Siirtyminen 4G-verkosta 5G-verkkoon, kuinka käy tietoturvan ja mitä mahdollisuuksia se luo?

Toni Koskela

Haaga-Helia ammattikorkeakoulu
Amk-opinnäytetyö
2021
Tradenomin tutkinto

Tiivistelmä

Tekijä(t)
Toni Koskela

Tutkinto
Tietojenkäsittelyn tradenomi

Raportin/Opinnäytetyön nimi
Siirtyminen 4G-verkosta 5G-verkkoon, kuinka käy tietoturvan ja mitä mahdollisuuksia se luo?

Sivu- ja liitesivumäärä
41 + 2

Tämän työn tarkoituksena oli selvittää 4G-verkosta 5G-verkkoon siirtymisen hyötyjä sekä riskejä. 5G-verkko on uutta teknologiaa, jonka käyttöönotto on ajankohtaista ja siihen siirrytään yhteiskunnan eri osa-alueilla jatkuvasti. 5G-verkon toiminta sekä sen tuomat mahdollisuudet voivat kuitenkin olla mysteeri. Työn tarkoituksena oli tuoda saataville informaatiota, joka on ymmärrettävää koskien 5G-verkkoa sekä avata sen eroavaisuutta 4G-verkkoon.

Työssä on käytetty lähteinä verkosta löytyviä tieteellisiä julkaisuja. 5G-verkkoa koskevat julkaisut ovat tuoreita, mutta 4G-verkkoa koskevista julkaisuista osa on jopa 10 vuotta vanhoja. Työ on tehty tietopohjaiseksi ja analyyttiseksi. Varsinkin 5G-verkkoa koskevia julkaisuja tulee päivittäin lisää, koska sitä tutkitaan jatkuvasti, joten osa julkaisuista voi sisältää myös vanhentunutta tietoa muun muassa verkon vaatimuksien, suorituskyvyn sekä tietoturvan osalta. Työ pitää sisällään paljon erilaisia käsitteitä sekä lyhenteitä, näitä on pyritty selventämään työstä löytyvällä käsiteluettelolla.

5G-verkko tulee tarjoamaan kiistattomia hyötyjä verrattuna 4G-verkkoon. 5G-verkko tulee muovaamaan maailmaa ja yhteiskuntaamme useilla eri tavoilla. 5G-verkon kaikkia tarjoamia mahdollisuuksia on mahdotonta tietää tässä vaiheessa. 5G-verkon tarjoamat tiedonsiirtonopeudet, olemattomat viiveet, verkon kapasiteetti sekä verkon priorisointi, eli viipalointi, mullistavat yhteiskunnallisia toimintoja sekä kuluttajien tottumuksia mobiiliverkon käytössä.

5G-verkko on myös altis hyökkäyksille kuten 4G-verkko. 5G-verkon tietoturvaratkaisut ovat suurimmalta osaksi riippuvaisia operaattorin käyttöönottamista tietoturva- sekä turvallisuustoimista. Operaattoreilla on tietyt pakolliset vastuut tietoturvan osalta, mutta mikäli operaattori ei tee muita kuin vaadittavat tietoturvaratkaisut, altistaa se 5G-verkkoa enemmän verkkohyökkäyksille. Verkon käyttäjien sekä verkon laitteiden oma tietoturva ennalta ehkäisee sekä estää yksinkertaisimpia verkkohyökkäyksiä tehokkaimmin.

Asiasanat
5G, 4G, tietoturva, mobiililaitteet, yhteiskunta

Sisällys

1 Johdanto

Tässä opinnäytetyössä perehdytään siihen, kuinka 4G- ja 5G-verkko eroavat toisistaan ja minkälaisia mahdollisuuksia käyttöönotettava 5G-verkko luo yhteiskunnassamme. Verkkojen eroavaisuuksissa kiinnitetään huomiota enimmäkseen uuden tietoliikenneverkon tarjoamiin parannuksiin muun muassa tiedonsiirtonopeuksissa sekä tietoturvaan.

Uuden tietoliikenneverkon tarjoamia mahdollisuuksia yhteiskunnan eri toiminnoissa on myös avattu ja pohdittu. Uusien mahdollisuuksien myötä, myös tietoturvaloukkaukset ovat mahdollisia, ja työssä onkin pyritty tarkastelemaan juuri 5G-verkkoon kohdistuvia tietoturvaloukkauksia sekä niiden mahdollisuuksia.

Opinnäytetyöaiheeksi transitio 4G-verkosta 5G-verkkoon valikoitui sen ajankohtaisuuden vuoksi. 5G-verkkoa ei ole vielä otettu laajalti käyttöön ja kaikilla ihmisillä ei ole tietoa siitä, miten 4G- ja 5G-verkko eroavat toisistaan. Tämän työn avulla on tarkoitus selventää verkkojen tarjoamia mahdollisuuksia ja ominaisuuksia.

Haluan selvittää opinnäytetyössä:

- Kuinka 4G- ja 5G-verkko eroavat toisistaan ominaisuuksien puolesta?
- Onko 5G-verkko paremmin suojattu kuin 4G-verkko? Minkälaiset tietoturvaratkaisut toimivat 5G-verkossa?
- Mitä hyötyä on siirtyä 4G-verkosta 5G-verkkoon?

Opinnäytetyö on tehty keräämällä aineistoa eri verkkojulkaisuista sekä analysoimalla ja tutkimalla näitä julkaisuja. Opinnäytetyöhön on kerätty aineisto, jonka olen kokenut tärkeäksi ja ajankohtaiseksi kyseessä olevaan transitioon liittyen.

2 Käsiteluettelo

Tähän käsiteluetteloon on koottu opinnäytetyössä esiintyviä käsitteitä ja niiden selitykset. Käsitteitä avataan myös opinnäytetyön sisällössä, mutta lukemisen ja ymmärtämisen helpottamiseksi tärkeimmät käsitteet on koottu myös luetteloon.

- 0-5G teknologia
    - 0-5G teknologialla tarkoitetaan teknologian sukupolvia, G = generation, esimerkiksi 0G-teknologialla tarkoitetaan ensimmäisiä langattomia viestintävälineitä kuten radiopuhelimia ja 4G-teknologia kattaa nykyaikaisen teknologian, joka mahdollistaa muun muassa teräväpiirtovideoiden katselun liikkuvalla laitteella.

- 3GPP SA3
    - 3rd Generation Partnership Project on yhteistyöorganisaatio, johon kuuluu useita standardointijärjestöjä. Organisaatio luo standardeja uuden sukupolven teknologioille. SA3 on 3GPP:n sisällä työskentelevä ryhmä, joka vastaa muun muassa 5G-teknologian ja IoT:n turvallisuuden kehittämisestä.

- AKA eli Authentication and Key Agreement
    - Turvallisuusprotokolla, jota on käytetty 3G-teknologiasta alkaen. AKA käyttää symmetristä salausta ja toimii haaste-vaste periaatteella. AKA:a voidaan käyttää myös kertaluonteisen salasanan generoimiseen.

- AMF eli Core Access and Mobility Management Function
    - AMF on osa 3GPP:n määrittämää 5G-arkkitehtuuria. AMF:n päätehtäviin kuuluu turvallisuuden ja pääsyn hallinta ja autentikointi, esimerkiksi laitteen saavutettavuuden hallinnointi sekä yhteyden hallinnointi.

- AN eli Access Network
    - Tietoliikenneverkko, jonka kautta tilaajat yhdistetään palveluntarjoajalle.

- APN eli Access Point Name
    - APN:ää voidaan käyttää esimerkiksi yrityksen käytössä olevien mobiililaitteiden ja yrityksen sisäisen verkon välillä, mahdollistaen yrityksen sisäisen verkon käyttämisen yrityksen hallinnoimilla mobiililaitteilla.

- ARPF eli Authentication Credential Repository and Processing Function
    - ARPF on UDM:n toiminnallinen osa, jonka tarkoituksena on luoda 5G Home Environment Authentication Vectors (5G HE AV) perustuen tilaajan jaettuun salaiseen avaimeen.

- AUSF eli Authentication Server Function
    - AUSF on osa 3GPP:n 5G arkkitehtuuria, AUSF johtaa 5G:n turvallisuusprosesseja.

- C-PDU eli Cell Protocol Data Unit
    - PDU koostuu ohjaus- ja käyttäjätiedoista. PDU:lla tarkoitetaan yksittäistä tietoyksikköä.

- C-RNTI eli Cell Radio Network Temporary Identifier
    - C-RNTI on yksilöllinen tunnistetieto, jolla tunnistetaan RRC-yhteys, joka on määrätty tietylle UE:lle. NB määrittää erilaiset C-RNTI arvot jokaiselle UE:lle.

- DoS, eli Denial of Service, hyökkäys
    - DoS tunnetaan myös nimellä palvelunestohyökkäys. Palvelunestohyökkäyksellä pyritään estämään tietyn verkkosivun toiminta esimerkiksi aiheuttamalla palvelimelle niin paljon liikennettä, että sivusto ei toimi.

- DRX-vaihe eli Discontinuous Reception
    - DRX-vaiheen tarkoituksena on pidentää UE:n akun kestoa. DRX-vaiheessa UE siirtyy lepotilaan ja tämän avulla säästetään UE:n akkua. DRX-vaiheessa UE ei vastaanota tietoa jatkuvasti, vaan UE silloin tällöin tiedustelee verkosta, onko saapuvia paketteja tulossa. DRX-vaihe mahdollistaa myös eNB:n resurssien allokoinnin muualle kuin kyseiseen UE:n, koska UE on lepotilassa eikä se lähetä tai vastaanota paketteja.

- EAP eli Extensible Authentication Protocol
    - EAP on käyttäjien tunnistusprotokolla. EAP on protokollan runko, jonka avulla voidaan neuvotella mitä todennusmekanismia käytetään.

- ECIES eli Elliptic Curve Integrated Encryption Scheme
    - Julkisella avaimella varmistettu salausmekanismi. ECIES yhdistää epäsymmetrisen salaustekniikan sekä symmetrisen salauksen salatakseen tiedon.
- eMBB eli Enhanced Mobile Broadband

    - Tarjoaa parempia nopeuksia, virtuaali- ja lisätyn todellisuuden, kokonaisuudessaan paremman käyttökokemuksen sekä enemmän yhdistettyjä laitteita.

- eNB eli Evolved Node B
    - eNB on LTE-protokollan E-UTRAN:ssa oleva elementti. eNB on suoraan yhteydessä mobiiliverkkoon, joka kommunikoi UE:n kanssa. eNB allokoi käyttäjäliikennettä verkossa sekä välittää NAS signaaleja MME:lle.

- EPC eli Evolved Packet Core
    - EPC:llä tarkoitetaan runkoa, joka pitää sisällään MME:n, S-GW:n sekä P-GW:n. EPC:n tarkoituksena on tiivistää 4G LTE-verkossa liikkuva ääni ja data.

- E-UTRAN/UTRAN eli Evolved – Universal Terrestrial Radio Access Network
    - UTRAN tarkoittaa verkon osaa, jossa on useampi UE sekä eNB.

- GUTI eli Globally Unique Temporary ID
    - LTE-verkossa MME määrittää GUTI:n UE:lle ja se pitää sisällään kaksi komponenttia. Nämä komponentit ovat GUMMEI (Globally Unique MME ID) sekä M-TMSI (MME-TMSI). GUMMEI, tunnistaa MME:n ja M-TMSI tunnistaa UE:n MME:n sisällä. GUTI tunnistetta käytetään IMSI:n tilalla käyttäjän tunnistamiseen.

- HSM eli Hardware Security Module
    - Tietojenkäsittelylaite, joka suojaa ja hallitsee digitaalisia avaimia, suorittaa salauksen ja salauksen purkutoimintoja.

- HSPA+ eli High Speed Packet Access+
    - HSPA+ -protokollaa on käytetty 3G-verkossa parantamaan lataus- sekä lähetysnopeuksia paketeille. 4G-verkossa siirryttiin täysin LTE-teknologiaan.

- HSS eli Home Subscriber Server
    - HSS on tilaajan päävarasto tiedoille. HSS pitää sisällään tilaajan tunnistetiedot, sijainnin, tilausprofiilin sekä turvallisuustietoja.

- IMEI eli International Mobile Equipment Identity
    - IMEI on yksilöivä tunniste mobiililaitteelle. Jokaisella laitteella on uniikki IMEI-koodi. IMEI koostuu TAC:sta (Type Approval Code), FAC:sta (Final

Assembly Code) sekä SNR:stä (Serial Number) sekä yhdestä ylimääräisestä numerosta.

- IMSI eli International Mobile Subscriber Identity
    - IMSI on yksilöivä tunniste jokaiselle tilaajalle. Yksilöivä tunniste toimii niin GSM, UMTS, LTE sekä 5G-verkoissa. IMSI koostuu MCC:stä (Mobile Country Code), MNC:stä (Mobile Network Code) sekä MSIN:stä (Mobile Subscriber Identification Number).

- IoT eli Internet of Things
    - IoT:lla tarkoitetaan miljardien laitteiden yhteyttä toisiinsa. Yleensä laitteilla tarkoitetaan jokapäiväisiä laitteita, jotka saavat sekä lähettävät dataa.

- IP-osoite/IP-osoitepohjainen
    - IP tarkoittaa Internet Protokollaa. IP-osoite on uniikki osoite, joka tunnistaa laitteen verkossa. IP-osoitteiden avulla voidaan lähettää tietoa laitteiden välillä verkossa.

- IPSEC eli IP Security
    - IPSEC tarjoaa turvaa yksittäisten pakettien tasolla. Paketit, jotka ovat IPSEC-suojattu voidaan varmentaa sekä salata ja myös niiden eheys voidaan tarkastaa.

- ITU/ITU-R eli International Telecommunication Union
    - Kansainvälinen televiestintäliitto

- K/KNAS/KRRC/KUP
    - Työssä esiintyvät K lyhenteet tarkoittavat Key:tä eli salausavainta. K:n perässä oleva lyhenne kertoo salausavaimen käyttökohteen.

- LTE eli Long Term Evolution
    - LTE on 4G:ssä käytettä verkko. LTE mahdollisti täysin IP-pohjaisen liikenteen E-UTRAN:ssa.

- MAC-taso eli Medium Access Control-layer
    - MAC-taso on mobiilissa laitteessa sekä eNB:ssä. MAC-tason tehtävänä on tukea signaalien kanavointia sekä käyttäjäpinnan liikennettä oikeille kuljetuskanaville.

- MME eli Mobility Management Entity
    - MME on vastuussa liikkuvuudesta sekä istunnon hallinta proseduureista EPC:ssä. MME kommunikoi mobiililaitteen kanssa NAS:n kautta. Päävastuisiin kuuluu muun muassa porttien valinta sekä NAS-turvallisuus.
- mMTC eli Massive Machine Type Communication
    - IoT-verkon keskeinen osa. mMTC:n avulla koneet tuottavat sekä vaihtavat dataa keskenään vähäisellä tai jopa ilman ihmisen apua.

- NAS eli Non Access Stratum
    - NAS on toiminnallinen taso, joka toimii UE:n ja ydinverkon välillä. NAS tukee liikennettä ja signaaliviestintää ydinverkon ja UE:n välillä.

- PCO eli Protocol Configuration Options
    - PCO:n avulla mobiililaite voi vaihtaa tietoja epäsuorasti P-GW:n kanssa.

- PDCP eli Packet Data Convergence Protocol
    - PDCP mahdollistaa datan pakkaamista. PDCP:n avulla pakataan muun muassa käyttäjäpinnan sekä ohjauspinnan välistä IP-liikennettä.

- PEI eli Permanent Equipment Identifier
    - Laitteen yksilöivä tunnistetieto

- P-GW eli Packet Data Network Gateway
    - P-GW toimii niin sisääntulo kuin ulosmeno porttina EPC:n sisälle.

- PLMN eli Public Land Mobile Network
    - Geneerinen nimi kaikille mobiileille langattomille verkoille jotka käyttävät maanpäällisiä radiolähettimiä tai asemia.

- RLC eli Radio Link Control
    - RLC:n avulla voidaan segmentoida ja koota dataa kuten RRC signaaleja tai käyttäjäpinnan dataa. Segmentoinnin ja uudelleen koonnin avulla voidaan varmistaa datan olevan oikean kokoista lähetystä varten.

- RRC eli Radio Resource Control
    - RRC on ohjauspinnassa oleva toiminto, joka tarjoaa informaation siirto NAS:lle.

- S1/SCTP eli Stream Control Transmission Protocol

    - SCTP:n avulla voidaan toimittaa korkeamman tason dataa peräkkäin ja luotettavasti.

- SCMF eli The Security Context Management Function
    - SCMF noutaa salausavaimen SEAF:sta, jonka avulla voidaan johtaa uusia salausavaimia.

- SEAF eli Security Anchor Function
    - SEAF muodostaa ensisijaisen autentikoinnin tuloksesta ankkuriavaimen, jota käytetään kaikkia pääsyjä varten.

- SEPP eli Security Edge Protection Proxy
    - SEPP:tä käytetään ohjauspinnan liikenteen suojaamiseen, joka liikkuu eri PLMN:n välillä. SEPP suodattaa viestejä, hallinnoi ja uudelleen järjestää API viestejä.

- S-GW eli Serving Gateway
    - S-GW toimii käyttäjädatatason sisään- ja ulostulopisteenä E-UTRAN:n puolelle EPC:ssä.

- (S)PCF eli Policy Control Function
    - PCF toiminto tukee yhtenäistä toimintaperiaatekehystä joka halinnoi verkkokäyttäytymistä.

- SUPI eli Subscriber Permanent Identifier
    - 5G-verkossa jokaiselle tilaajalle allokoidaan oma uniikki SUPI. SUPI koostuu IMSI:tä ja NAI:sta (Network Access Identifier).

- SUCI eli Subscription Concealed Identifier
    - UE luo SUCI:n käyttäen ECIES-suojausta kotiverkon julkisella avaimella. Julkinen avain on annettu Sim-kortille Sim-kortin rekisteröinnin yhteydessä.

- TMSI/S-TMSI/M-TMSI eli Temporary Mobile Subscriber Identity
    - TMSI:n tarkoituksena on suojata tilaajan identiteettiä luomalla väliaikainen tunniste. Väliaikaisen tunnisteen avulla pyritään suojaamaan tilaajan IMSI:ä NAS yhteyden aikana, kuin myös suojaamaan MME:n identiteettiä, joka on vastuussa UE:sta.

- UDM eli Unified Data Management

    - UDM säilöö pitkäaikaisia turvallisuustunnisteita, joita käytetään AKA-prosessissa. UDM säilöö myös tilaajatietoja.

- UE eli User Equipment
    - UE:sta puhuttaessa tarkoitetaan mobiililaitetta.

- UICC eli Universal integrated circuit card
    - Toinen nimitys SIM-kortille.

- URLLC eli Ultra-Reliable and Low Latency Communication
    - Luotettava ja viiveetön viestintä.

- WGN eli White Gausian Noise
    - Kaistan häirintä lämpökohinalla.

- WiMAX eli World Wide Interoperability for Microwave Access
    - WiMAX oli yksi 4G-teknologialle kehitettävistä verkkoteknologioista, mutta sen kehitys ei ollut niin tuloksekas kuin LTE:n.

3 4G-verkko

4G:llä tarkoitetaan neljännen sukupolven (4th generation) teknologiaa. 4G-teknologia on 3G-teknologian kehittyneempi versio ja se tarjoaa enemmän palveluita sekä parempaa siirtonopeutta kuin 3G. (Bhavesh Hemnani 2018, 1). 4G-verkon suunnittelu aloitettiin vuonna 2000 ja sen tarkoituksena oli vastata jo olemassa olevien matkapuhelin- sekä tiedonsiirtoverkkojen kapasiteetti- sekä nopeusongelmiin. 4G-verkon tarkoituksena oli tarjota asiakkailleen paremmat tiedonsiirtonopeudet sekä IP-osoitepohjaiset multimediapalvelut. IP-osoitepohjaisten multimediapalveluiden tavoitteena oli luoda integroitu, maailmanlaajuinen verkko, jonka avulla voidaan vastaanottaa sekä lähettää ääntä, dataa sekä toistaa suorana multimediaa verkon käyttäjille missä vain ja milloin vain. 4G-verkon avulla kyettiin yhdistämään aikaisemmin erikseen toimineet toiminnot yhtenäiseksi toiminnoksi. 4G-verkon avulla voidaan yhdistää päätelaitteet, verkot sekä järjestelmät saman yhden yhtenäisen verkon alle. (A. H. Khan, M. A. Qadeer, J. A. Ansari and S. Waheed 2009, 1.)

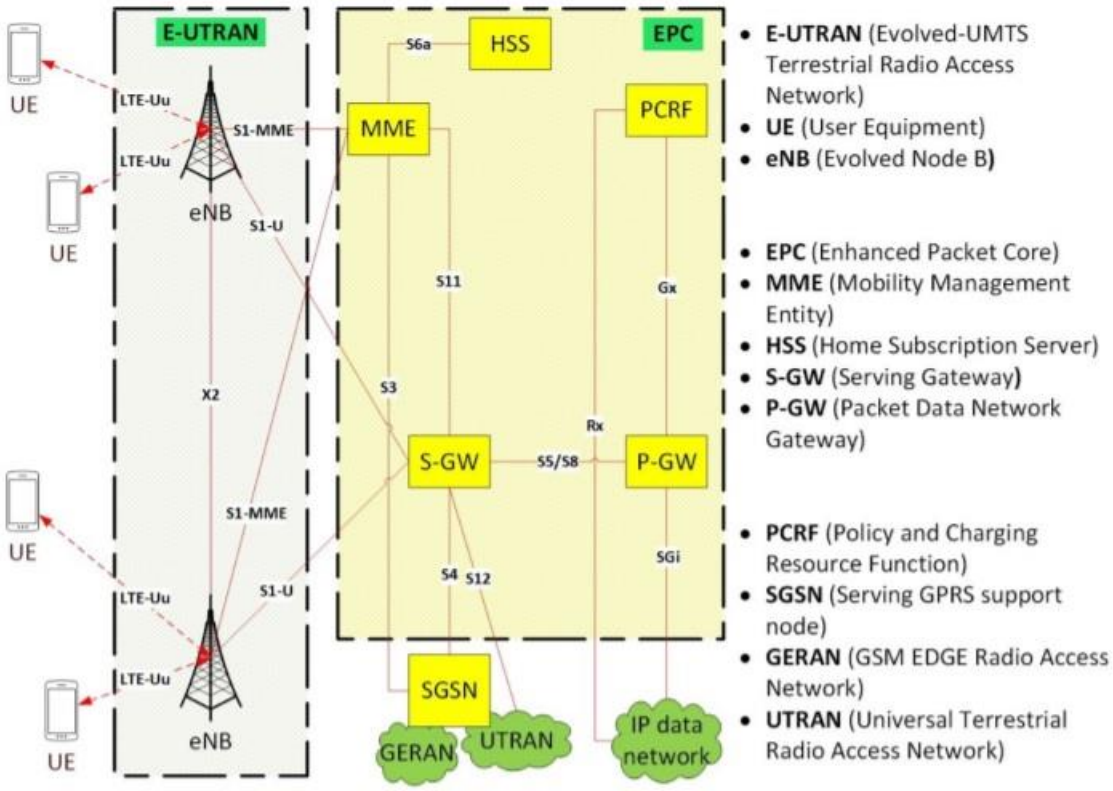
4G-teknologia mahdollistaa tiedonsiirtonopeuden, joka on jopa yli 100 megabittiä/sekunnissa sekä pienentää verkossa olevaa viivettä. 4G-teknologian avulla on mahdollistettu esimerkiksi hienot ja visuaaliset käyttöliittymät sekä HD-laatuisten videotiedostojen katseleminen mobiililaitteilla. 4G-teknologia on mahdollistanut myös paikkapohjaisten tietojen, kuten liikenneruuhkien sekä säätietojen, välittämisen käyttäjälle matkapuhelimeen tai tietokoneelle. (Bhavesh Hemnani 2018, 1.)

Marraskuussa 2008 Kansainvälinen televiestintäliitto (The International Telecommunication Union, ITU-R) määritti 4G-teknologialla vaadittavat nopeus- sekä yhteysstandardit. Standardien mukaan mobiiliyhteyksien huippunopeus tulee olla 10 megabittiä/sekunnissa ja kiinteiden yhteyspisteiden vähintään 1 gigabitti/sekunnissa. (Khaldoon Alshouiliy and Dharma P. Agrawal 2021, 4.) Muita kriteerejä 4G-verkon standardeille ovat pieni viive, matalat kustannukset bittiä kohden, hyvä palvelunlaatu (QoS, Quality of Service), verkon toimivuus kovissa nopeuksissa sekä korkea verkon kapasiteetti. (N. Seddigh, B. Nandy, R. Makkar and J. F. Beaumont 2010, 1.)

4G-verkolla on myös useita erilaisia standardeja, jotka riippuvat siitä, miten 4G-verkko on julkaistu yleisön käyttöön verkko-operaattorin toimesta. 4G-verkon standardeja ovat muun muassa LTE, WiMAX sekä HSPA+. LTE (Long Term Evolution) on laajimmin käytetty 4G-standardi. 4G sekä 4G LTE eivät ole sama asia, vaikka ihmiset puhuvat niistä samana asiana. Matkapuhelinta käytettäessä 4G tarjoaa paremman tehokkuuden sekä laajemman verkon kattavuuden, mutta 4G LTE mahdollistaa nopeamman tiedonsiirron. (Khaldoon Alshouiliy and Dharma P. Agrawal 2021, 5.)

Verkkojen turvallisuutta on parannettu aina sukupolvesta seuraavaan. 4G LTE-verkoissa turvallisuutta on parannettu esimerkiksi siten, että siihen on lisätty abstraktiotasoja uniikkien tunnistetietojen muodossa mobiililaitteisiin. Tilapäiset uniikit tunnistetiedot pienentävät ikkunaa, jolloin tunkeutujalla on mahdollisuus päästä käsiksi laitteen tietoihin. 4G-verkoon on lisätty myös salattu signaali käyttäjän mobiililaitteen sekä MME:n (Mobile Management Entity) välille. (N. Seddigh ym. 2010, 4.)

4G-laitteiden sekä yhteyksien tietoturva-arkkitehtuurin tulisi täyttää seuraavat vaatimukset: vakaampi kuin 3G, käyttäjän henkilöllisyyden luotettava salaaminen, käyttäjän sekä verkon vahva tunnistaminen, datan eheys, luotettavuus sekä toimiva tietoturva myös muilla yhteysalueilla. (Mobile Management Entity) välille. (N. Seddigh ym. 2010, 4.)



Kuva 1. 4G LTE-verkon arkkitehtuuri. (Omar Dawood Sulaiman Al-Gbur 2021.)

3.1 LTE-verkon turvallisuusarkkitehtuuri ja suunnittelu

4G LTE verkon turvallisuusvaatimukset on jaettu kolmeen tasoon. Taso 1 joka suojaa käyttäjän mobiililaitteen sekä MME:n (Mobile Management Entity) tai UTRAN (UMTS Terrestrial Radio Access Network) välistä kommunikaatiota, taso 2 joka suojaa verkossa liikkuvia elementtejä sekä taso 3 joka mahdollistaa turvallisen pääsyn liikkuviin tukiasemiin. (N. Seddigh ym. 2010, 5.)

LTE-verkko käyttää 5 erilaista avainta, jokaista näistä avaimista käytetään tiettyyn tarkoitukseen ja ne ovat voimassa vain tietyn ajan. Avaimia käytetään E-UTRAN sekä EPS:n

(Evolved Packet System) kanssa kommunikointiin. Nämä 5 avainta ovat $KNAS_{int}$, $KNAS_{enc}$, KUP_{enc}, $KRRC_{int}$ sekä $KRRC_{enc}$. (N. Seddigh ym. 2010, 5.)

$KNAS_{int}$ ja $KNAS_{enc}$ avaimia käytetään suojaamaan NAS (Non-Access Stratum) liikennettä käyttäjän laitteen sekä MME:n välillä. KUP_{enc} avaimella suojataan käytäjädata liikennettä käyttäjän laitteen sekä eNodeB:n(eNB) välillä. $KRRC_{int}$ ja $KRRC_{enc}$ ovat eheys ja salausavaimia, joita käytetään suojelemaan RRC (Radio Resource Control) liikennettä käyttäjän laitteen ja eNodeB:n välillä. (N. Seddigh ym. 2010, 6.)
LTE-verkon varmennus, salaus sekä eheys suojausproseduurit keskittyvät kolmeen asiaan. Varmennus vektorit, jotka ovat varmentamisen keskiössä, ovat tuoreita, eli niitä ei ole aikaisemmin käytetty. Turvallisuusalgoritmit ovat yhdensuuntaisia matemaattisia funktioita, joissa tulos saadaan käyttämällä ennalta määrättyä algoritmia ja LTE-verkossa käytetään IPSEC-protokollaa. IPSEC-protokolla takaa käyttäjäliikenteen luotettavuuden LTE EPS pisteiden välillä. IPSEC-protokollan käytön vuoksi on tärkeää, että S-GW ja MME pisteillä on tarpeeksi prosessointikykyä selvitäkseen salauksen purkamisesta ja salaamisesta vaadituilla nopeuksilla, ettei suorituskyky kärsi. (N. Seddigh ym. 2010, 6.)

LTE:n avainhallinnan toimintoihin kuuluvat avaimen perustaminen, avaimen jakaminen ja avaimen generointi. Ilman turvallista avainhallintaa sekä protokollaa avaimet voivat vuotaa ulkopuolisille ja näin ollen vaarantaa salaus sekä eheys mekanismit. LTE-verkossa käytetään AKA (Authentication and Key Agreement) proseduuria avainten perustamiseen ja varmentamiseen. LTE-verkko käyttää tarkemmin EPS-AKA proseduuria. AKA:ssa on kolme vaihetta: initiaatio, pääsytiedon siirto sekä haasto-vastaus vaihto. Initiaatio vaiheessa käyttäjän mobiililaite kertoo verkolle oman identiteettinsä, joko IMSI:n (International Mobile Subscriber Identity) tai TMSI:n (Temporary Mobile Subscriber Identity). Tämän identiteetin perusteella LTE-verkko aloittaa AKA-prosessin. (N. Seddigh ym. 2010, 6.)

LTE-verkon yksi tärkeimmistä turvallisuustoiminnoista on se, että verkko yrittää estää tunkeutujia saamasta tietoonsa käyttäjien yksilöllisiä tunnisteita käyttäjien laitteista. Mikäli käyttäjän laitteen yksilöivä numero paljastuu, altistaa se käyttäjän laitteen turvallisuusuhille kuten laitteen seurantaan ja profilointiin, verkon pääsyyn oikeudetta sekä palvelunestohyökkäyksille. Yksilöllisiä tunnisteita on kuusi kappaletta: IMSI, IMEI (International Mobile Equipment Identity), M-TMSI (M-temporary TMSI), S-TMSI, GUTI (Globally Unique Temporary UE Identity), C-RNTI (Cell Radio Network Temporary Identifier). IMSI on vakituinen käyttäjän tunnistetieto, joka lähetetään, kun käyttäjä yrittää liittyä verkkoon ensimmäisen kerran. IMEI on mobiililaitteen vakituinen sekä yksilöivä tunnistetieto, eikä se muutu, vaikka vaihtaisi SIM-korttia. M-TMSI on väliaikainen tunnistetieto, jota käytetään käyttäjän laitteen tunnistamiseen MME:n sisällä. Verkko määrittää M-TMSI:n laitteelle salauksen jälkeen. M-TMSI:n avulla suojaudutaan identiteettivarkaus riskejä vastaan, mutta

se ei estä laitteen paikantamista. S-TMSIä käytetään käyttäjän laitteen kutsumiseen. GUTI:n avulla suojataan käyttäjän laitteen identiteettiä. GUTI tunnistaa yksilöllisesti MME:n joka loi GUTI:n ja tunnistaa käyttäjän laitteen mainitun MME:n sisällä. C-RNTI luo yksilöllisen ja väliaikaisen käyttäjän laitteen tunnisteen signaalitasolla. Verkko, jonka alueella käyttäjän laite on, luo laitteelle C-RNTI tunnisteen signaalitasolla. (N. Seddigh ym. 2010, 6.)

Yhteinen todentaminen käyttäjän laitteen ja verkon välillä on LTE-verkon turvallisuuden kulmakiviä. AKA-proseduuria käytetään tämän saavuttamiseksi ja varmistamiseksi, että palvelua tarjoava verkko todentaa käyttäjän identiteetin ja käyttäjä todentaa verkon oikeellisuuden. AKA-proseduuria käytetään myös salaus- ja eheysavainten luontiin. Kolme pistettä on mukana todentamisprosessissa: UE (User Equipment), MME sekä HSS (Home Subscriber Server). HSS pitää sisällään tilaajan tietoja ja pystyy todentamaan UE:n pyynnöt sekä luomaan todentamisdataa, jonka se edelleen välittää MME:lle prosessointia varten. UE:n todentamisprosessi alkaa aina, kun UE yrittää liittyä EPS:n. (N. Seddigh ym. 2010, 6.)

Signaalien luotettavuus ja eheys on turvattu RRC signaalein UE:n ja eNB:n välillä, NAS signaalein UE:n ja MME:n väillä sekä S1(Stream Control Transmission Protocol, SCTP) signaalein. RRC signaalit on salattu ja eheys suojattu PDCP:n (Packet Data Convergence Protocol) avulla kun taas NAS signaali suojaa itse itsensä. S1 suojaus on vaihtoehtoinen eikä sitä käytetä jokaisen UE yhteyden kanssa, vaan enneminkin eNB ja S-GW:n välisessä liikenteessä. LTE-verkossa on myös turvallisuusominaisuus, joka salaa käyttäjän datan sekä äänen UE:n ja eNB:n välillä. PDCP-protokolla salaa ja purkaa salauksen UE:n ja eNB:n välillä. (N. Seddigh ym. 2010, 7.)

3.2 LTE-verkon tietoturvaongelmat

LTE-verkolla on kaksi avain haavoittuvuutta fyysisellä kerroksella: häirintä sekä hyökkäykset. LTE-verkkoon kohdistettavaa häirintää voidaan tehdä lisäämällä liikennettä, eli ääntä, verkossa. LTE-verkon häirinnät voidaan jakaa kahteen kategoriaan, ääni- ja monikantoaaltohäirintä. Äänihäirintää voidaan tehdä WGN:ää (White Gaussian Noise) käyttämällä. Monikantoaaltohäirinnässä hyökkääjä tunnistaa järjestelmän käyttämät kantoaallot ja syöttää todella kapeakaistaisen signaalin näihin aaltoihin. Häirintä on suhteellisen helppoa tehdä, koska laitteisto ja tieto häirinnän suorittamiseksi on laajasti saatavilla. Hyökkäykset LTE-verkkoon kohdistetaan tiettyyn kehykseen tai kehyksen osaan. Hyökkääjä voi kohdentaa hyökkäyksen esimerkiksi tietyn käyttäjän hallintatietoon häiritäkseen palvelua. Hyökkäystä varten hyökkääjän täytyy olla todella taitava ja tietää tietyt kehykset ja aikaikkunat onnistuakseen hyökkäyksessä. (N. Seddigh ym. 2010, 7.)

LTE-verkon MAC-tasolla merkittäviä tietoturvauhkia on neljä kappaletta: käyttäjälaitteen paikantaminen, kaistan varastaminen, avoimen arkkitehtuurin luomat tietoturvaongelmat sekä DoS-hyökkäykset (Denial-Of-Service). (N. Seddigh ym. 2010, 9.)

Käyttäjälaitteen paikantaminen onnistuu C-RNTI signaalien avulla tai RLC, PDCP sekä RRC ja NAS pakettien numeroiden avulla. (N. Seddigh ym. 2010, 9.)

Kaistaa voidaan varastaa käyttämällä LTE verkon DRX-vaihetta. DRX-vaiheessa UE pysyy aktiivisena, mutta sammuttaa radiosignaalien vastaanottimen virran säästämiseksi. Kyseisen DRX-vaiheen aikana UE pysyy aktiivisena eNB:ssä ja UE saa silti lähettää paketteja, koska UE:lla voi olla kiireellistä liikennettä ulospäin, vaikka DRX-vaihe on käynnistynyt. Tämä luo hyökkääjälle mahdollisuuden syöttää C-PDU käyttäen C-RNTI tunnistetietoa pitkän DRX-vaiheen aikana UE:n sisään. (N. Seddigh ym. 2010, 9.)

LTE-verkko on IP-pohjainen verkko, jossa on useita laitteita, joista suurin osa on vielä mobiililaitteita. Laitteiden aktiiviajat vaihtelevat muutamista sekunneista tunteihin. Laitteiden monimuotoisuus ja laitteiden vaihtelevat tietoturvatasot luovat tietoturvariskin avoimen arkkitehtuurin ja IP-pohjaisessa LTE-verkossa. (N. Seddigh ym. 2010, 9.)

Palvelunestohyökkäyksiä voidaan suorittaa käyttämällä samaa kaavaa kuin kaistan varastamisessa. (N. Seddigh ym. 2010, 9.)

3.3 4G-verkon yleisimmät käyttösovellukset

Kun 4G-verkko otettiin käyttöön, oli sen tarkoituksena mahdollistaa käyttäjille IP-pohjaiset ratkaisut jokapäiväiseen viestintään sekä parantaa mobiililaitteiden käyttöä. Käyttäjät voivat vastaanottaa ääntä, dataa sekä suoratoistaa multimediaa paremmilla tiedonsiirto nopeuksilla kuin aikaisemmin. 4G-teknologia on mahdollistanut tiedonsiirron missä ja milloin vain. (Richa Jain, Nahita Pathania 2019, 1.)

4G-verkon uudet toiminnot voidaan jakaa neljään päätoimialueeseen: palvelut ja sovellukset, palvelualusta, pakettipohjainen ydinverkko sekä uusi radioliityntäverkko. (Richa Jain, Nahita Pathania 2019, 4.)

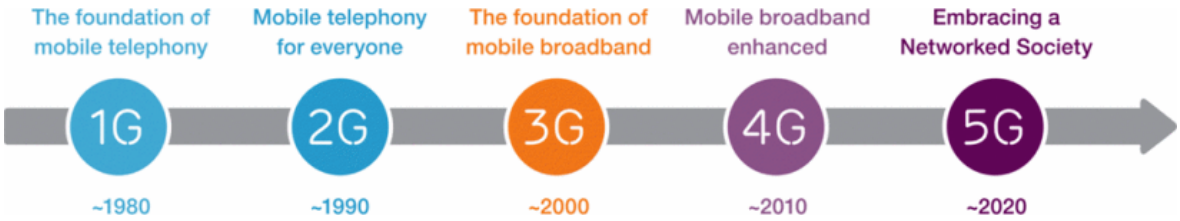
4G-verkko on mahdollistanut huomattavasti nopeammat tiedonsiirtonopeudet kuin 3G-verkko ja tämän avulla olemme saaneet useita uusia toimintoja käyttöömme 4G-verkon avulla. 4G-verkko on mahdollistanut tiedon siirron liikkeellä mobiililaitteissa, kovemmissa nopeuksissa kuin 3G-verkko.

Toimialue/toiminto	Mobiililaite	Kodinelektroniikka	Yritykset
Ääni ja data (puhelut, videopuhelut, viestit, sähköpostit ym.)	Kyllä	Kyllä, tietyt kotoa löytyvät kodinkoneet.	Kyllä
Paikannus ja navigaatio	Kyllä	Kyllä, tietyt kotona olevat kodinkoneet ovat paikannettavissa.	Kyllä, yrityksen tietyt omaisuudet voivat olla paikannettavissa.
Etäkäyttö (tietokoneet, hälytykset, virtuaalialustat ym.)	Kyllä, mobiililaitteen avulla voidaan etäkäyttää muun muassa virtuaalialustoja, oman kodin hälytysjärjestelmiä ym.	Kyllä, tiettyjä kodinkoneita sekä järjestelmiä voidaan käyttää etänä.	Kyllä, muun muassa yrityksen virtuaalialustoja on mahdollista käyttää kotikoneelta.
Viihde (TV, pelit, musiikki ym.)	Kyllä	Kyllä	Kyllä
Pääsy internettiin	Kyllä	Kyllä	Kyllä

Kuva 2. 4G-verkon sovellusalat (mukaillen Richa Jain, Nahita Pathania 2019).

4 5G-verkko

Uuden sukupolven teknologioita on otettu käyttöön noin 10 vuoden välein 1G:stä alkaen, eli matkapuhelimesta, joka tuli markkinoille vuonna 1982. Ensimmäinen 2G teknologia tuli markkinoille 1992, 3G-teknologia 2001. Ensimmäiset standardisoidut 4G-ratkaisut tulivat vuonna 2012, ja nyt on 5G-teknologian vuoro astua esiin. 5G-teknologian, kuten aikaisemmin jokaisen uuden sukupolven teknologian, on tuotettava huomattavia parannuksia edelliseen sukupolveen, jotta operaattoreiden on järkevää investoida uuteen teknologiaan. Yksi 5G-verkon vaatimuksista on saada laajempi kattavuus kuin aikaisemman sukupolven teknologioilla, sekä kattavuuden reuna-alueiden stabiilimpi kuuluvuus ja toiminta. (Sandhya Shinde, Amruta Nikam, Swati Joshi 2016, 2.)



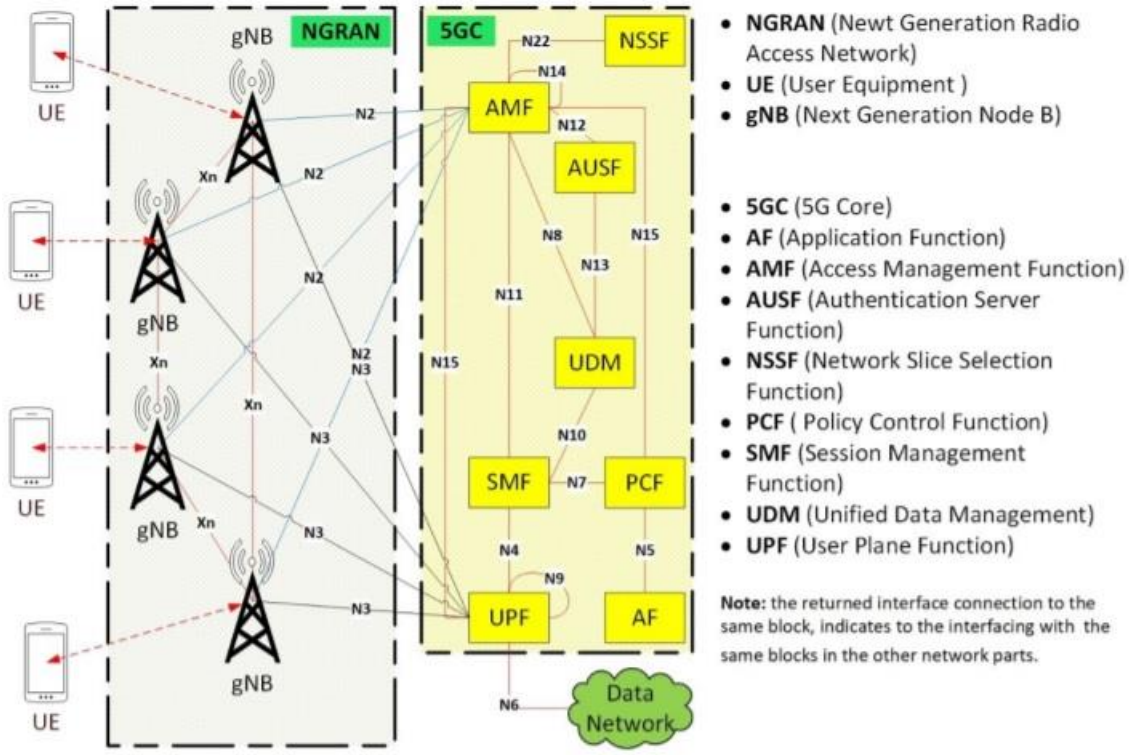
Kuva 3. Mobiiliteknologian kehitysvaiheet. (Sven Mattison, 2017.)

5G-teknologia tulee hyödyntämään jo olemassa olevia teknologioita sekä luo uusia toimivia ratkaisuja. 5G-teknologiassa hyödynnetään WiFi, 3G- sekä 4G-teknologiaa. 5G:n tarjoaman kehityksen avulla matkapuhelinverkot voivat palvella uusia käyttötarpeita, enemmän liikennettä, enemmän laitteita sekä useita erilaisia laitteita, vaikka laitteissa olisikin erilaiset toimintavaatimukset. Näin ollen 5G-teknologia tulee tarjoamaan paljon muutakin kuin parempaa suorituskykyä. Yksi suurimmista motivaattoreista 5G-verkon sekä 5G-teknologian kehittämiseen on koneiden välisen kommunikaation, Internet-of-Things (IoT), kehittäminen. (Sven Mattison 2017, 1–2.)

5G-verkolta vaaditaan enemmän kuin 4G-verkolta, ilman kovempia vaatimuksia, ei verkon taikka teknologian kehittämisessä ole järkeä. 5G-verkolta vaaditaan jopa 20 gigabitin/sekunnissa tarjoamaa huippunopeutta. 5G-verkon tulee myös toimia, vaikka laite liikkuisi 500 km/h. Laitteen viive saisi olla korkeintaan 1 ms. 5G-verkon tulee tarjota käyttäjälle 100 megabittiä/sekunnissa tiedonsiirtonopeutta. (Gordana Barb, Marius Otesteanu 2020, 1.)

5G-teknologia perustuu kolmeen konseptiin: nanoteknologiaan, pilvipalveluihin sekä täysin IP-pohjaiseen alustaan. Nanoteknologialla tarkoitetaan pienten, 0.1–10 nanomillin, kokoisten toimivien teknisten laitteiden ja ratkaisujen rakentamista. Pilvipalvelut mahdollistavat palveluiden ja resurssien käyttöä internetin avulla matalien kustannusten sekä mahdollistaa resurssien ja palveluiden käyttämisen, milloin ja missä vain. Täysin IP-pohjainen alusta on pakettipohjainen verkko. Pakettipohjaisessa verkossa kaikki data siirtyy samalla

tavalla ja se on riippumaton datan siirtoteknologiasta. Verkko tukee yleistä liikkuvuutta ja näin ollen takaa käyttäjille jatkuvan ja katkeamattoman palvelun. Verkko tarjoaa myös rajoittamattoman verkon käytön myös muiden, kuin oman operaattorin alueella. (Tushant Sharma, Kumar Ritesh, Neha Chauhan, Sarika Agarwal 2016, 3.)



Kuva 4. 5G-verkon arkkitehtuuri. (Omar Dawood Sulaiman Al-Gbur, 2021.)

4.1 5G-verkon tietoturva

5G-verkon myötä myös tietoturva tulee kehittymään. Verkon perusturvallisuus pohjautuu 4G-verkossa käytettyihin tietoturvaratkaisuihin, tästä huolimatta tarvitaan myös uusi varmennuskehys. (Xiaowei Zhang, Andreas Kunz, Stefan Schröder 2017, 1.)

Uusia turvallisuus entiteettejä 5G-verkossa ovat: SEAF (Security Anchor Function), AUSF (Authentication Server Function), ARPF (Authentication Credential Repository and Processing Funtion), SCMF (Security Context Management Function) sekä (S)PCF (Security policy control function). (Xiaowei Zhang ym. 2017, 2.)

Turvallisuus entiteetti SEAF sijaitsee AMF:ssä (Core Access and Mobility Management Function). SEAF luo ensisijaiselle autentikoinnille yksilöllisen ankkuriavaimen K_{SEAF}:n jota käytetään käyttäjän laitteen sekä verkon välisen kommunikoinnin suojaamiseen. AUSF lopettaa SEAF:n pyynnöt, jonka jälkeen AUSF jatkaa kommunikointia ARPF:n kanssa. ARPF esiintyy UDM:n (Unified Data Management) kanssa ja säilyttää pitkäkestoisia turvallisuusvaltuutuksia kuten avainta K EPS AKA:ssa varmennusta varten. ARPF voi suorittaa kryptograafisia algoritmeja käyttäen pitkäkestoisia turvallisuusvaltuutuksia syötteenä ja

luoden varmennusvektoreita. SCMF voi esiintyä SEAF:n kanssa AMF:ssä ja noutaa salausavaimen SEAF:lta. SPCF luo turvallisuusprotokollat verkon entiteeteille sekä käyttäjän laitteelle. Turvallisuusprotokolla voi pitää sisällään tietoa AUSF:n valinnasta, luotettavuuden suojaus algoritmista, eheyden suojaus algoritmista, salausavaimen pituudesta ja eliniästä. K_{SEAF}:n perimmäinen tarkoitus on salata paremmin AN (Access Network) avain K_{AN} sekä NAS avaimet K_{NAS}. (Xiaowei Zhang ym. 2017, 2-3.)

Joustavat varmennusmetodit ovat välttämättömiä 5G-verkossa lisääntyvien laitteiden ja liikenteen vuoksi. Esimerkiksi IoT vaatii joustavia varmennusmetodeja toimiakseen. 3GPP SA3 on määrittänyt ensisijaisen varmennuksen, joka on pakollinen, sekä toissijaisen varmennuksen, joka on vapaaehtoinen. Toissijainen varmennus käynnistyy vasta sitten, kun ensisijainen varmennus on tapahtunut onnistuneesti. Ensisijainen varmennus antaa pääsyn 5G-verkon ytimeen. Toissijainen varmennus perustuu PCO:n (Protocol Configuration Options), jossa käyttäjän laite antaa käyttäjän tiedot. Toissijaista varmennusta käytetään esimerkiksi yrityksen ja käyttäjän laitteen välillä, jotta käyttäjä pääsee luotettavasti käsiksi yrityksen APN:n. Molemmat varmennukset tukevat EAP:a. Tällä tavoin 5G:tä voidaan käyttää eri vaatimuksiin erilaisissa tapauksissa. IMSI:n salausta on myös parannettu 5G-verkossa. 5G-verkossa IMSI on saanut nimekseen SUPI (Subscriber Permanent Identifier). 4G LTE verkossa käyttäjän laite lähettää IMSI:n kun se liittyy verkkoon, mutta 5G-verkossa se on salattu yleisellä salausavaimella. (Xiaowei Zhang ym. 2017, 3.)

Kun käyttäjän laite saa palvelua RRC:n kautta toimettomana, se ei vahvista eNB:tä(Evolved Node B) ja tämän takia käyttäjän laite on paikallaan väärällä asemalla. Tämä altistaa käyttäjän laitteen DoS (Denial of Services) hyökkäyksille. 5G-verkossa käyttäjän laite pakotetaan kommunikointiin verkon kanssa, jottei laite olisi toimettomana väärällä asemalla. (Xiaowei Zhang ym. 2017, 3-4.)

4.2 5G-verkon tietoturvauhat

5G-verkon mainittavimmat tietoturvauhat koostuvat muun muassa väärennöksistä (spoofing), peukaloinnista (tampering), torjumisesta (repudiation), tiedon paljastamisesta (information disclosure), palvelunestohyökkäyksestä (denial of service) sekä käyttöoikeuden korottamisesta (elevation of privilege). (Gerrit Holtrup, William Lacube, Dimitri Percia David, Alain Mermoud, G´erˆome Bovet, Vincent Lenders 2021, 25-29.)

4.2.1 Väärentäminen

5G-verkossa on mahdollista spooffata gNB, laite, reunasuojauksen välityspalvelin sekä turvallisuusyhteys. Vale gNB:n asentaminen ei ole kallista ja se onnistuu ohjelmistoradio (software defined radio, SDR) ratkaisuja käyttämällä. Vale gNB pyritään asentamaan

verkko-operaattorin verkon sisään. Mikäli tässä onnistutaan voi vale gNB varastaa UE:lle määrätyn avaimen ja sen avulla pääsee käsiksi UE:n ja gNB:n välisen käyttäjäpinnan kommunikointiin. Spooffatulla laitteella hyökkääjä voi pyrkiä peittämään oikean laitteen varkautta tai hyökkääjä haluaa saada aikaan paljon liikennettä. Reuna suojauksen välityspalvelin voidaan spooffata SEPP:n (Security Edge Protection Proxy) kautta, mutta se vaatii sen, että hyökkääjä tietää SEPP:n valtuutukset. Mikäli hyökkääjä onnistuu tässä, voi hyökkääjä luoda vale PLMN (Public Land Mobile Networks). Spooffattu välityspalvelin voisi keskustella siihen yhteydessä olevien verkkojen kanssa, kunnes valtuutukset muuttuvat. Spooffattu turvallisuusyhteys vaatii tietämyksen jo olemassa olevista salausavaimista. (Gerrit Holtrup ym. 2021, 25–26.)

4.2.2 Peukalointi

Peukaloinnilla voidaan vaikuttaa gNB:n tai laitteen toimintaan. On oletettavaa, että gNB:tä päivitetään ohjelmiston kautta. Mikäli gNB:n laiteohjelma sisältää takaoven, takaoven on voinut asentaa hyökkääjä tarkoituksella tai se voi olla kehittäjän jättämä takaovi mahdollisten ohjelmistovirheiden korjaamiseen, niin tämä peukaloitu gNB voi altistaa käyttäjän salaisuudet, mikäli takaovi ohittaa aktivoidut turvallisuusominaisuudet kuten IPsec ominaisuuden. Mikäli hyökkääjä onnistuu saamaan UE:n pääsytiedot, on mahdotonta erottaa oikea ja kloonattu laite toisistaan. Kloonatun laitteen avulla voidaan esimerkiksi suorittaa DoS-hyökkäystä tiettyyn gNB:n. (Gerrit Holtrup ym. 2021, 26.)

4.2.3 Torjuminen

5G-verkossa gNB:ssä on vain avain, jolla suojataan kanavaa UE:n ja gNB:n välillä. Kotiverkon ulkopuolella vain AMF:llä on pääsy UE:n SUPI-tietoihin. Vaikka vale-gNB onnistuisi liittymään ydinverkkoon ei vale-gNB:n avulla voida jäljittää UE:ta, koska gNB:llä ei ole pääsyä laitteen SUPI-tietoihin. Mikäli vale-gNB hyväksytään ydinverkkoon, on sitä mahdotonta tunnistaa vale-gNB:ksi ja tämän takia vale-gNB:n on mahdollista poistaa RRC-tason sekä käyttäjäpinnan datan salaus. (Gerrit Holtrup ym. 2021, 26–27.)

4.2.4 Tiedon paljastaminen

SUPI on piilotettu käyttäen epäsymmetristä salausta. Tämä salausmekanismi tarjoaa varman suojauksen SUPI:lle suoraa hyökkäystä kohden. SUPI on mahdollista saada tietoon, mikäli operaattorin yksityinen avain päätyy hyökkääjän tietoon. Operaattorin yksityisen avaimen vaihtaminen UE:n on haastavaa, eli sen kumoaminen ja korvaaminen ovat vaikeita suorittaa. Mikäli hyökkääjä tietää operaattorin yksityisen avaimen voi hyökkääjä paljastaa käyttäjän SUCI-tiedon ja näin rakentaa SUPI/IMSI-kerääjän kyseisen operaattorin verkkoon. (Gerrit Holtrup ym. 2021, 27.)

4.2.5 Palvelunestohyökkäys

UE:ta on mahdollista häiritä vale-gNB:n avulla. Vale-gNB:ssä ollessaan laite siirtyy verkkovierailu kielletty tilaan. Mikäli UE liittyy vale-gNB:n, UE ei yritä rekisteröityä uudelleen, ennen kuin UE käynnistetään uudestaan tai SIM-kortti poistetaan ja laitetaan takaisin UE:n sisään. Laitteiden välisessä kommunikaatiossa tämä voi johtaa tilanteeseen, missä kommunikointi käyttöliittymä sulkeutuu pysyvästi. (Gerrit Holtrup ym. 2021, 28.)

gNB on toiminnassa vain niin kauan kuin sen hajasaantikanava toimii oikein. Hyökkääjän on mahdollista häiritä hajasaantikanavaa ja näin estää laitteita rekisteröitymästä kyseiseen gNB:n. Vaikka tämänkaltainen häirintä ei ole pitkäkestoista, vaikuttaa se jokaiseen UE:n joka on rekisteröitynyt kyseiseen gNB:n. (Gerrit Holtrup ym. 2021, 28.)

Mikäli hyökkääjä saa tietoonsa gNB:n ja ydinverkon väliset fyysiset tiedonsiirtokaapelit, on hyökkääjän mahdollista suorittaa fyysinen hyökkäys ja katkaista kyseiset kaapelit. Vaikka operaattori käyttäisi virtualisointia sekä pilvipalveluja verkon toimintoihin on gNB:n oltava fyysisesti saatavilla paikallaan, jotta sitä voidaan käyttää. (Gerrit Holtrup ym. 2021, 28.)

4.2.6 Käyttöoikeuksien korottaminen

Mikäli hyökkääjä onnistuu muokkaamaan laiteohjelmaa gNB:n sisällä, voi hyökkääjä asentaa rinnakkaisen kommunikaatiokanavan, joka toimii MitM:nä (Man in the middle) UE:n sekä verkon välillä. MitM:n toimisi sekä käyttäjä- että ohjauspinnan tasolla. Mikäli verkon toimintoihin käytetään paljon pilvipalveluja, on niiden koskemattomuuden hallinta kolmannella taholla eikä itse verkko-operaattorilla. (Gerrit Holtrup ym. 2021, 29.)

4.3 5G-verkon käyttösovellukset

5G-verkon tavanomaiset käyttösovellukset ovat samat kuin 4G-verkolla, mutta sen toimintaa on kehitetty ja suurimmat muutokset on pyritty tekemään kolmelle eri osa-alueelle. Nämä osa-alueet ovat: eMBB (Enhanced Mobile Broadband / Extreme Mobile Broadband), URLLC (Ultra-Reliable and Low Latency Communication) sekä mMTC(Massive Machine Type Communication). 5G-verkkoa tullaan soveltamaan muun muassa sähköverkoissa, kodeissa, terveydenhuollossa, ajoneuvoissa sekä IoT:ssä. 5G-verkon odotetaan parantavan myös ihmisten elämänlaatua sen monikäyttöisyyden vuoksi, kun 4G-verkko keskittyi enemmän vain mobiilidatan siirtonopeuksiin. (Gordana Barb, Marius Otesteanu 2020, 4.)

Mitä 5G tuo käyttäjälle?	Mitä uutta 5G-verkossa?	5G-sovellusalat
Valtavat määrät, todella nopeasti	Spektrin laajennus, millimetriaallot, tiheämmin tukiasemia, kehittyneemmät antennit, uusia elektronisia komponentteja, laitteiden välinen viestintä, liikkuvat tiedonsiirtoverkot ym.	Hologrammi TV, lisätty todellisuus, äärimmäisen suuret tiedonsiirrot, immersiivinen läsnäolo
Aina hyvin yhdistetty verkkoon	Yhdistelmä 3G-, 4G- ja WiFi- verkkoa sekä radioliityntäverkkoa. Näin luodaan integroitu ja dynaaminen radioliityntäverkko.	Pysytään verkossa aina ja kaikkialla, mukaan lukien junat, lentokoneet ja ihmismassat.
Ei näkyvää viivettä	Äärimmäisen alhainen viive, laitteiden välinen viestintä, verkkoäly lähemmäs käyttäjää ym.	Käsinkosketeltava internet, reaktiiviset käyttöliittymät, sähköverkkojen hallinnointi, ajoneuvojen välinen viestintä, robottien ohjaus, yhdistetyt ajoneuvot ym.
Valtava määrä yhdistettyjä asioita ja ihmisiä	Tiheämmin tukiasemia, paljon vähemmän signaaliliikennettä eikä synkronisointia, RAN-arkkitehtuuri ym.	IoT, älykaupungit, yhdistetyt ajoneuvot ym.
Energia tehokkuus	Lepotilan optimointi, ympäröivän energian varastointi, mMTC, käyttö tarvittaessa ym.	80 % energian säästö, käyttöönotto kehittyvissä maissa
Joustavat ohjelmoitavat verkot	Ohjelmointirajapinnat, ohjelmallisesti määritetty verkko, verkon toimintojen virtualisointi ym.	Uusia liiketoimintamalleja innovatiivisille PK-yrityksille jotka tarjoavat verkkoratkaisuja, nopeammat innovaatiot verkkopalveluissa ym.
Turvalliset verkot	Virtuaalinen todentaminen, fyysisen tason todentaminen	Verkkoja poliisille sekä turvallisuusalan ammattilaisille, yksityisyyttä

Kuva 5. 5G-verkon tarjoamat sovellusalat (mukaillen EU-komissio).

5 4- ja 5G verkkojen vertailu

Tässä luvussa tullaan tarkastelemaan 4- ja 5G-verkkojen eroja suurpiirteittäin. Vertailussa tullaan keskittymään suurimmaksi osaksi kuluttajiin vaikuttaviin eroavaisuuksiin sekä taajuuksiin ja tietoturvaan. 5G-verkko on kehittyneempi versio 4G-verkosta, vaikkakin 5G-verkon teknologia pohjautuu pitkälti 4G-verkon arkkitehtuuriin, sitä on kehitetty huomattavasti.

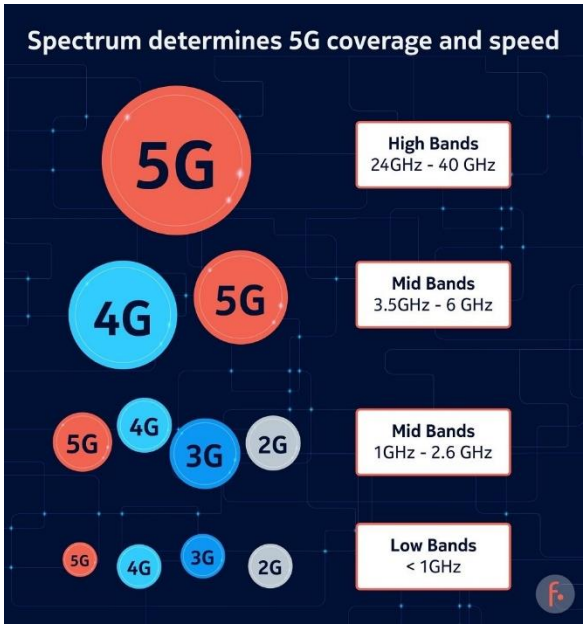
Kansainvälinen televiestintäliitto, ITU-R, on määrittänyt vaatimukset sille, että jokaisen uuden sukupolven teknologian tulee kehittyä edellisestä teknologiasta huomattavasti (Khaldoon Alshouiliy and Dharma P. Agrawal 2021, 4.).

Alla olevaan kuvaan on listattu 4G LTE- ja 5G-verkon väliset eroavaisuudet.

Key Requirements	4G (LTE)	5G
Peak Data Rate	1 Gbit/s	20 Gbit/s
User Experienced Data Rate	10 Mbit/s	100 Mbit/s
Mobility	350 Km/h	500 km/h
Latency	10 ms	<1 ms
Connection Density	10^5 devices/km^2	10^6 devices/km^2
Area Traffic Capacity	0.1 Mbit/s/m^2	10 Mbit/s/m^2

Kuva 6. 4G- ja 5G-verkon vaatimukset. (Gordana Barb, Marius Otesteanu 2020.)

4G LTE- ja 5G-verkko toimivat myös eri taajuuksilla. 4G-verkko toimii alle 1 GHz – 6 GHz taajuudella, kun taas 5G-verkko toimii alle 1 GHz – 40 GHz taajuudella.



Kuva 7. Eri verkkojen taajuudet. (Nokia.)

5.1 Uudet turvallisuusominaisuudet 4G vs. 5G-verkko

5G-verkkoon on otettu käyttöön uusia turvallisuusominaisuuksia. Turvallisuusominaisuuksia on lisätty sen mukaan, mitä haavoittuvuuksia 4G-verkossa havaittiin. 5G-verkossa UE:n sim-kortti sisältää epäsymmetrisen avainominaisuuden, kotiverkon julkisen salausavaimen. Salausavainta käytetään elliptisten käyrien salausmenetelmissä. Epäsymmetriset kryptografiset algoritmit mahdollistavat luottamuksellisen tiedon siirtymisen ydinverkkoon. Tämä mekanismi estää käyttäjän laitteen IMSI-tietojen keräämisen IMSI-kerääjä hyökkäyksellä. IMSI-kerääjä hyökkäyksellä voidaan seurata laitetta. IMSI on korvattu tarkoituksenmukaisesti monimutkaistetulla SUCI:lla alkuperäisessä rekisteröinti pyynnössä. 5G-verkko ei ole täydellinen, mutta se on turvallisempi IMSI-keräystä vastaan kuin aikaisemmat protokollat mikäli operaattori ottaa käyttöönsä kaikki 3GPP:n suositukset. (Gerrit Holtrup ym. 2021, 13.)

Turvallisuus ominaisuus	Löytyy 4G:stä	Löytyy 5G:stä
IMSI:n tarkoituksenmukainen monimutkaistaminen	Ei	Kyllä, käyttäen ECIES salausta
Käyttäjäpinnan salaus tukiaseman ja laitteiston välillä	Kyllä (operaattorin valinta)	Kyllä (operaattorin valinta)
Käyttäjäpinnan eheyden suojaus tukiaseman ja laitteiston välillä	Ei	Kyllä (operaattorin valinta)
RRC viestien eheyden suojaus	Kyllä, EIA0-algoritmi sallii vain hätäpuhelut	Kyllä, NIA0-algoritmi sallii vain hätäpuhelut
RRC viestien salaus	Kyllä (operaattorin valinta)	Kyllä (operaattorin valinta)
NAS viestien eheyden suojaus	Kyllä, EIA0-algoritmi sallii vain hätäpuhelut	Kyllä, NIA0-algoritmi sallii vain hätäpuhelut
NAS viestien salaus	Kyllä (operaattorin valinta)	Kyllä (operaattorin valinta)
UE:n varmentaminen palvelevaan verkkoon	Kyllä	Kyllä
UE:n varmentaminen kotiverkkoon, vaikka käytetään ei-luotettua palvelevaa verkkoa	Ei	Kyllä
Verkon viipalointi eri käyttötarkoituksiin ja eri applikaatioille.	Ei	Kyllä

Kuva 8. 4- ja 5G-verkon turvallisuusominaisuuksien vertailu. (mukaillen Gerrit Holtrup ym. 2021.)

6 Uhka-analyysi ja torjuntatoimet

Tähän lukuun on koottuna 5G- ja 4G-verkkoihin kohdistuvat uhkakuvat todennäköisyyksineen. Analyysissa käytetään STRIDE-menetelmää. STRIDE-menetelmällä voidaan tarkentaa tietyn uhan hyökkäysvektoreita. STRIDE on lyhenne verkkoon kohdistuvista hyökkäys menetelmistä eli Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service sekä Elevation of Privilige. Jokaisella menetelmällä vaikutetaan eri osa-alueeseen. Luvussa perehdytään myös siihen, kuinka kyseisiä hyökkäyksiä voi torjua niin palvelun tarjoajan kuin käyttäjänkin näkökulmasta.

Alla kuvatussa taulukossa on kuvattuna eri hyökkäys menetelmät selityksineen.

	Hyökkäys menetelmä	**Mihin hyökättiin**	**Kuinka hyökättiin**
S	Spoofing	Autentikointiin	Tekeytymällä tunnetuksi ja luotettavaksi tahoksi
T	Tampering	Eheyteen	Muokkaamalla dataa verkossa, muistissa, kovalevyllä ym.
R	Repudiation	Torjumiseen	Estämällä toimintojen suorittaminen
I	Information Disclosure	Luotettavuuteen	Tarjoamalla informaatiota taholle, jolla ei ole valtuuksia
D	Denial of Service (DoS)	Saatavuuteen/saavutettavuuteen	Estämällä tai häiritsemällä pääsyä palveluihin
E	Elevation of Privilige	Valtuuttamiseen	Annetaan pääsy jollekin ilman oikeanlaista valtuutusta

Kuva 9. STRIDE-menetelmä.

6.1 Mahdollisia uhkakuvia

Kappaleeseen on koottu tietoverkkoihin kohdistuvia uhkakuvia. Tietoverkkoihin kohdistuvat uhkakuvat eivät rajoitu pelkästään taulukosta löytyviin mahdollisuuksiin

Nro	STRIDE	Hyökkäyksen kohde	Uhkakuva	Kuvaus	Vaikutukset	Todennäköisyys
1	STRIDE	UE:n pitkäaikaiset avaimet verkossa	Työntekijällä on pääsy UE:n avainten tietokantaan. Työntekijä tekee kopioi avaimet ja myy ne eteenpäin	UDM pitää sisällään kaikki verkossa käytetyt avaimet	Kriittinen	Epätodennäköinen
2	SRIE	SEPP käyttää yksityistä avainta rekisteröityäkseen muihin verkkoihin	Yksityisen avaimen varastaminen SEPP:n kautta. Avaimen saatuaan hyökkääjä voi esiintyä SEPP:nä ja luoda valeverkon, jonka avain vastaa anastettua SEPP:n avainta	Verkot varmentavat toisiaan SEPP:n kautta	Todella korkea	Epätodennäköinen
3	SRIDE	Laiteavaimet, datan lähettäminen ja vastaanottaminen, laitteen toiminnan jatkuvuus	Laiteavaimen anastaminen laitehyökkäysten kautta. Avain anastetaan ensin oikean	Hyökkäyksen vaikeus riippuu UICC:n suojauksesta	Korkea	Epätodennäköinen

			laitteen UICC:stä. Oikeasta avaimesta tehdään klooneja, joilla hyökkäys suoritetaan			
4	SRIDE	Laitteen turvallisuus, datan luotettavuus ja eheys	Haittaohjelma mobiililaitteelle. Haittaohjelman avulla anastetaan avaimet, joiden avulla voidaan tekeytyä laitteeksi ja purkaa aikaisemman viestinnän ja datan salaus verkossa	Rekisteröinnin yhteydessä luodut avaimet säilytetään UICC:n ulkopuolella mobiililaitteessa	Korkea	Todennäköinen
5	D	Palvelun saavutettavuus	Laitteiden häirintä vale gNB:n avulla	Häirintä vain vale gNB:n kantaman alueella	Kohtalainen	Todennäköinen
6	I	Paikantaminen	Osittainen SUCI:n ja PEI:n sieppaaminen radio linkkien kautta	Laitteen yksilöivien tunnistetietojen saaminen	Kohtalainen	Erittäin todennäköinen

7	D	Palvelun saavutettavuus	gNB:n häirintä	Yhdellä häirintälaitteella voidaan häiritä vain yhtä gNB:tä kerrallaan	Kohtalainen	Todennäköinen
8	TRIDE	Palvelun saavutettavuus, datan luotettavuus ja eheys, laitteen sijainti	Käyttäen ohjelmiston haavoittuvuutta gNB:ssä asentaakseen takaovia	Peukaloitu gNB voi jakaa dataa, voi antaa pääsyn gNB:n avaimiin. Haavoittuvuus voi olla ohjelmistossa vahingossa tai hyökkääjän asentamana	Korkeasta katastrofaaliseen	Todennäköinen
9	TRID	Palvelun saavutettavuus, datan luotettavuus ja eheys	Ohjelmiston haavoittuvuuden hyödyntäminen verkon toiminnoissa voi johtaa UE:n uudelleen konfiguraatioon, datan vuotamiseen sekä	Peukaloitu verkkotoiminto (esim. AMF) voi paljastaa laitteen turvallisuusprotokollat	Todella korkea	Epätodennäköinen

			turvatoimien ohittamiseen.			
10	TI	Laitteen data	Avainten anastaminen tukiasemasta. gNB:ssä avaimet eivät välttämättä ole turvallisesti säilötty	gNB:n ohjelmiston haavoittuvuudet voivat altistaa hyökkäykselle	Korkea	Erittäin todennäköinen
11	D	Palvelun saavutettavuus ja verkon suorituskyky	gNB:n asetusten fyysinen varastaminen tai muokkaaminen	Tukiaseman fyysinen vahingoittaminen	Kohtalainen	Erittäin todennäköinen
12	D	Verkon suorituskyky	Tietoverkkoliikenteen priorisoiminen korkeaksi, vaikka tarve ei olisi korkea	Korkean prioriteetin liikennettä voi olla vain tietty määrä	Kohtalainen	Erittäin todennäköinen

Kuva 10. Tietoverkon uhkakuvat (mukaillen Gerrit Holtrup ym. 2021.)

6.2 Hyökkäysten kuvaus ja mahdolliset torjuntatoimet

Kappaleessa keskitytään yllä olevan taulukon uhkakuvien kuvaamiseen, mahdolliseen torjuntaan ja ennalta estämiseen sekä mahdollisen hyökkääjän profiiliin.

- Tapaus 1
    - Hyökkäystä voidaan ennalta ehkäistä fyysisen pääsyn rajoittamisella UDM:n. Myös HSM:n käyttö suojaa avaimia. Mikäli hyökkääjä saisi käsiinsä HSM:n on se aikaa vievää hyökkääjältä purkaa avaimet HSM:stä. Mahdollinen hyökkääjä voisi olla tyytymätön työntekijä tai työntekijä, joka on uhkailun taikka kiristyksen kohteena. Työntekijällä tulisi olla pääsy UDM säilöön. Anastetusta tiedosta voisi hyötyä esimerkiksi valtiollinen toimija.

- Tapaus 2
    - Hyökkääjä voisi rakentaa itselleen rinnakkaisen verkon käyttämällä omia tukiasemia. Verkon luontia varten hyökkääjän pitäisi saada haltuunsa alkuperäiset SEPP avaimet, jonka jälkeen hyökkääjä sulkisi alkuperäisen SEPP:n ja korvaisi sen omallaan. Valeverkon rakentaminen vaatisi oikeaa infrastruktuuria tukiasemien rakentamiseen ja näin ollen mahdollinen hyökkääjä voisi olla esimerkiksi valtiollinen toimija. Valeverkko toimisi kuten oikea verkko ja näin ollen hyökkääjän verkko pitäisi sisällään laitteiden lähettämät yksilöivät tunnistetiedot. Mikäli valeverkko saataisiin toimintaan samanaikaisesti kuin alkuperäinen, liittyy käyttäjän laite kuitenkin aina kotiverkkoon, eli alkuperäiseen verkkoon.

- Tapaus 3
    - UICC pitää sisällään käyttäjän laitteen ja verkon väliseen kommunikointiin vaadittavat salausavaimet. Mikäli hyökkääjä onnistuisi saamaan avaintiedot UICC:ta, voitaisiin avaintietoja käyttää useaan eri tarkoitukseen. Hyökkääjä voi esimerkiksi luoda laitteesta klooneja. Tietoverkon tulisi kuitenkin toimia niin, että se hyväksyy vain yhden yksittäisen laitteen samoilla turvallisuustunnisteilla kerrallaan. Mikäli hyökkäys suoritetaan käyttäjän laitteeseen käyttäjän tietämättä sitä, on laitteen sisällön seuraaminen ja kuuntelu mahdollista. Tämä hyökkäys kohdistuu aina vain tiettyyn UICC:n, eikä se vaaranna useita laitteita kerrallaan. Mahdollisia hyökkääjiä voisi olla valtiollinen toimija tai rikollisorganisaatio. Myös tietoturvan testaajat suorittavat tämänkaltaisia hyökkäyksiä kokeillakseen tuotteiden turvallisuutta sekä kokeillakseen teknistä osaamista.

- Tapaus 4
    - Väliaikainen avain voidaan anastaa mobiililaitteesta käyttäen esimerkiksi haittaohjelmaa. Mikäli tietoverkko ei uudelleen lähetä turvallisuustietoja, pysyy avain voimassa. Esimerkiksi IoT-laitteilla tietoliikenne halutaan pitää minimissään, ja näin ollen turvallisuustiedot voivat olla pitkään samalla avaimella suojattuna. Väliaikaisen avaimen turvallisuus riippuu paljon mobiililaitteen omasta suojauksesta. Mahdollisia hyökkääjiä ovat esimerkiksi hakkerit sekä tietoturvatestaajat.

- Tapaus 5
    - Laitteiden häirintä vaikuttaa käyttäjän laitteeseen vain niin kauan kuin itse häirintälaite on käynnissä. Paikallaan olevien IoT-laitteiden häirintä on haastavampaa kuin liikkuvien. Paikallaan olevat IoT-laitteet eivät vaihda

tukiasemaa eivätkä näin ollen lähetä uusia rekisteröintisignaaleja, jota kautta häirintälaite voisi suorittaa häirintää. Liikkuvat IoT-laitteet vaihtavat tukiasemaa useammin ja näin ollen niiden häirintäkin on helpompaa. Häirintää suoritetaan lähtökohtaisesti vale-gNB:llä. Laitteiden häirintää käyttävät mahdolliset hyökkääjät voisivat olla esimerkiksi rikolliset ja terroristit.

- Tapaus 6
    - Tietoverkossa radiosignaalien eheys on suojattu. Hyökkääjä voi kaapata radiosignaalin. Radiosignaalien kautta lähetetään vain osittainen SUPI suojattuna, mutta hyökkääjä voi silti saada tietoonsa saman määrän informaatiota osittaisen SUPI:n sekä operaattorin tietojen avulla. Mikäli signaalin dataa ei ole suojattu, on laitteen seuranta mahdollista. Mahdollisia hyökkääjiä ovat esimerkiksi valtiolliset toimijat.

- Tapaus 7
    - Tukiaseman häirintää voidaan suorittaa laitteilla, jotka tukkivat tietyn tukiaseman liityntäkanavat. Tukkimalla liityntäkanavat estetään uusien laitteiden rekisteröityminen tiettyyn tukiasemaan. Hyökkäys kohdistuu aina tiettyyn tukiasemaan kerrallaan.

- Tapaus 8
    - Tukiasemien ohjelmistot ovat monimutkaisia. Tukiaseman valmistaja ei välttämättä jaa ohjelmiston tietoja edes operaattorille. Tukiasemien ohjelmistot ovat päivitettäviä, mutta tukiasemien ohjelmistoihin on voitu jättää takaovia esimerkiksi valtion määräämänä taikka laitevalmistajan toimesta. Nämä takaovet altistavat tukiasemat mahdollisille hyökkäyksille. Hyökkäysten kautta voitaisiin mahdolliset kaataa koko tietoverkkoinfrastruktuuri. Mahdollisia hyökkääjiä voisi olla esimerkiksi valtiollinen toimija, tyytymätön työntekijä sekä ohjelmistokehittäjän inhimillinen virhe takaoven asennuksen kanssa.

- Tapaus 9
    - Hyökkääjän on mahdollista kohdistaa hyökkäys verkon toimintoon kuten AMF:n. AMF:n kautta hyökkääjä saisi pääsyn AMF:ssä käsiteltäviin turvallisuus protokolliin ja toimintoihin. 5G-verkon avaimet on suojattu siten, että alemman tason avaimilla ei ole pääsyä ylemmille tasoille, esim. gNB:n avaimella ei ole pääsyä AMF:n. Mikäli toimintoja on virtualisoitu ja toiminnot toimivat pilvipalvelun kautta riippuu turvallisuus pilvipalvelun tarjoajan tietoturvasta. Mahdollisia hyökkääjiä voisi olla esimerkiksi hakkeri, mikäli verkon toimintojen ohjausyksikkö on saatavilla internetissä sekä vieraan valtion vihamielinen toiminta kuten vakoilu tai infrastruktuuriin vaikuttaminen.

- Tapaus 10
    - Parhaassa tapauksessa operaattori ei luota verkon fyysiseen suojaukseen datan siirrossa, kun data liikkuu toimintojen välillä. Riippuen IPSec:n käyttöönotosta voi olla mahdollista anastaa avaimet verkon sisällä olevan toiminnon ohjelmistosta. Mikäli verkon laitteistoon on mahdollista päästä fyysisesti käsiksi, on hyökkääjän mahdollista kohdistaa myös fyysinen hyökkäys laitteistoon avainten saamiseksi. Mahdollisia hyökkääjiä ovat rikolliset, hakkerit sekä tietoturvatestaajat.

- Tapaus 11
    - gNB:n fyysinen sabotointi tai jopa antennien varastaminen on myös potentiaalinen uhkakuva. Mahdollisia toimijoita voisivat olla aktivistihakkerit. Näiltä operaattori voi suojautua mahdollistamalla riittävät fyysiset turvatoimet gNB:llä.

- Tapaus 12
    - RAN:n jaossa on mahdollista se, että operaattori ei pysty tarjoamaan tarpeeksi kaistaa korkean prioriteetin siivuille. Tämä saattaa konkretisoitua silloin, mikäli liikenne on erityisen kuormittavaa muilla kuin korkean prioriteetin siivuilla, niin kaistan leveys korkeammilla prioriteeteilla pienenee. Hyökkäyksen mahdollisuus riippuu täysin siitä, miten operaattori on konfiguroinut oman verkkonsa. Mahdollisia hyökkäyksen suorittajia ovat esimerkiksi rikolliset ja terroristit.

7 Vaikutukset yhteiskunnan eri osa-alueilla siirryttäessä 4G-verkosta 5G-verkkoon

Kuinka 5G-verkko tulee vaikuttamaan yhteiskuntaamme? Onko siitä mitään käytännön hyötyjä kuluttajan näkökulmasta? Kuinka toiminta tulee muuttumaan uuden teknologian myötä? Kuinka näillä osa-alueilla voidaan varautua 5G-verkon tietoturvauhkiin?

7.1 Operaattorit

5G-verkon myötä operaattoreiden on mahdollista jakaa verkkonsa siivuihin mikä ei aikaisemmin ollut mahdollista. Siivuttamalla verkkoa, operaattorit pystyvät varaamaan enemmän verkon kaistaa tärkeämmille toiminnoille ja tietyille toiminnoille voidaan antaa niin sanottu etuajo-oikeus. Mitä tärkeämpi toiminto on, sitä nopeammin se suoritetaan ja vähemmän tärkeät toiminnot suoritetaan vasta sen jälkeen.

5G-verkon vielä ollessa uusi, luo 5G-verkon käyttöönotto tietyille operaattoreille uusia liiketoimintamahdollisuuksia uusien asiakkuuksien myötä. Mitä nopeammin operaattori ottaa käyttöönsä 5G-verkon, sitä todennäköisemmin operaattori saa uusia asiakkaita niin kuluttajista kuin yrityksistäkin.

Operaattorit tulevat virtualisoimaan verkon toimintoja ja ottamaan käyttöön uusia arkkitehtuureja 5G-toiminnoissa. Virtualisoinnin avulla operaattorit pystyvät tarjoamaan ja priorisoimaan siivuja dynaamisesti kysynnän mukaan. Operaattorit voivat hyödyntää virtualisointia ja siivuttamista uusiin liiketoimintamalleihin. Operaattorit voivat esimerkiksi luoda oman verkon pelaajille, jossa tarjottaisiin yhteyttä minimaalisella viiveellä. Pelaajille luotu verkko olisi täysin itsenäinen muusta verkosta, eikä se rasittaisi muiden kuluttajien kaistaa.

Operaattoreiden tulee tehdä mittavia investointeja tämän kaiken toteuttamiseksi. Dynaaminen resurssien jakaminen vaatii automatisoidut prosessit ja toiminnot. Koneoppiminen ja tekoäly mahdollistavat tämän operaattoreille. Oppiva tekoäly pystyy analysoimaan tulevaa dataa ja muokkaamaan verkon siivujen priorisointeja oppimansa perusteella ja ennakoimalla verkon tarpeita.

5G-verkko tulee luomaan operaattoreille uusia liiketoimintamahdollisuuksia sekä tekemään operaattoreista enemmän kilpailukykyisiä yrityksiä, jotka voivat myydä tuotteitaan enenevissä määrin kuluttajille, yrityksille sekä viranomaisille.

7.1.1 Operaattoreiden tietoturva 5G-verkossa

5G-operaattoreilla on suuri vastuu 5G-verkon tietoturvasta. Operaattorit pystyvät omilla valinnoillaan vaikuttamaan suuresti loppukäyttäjän tietoturvaan sekä uhkien mahdollistamiseen. Mikäli operaattori ottaa kaikki pakolliset sekä vaihtoehtoiset turvallisuustoimet käyttöön 5G-verkossa, on suurin osa hyökkäyksistä mahdoton suorittaa. 5G-verkon tuomat uudet liiketoimintamahdollisuudet toivottavasti motivoivat operaattoreita mahdollisimman hyvään tietoturvaan loppukäyttäjälle. Tietoturvaratkaisujen ja niiden käyttöönoton markkinoinnilla voidaan luoda hyvää kuvaa omasta toiminnasta ja sen avulla markkinoida omia tuotteitaan uusille asiakkaille.

Mikäli operaattori ulkoistaa virtualisoinnin sekä pilvipalvelut, tulee turvallisuuden takaamiseen yksi linkki lisää. Voiko operaattori olla varma palveluntarjoajan palkkaamista työntekijöistä? Onko palveluntarjoajalla lisää omia alihankkijoita? Operaattori on kuitenkin vastuussa kuluttajalle tarjoamastaan palvelusta, vaikka käyttäisikin alihankkijoita tai palveluntarjoajia. Operaattori voi tietenkin sopimuksissa edellyttää palveluntarjoajia samoihin turvallisuusratkaisuihin mihin operaattori on ryhtynyt, näin voidaan ennalta estää tietoturvauhkia.

Myös fyysiseen uhkaan operaattorin tulee varautua. Nykyaikana löytyy edelleen 5G-verkon vastustajia ja tämä asettaa esimerkiksi 5G-tukiasemat tietynlaisen vandalismin kohteeksi. Operaattorit voivat ennaltaehkäistä tätä uhkaa avoimella keskustelulla ja riittävillä fyysisillä turvatoimilla tukiasemien läheisyydessä. 5G-tukiasemien fyysinen vahingoittaminen on helpompaa ja kuin 5G-verkon sisällä tapahtuvat hyökkäykset. Fyysiseen hyökkäykseen pystyy kuka vaan, mutta verkossa tapahtuvat hyökkäykset vaativat erityistietoja ja -taitoja.

Operaattoriin kohdistuvilla verkkohyökkäyksillä pyritään luomaan epävakauksia verkkoyhteyksiin ja yleensä niiden motiiveina ovat vain häirintä. Operaattorit hallinnoivat myös paljon henkilötietoja, joten hyökkääjillä voi olla myös motiivina saada näitä henkilötietoja itselleen. Henkilötietoja voidaan myydä edelleen ja näin saadaan taloudellista hyötyä.

On toki myös mahdollista, että kilpailevat verkko-operaattorit haluaisivat häiritä toistensa verkkoja, nostaakseen omaa markkina-asemaansa, mutta itse en näe tätä todennäköisenä ainakaan Suomessa.

7.2 Julkinen sektori

5G-verkko tulee mullistamaan myös julkisen sektorin toimijoiden palveluja merkittävästi. 5G-verkon tarjoamat tiedonsiirtonopeudet ja olemattomat viiveet tiedonsiirrossa tarjoavat lukemattomia mahdollisuuksia niin terveydenhuollon, turvallisuuden sekä muiden julkisen

sektorin palvelualoille. 5G-verkossa kaavaillut toiminnot ovat vasta suunnitteluvaiheessa ja on mahdotonta sanoa tässä vaiheessa, mitkä toiminnoista tulevat toteutumaan, mutta 5G-verkko luo teoreettiset mahdollisuudet uskomattomiin asioihin mitä ei aikaisemmin ole voitu suorittaa.

Terveydenhuollossa 5G-verkko mahdollistaa esimerkiksi potilaiden etäseurannan reaaliajassa. Reaaliaikainen potilaan seuranta sensorien ja kannettavien älylaitteiden, kuten älykellot, avulla saadaan reaaliaikaista dataa ihmisen terveydentilasta ja poikkeamiin pystytään puuttumaan entistä tehokkaammin. Etäyhteyden avulla voidaan suorittaa myös vaikka leikkauksia haja-asutusalueilla ilman lääkärin fyysistä läsnäoloa. Lääkäri käyttäisi apunaan 5G-verkkoa sekä haja-asutusalueella olevaa automatisoitua leikkaussalia ja leikkauksen suorittaisi robotti lääkärin ohjauksessa. AR/VR-maailma mahdollistaa myös visuaaliset avut näkövammaisille ihmisille (STL Partners, 2021).

Julkisessa liikenteessä sekä liikenneinfrastruktuurissa, kuten liikennevaloissa, 5G-verkon avulla voidaan tuottaa reaaliaikaista dataa ja reaaliaikaisen datan avulla saadaan liikenteestä sujuvampaa, kun voidaan luopua ennalta määrätyistä ajastuksista sekä toimintamalleista ja siirtyä reaaliaikaiseen jopa proaktiiviseen ajastukseen sekä toimintamalleihin. Voidaan avata liikenteen solmukohtia kontrolloimalla liikennevaloja ja näin ollen kontrolloida liikennevirtoja.

5G-verkossa olevista laitteista saatava reaaliaikainen data auttaa myös ensihoito- ja pelastustointa sekä poliisia. Reaaliaikaisen datan avulla esimerkiksi onnettomuuspaikalle saapuvat yksiköt voisivat saada dataa kaikista lähistöllä olevista laitteista onnettomuuden olosuhteista ja riskeistä pelastustoimelle.

7.2.1 Julkisen sektorin tietoturva 5G-verkossa

5G-verkon käyttäjät ovat lähtökohtaisesti riippuvaisia operaattorin käyttöönottamista turvallisuusratkaisuista 5G-verkossa. Loppukäyttäjät, tässä tapauksessa viranomainen, voi vaikuttaa vain tiettyihin osa-alueisiin tietoturvan osalta. Näitä osa-alueita ovat esimerkiksi 5G-verkossa olevan laitteen fyysinen tietoturva sekä henkilöstön koulutus tietoturvaan liittyen. Lähtökohtaisesti julkiselle sektorille sekä viranomaisille on tietyt laissa, asetuksissa ja ohjeissa määrätyt velvollisuudet oikeanlaisen tietoturvan hoitamiseen aina henkilötietojen käsittelystä rekisterien ja tietojärjestelmien ylläpitoon.

Julkinen sektori käyttää tietyillä osa-alueilla ja toiminnoilla omia palvelimiaan, joita ylläpidetään virastojen sisällä. Palvelimet tietenkin liittyvät avoimeen verkkoon avoimen internetin kautta ja näin ollen internetin tarjoajan turvallisuusratkaisut vaikuttavat myös näihin, mutta omien palvelimien suojaaminen on myös tärkeässä asemassa.

Julkisella sektorilla tulisi paneutua henkilöstön kouluttamiseen esimerkiksi mobiililaitteiden turvallisessa käytössä sekä salasanojen monimutkaisuuden sekä vaihtovälin avulla. Nykyaikana tietoturvan heikoin lenkki on kuitenkin ihminen. Työntekijöiden huolimattomuus voi johtaa suuriinkin vahinkoihin ja tietoturvaloukkauksiin. Lähtökohtaisesti julkisen sektorin työntekijöiltä odotetaan ymmärrystä luottamuksellisen tiedon käsittelystä sekä sen sensitiivisyydestä.

Viranomaisilla ja julkisella sektorilla on vielä erityinen vastuu omasta tietoturvastaan. Lähtökohtaisesti viranomaiset käsittelevät jonkun muun henkilön tai tahon tietoja ja niiden päätymisellä oikeudetta jonkun kolmannen tahon käsiin voi olla isojakin seurauksia. Oikeudetta saatuja tietoja voidaan käyttää esimerkiksi vaikutusvälineenä johonkin tiettyyn henkilöön ja niillä voidaan yrittää saada taloudellista hyötyä.

Julkiseen sektoriin sekä viranomaisiin kohdistuvien verkkohyökkäysten motiivit voivat olla moninaiset. Hyökkäyksen motiiveina voi olla esimerkiksi salassa pidettävän tiedon saaminen ja sen hyväksi käyttäminen jonkun muun valtion hyväksi sekä henkilötietojen saaminen taloudellisen hyödyn saamiseksi. Myös DoS-hyökkäykset viranomaisia kohtaan ovat yleisiä, ja niitä käytetään yleensä kiusantekona ja viranomaisten nöyryyttämisenä.

7.3 Yksityinen sektori

Yksityisellä sektorilla 5G-verkkoa voidaan hyödyntää esimerkiksi maanviljelyssä, tehtaiden edelleen automatisoinnissa sekä palveluiden kohdentamiseen oikea-aikaisesti sekä oikeapaikkaisesti.

Maanviljelyssä maanviljelijät voivat maksimoida omien viljelmiensä tuotannon reaaliaikaisen datan avulla. Datan avulla voidaan kohdistaa esimerkiksi lannoitusta sekä kastelua entistä tarkemmin oikeaan aikaan ja paikkaan. Oikein kohdistetulla ja kontrolloidulla kastelulla voidaan säästää huomattavasti luonnonvaroja sekä ennalta ehkäistä ilmastonmuutosta. Tulevaisuudessa voi olla jopa mahdollista, että 5G-verkossa toimivan lennokin avulla voidaan ohjata automatisoitua traktoria työskentelemään pellolla (CB Insights, 2021).

Tehtaiden edelleen automatisointi IoT-laitteiden avulla parantaa tehtaiden tuottavuutta sekä vähentää hävikkiä sekä päästöjä. IoT-laitteiden tuottama reaaliaikainen data mahdollistaa ennakoivan analyysin tehtaan toiminnoista ja näin tehtaan tuotantoa ja toimintoja voidaan allokoida oikeaan paikkaan. Tehtaassa tuotettujen tuotteiden varastointi sekä kuljetus tulee myös kehittymään.

Nykyaikana suosion saanut verkko-ostaminen tulee myös kehittymään kuluttajaystävällisempään suuntaan. 5G-verkko mahdollistaa esimerkiksi VR/AR-sovitushuoneet, joiden avulla kuluttaja pääsee kokeilemaan vaatteita ilman fyysistä kaupassakäyntiä.

7.3.1 Yksityisen sektorin tietoturva 5G-verkossa

Yksityinen sektori, kuten julkinenkin sektori, on riippuvainen operaattorin käyttöönottamista tietoturvaratkaisuista. Yksityisellä sektorilla korostuu entisestään työntekijöiden koulutus tietoturvaan liittyvissä asioissa.

Yksityisellä sektorilla yritykset vastaavat omasta tietoturvastaan ja sen käyttöönotosta henkilöstön keskuudessa. Yritykset ovat itse vastuussa tietoturvan tasosta ja siitä, miten hallinnoivat omia tietojaan. Yksityisellä sektorilla ei ole samanlaista velvollisuutta noudattaa tietoturvaohjeita kuten operaattoreilla ja julkisella sektorilla. Mikäli yksityisen sektorin toimija laiminlyö omaa tietoturvaansa voi siitä koitua merkittävää mainehaittaa.

Yksityisellä sektorilla voidaan kokea uhkana esimerkiksi yritysvakoilu, joka sekin on siirtynyt enenevissä määrin verkkoon. Verkon kautta tapahtuva yritysvakoilulla voidaan tavoitella kilpailuetua muihin saman alan toimijoihin nähden. 5G-verkossa tapahtuva yritysvakoilu voisi kohdistua esimerkiksi yrityksen käyttöönottamiin IoT-laitteisiin, jotka välittävät yritykselle tärkeää dataa jatkuvasti.

8 Käytännön esimerkkejä hyökkäyksistä 4G- ja 5G-verkoissa

Ihmiset, yhteisöt, yritykset ja jopa itsenäiset valtiot ovat joutuneet sekä joutuvat edelleen verkkohyökkäysten kohteiksi mobiiliverkkoja hyväksikäyttäen. Verkkohyökkäysten motiivit voivat olla moninaiset, niillä voidaan tavoitella esimerkiksi taloudellista hyötyä, kilpailuetua, haittaamiseksi ja häiritsemiseksi, yleisen edun ja turvallisuuden turvaamiseksi sekä infrastruktuurin lamauttamiseksi. Hyökkäyksiä voivat suorittaa erinäiset toimijat kuten viranomaiset, rikollisjärjestöt, hakkerit sekä vieraan vallan toimijat.

4G-verkossa viranomainen voi esimerkiksi kaapata kansalaisen mobiililaitteen IMSI:n käyttämällä IMSI-sieppaajaa. IMSI-sieppausta voitaisiin käyttää esimerkiksi mielenosoituksessa ja sen avulla saataisiin tietoon kaikkien mobiililaitteiden IMSI-tiedot siepparin vaikutusalueelta. Mikäli mobiililaite on sammutettu tai lentokonetilassa, ei mobiililaite ole yhteydessä mihinkään verkkoon ja näin ollen IMSI:ä ei voida siepata. IMSI-kaappaus toteutetaan siten, että viranomainen luo oman valetukiasemaan johon tukiaseman alueella olevat mobiililaitteet pakotetaan liittymään. Näin valetukiasema kerää liittyvistä mobiililaittesta niiden tiedot. Viranomainen voi perustella IMSI-kaappausta esimerkiksi kansallisella turvallisuudella sekä mahdollisten rikosten ennalta ehkäisemisellä. 5G-verkossa tähän on yritetty puuttua siten, että käyttäjän mobiililaite ei lähetä omaa IMSI:ä verkkoon. Laitteen yksilöivä tunniste on ainoastaan operaattorin tiedossa.

IoT-laitteiden lisääntymisen myötä, myös hyökkäykset IoT-laitteita kohtaan ovat lisääntyneet. IoT-laitteet toimivat myös mobiiliverkon kautta. IoT-laitteisiin tehtyjen hyökkäyksien motiiveina ovat muun muassa DoS-hyökkäykset, luottamuksellisen tiedon varastaminen sekä IoT-laitteiden käyttäminen kryptovaluuttojen louhintaan. IoT-laitteisiin voidaan kohdistaa mobiiliverkossa aktiivisia sekä passiivisia hyökkäyksiä. Passiivisia hyökkäyskeinoja ovat esimerkiksi lähetetyn datan anastaminen sekä valvonta. Aktiivisia hyökkäyskeinoja ovat esimerkiksi valetukiasemien luonti, DoS-hyökkäykset sekä reititys hyökkäykset.

Kuluttajien käyttämät mobiililaitteet altistuvat myös verkkohyökkäyksille. Mobiililaitteen suojaustaso riippuu paljon kuluttajasta itsestään ja nykyään mobiililaitteet pitävät sisällään paljon henkilökohtaista tietoa, aina paikkatiedoista pankkikortin tietoihin. Rikollisilla on yleensä taloudelliset motiivit mobiililaitteen sisältämien tietojen anastamiseen. Mobiililaitteisiin voidaan hyökätä esimerkiksi suojaamattomien Wi-Fi-verkkojen sekä haitalisten sovellusten kautta. Hyökkääjä voi myös luoda täysin tekaistun verkon johon kuluttaja liittyy omalla mobiililaitteella ja näin ollen altistaa oman laitteensa hyökkäykselle. Kuluttajien mobiililaitteisiin voidaan kohdistaa samanlaisia hyökkäysmetodeja kuin IoT-laitteisiin.

Mobiiliverkkojen avulla voidaan myös suorittaa hybridisodankäyntiä. Hybridisodassa vieraan vallan toimija pyrkii vaikuttamaan toisen valtion tärkeisiin toimintoihin kuten sairaaloihin, sähköverkkoihin sekä teollisiin tuotantolaitoksiin. Hybridisodankäynnissä hyökkäyksiä voidaan suorittaa erittäin aggressiivisesti sekä huomaamattomasti. Hybridisodankäynnissä keinovalikoima on laaja ja hyökkääjän resurssit ovat huomattavasti mittavammat kuin muilla. Hyökkäyskeinoina voi olla esimerkiksi fyysiset hyökkäykset tukiasemia kohtaan, omien valetukiasemien perustaminen sekä omien WiFi-verkkojen luominen.

9 Päätelmä

Tätä työtä lähdettiin tekemään sen takia, että saadaan selvitettyä 4G- ja 5G-verkkojen tietoturvaan kohdistuvia erovaisuuksia yhteiskunnan eri osa-alueiden näkökulmista. Halusin selvittää sen, onko uuden sukupolven tietoverkolla kuinka paljon annettavaa tulevaisuudessa ja miten se vaikuttaa yhteiskuntamme toimintoihin aina viranomaisista kuluttajiin. Parantuuko käyttämiemme laitteiden tietoturva, ja tuleeko mobiiliverkkojen käytöstä vieläkin turvallisempaa.

9.1 Päätulokset

9.1.1 5G-verkko ja yhteiskunta

5G-verkon oletetaan parantavan käyttäjien käyttökokemuksia huomattavasti mobiiliverkosta. 5G-verkko tulee tarjoamaan nopeampia yhteyksiä pienemmällä viiveellä ja se toimii eri taajuuksilla kuin 4G-verkko. 5G-verkko tarjoaa parempaa kapasiteettia liikenteelle sekä verkkoa voidaan priorisoida tärkeille toiminnoille viipaloinnilla. Verkon viipalointi sekä verkon kapasiteetti tulevat olemaan avainasemassa mobiiliverkossa, joka pitää sisällään miljardeja eri laitteita.

5G-verkon tarkoituksena on luoda lukemattomia uusia mahdollisuuksia yhteiskunnassa, eikä kaikkia 5G-verkon käyttösovelluksia pystytä vielä edes hahmottamaan. Vain aika tulee näyttämään mitä kaikkea 5G-verkko mahdollistaa. Teoreettisesti 5G-verkko voi säästää luonnonvaroja, ennalta ehkäistä ilmastonmuutosta, saattaa terveydenhuollon ihmisten saataville paikkoihin missä sitä ei ole ollut, mahdollistaa entistä tehokkaamman tuotannon, tuoda uusia liiketoimintamalleja yrityksille, mahdollistaa viranomaisten työturvallisen toiminnan

9.1.2 5G-verkko ja tietoturva

Tietoturvan osalta 5G-verkko tulee olemaan turvallisempi kuin 4G-verkko, mutta 5G-verkossa on omat tietoturvauhkansa. 5G-verkossa tulee olemaan paljon enemmän liikennettä kuin 4G-verkossa ja näin ollen verkossa on enemmän reitityspisteitä. Reitityspisteiden valvonnalla voidaan estää tietoturvaloukkauksia, mutta tämä on käytännössä mahdotonta liikenteen volyymin vuoksi. Valvomattomat reitityspisteet altistavat myös verkon muita osia hyökkäyksille. Operaattorien vastuut sekä operaattorien käyttöönottamat turvallisuustoimet merkitsevät erittäin paljon 5G-verkon tietoturvallisuudessa.

IoT-laitteiden lisääntyvä määrä lisää myös riskiä verkkohyökkäyksille 5G-verkossa. Kaikki valmistajat eivät kiinnitä huomiota IoT-laitteiden tietoturvaan ja näiden laitteiden lisääntyminen verkossa tulee altistamaan verkon hyökkäyksille IoT-laitteiden kautta. Miljardit

uudet laitteet verkossa, kuten televisiot, jääkaapit, älylukot ja vaikkapa akvaariot luovat uusia hyökkäyspisteitä 5G-verkkoon. Näiden kaikkien hyökkäyspisteiden reaaliaikainen valvonta tulee olemaan haastavaa, jollei mahdotontakin.

5G-verkkoon liityttäessä salausprosessi on vajavainen. Kun liitytään verkkoon laite ilmoittaa esimerkiksi käyttöjärjestelmän sekä laitteen tyypin. Tämän avulla voidaan kohdistaa hyökkäyksiä juuri näihin tiettyihin laitteisiin.

Verkko-operaattoreiden suorittama 5G-verkon virtualisointi altistaa myös verkon hyökkäyksille. Verkko-operaattorit joutuvat luottamaan verkon toiminnoissa kolmanteen osapuoleen, kuten pilvipalveluiden tarjoajiin, ja kolmannen osapuolen tarjoamat tietoturvaratkaisut eivät ole operaattorin käsissä.

5G-verkon tuomat tietoturvaparannukset vaativat entistä enemmän hyökkääjältä ja verkkoon kohdistuvat suorat hyökkäykset on tehty vaikeammiksi. 5G-verkossa oleviin mobiililaitteisiin kohdistuvat hyökkäykset ovat edelleen viime kädessä käyttäjän oman tietämyksen ja osaamisen varassa. Tavallisen käyttäjän näkökulmasta omilla tietoturvaratkaisuilla vaikutetaan eniten 5G-verkon tietoturvalliseen käyttöön.

9.2 Tulosten luotettavuus

Tähän työhön kerätty aineisto, jonka pohjalta tuloksiin on päädytty, on kerätty tieteellisistä julkaisuista. 5G-verkkoa koskevat julkaisut ovat melko tuoreita, mutta osa 4G-verkkoa koskevista julkaisuista ovat yli 10 vuotta vanhoja. 4G-verkkoa koskevia julkaisuja ei enää muutamaan vuoteen ole tullut samanlaisella tahdilla ja laadulla kuin 10 vuotta sitten. Julkaisut ovat tieteellisesti hyväksyttyjä, joten niiden pitäisi olla luotettavia.

Laadullisessa analyysissa riskinä on se, että uutta analysoitavaa tulee jatkuvasti lisää. 5G-verkkoa koskien uutta informaatiota sekä julkaisuja tulee lähes päivittäin, joten myös tietämys sekä vaatimukset 5G-verkon osalta ovat voineet muuttua tämän työn aikana. Myös operaattoreiden sekä yritysten teknologia kehittyy jatkuvasti, joten tämäkin kehitys voi luoda epätarkkuutta tuloksiin.

Perusperiaatteet 4G- ja 5G-verkon tietoturvasta sekä rakenteesta ovat paikkansa pitäviä.

Tämä työ on tehty hyvin tietopohjaiseksi ja käytännön esimerkkejä on vähän. Työ pitää sisällään paljon informaatiota 4G- ja 5G-verkosta, mutta verkkojen toimintojen, tietoturvan sekä mahdollisuuksien avaaminen asiasta perehtymättömälle voi olla haastavaa. Yksi syy esimerkkien puuttumiseen on se, että 5G-verkkoa koskevia oikean elämän

tapausesimerkkejä ei ole kauheasti saatavilla. Esimerkkien puute taas johtuu siitä, että 5G-verkkoa ei ole otettu käyttöön vielä laajalla skaalalla.

9.3 Jatkokehitys

Työtä voisi edelleen jatkaa keräämällä päivitettyjä esimerkkejä 5G-verkon käyttöönotosta maailmalla ja sen luomista mahdollisuuksista sekä ongelmista. Myös 5G-verkkoa koskevan informaation edelleen kerääminen voisi tuoda työlle lisää sisältöä, niin verkon tarjoamien mahdollisuuksien, toimintojen kuin tietoturvankin osalta.

Muutaman vuoden päästä olisi mielenkiintoista tarkastella tätä työtä ja verrata sitä siihen, miten ja millä osa-alueilla 5G-verkko on otettu käyttöön yhteiskunnassa. Myös 5G-verkon laajempi käyttöönotto luo mahdollisuuden analysoida ja tutkia 5G-verkon tietoturvariskejä sekä -ratkaisuja syvemmin.

Koen, että tätä työtä voisi käyttää pohjana tulevaisuudessa tutkittaessa 5G-verkon käyttöönottoa ja sen onnistumista yhteiskunnassa.

9.4 Opinnäytetyöprosessi

Alun perin opinnäytetyöni piti käsitellä 4G- ja 5G-verkkojen eroja täysin viranomaisnäkökulmasta. Tavoitteenani oli selvittää, minkälaisia tietoturvaeroja taikka tietoturvauhkia liittyy siihen, kun viranomainen liikkuvassa tilanteessa siirtyy 4G-verkon alueelta 5G-verkon alueelle ja toisinpäin.

Alkuperäistä aihetta piti käsitellä asiantuntijahaastatteluin, mutta asiantuntijoiden saaminen haastatteluihin osoittautui haastavaksi. Sain yhteystiedot muutamasta asiantuntijaorganisaatiosta, mutta yhteydenotot eivät johtaneet ikinä haastatteluihin asti.

Päädyin vaihtamaan aiheeni 4G- ja 5G-verkkojen vertailuun ja yhteiskunnalliseen merkitykseen siinä vaiheessa, kun olin jo koostanut perustiedon alkuperäistä opinnäytetyötä varten. Lähdin siis alun perin työstämään alkuperäistä ideaani, jota varten kasasin pohjatietoja, mutta haastattelujen mahdottomuuden vuoksi, päädyin vaihtamaan aihetta. Onneksi sain jalostettua jo tehdystä työstä itselleni lopullisen opinnäytetyöaiheen.

Tämän työn tekeminen ja prosessi itsessään on ollut vaativa ja haastava. Työtä tehdessä on tullut paljon uusia käsitteitä mitä minun on pitänyt sisäistää. Välillä tietojen kerääminen muuttui hyvin tekniseksi, joka sekin oli hieman raskasta sekä vaikeaselkoista kirjoittajalle, joka ei omaa minkäänlaista insinööritaustaa.

Koen, että tämän opinnäytetyön tekeminen on opettanut minulle paljon 5G-verkosta, sen mahdollisuuksista, tietoturvasta sekä tekniikasta.

Yksi työn haasteista oli myös lopullisen aiheen rajaaminen ja käsitteleminen. Aiheena 5G-verkko ja sen tuomat mahdollisuudet ovat erittäin laajat, ja minun piti vain tehdä se ratkaisu, millä laajuudella käsittelen aiheita ja mihin keskityn. Tässä työssä aiheita 5G-verkon mahdollisista käyttösovelluksista käsiteltiin kuitenkin melko suppeasti. 5G-verkon käyttösovelluksista pystyisi tehdä paljon laajemmatkin opinnäytetyöt.

Lähteet

4G LTE-verkon arkkitehtuuri, kuva. 5G-verkon arkkitehtuuri, kuva. Dawood Al-Gburi, O. “General Overview of 4G and 5G with field measurements and performance comparison”, 2021. Luettavissa: https://trepo.tuni.fi/bitstream/handle/10024/125111/AlgburiOmar.pdf?sequence=2. Luettu: 18.9.2021.

5G-verkon tarjoamat sovellusalat, kuva. Nähtävissä: https://5g-ppp.eu/european-commission-additional-news/. Luettu: 13.11.2021

Khan A.H, Qadeer M. A, Ansari J. A ja Waheed S. "4G as a Next Generation Wireless Network”, 2009. Luettavissa: https://ieeexplore.ieee.org/document/5189800. Luettu: 08.06.2021

Hemnani B. ”An Overview of 4G Technology”, 2018. Luettavissa: https://www.irejournals.com/formatedpaper/1700543.pdf. Luettu: 08.06.2021

CB Insights, ”5G & The Future Of Connectivity: 20 Industries The Tech Could Transform”, 2021. Luettavissa: https://www.cbinsights.com/research/5g-technology-disrupting-industries/
Luettu: 16.1.2022

Eri verkkojen taajuudet, kuva. Nokia. Luettavissa: https://www.nokia.com/networks/insights/spectrum-bands-5g-world/. Luettu: 18.9.2021

Holtrup G, Lacube W, David D. P, Mermoud A, Bovet G ja Lenders V. “5G System Security Analysis”, 2021.
Luettavissa: https://arxiv.org/pdf/2108.08700.pdf Luettu: 18.9.2021

Barb G ja Otesteanu M. “4G/5G: A Comparative Study and Overview on What to Expect from 5G”, 2020. Luettavissa: https://ieeexplore.ieee.org/abstract/document/9163402
Luettu: 1.8.2021

Alshouiliy, K ja Agrawal D. P. “Confluence of 4G LTE, 5G, Fog, and Cloud Computing and Understanding Security Issues”, 2021. Luettavissa: https://books.google.fi/books?hl=fi&lr=&id=ch8SEAAAQBAJ&oi=fnd&pg=PA3&ots=TzDswwkoTX&sig=rX7QEDQqPggXC7fviQgUgXsPT-I&redir_esc=y#v=onepage&q&f=false.
Luettu: 08.06.2021

Seddigh N, Nandy B, Makkar R. ja Beaumont J. F. "Security advances and challenges in 4G wireless networks," 2010. Luettavissa: https://ieeexplore.ieee.org/document/5593244 . Luettu: 08.06.2021, 20.7.2021

Jain R. ja Pathania N. “A Short Review on 4G Technology”, 2019. Luettavissa: https://thinkindiaquarterly.org/index.php/think-india/article/view/18162/13141. Luettu: 13.11.2021

Shinde S, Nikam A. ja Joshi S. ”An Overview of 5G Technology”, 2016. Luettavissa: https://d1wqtxts1xzle7.cloudfront.net/54619691/IRJET-V3I4475-with-cover-page-v2.pdf?Expires=1627802758&Signature=NykRJot5subxcHLfzSxHzohO-tyY1xpizi7sp8lBGKEwr-c4Dtmy9LIbNWA00KmMPaJ1XlFTKDCGGmXqzTTMRNOHsx-qyxz-pJM5LH6LFp5oSJPoUEIB6moZkvjfdq3x1Bznp32SFpxAh2WD9u-pu9avnmYPC2Mbcw9JBouU5BMjuPtdYaD6hBADslYpbgYYV0Y7nXB3tmZMri0vORtQ~yrnI0VCxKHZ46DQ2Cn3Y5GxkixAEQdYOBnxUpgqbgCn1v2RwJBHSIde-Dp~gaU543u47TFhD1j83DR8JFbNxFFM4M5RRYcInkxrdCv~~x~suvdmW5DNg-FDx58QGi8IKRVBQ__&Key-Pair-Id=APKAJLOHF5GGSLRBV4ZA
Luettu: 1.8.2021

STL Partners, “10 5G Healthcare use cases transforming digital health”. Luettavissa: https://stlpartners.com/digital_health/10-5g-healthcare-use-cases/
Luettu 19.1.2022

Mattison S.” Overview of 5G requirements and future wireless networks”, 2017. Luettavissa: https://ieeexplore.ieee.org/abstract/document/8094511
Luettu: 1.8.2021

Sharma T, Ritesh K, Chauhan N. ja Agarwal S. ”Analogous Study of 4G and 5G”, 2016. Luettavissa: https://ieeexplore.ieee.org/abstract/document/7724643
Luettu: 1.8.2021

Zhang X, Kunz A. ja Schröder S. ” Overview of 5G Security in 3GPP”, 2017. Luettavissa: https://ieeexplore.ieee.org/abstract/document/8088619
Luettu: 1.8.2021