksen avulla, kun tiedetään muiden tukiasemien sijainnit. [40]

Aktiivisen valetukiaseman käyttö on mahdollista, sillä tunnistusprosessi ei estä MITM-hyökkäystä. Tällaisessa hyökkäyksessä luodaan valetukiasema ja pakotetaan käyttäjälaite liittymään siihen. Tämä onnistuu suhteellisen helposti, sillä käyttäjälaitteen verkosta poistamiseen käyttettävien viestien eheyttä ei tarkisteta [41]. AKA-prosessissa ei ole kuitenkaan havaittu vääriä tunnistamistuloksia aiheuttavia tai salausavaimia vaarantavia haavoittuvuuksia, joten hyökkääjään täytyy käyttää hyväkseen oikeaa verkkoa, eikä tämä pysty purkamaan liikenteen salausta. Käytännössä hyökkääjä esiintyy käyttäjälaitteelle tukiasemana ja tukiasemalle käyttäjälaitteena. Hyökkääjä lähettää tunnistusprosessin viestit edelleen molemmille osapuolille, jolloin saadaan aikaan tunnistettu yhteys sekä käyttäjälaitteelle että tukiasemalle. LTE:ssä sekä kontrolliliikenne että käyttäjädata lähetetään salattuna, mutta vain kontrolliliikenteen eheys on suojattu. Tämä tarkoittaa sitä, että hyökkääjän on mahdollista manipuloida käyttäjädataa.

Rupprecht et al. esittävät tutkimuksessaan [42] kolme edellä mainittua heikkoutta hyväksikäyttävää hyökkäystä. Esitetyt hyökkäykset toimivat siirtoyhteyskerroksella, jossa AKA-prosessista ei ole hyötyä, sillä se toimii verkkokerroksella. Passiivisesti voidaan saada selville käyttäjän sijainti ja identiteetti sekä käytettyjä verkkosivuja. Sijainnin selvittäminen tapahtuu kuten edellä on selitetty, mutta käytettyjen verkkosivujen seuraaminen perustuu fingerprinting-tekniikkaan. Tätä tekniikkaa käytettäessä seurataan salattua liikennettä ja pyritään löytämään siitä toistuvia osia. Hyökkääjä voi myös mallintaa tiettyjen palvelujen aiheuttamaa liikennettä ja verrata sitä käyttäjän liikenteeseen.

Kolmantena voidaan aktiivisen hyökkäyksen avulla manipuloida nimipalvelinjärjestelmän (domain name system, DNS) paketteja, jolloin voidaan ohjata laite käyttämään hyökkääjän DNS-palvelinta. DNS-paketit on helppo havaita muun liikenteen joukosta, sillä ne ovat keskimäärin merkittävästi muita paketteja pienempiä. Itse muokkaaminen tapahtuu modulo 2 -yhteenlaskun avulla, sillä LTE-verkoissa käytettävän jatkuvan salakirjoituksen avain luodaan käyttäen AES (advanced encryption standard) -salausta CTR (counter) -menetelmällä, ja laskemalla salattava data yhteen avaimen kanssa modulo 2 -yhteenlaskuna. [42] Koska käyttäjädataa ei myöskään eheystarkisteta, ei muokkaamista samalla menetelmällä havaita. Tämä on merkittävä heikkous, mutta se voidaan viranomaisverkoissa kiertää sallimalla runkoverkon puolella DNS-kyselyt vain hyväksytylle palvelimelle. Tietenkään tämä ei poista mahdollisuutta muokata mitä tahansa muita paketteja.

Runkoverkon puolella LTE:ssä kaikkea liikennettä ei oletuksena salata, mikä mahdollistaa esimerkiksi sopivassa kohtaa verkossa sijaitsevien verkkolaitteiden tai palvelimien haavoittuvuuksien käyttämisen liikenteen kuunteluun. Tämän liikenteen suojaamiseen voidaan kuitenkin 3GPP:n määrittelyn mukaan käyttää IPsec (internet protocol security) -

pohjaista ratkaisua. LTE:n tapauksessa tämä on pakollista vain osalle kontrolli- ja käyttäjäliikenteestä. [36] IPsec:ä on perinteisesti käytetty VPN (virtual private network) -ratkaisuna kahden laitteen tai verkon yhdistämiseen tuntemattomien linkkien yli, joten se soveltuu vahvaa salausalgoritmia käytettäessä hyvin liikenteen suojaamiseen. Kaiken liikenteen salaaminen voi kuitenkin aiheuttaa verkolle lisää kuormaa, kun pakettien koko kasvaa IPsec-otsikkojen vuoksi.

Liikenteen kuuntelun runkoverkossa mahdollistava haavoittuvuus ei välttämättä ole vahinko. Valtiolliset tiedusteluorganisaatiot voivat pyrkiä vaikuttamaan standardien valmisteluun tai maassa valmistettaviin laitteisiin ja ohjelmistoihin. Tämän tyyppisen vaikuttamisen seurauksena voi tuotteisiin jäädä takaovia, eli tarkoituksellisia haavoittuvuuksia. Esimerkiksi Yhdysvaltain kansallisen turvallisuuden virasto NSA:n (National Security Agency) on kerrottu pyrkineen systemaattisesti heikentämään salausteknologioita Bullrun-projektinsa kautta. Projektin näkyvin osa oli pyrkimys saada standardoitua salausteknisesti turvallinen näennäissatunnaislukugeneraattori, jossa käytettiin kahta pistettä elliptiseltä käyrältä näennäissatunnaislukujen tuottamiseen. Generaattorin käytettäväksi määritellyt elliptiset käyrät ja muut lähtoarvot oli kuitenkin valittu niin, että tuotetut luvut olivat ennustettavissa. [43] Tämä on vakava heikkous, sillä salausalgoritmien perusteena olevat matemaattiset ongelmat perustuvat olennaisesti lukujen satunnaisuuteen. Salaustekniikan turvallisuus on viranomaistoiminnassa erityisen tärkeää, sillä tiedon luottamuksellisuus, ja useissa tilanteissa eheys, riippuvat salauksen toimivuudesta.

Takaovet ovat riski myös laitteistotasolla. Yhdysvallat sekä muutamat muut maat ovat kieltäneet Huawein ja ZTE:n (Zhong Xing Telecommunication Equipment Company) laitteiden käytön, sillä Kiinan hallituksen väitetään käyttävän kiinalaisyrityksiä osana tiedustelutoimintaansa. Yhdysvallat on tiettävästi esittänyt liittolaisilleen todisteita takaovien olemassaolosta, mutta niitä ei ole tuotu julkisuuteen. [44] Suomen lainsäädännössä on varauduttu myös tietoturvattomiin laitteisiin, ottamatta kuitenkaan kantaa laitteen valmistajaan tai tietoturva-aukon tahallisuuteen. Tämä varautuminen näkyy laissa sähköisen viestinnän palveluista, jossa säädetään, että viestintäverkon kriittisissä osissa ei saa käyttää laitteita, jotka voivat aiheuttaa häiriötä tai muodostaa turvallisuusuhan. Lisäksi liikenne- ja viestintävirasto voi velvoittaa verkon omistajaa poistamaan laitteita verkosta, jos ne täyttävät edellä mainitut kriteerit. [45] Tällä lähestymistavalla on mahdollista reagoida uusiin tietoturvauhkiin nopeasti, mikä on tärkeää nopeasti kehittyvän teknologian kanssa.

Nopeasti kehittyvä teknologia aiheuttaa myös inhimillisiä haasteita, sillä työntekijät täytyy kouluttaa uusien laitteiden käyttöön sekä varautumaan uudenlaisiin tietoturvauhkiin. Ehkä suurin hyökkäysvektori mitä tahansa järjestelmää kohtaan on järjestelmän käyttäjät, olivat he sitten johtajia, tukihenkilöitä tai tietoturva-asiantuntijoita. Usein tehokkainta on räätälöidä kalasteluhyökkäys tiettyä organisaatiota tai sen avainhenkilöitä kohtaan. Varsinkin hyvin organisoitua hyökkäystä voi olla vaikea tunnistaa, ja näiden hyökkäysten seurauksena voi päätyä luottamuksellista tietoa tai käyttäjätunnuksia vääriin käsiin.

4. VIRANOMAISVERKKOJEN TULEVAISUUS

Lähitulevaisuus tulee olemaan mielenkiintoinen mobiiliverkkojen kannalta. Viidennen sukupolven verkkojen käyttöönotto on edistynyt melko pitkälle, esineiden internetin (Internet of Things, IoT) sovellukset ovat kehittyneet huomattavasti sekä tekoäly ja muita uusia teknologioita on noussut pelkkien mainossanojen tasalta varteenotettaviksi työkaluiksi. Viranomaisverkotkin tulevat saamaan tästä kehityksestä osansa. Esimerkiksi Virve 2.0 -projektin mobiilistrategiassa [46] on mainittu kriittinen IoT, dronet sekä etälääketiede mahdollisina käyttökohteina. Lisäksi projektille on luotu erillinen tekoälystrategia [47], mikä kertoo siitä, että tekoälysovellusten odotetaan tehostavan viranomaistoimintaa tulevaisuudessa.

4.1 5G-matkapuhelinverkkojen vaikutus

ITU on kansainvälisiä mobiiliverkkoja koskevassa suosituksessaan [48] määrittänyt havaitsemiensa kehityssuuntien perusteella matkapuhelinverkkojen palveluille 3 kategoriaa. Nämä kategoriat ovat parannettu mobiililaajakaista (enhanced mobile broadband, eMBB), massiivinen konetyypin kommunikaatio (massive machine type communications, mMTC) sekä erittäin luotettava pienen viiveen kommunikaatio (ultra-reliable low latency communications, URLLC). Viidennen sukupolven matkapuhelinverkoista puhuttaessa usein nousee esiin eMBB, sillä se näkyy tavallisille käyttäjille eniten. Silti viranomaisverkot eivät ainakaan lähitulevaisuudessa tule käyttämään 5G:n eMBB-ominaisuuksia ja millimetriaaltoaluetta, mutta Virve 2.0:n runkoverkko toteutetaan niin, että uusia radioverkon ominaisuuksia ja taajuusalueita voidaan ottaa käyttöön helposti [4]. Korkeataajuisten signaalien eteneminen estyy melko helposti, joten esimerkiksi metsässä toimiminen olisi lähes mahdotonta, sillä tukiasemia tarvittaisiin hyvin tiheään. MMTC ja URLLC toimivat myös matalammilla taajuuksilla, sillä millimetriaaltoaluetta käytetään lähinnä gigabittiluokan datanopeuksien saavuttamiseen. Viranomaisverkoille tärkeämpiä ja hyödyllisempiä ovat siis mMTC ja URLLC.

Aiemmissa matkapuhelinverkkostandardeissa erityisesti liikenteen satunnainen luonne sekä laitteiden suuren tiheyden saavuttaminen ovat aiheuttaneet ongelmia. IoT-laitteet ovat tyypillisesti sensoreita tai erilaisia verkkoon kytkettyjä koneita ja laitteita, joita ei perinteisesti ole liitetty verkkoon. Erityisesti sensoreiden tarvitsee siirtää pieniä datamääriä

suhteellisen harvoin, jolloin jatkuvaa liikennettä varten suunnitelluissa verkoissa kontrolliliikenteen ja otsikkotietojen rasite nousee suureksi. [49] Lisäksi uusia verkkoyhteyttä vaativia laitteita tuodaan markkinoille jatkuvasti, joten verkkoon liitettävien laitteden määrä tulee nousemaan nopeasti, vaikka uusien matkapuhelinliittymien markkina onkin jo saturoitunut [50]. Tämä ongelma pyritään ratkaisemaan mMTC:n avulla. LTE-standardiin on jo lisätty osittainen tuki kapean kaistan IoT-laitteille, mutta se ei täytä kaikkia mMTC:lle asetettuja vaatimuksia, kuten laitteiden suurta määrää [49].

MMTC:n tavoitteena oleva laitteiden tiheys on luokkaa $10^6/km^2$ [48]. Tämä tuo haasteita erityisesti kontrolliliikenteen ja kapasiteetin suhteen. LTE-verkossa pienenkin datamäärän lähettäminen tai vastaanottaminen aiheuttavat aina siirtymisen valmiustilasta yhdistettyyn tilaan, joka puolestaan vaatii huomattavasti kontrolliliikennettä. Lisäksi yhdistettyyn tilaan siirryttäessä laitteelle varataan resursseja, mutta LTE:n resurssienvarausprosessissa ei ole törmäyksenselvitysmekanismia. [49] Tämä johtaa siihen, että verkon ruuhkatilanteessa laitteet eivät välttämättä saa yhteyttä luotua, jolloin esimerkiksi hälytysjärjestelmän lähettämä hälytys ei mene perille. Lisäksi kontrolliliikenne ja lähetysten uudelleen yrittäminen aiheuttavat ylimääräistä virrankulutusta, joka on usein paristokäyttöisille sensoreille haitallista.

Virrankulutusta LTE-verkoissa aiheuttavat myös hakuviestit, joita laitteiden tulee kuunnella jatkuvasti vastaanottaakseen niille tulevat lähetykset. Hakuviestit ovat usein turhia IoT-laitteiden tapauksessa, sillä nämä laitteet harvoin liikkuvat solujen välillä. 5G-verkkojen mMTC-ominaisuuksien standardointi on vielä kesken, mutta erityisesti virrankulutusta voisi vähentää parantamalla yhteydenmuodostusprosessia sekä muuttamalla hakuviestejä niin, että laite pyytää verkolta uusia lähetyksiä tietyin väliajoin. [49]

Viranomaisverkoissa mMTC-tuesta voisi olla hyötyä esimerkiksi erilaisten valvontajärjestelmien muodossa. Suomella on Venäjän kanssa huomattavan pitkä raja, joka on myös Euroopan unionin ulkoraja. Tätä rajaa ei ole mahdollista valvoa aukottomasti pelkin ihmisvoimin, joten pitkin rajavyöhykettä asetetut sensorit voisivat toimia rajavalvonnan tukena. Lisäksi verkkoon liitettyjä sensoreita voi käyttää etälääketieteen apuna, jolloin potilaan ei tarvitsisi välttämättä lähteä kotoaan tutkimuksia varten. Tämä käyttökohde ei välttämättä tarvitse juuri viranomaiskäyttöön varattua radioverkkoa, mutta tiedot vastaanottava palvelin todennäköisesti tietoturva- ja -suojavaatimusten vuoksi tulisi sijaitsemaan jossakin viranomaisten verkossa.

URLLC:n tarkoitus on täyttää kriittisen infrastruktuurin viive- ja luotettavuusvaatimukset. Viiveiden alentaminen perustuu osittain palveluiden ja palvelinten tuomiseen tukiaseman lähelle, mutta myös pakettien siirtostrategiaa on muutettu. Suuret datanopeudet voidaan saavuttaa lähettämällä suurempia paketteja, mutta tällöin pieni viive ja hyvä luotettavuus ovat vaikeampia saavuttaa. URLLC:n tapauksessa on siis käytettävä pienempiä paketteja, mutta kontrolliliikenteen aiheuttama rasite viiveelle ja kanavan kapasiteetille on myös

ratkaistava ennen kuin tekniikka voidaan ottaa laajasti käyttöön. [51]

Edellä mainitut osa-alueet tuotetaan samalla radioverkolla. Koska näiden osa-alueiden vaatimukset ja liikenteen luonne ovat hyvin erilaisia toisistaan, täytyy ne jotenkin erotella toisistaan. 5G:n tapauksessa tätä kutsutaan verkon viipaloinniksi (slicing). Käytännössä viipalointi tarkoittaa verkon radioresurssien, runkoverkon sekä palvelinkapasiteetin jakamista eri osien kanssa [52]. Viipalointia voidaan myös käyttää radioverkon jakamiseen esimerkiksi operaattorin kuluttaja-asiakkaiden ja viranomaisverkon välillä. Tässä tapauksessa viranomaisliikenteelle annetaan käyttöön tietty määrä resursseja ja kuluttajaverkoille loput.

Radioverkon resurssit on tähän mennessä jaettu ortogonaalisilla monikäyttömenetelmillä, jolloin eri osilla on omat taajuuslohkonsa. Myös ei-ortogonaalisia menetelmiä on tutkittu [52], ja on huomattu, että ei-ortogonaalisilla menetelmillä voidaan parantaa verkon suorituskykyä huomattavasti. Ei-ortogonaalinen viipalointi tarkoittaa käytännössä sitä, että taajuuslohkot voidaan jakaa dynaamisesti liikenteen määrän mukaan. Esimerkiksi mMTC-liikenteen ollessa vähäistä, voidaan eMBB-asiakkaille antaa enemmän taajuuslohkoja. Tämä voi kuitenkin johtaa tilanteeseen, jossa kaikkien osien palvelutaso heikkenee, mikäli liikennettä on paljon kaikilla osilla. Viranomaisverkoille voikin tästä syystä olla parempi vaihtoehto allokoida pysyviä taajuuslohkoja ainakin niin, että perusvaatimukset pystytään täyttämään.

4.2 Integraatiot nousevien teknologioiden kanssa

Nousevia teknologioita on millä tahansa ajanhetkellä useita, joten tähän työhön on valittu niistä viranomaisverkkojen kannalta olennaisimpia. IoT-laitteiden käyttöä 5G-verkoissa käsiteltiin edellisessä alaluvussa, joten tässä alaluvussa tarkastellaan LTE-verkon tarjoamia mahdollisuuksia erityisesti NB-IoT (narrowband IoT) -teknologian kautta. Lisäksi tekoälysovelluksia on kehitetty useita kasvon- ja puheentunnistuksesta älykkääseen verkkoliikenteen seurantaan, joten viranomaisille hyödyllisiä käyttökohteita on myös. Suomessa poliisi on jo ottanut käyttöön paljon drone-lennokkeja ja onkin edelläkävijän asemassa monien muiden maiden poliisiorganisaatioihin verrattuna [4]. Nämä pienikokoiset ja kauko-ohjattavat lennokit mahdollistavat esimerkiksi rikospaikan havainnoinnin turvallisen matkan päästä tai toisesta perspektiivistä huomattavasti helpommin kuin esimerkiksi helikopterit.

NB-IoT:n tarkoitus on laajentaa LTE-standardeja tarjoamaan IoT-laitteille paremmin soveltuva kommunikaatiomuoto. Se on nimensä mukaisesti kapeakaistainen, liikennöintiin allokoidaan vain yksi resurssilohko, joten itse hyötykuorman kaistanleveydeksi jää 180 kHz [28]. Tämä on hyvä asia, sillä näin IoT-laitteet eivät vie resursseja suurempia datanopeuksia tarvitsevilta laitteilta. NB-IoT-liikenteeseen, erityisesti kontrolliliikenteeseen, on myös tehty muita liikennöinnin tarvetta vähentäviä muutoksia [53]. NB-IoT ei kuitenkaan vält-

tämättä sovellu kriittisimpiin sovelluksiin, sillä LTE-verkkojen viiveet ovat liian suuria ja luotettavuus liian heikko reaaliaikaisuutta vaativien järjestelmien käyttöön. 5G:n URLLC voisi soveltua paremmin kriittisten IoT-laitteiden käyttöön. Tällainen järjestelmä voisi olla aiemmin mainittujen savusukeltajien elintominitoja sekä varusteita seuraavat sensorit, jotka raportoivat esimerkiksi ilmasäiliön tyhjenemisestä. Silti myös viranomaisverkoissa voi olla tarvetta esimerkiksi varastotilojen lämpö- ja kosteussensoreille, joiden mittausdatalle riittää pidempikin raportointiväli.

Tekoälysovelluksia on paljon, ja myös sovellukset on otettu huomioon myös viranomaisverkkojen kehityksessä. Virve 2.0 -tekoälystrategiassa [47] mainitaan esimerkiksi hahmontai kasvojentunnistus, autonomiset dronet ja robotit, puheentunnistus sekä tilanteiden ennustaminen. Yksinkertaistettuna tekoälysovelluksissa käytetään erilaisia algoritmeja, joita tuetaan koneoppimisen avulla. Käytännössä tämä voidaan toteuttaa monella eri tapaa, mutta niiden käsittely kattavasti vaatisi toisen kandidaatintyön. Edellä mainitut esimerkit tekoälysovelluksista voidaan toteuttaa opettamalla tekoäly sopivalla tietoaineistolla tekemään oikeita päätöksiä sille annettavan informaation perusteella.

Hahmontunnistusta voidaan käyttää esimerkiksi rekisterikilpien automaattisessa lukemisessa, tai vaikkaapa tietyn automallin tunnistamisessa ilmakuvista. Kasvontunnistukselle on myös useita mahdollisia käyttökohteita, mutta se on herättänyt kysymyksiä yksityisyydensuojasta. Autonomiset pelastusrobotit voisivat liikkua esimerkiksi onnettomuusalueella itsenäisesti apua tarvitsevia etsien. Esimerkiksi suuren meripelastustehtävän suorittaminen voisi helpottua, jos autonomisia pelastuslauttoja voisi lähettää useita onnettomuusalueelle, ja ne etsisivät veden varassa olevia ihmisiä itsenäisesti esimerkiksi lämpökameroiden avulla. Puheentunnistus taas voisi helpottaa muistiinpanojen tekemistä kentällä ja siten säästää aikaa muihin tehtäviin. Lisäksi tekoälyn avulla voisi olla mahdollista ennustaa tilanteiden kehittymistä aiempien tietojen perusteella paljon nopeammin kuin ihminen siihen pystyisi. Tällöin nopeastikin kehittyvästä tilanteesta voitaisiin saada useita skenaarioita päätöksenteon avuksi.

Kuten aiemmin jo mainittiin, Suomen poliisi on jo pitkällä miehittämättömien lennokkien käytössä kenttäolosuhteissa. Vuoden 2020 loppuun mennessä poliisilla odotetaan olevan yli 500 drone-lentäjää, ja vuonna 2019 lennettiin yli 4200 tehtävää. Tehtävätyyppejä olivat koulutus, dokumentointi, henkilöiden etsintä sekä tilannekuvan tuottaminen. [54] Poliisin lisäksi myös muut viranomaiset voivat hyötyä dronejen käytöstä. Esimerkiksi palohälytyksen ensivaste voisi olla drone, joka pääsee paikalle perinteisiä paloautoja nopeammin. Drone voisi välittää tietoa tilanteen vakavuudesta sillä aikaa, kun pelastushenkilöstö valmistautuu lähtöön. Päätös lähetettävien yksiköiden määrästä voitaisiin siis tehdä paremmin informoituna, jolloin yksiköitä lähtee oikea määrä.

5. YHTEENVETO

Viranomaisverkot ovat maailmanlaajuisesti murrosvaiheessa, kun TETRA-pohjaiset verkot eivät enää täytä kasvavia vaatimuksia esimerkiksi datanopeuksien suhteen. Tähän on vastattu ottamalla käyttöön LTE-pohjaisia verkkoja. LTE-verkkojen käyttö kuitenkin aiheuttaa haasteita muun muassa korkeampien taajuuksien aiheuttamien kuuluvuusongelmien vuoksi. Lisäksi LTE:tä ei ole suunniteltu viranomaiskäyttöön, ja monissa maissa on myös kustannussyistä valittu kaupallinen radioverkko. Vaikka 3GPP onkin standardeissaan pyrkinyt ratkaisemaan näitä ongelmia esimerkiksi saareketukiasemien, tehtäväkriittisten palveluiden ja tietoturvaominaisuuksien avulla, työ on edelleen kesken.

LTE:ssä on myös paljon hyviä ominaisuuksia, joista viranomaisverkoille on hyötyä. Edellä mainittujen saareketukiasemien ansiosta verkko voi toimia, vaikka se olisi täysin eristetty. Myös laitteesta laitteeseen -kommunikaatio voi laajentaa kattavuutta kriittisissä tilanteissa nopeasti. Tehtäväkriittisten palveluiden priorisointi- ja etuoikeusmäärittelyt mahdollistavat viranomaistoiminnan myös suurten väkijoukkojen keskellä. Häiriönsieto on LTE-verkoissa myös normaalitilanteissa suhteellisen hyvällä tolalla, vaikkei viranomaisverkoille standardeissa olekaan tarjottu parempia ominaisuuksia. Kohdennetun häirinnän osaava hyökkääjä voi kuitenkin onnistua paikallisten häiriöiden tuottamisessa suhteellisen pienillä resursseilla.

Tietoturvaominaisuuksissa on myös parantamisen varaa. Siitä huolimatta, että tässä työssä esitellyt hyökkäykset eivät suoraan vaaranna koko järjestelmän toimivuutta tai monien käyttäjien tietoja, on ne otettava vakavasti. Valtiollisen tason hyökkääjillä on usein paljon resursseja käytössään, ja kohdennetuilla hyökkäyksillä voidaan joissakin tapauksissa esimerkiksi kalastella tai kiristää tietoja hyvinkin tehokkaasti. Viranomaistoimijoiden tulee siis olla vahvasti mukana standardointityössä, jotta heidän tarpeensa eivät jää voittoa tavoittelevien operaattorien tai laitevalmistajien tehokkuusvaatimusten jalkoihin.

LTE tuo myös uusia ulottuvuuksia viranomaistoimintaan ja mahdollistaa täysin uusia toimintatapoja. Esimerkiksi drone-lennokit ja IoT-laitteet ovat eräitä merkittäviä uusia työkaluja. Lennokeista saatavan korkealaatuisen videokuvan siirto vaatii huomattavasti dataa, joten LTE:n suuria datanopeuksia tarvitaan tähän. IoT-laitteiden datanopeudet sen sijaan myös TETRA-verkko pystyisi tarjoamaan, mutta laitteiden suuri määrä aiheuttaisi ongelmia TETRAn kapasiteetin kanssa. LTE:stä eteenpäin mentäessä 5G-verkot voivat tuoda

paljon parannuksia kriittisen infrastruktuurin toimintaan ja vielä suurempien IoT-verkkojen mahdollisuuden. Jatkotutkimusaiheita on siis runsaasti sekä jo olemassa olevien osien parantamisessa että täysin uusien käyttökohteiden luomisessa.

LÄHTEET

[1] *TETRA*. European Telecommunications Standards Institute (ETSI). URL: https://www.etsi.org/technologies/tetra (viitattu 14. 02. 2021).

[2] *Om Rakel*. Myndigheten för samhällsskydd och beredeskap (Ruotsi). URL: https://www.msb.se/sv/verktyg--tjanster/rakel/om-rakel/ (viitattu 14. 02. 2021).

[3] *Virve siirtyy uuteen teknologiaan 2020-luvulla*. Suomen Erillisverkot Oy. URL: https://www.erillisverkot.fi/virve2-0/ (viitattu 13. 02. 2021).

[4] *Kari Junttilan haastattelu kandidaatintyötä varten*. 16. helmikuuta 2021.

[5] *Middle Class Tax Relief and Job Creation Act of 2012*. Osa IV, alaosa B. Yhdysvallat, 2012. URL: https://www.congress.gov/112/plaws/publ96/PLAW-112publ96.pdf.

[6] *Emergency Services Network: overview*. Home Office (Yhdistynyt kuningaskunta). URL: https://www.gov.uk/government/publications/the-emergency-services-mobile-communications-programme/emergency-services-network (viitattu 14. 02. 2021).

[7] *Kommunikation för vår gemensamma säkerhet*. Justitiedepartmentet (Ruotsi), 2017. URL: https://www.regeringen.se/493a2f/contentassets/47c055d398a5487b8a0585d4d1d0b32e/kommunikation-for-var-gemensamma-sakerhet-ds-20177.

[8] Jarwan, A., Sabbah, A., Ibnkahla, M. ja Issa, O. LTE-Based Public Safety Networks: A Survey. *IEEE Communications surveys and tutorials* 21.2 (2019). ISSN: 1553-877X.

[9] Marco Alaez, R., Alcaraz Calero, J. M., Belqasmi, F., El-Barachi, M., Badra, M. ja Alfandi, O. Towards an open source architecture for multi-operator LTE core networks. *Journal of network and computer applications* 75 (2016), s. 101–109. ISSN: 1084-8045.

[10] Sato, H., Takase, M., Konno, Y. ja Arai, T. MVNO solution to embody diversifying market needs. *Fujitsu scientific & technical journal* 52.2 (2016), s. 41–48. ISSN: 0016-2523.

[11] *Sharing and compatibility studies between digital terrestrial television broadcasting and terrestrial mobile broadband applications, including IMT, in the frequency band 470-694/698 MHz*. Kansainvälinen televiestintäliitto, marraskuu 2018. URL: https://www.itu.int/pub/R-REP-BT.2337-1-2018.

[12] *Mission Critical Push to Talk (MCPTT); Stage 1*. Technical Specification (TS) 22.179. Versio 16.5.0. 3rd Generation Partnership Project (3GPP), maaliskuu 2019. URL: http://www.3gpp.org/DynaReport/22179.htm.

[13] *Mission Critical Data (MCData) signalling control; Protocol specification*. Technical Specification (TS) 24.282. Versio 16.4.0. 3rd Generation Partnership Project (3GPP), joulukuu 2020. URL: http://www.3gpp.org/DynaReport/24282.htm.

[14] *Mission Critical Video (MCVideo) signalling control; Protocol specification*. Technical Specification (TS) 24.281. Versio 16.6.0. 3rd Generation Partnership Project (3GPP), heinäkuu 2020. URL: http://www.3gpp.org/DynaReport/24281.htm.

[15] *Laki sähköisen viestinnän palveluista*. 250 b § (18.1.2019/52) Viranomaisviestintään liittyvän verkkopalvelun tarjoaminen.

[16] *Laki julkisen hallinnon turvallisuusverkkotoiminnasta*. 6 § (18.1.2019/53) Verkko- ja infrastruktuuripalvelujen tuottaja.

[17] *Laki julkisen hallinnon turvallisuusverkkotoiminnasta*. 12 § (18.1.2019/53) Varautumisvelvollisuus.

[18] *Valtioneuvoston asetus julkisen hallinnon turvallisuusverkkotoiminnasta*. 9 § (1109/2015) Tietoturvallisuusvaatimukset.

[19] *Kuuluvuuskartta*. Elisa Oyj. URL: https://elisa.fi/kuuluvuus/ (viitattu 09. 03. 2021).

[20] *Isolated Evolved Universal Terrestrial Radio Access Network (E-UTRAN) operation for public safety; Stage 1*. Technical Specification (TS) 22.346. Versio 16.0.0. 3rd Generation Partnership Project (3GPP), heinäkuu 2020. URL: http://www.3gpp.org/DynaReport/22346.htm.

[21] *Proximity-based services (ProSe); Stage 2*. Technical Specification (TS) 23.303. Versio 16.0.0. 3rd Generation Partnership Project (3GPP), heinäkuu 2020. URL: http://www.3gpp.org/DynaReport/23303.htm.

[22] *Quality of Service (QoS) concept and architecture*. Technical Specification (TS) 23.107. Versio 16.0.0. 3rd Generation Partnership Project (3GPP), heinäkuu 2020. URL: http://www.3gpp.org/DynaReport/23107.htm.

[23] *Policy and charging control architecture*. Technical Specification (TS) 23.203. Versio 16.2.0. 3rd Generation Partnership Project (3GPP), joulukuu 2019. URL: http://www.3gpp.org/DynaReport/23203.htm.

[24] *Multimedia priority service*. Technical Specification (TS) 22.153. Versio 16.0.0. 3rd Generation Partnership Project (3GPP), lokakuu 2019. URL: http://www.3gpp.org/DynaReport/22153.htm.

[25] *Service accessibility*. Technical Specification (TS) 22.011. Versio 16.5.0. 3rd Generation Partnership Project (3GPP), lokakuu 2020. URL: http://www.3gpp.org/DynaReport/22011.htm.

[26] *Radio Regulations*. Kansainvälinen televiestintäliitto, 2020. URL: http://handle.itu.int/11.1002/pub/814b0c44-en.

[27] *Evolved Universal Terrestrial Radio Access (E-UTRA); Physical layer procedures*. Technical Specification (TS) 36.213. Versio 16.4.0. 3rd Generation Partnership Project (3GPP), tammikuu 2021. URL: http://www.3gpp.org/DynaReport/36213.htm.

[28] *Evolved Universal Terrestrial Radio Access (E-UTRA); Physical channels and modulation*. Technical Specification (TS) 36.211. Versio 16.4.0. 3rd Generation Partnership Project (3GPP), tammikuu 2021. URL: http://www.3gpp.org/DynaReport/36211.htm.

[29] *Evolved Universal Terrestrial Radio Access (E-UTRA); Physical layer; Measurements*. Technical Specification (TS) 36.213. Versio 16.1.0. 3rd Generation Partnership Project (3GPP), heinäkuu 2020. URL: http://www.3gpp.org/DynaReport/36214.htm.

[30] *Evolved Universal Terrestrial Radio Access (E-UTRA) and Evolved Universal Terrestrial Radio Access Network (E-UTRAN); Overall description; Stage 2*. Technical Specification (TS) 36.300. Versio 16.4.0. 3rd Generation Partnership Project (3GPP), tammikuu 2021. URL: http://www.3gpp.org/DynaReport/36300.htm.

[31] Hamid, U., Qamar, R. A. ja Waqas, K. Performance comparison of time-domain and frequency-domain beamforming techniques for sensor array processing. *Proceedings of 2014 11th International Bhurban Conference on Applied Sciences & Technology (IBCAST) Islamabad, Pakistan, 14th - 18th January, 2014*. IEEE, 2014, s. 379–385.

[32] Duplicy, J., Badic, B., Balraj, R., Ghaffar, R., Horváth, P., Kaltenberger, F., Knopp, R., Kovács, I. Z., Nguyen, H. T., Tandur, D. ja Vivier, G. MU-MIMO in LTE Systems. *EURASIP journal on wireless communications and networking* 2011.1 (2011), s. 1–13. ISSN: 1687-1472.

[33] Magnuski, H. Jamming of Communication Systems Using FM, AM, and SSB Modulation. *IRE transactions on military electronics* MIL-5.1 (1961), s. 8–11. ISSN: 0096-2511.

[34] Clancy, T. C. Efficient OFDM Denial: Pilot Jamming and Pilot Nulling. *2011 IEEE International Conference on Communications (ICC)*. IEEE, 2011, s. 1–5.

[35] Sanastokeskus ry. *Kyberturvallisuuden sanasto (TSK 52)*. 2018. ISBN: 978-952-5608-49-6.

[36] *3GPP System Architecture Evolution (SAE); Security architecture*. Technical Specification (TS) 33.401. Versio 16.3.0. 3rd Generation Partnership Project (3GPP), heinäkuu 2021. URL: http://www.3gpp.org/DynaReport/33401.htm.

[37] *USIM and IC card requirements*. Technical Specification (TS) 21.111. Versio 16.1.0. 3rd Generation Partnership Project (3GPP), joulukuu 2020. URL: http://www.3gpp.org/DynaReport/21111.htm.

[38] *The international identification plan for public networks and subscriptions*. Recommendation ITU-T E.212. Kansainvälinen televiestintäliitto, syyskuu 2016. URL: https://www.itu.int/rec/T-REC-E.212-201609-I.

[39] *Numbering, addressing and identification*. Technical Specification (TS) 23.003. Versio 16.6.0. 3rd Generation Partnership Project (3GPP), maaliskuu 2021. URL: http://www.3gpp.org/DynaReport/23003.htm.

[40] Shaik, A., Borgaonkar, R., Asokan, N., Niemi, V. ja Seifert, J.-P. Practical attacks against privacy and availability in 4G/LTE mobile communication systems. *23rd Annual Network and Distributed System Security Symposium (NDSS 2016)*. Internet Society, 2016.

[41] *Non-Access-Stratum (NAS) protocol for Evolved Packet System (EPS); Stage 3*. Technical Specification (TS) 24.301. Versio 16.8.0. 3rd Generation Partnership Project (3GPP), joulukuu 2020. URL: http://www.3gpp.org/DynaReport/24301.htm.

[42] Rupprecht, D., Kohls, K., Holz, T. ja Popper, C. Breaking LTE on Layer Two. *2019 IEEE Symposium on Security and Privacy (SP)*. IEEE, 2019, s. 1121–1136.

[43] Bernstein, D., Lange, T., Niederhagen, R., Ryan, P., Naccache, D. ja Quisquater, J. Dual EC: a standardized back door. *Lecture notes in computer science*. Vol. 9100. Lecture Notes in Computer Science. Berlin, Heidelberg: Springer, 2016, s. 256–281.

[44] Pancevski, B. U.S. Officials Say Huawei Can Covertly Access Telecom Networks; Trump administration ramps up push for allies to block Chinese company. *The Wall Street journal. Eastern edition* (helmikuu 2020). ISSN: 2574-9579.

[45] *Laki sähköisen viestinnän palveluista*. 244 a § (30.12.2020/1207) Viestintäverkon kriittisissä osissa käytettävät laitteet.

[46] *Virve 2.0 -mobiilistrategia*. Suomen Erillisverkot Oy. Maaliskuu 2021. URL: https://www.erillisverkot.fi/uploads/2021/04/virve-mobiilistrategia-2021-versio-1.1_03_2021.pdf (viitattu 22. 04. 2021).

[47] *Tekoälystrategia*. Suomen Erillisverkot Oy. Tammikuu 2020. URL: https://www.erillisverkot.fi/uploads/2020/10/ai-strategia_tammikuu2020pub.pdf (viitattu 22. 04. 2021).

[48] *IMT Vision - "Framework and overall objectives of the future development of IMT for 2020 and beyond"*. Recommendation ITU-R M.2083. Kansainvälinen televiestintäliitto, lokakuu 2015. URL: https://www.itu.int/rec/R-REC-M.2083-0-201509-I.

[49] Bockelmann, C., Pratas, N. K., Wunder, G., Saur, S., Navarro, M., Gregoratti, D., Vivier, G., De Carvalho, E., Ji, Y., Stefanovic, C., Popovski, P., Wang, Q., Schellmann, M., Kosmatos, E., Demestichas, P., Raceala-Motoc, M., Jung, P., Stanczak, S. ja Dekorsy, A. Towards Massive Connectivity Support for Scalable mMTC Com-

munications in 5G Networks. *IEEE access* 6 (2018), s. 28969–28992. ISSN: 2169-3536.

[50] *Matkaviestinverkon liittymät*. Liikenne- ja viestintävirasto. 28. joulukuuta 2018. URL: https://www.traficom.fi/fi/tilastot/matkaviestinverkon-liittymat (viitattu 22. 04. 2021).

[51] Ji, H., Park, S., Yeo, J., Kim, Y., Lee, J. ja Shim, B. Ultra-Reliable and Low-Latency Communications in 5G Downlink: Physical Layer Aspects. *IEEE wireless communications* 25.3 (2018), s. 124–130. ISSN: 1536-1284.

[52] Le, T.-K., Salim, U. ja Kaltenberger, F. An Overview of Physical Layer Design for Ultra-Reliable Low-Latency Communications in 3GPP Releases 15, 16, and 17. *IEEE access* 9 (2021), s. 433–444. ISSN: 2169-3536.

[53] *General Packet Radio Service (GPRS) enhancements for Evolved Universal Terrestrial Radio Access Network (E-UTRAN) access*. Technical Specification (TS) 23.401. Versio 16.10.0. 3rd Generation Partnership Project (3GPP), maaliskuu 2021. URL: http://www.3gpp.org/DynaReport/23401.htm.

[54] *Miehittämätön ilmailu*. Poliisi. URL: https://poliisi.fi/miehittamaton-ilmailu (viitattu 03. 05. 2021).

LIITE A: HAASTATTELUKYSYMYKSET

Kysymykset laadittiin ja haastattelu tehtiin yhteistyössä Heidi Melkon kanssa.

Mikä on Virve 2.0?
Miksi on siirrytty LTE-pohjaiseen verkkoon, eikä jatkettu TETRAn kehitystä?
Missä vaiheessa ollaan menossa hankkeessa?

Mitkä ovat käyttäjien eniten toivomat vaatimukset Virve 2.0:lta?
Vaatiiko Virve 2.0 järjestelmä uutta koulutusta käyttäjille?
Jatkuuko yhteys Ruotsin ja Norjan viranomaisverkkoihin?
Tapahtuuko käyttöönotto valtakunnallisesti samanaikaisesti?

Miten radioverkon jakaminen vaikuttaa palvelun laatuun kattavuuden ja kapasiteetin osalta?
Entä tietojen luottamuksellisuuteen ja eheyteen?
Miten voidaan taata tiedonsiirtonopeus ja eheys myös kuormittuneessa mobiiliverkossa?
Mitä muutoksia aiheuttaa siirtyminen kaupalliseen radioverkkoon?
Näkyykö tämä verkkoarkkitehtuurissa?

Miten taataan riittävä kattavuus ja kapasiteetti hätätilanteessa?
Miten kaupunkialueella jaetaan kapasiteetti viranomaisten ja tavallisten käyttäjien kesken?
Miten saadaan nopeasti lisää peittoa verkolle paikkaan, jossa ei ole valmista verkkoinfrastruktuuria?

Miten viranomaisverkko eroaa häiriöiden siedon kannalta kuluttajaverkoista?
Vaikuttaako esimerkiksi metsäpalojen aiheuttama ylimääräinen säteily?
Miten varaudutaan viallisten laitteiden tai tahallisen häirinnän aiheuttamiin paikallisiin häiriöihin?
Miten estetään mahdolliset ulkoiset hyökkäykset?
Miten edellä mainittuihin varaudutaan? Miten ne torjutaan tai kierretään?
Kuinka huonot kanavaolosuhteet havaitsemitaan?
Käyttäjämäärä mahdollisesti kasvaa, kuinka ruuhkautuminen estetään?

Onko integraatioita IoT-tyyppisten laitteiden kanssa suunniteltu?
Miten tällaiset vaikuttaisivat viranomaistoimintaan?

Miten esimerkiksi dronet, ajoneuvot tai hälytysjärjestelmät voidaan integroida verkkoon?
Mitä muita integraatioita tulevaisuudessa voisi olla?
Mitä hyötyä tällaisesta sensoridatasta voi olla?
Voiko ulkoinen älylaite aiheuttaa tietoturvaongelmia?
Voiko tekoälyn hyödyntämisessä olla eroja käyttäjän taitojen mukaan?
Kuinka tämä voidaan minimoida?

Onko 5G:n käyttöä tulevaisuudessa suunniteltu?
Mitä uutta 5G voisi tuoda viranomaisverkkoihin?
Onko 4G:n tai 5G:n käytöllä eroja verkon toimivuudelle?

Mitä muuta on näkyvissä tulevaisuudessa?
Voivatko Virve 2.0:n resurssit loppua aikanaan?