Ville Paju

Laitteiston tietoturva 5G-verkoissa

Tietotekniikan kandidaatintutkielma

22. toukokuuta 2020

Jyväskylän yliopisto

Informaatioteknologian tiedekunta

Tekijä: Ville Paju

Yhteystiedot: ville.v.paju@student.jyu.fi

Ohjaaja: Tytti Saksa

Työn nimi: Laitteiston tietoturva 5G-verkoissa

Title in English: Hardware security in 5G networks

Työ: Kandidaatintutkielma

Opintosuunta: Informaatioteknologia

Sivumäärä: 15+0

Tiivistelmä: Tässä tutkimuksessa verrataan 5G-yhteyksien tietoturvaomi-naisuuksia jo olemassaolevien langattomien tiedonsiirtoteknologioiden kanssa, sekä tarkastel-laan 5G-yhteyksien ominaisuuksien myötä ilmeneviä tietoturvaan liittyviä seikkoja.

Avainsanat: esineiden internet, IoT, 5G, tietoturva

Abstract: This thesis compares the data security properties of 5G connections with pre-existing wireless data transfer technologies, and inspects information security related as-pectsthat come along with the new properties of 5G connections.

Keywords: Internet of Things, IoT, 5G, data security

Termiluettelo

3GPP	3rd Generation Partnership Project, mobiilitiedonsiirtoteknologioiden standardointiprojekti
D2D	Device-to-Device, eli suora tukiasematon laitteidenvälinen yhteys
eMBB	Enhanced mobile broadband, nopeaan ja tehokkaaseen tiedonsiirtoon keskittyvä 5G-käyttötapauskategoria
IoT	Esineiden internet, nimitys internetin välityksellä kommunikoivalle laitteistojärjestelmälle
LPWAN	Low-powered wide-area network, eli langaton laaja-alainen verkko pienten datamäärien siirtämiseen
mMTC	Massive machine type communications, 5G-käyttötapauskategoria joka keskittyy tehokkaaseen laitteiden väliseen viestintään
SDN	Software-defined networking, eli ohjelmallisesti määritetty verkko on menetelmä verkon hallinnan ja datan eriyttämiseen joustavuuden lisäämiseksi
URLLC	Ultra-reliable critical communication services, luotettaviin ja nopeisiin laitteiden välisiin yhteyksiin keskittyvä 5G-käyttötapauskategoria

Kuviot

Sisältö

1 Johdanto

Uusien tiedonsiirtoteknologioiden käyttöön siirtymisessä eräs tärkeimmistä huomioitavista seikoista on tietoturva. Seuraavan sukupolven yhteyksien odotetaan olevan aiempia parempia ja rakenteellisesti erilaisia, joten uusien ominaisuuksien tuomat haasteet ovat suuressa osassa tietoturvan kannalta. Eräs huomattavimmista 5G-yhteyksille suunnitelluista ominaisuuksista on täysi tuki esineiden internetille (Internet of Things, lyh. IoT). Tässä tutkimuksessa tarkastellaan 5G-teknologioiden tietoturvaominaisuuksia ja turvallisen tiedonsiirron vaatimuksia esineiden internetin laitteistokeskeisen rakenteen kannalta.

Tutkimuksessa selvitetään aluksi esineiden internetin mahdollisuuksia (luku 2) ja mitä uusien teknologioiden käyttöön siirtyminen vaatii teknisesti tietoturvan kannalta erilaisissa IoT-käyttötapauksissa (luku 3), minkä jälkeen perehdytään uuden verkkoarkkitehtuurin mahdollisiin turvatoimiin yleisiä tietoturvauhkia vastaan (luku 4).

2 Laitteisto 5G-verkossa

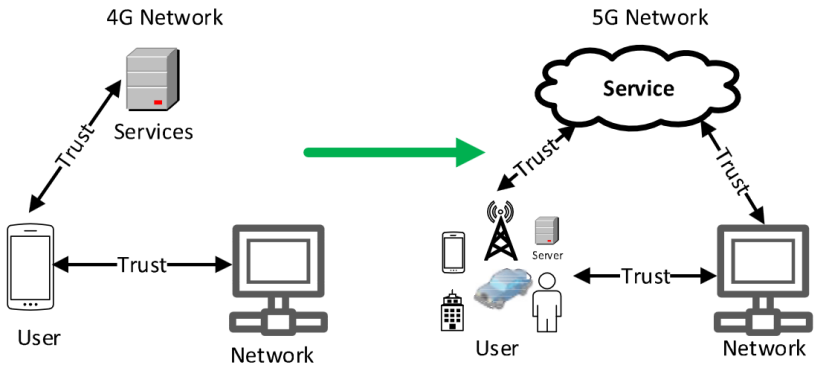
Esineiden internetin laitteiston keskenäinen viestinvaihto tapahtuu yleisesti pieniä alueita kattavien tiedonsiirtoteknologioiden, kuten langattoman lähiverkon tai Bluetoothin, tai pienitehoisten LPWAN-verkkojen (low-power wide-area network) välityksellä (Cao ym. 2020). Tämänlaiset pieniä datamääriä tehokkaasti siirtävät teknologiat ovat toimivia ratkaisuja sensoreiden kaltaisia vähäresurssisia laitteita varten, mutta eivät sovellu käyttökohteisiin, joissa vaaditaan kattavamman datan siirtoa ja minimaalista viivettä.

Eräs suurimmista kehityksen kohteista 5G-teknologioiden suunnittelussa on ollut vastaavanlainen IoT-ympäristöä tukeva arkkitehtuuri. 5G-verkkojen odotetaan tukevan turvallista laitteidenvälistä kommunikointia myös ilman erillistä tukiasemaa laitteiden välillä joustavan ja ketterän tiedonsiirron vuoksi, mikä on olennaista esimerkiksi itseohjautuvien autojen kannalta (Hussain, Hussain ja Zeadally 2019). 5G-teknologioiden mahdollistamassa virtuaaliverkossa laitteiden hallinta on edeltäviä teknologioita tehokkaampaa nopeampien yhteyksien vuoksi. Pienempi viive tiedonsiirrossa mahdollistaa suurempien datamäärien siirron ja tehostaa laitteiden hallintaa. Tehokas laitteiston hallinta on erityisen olennaista esimerkiksi ajoneuvojen hallinnassa ja IoT-laitteiden lääketieteellisessä käytössä. (Hussain, Hussain ja Zeadally 2019)

5G-teknologian kehityksessä on huomioitava esineiden internetin laajamittaisuus niin IoT-laitekokonaisuuksien yleistymisen kuin lukuisten käyttötapausmahdollisuuksienkin vuoksi. Useat skenaariot ja lukuiset mahdolliset tietoturvariskit vaativat kattavaa tutkimusta tietoturvan kannalta luotettavan ja tehokkaan IoT-laitteiston käyttöönottoa varten. (Ji ym. 2018)

3 5G-teknologian tietoturvavaatimukset

Mobiilitiedonsiirtoteknologiat on perinteisesti kehitetty edeltävien sukupolvien yhteyksien pohjalta, joten 5G-yhteyksiä kehitettäessä on otettava huomioon 4G-teknologioiden tietoturvarajoitteet ja -ominaisuudet. 5G-teknologioita suunnitellaan käytettävän laajamittaisemmin kuin 4G-yhteyksiä, joten ne poikkeavat edeltäjästään sekä käsitteellisesti että rakenteellisesti, minkä vuoksi tietoturvavaatimusten määrittäminen eri osa-alueilla on tärkeää. Mobiilitiedonsiirtoteknologioiden standardoinnista vastaa 3GPP-projekti (3rd Generation Partnership Project), joka koostuu seitsemästä erillisestä standardointiorganisaatiosta (3GPP 2020).



Kuvio 1. 4G- ja 5G-verkkojen luottamusmallit (Fang, Qian ja Hu 2017)

4G-yhteyksien luottamusmalli perustuu luotettuun yhteyteen käyttäjän ja verkon välillä, jättäen suojatun yhteyden muodostamisen palveluun käyttäjäosapuolen hoidettavaksi . Erona tähän, 5G-teknologia pyrkii sisällyttämään kaikki osapuolet järjestelmään muodostamalla autentikoidun yhteyden jokaisen välille hyödyntäen verkon paloittelua (network slicing) (Hussain, Hussain ja Zeadally 2019). Verkon paloittelulla tarkoitetaan verkon jakamista erillisiin solmuihin, joista jokaista pystytään hallita ja optimoida dynaamisesti. Verkon jakaminen osiin mahdollistaa virtuaaliverkkojen käytön verkkoarkkitehtuurissa ja on näin ollen 5G-verkkojen luottamusmallin oleellisimpia ominaisuuksia. Uuden luottamusmallin ja verkon virtualisoinnin etuna on tehokkaampi identiteetinhallinta palveluntarjoajien ja verkon välillä. Useiden molemminpuolisten yhteyksien muodostaminen vaatii kuitenkin erinäisten tietoturvaseikkojen huomiointia, kuten yhteyksien autentikointi ja saatavuus. (Zhang, Wang ja Zhou 2019)

3.1 Esineiden internet

5G-teknologian uudenlainen luottamusmalli on erityisen tärkeä esineiden internetin kannalta, sillä IoT-laitteiston tulee pystyä kommunikoimaan turvallisesti internetin välityksellä käyttäjäsovelluksen kanssa. Esineiden internetin laajojen sovellusmahdollisuuksien vuoksi myös tietoturvavaatimukset ovat laajat, joten 5G-yhteyksissä tulee käyttää oikeanlaisia suojausmekanismeja erilaisissa tilanteissa, jotka voidaan yleisesti jakaa kolmeen eri kategoriaan: parannettu mobiililaajakaista (Enhanced mobile broadband, lyh. eMBB), massiivinen konetyyppinen viestintä (Massive machine type communications, lyh. mMTC) ja erittäin luotettavat kriittiset viestintäpalvelut (Ultra-reliable critical communication services, lyh. URLCC) (Zhang, Wang ja Zhou 2019).

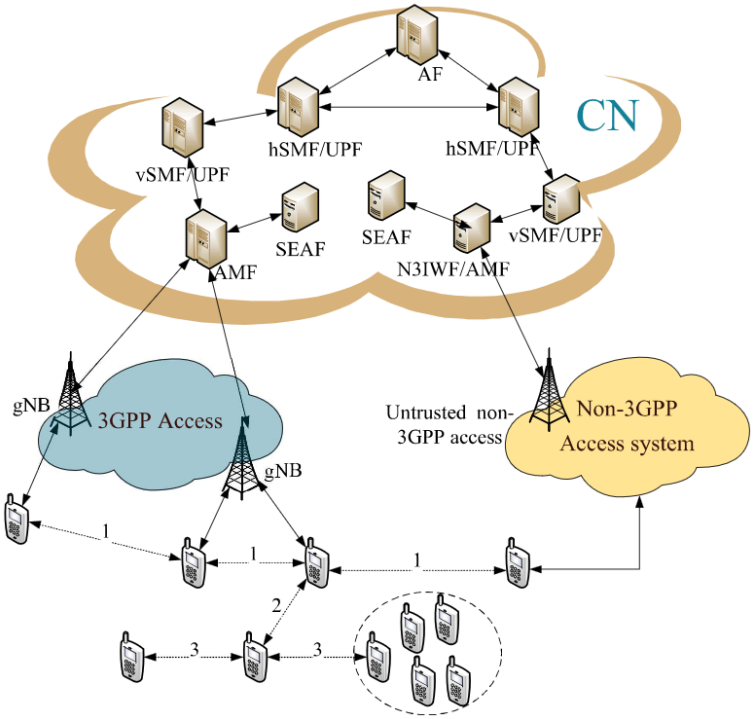
Sovellukset, jotka vaativat yhteyksiltä suurta kaistanleveyttä ja keskittyvät pääasiassa käyttäjäkokemukseen, luokitellaan eMBB-sovelluksiksi. Esimerkiksi suoratoistopalvelut ja virtuaalitodellisuussovellukset kuuluvat tähän kategoriaan. Tietoturvavaatimukset määräytyvät näissä tapauksissa yksilöllisesti yritysten omien säädösten mukaan. mMTC-laitteet pyrkivät olemaan energia- ja kustannustehokkaita suunnittelussaan, minkä vuoksi myös niiden tietoturvaprotokollien ja -algoritmien on oltava kevyitä. Tietoturvavaatimukset mMTC-laitteissa voivat vaihdella suuresti, sillä esimerkiksi terveydentilaa mittaavan sensorin dataa voidaan pitää lämpömittarin dataa arkaluonteisempana. URLLC-käyttötapauksissa keskitytään yhteyden viiveen minimoimiseen ja korkeaan turvatasoon. Tämän kategorian vaatiman reaaliaikaisuuden vuoksi myös tietoturva-algoritmien on kyettävä suojaamaan yhteydet ja laitteet aiheuttamatta ylimääräistä viivettä (Ji ym. 2018).

3.2 D2D-yhteydet

5G-teknologia mahdollistaa myös suorat laitteidenväliset yhteydet (Device-to-Device, lyh. D2D), joiden ensisijaisena etuna on verkon tukiaseman (Base station, lyh. BS) kuormituksen vähentäminen sekä viiveen vähentäminen tiedonsiirrossa. (Cao ym. 2020) Suorien yhteyksien suurimpana heikkoutena on niiden epävarmuus turvallisuuden kannalta, koska esimerkiksi yhteyden eheyden ja autentikoinnin varmistaminen on hankalaa ilman tukiasemaa.

D2D-yhteyksien turvallisen käytön takaamiseksi laitteiden tulee löytää toisensa turvallisesti

ja myös ylläpitää yhteyksien turvallisuutta. Yhteyksien aikana on esimerkiksi varmistuttava siitä ettei ulkopuolinen hyökkääjä pääse imitoimaan laitetta tai laiteryhmän jäsentä, eikä esimerkiksi salakuuntelemaan tiedonsiirtoa. (Cao ym. 2020) Avaintenhallintaa varten D2D-laiteryhmissä tulee varmistaa ettei aiemmin ryhmässä ollut laite pääse käsiksi uusiin avaimiin eikä uusien ryhmään liittyvien laitteiden tule päästä käsiksi vanhoihin avaimiin. Lisäksi avainten on oltava ryhmälle uniikkeja, eikä hyökkääjä tai muun ryhmän laite saa pystyä arvaamaan tai saamaan ryhmän keskeistä salaista avainta. (Fang, Qian ja Hu 2017)



Kuvio 2. D2D-yhteyksiä 5G-arkkitehtuurissa (Cao ym. 2020)

4 5G-tietoturvateknologiat

5G-teknologioiden tietoturvateknologiat perustuvat laajalti 4G-yhteyksien kaksipuolisiin salausalgoritmeihin, joita myös pyritään kehittämään entistä monipuolisemman datan suojaamiseksi. 5G-teknologian kehityksessä pyritään paikkaamaan 4G-arkkitehtuurin heikkouksia uudenlaisella rakenteella, sekä suojautumaan uusien teknologioiden tuomilta uhilta. 5G-tietoturvan takaamiseksi kehitteillä on ollut useita ratkaisuja uuden arkkitehtuurin turvaamiseksi, mutta 3GPP:n tietoturvateknologioiden standardisointi on ollut hidasta.

4.1 Autentikointi

Erityyppisten hyökkäyksien estämiseksi 5G-yhteyksiltä odotetaan entistä tehokkaampaa yhteyksien autentikointia. Edeltäjästään poiketen, 5G-yhteydet vaativat autentikoidun yhteyden muodostamisen useamman osapuolen kanssa, kuitenkin pyrkien pitämään yhteyksien viiveen mahdollisimman pienenä. Eräs mahdollisuus nopean autentikoinnin toteuttamiseksi on hyödyntää ohjelmallisesti määritetyn verkon (Software-defined networking, SDN) etuja käyttämällä laitteiston fyysisen tason attribuutteja tunnisteina verkkosolmujen yhteyksien autentikoinnin yhteydessä. Näin ulkopuolisen hyökkääjään on vaikeampi päästä käsiksi yhteyksiin kun autentikoitu yhteys muodostetaan laitekohtaisten ominaisuuksien avulla digitaalisen salauksen sijaan (Fang, Qian ja Hu 2017).

Erityisesti IoT-laitteiston autentikointia varten on kehitetty teknologioita, jotka perustuvat laitteiden yhdistämiseen verkossa niin että yksi verkon komponentti vastaa jokaisen laitteryhmän laitteen yhteyksien autentikoinnista. Vielä toistaiseksi ei kuitenkaan ole olemassa 3GPP:n standardisoimaa 5G-arkkitehtuuria IoT-laitteiden monimuotoisille käyttötapauksille. (Cao ym. 2020).

Suorien D2D-laiteyhteyksien tietoturvaominaisuudet ovat vielä kehitysvaiheessa, mutta autentikointi tällaisissa yhteyksissä voidaan suorittaa esimerkiksi vertaamalla datakuvioita. Käytännössä tässä ratkaisussa laitteet vertailevat lähetettyjä ja vastaanotettujen pakettien dataa autentikointikeinona, ja paketteihin voidaan myös lisätä ylimääräisiä bittijonoja hyökkäysten tunnistamiseksi. (Fang, Qian ja Hu 2017) Tämä ei kuitenkaan ole täydellinen ratkaisu,

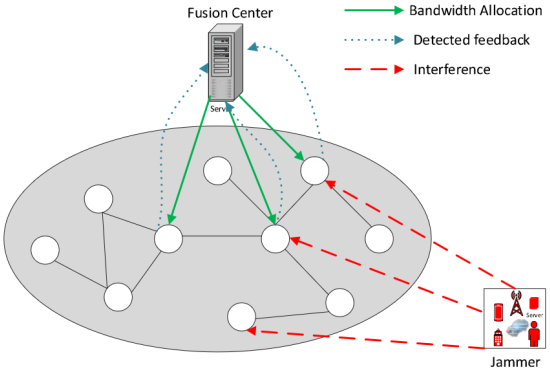
sillä vaikka autentikoitu yhteys saadaankin muodostettua, identiteettien yksityisyyttä ei voida taata. D2D-yhteyksien autentikointialgoritmit saattavat myös vaatia paljon laskentatehoa laitteilta, hidastaen näin yhteyksien muodostamista. (Cao ym. 2020)

4.2 Yhteyden eheys

5G-teknologian lukuisten käyttöalueiden vuoksi on tärkeää että yhteydet ovat luottamuksellisia, eli että valtuuttamattomat tahot eivät pääse yhteyksiin käsiksi ja että viesti ei pääse muuttumaan tai katoamaan tiedonsiirron aikana. Yhteyksien turvaamiseksi on kehitelty useita erityyppisiä menetelmiä eri tilanteiden mukaan, mutta yleisesti ottaen yhteyksien salausmekanismit kykenevät pitämään viestin koskemattomana sen lähetyksen ajan (Zhang, Wang ja Zhou 2019) eMBB-tyyppisissä käyttötapauksissa. Nykypäivän salausalgoritmit ovat kuitenkin usein melko hitaita ja käyttävät helposti paljon resursseja, mikä on ongelmallista etenkin IoT-laitteiden suhteen. Tämän vuoksi kehitteillä on ollut laitteiden identiteettiin perustuvia kevytrakenteisia salausjärjestelmiä vastaavanlaisia käyttötapauksia varten (Zhang, Wang ja Zhou 2019).

4.3 Saatavuus

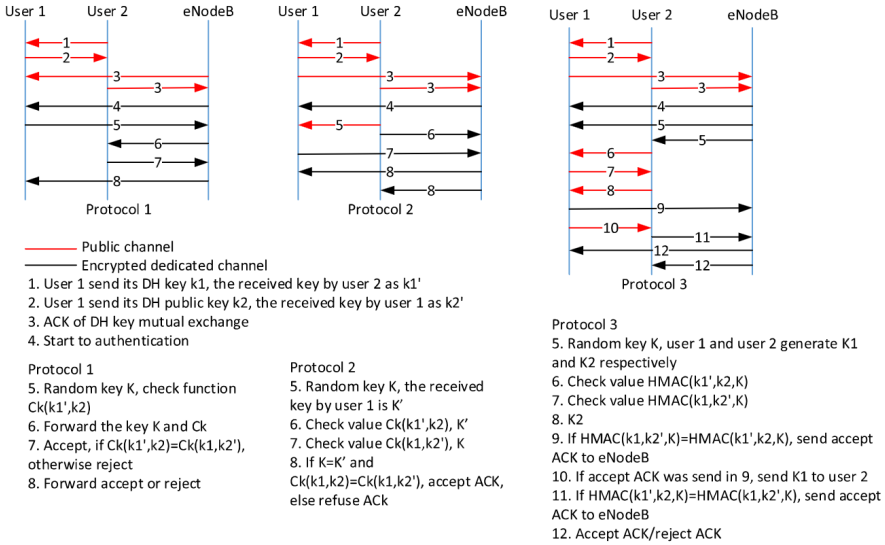
5G-yhteyksien halutunlaisen toimivuuden takaamiseksi on varmistuttava siitä että ne ovat luotettavasti saatavilla kaikkina aikoina, joten niiden tulee pystyä arkkitehtuurisesti välttymään esimerkiksi palvelunestohyökkäyksiltä. Yleisesti ottaen hyökkäysten torjunta on toteutettava hajautetun verkon solmuissa, joiden resursseja voidaan tarvittaessa jakaa verkon muille solmuille. Eräs ehdotettu turvatoimi resursseja kuluttavia hyökkäyksiä vastaan on ottaa käyttöön järjestelmä, joka vaihtelee datan siirtoaikoja sekä lähetyskanavia satunnaisesti estäen siten hyökkääjän häirintämahdollisuudet(Fang, Qian ja Hu 2017). Kyseinen turvatoimi on erityisen lupaava D2D-yhteyksien kannalta sen suorituskyvyn ja näiden yhteyksien kevyiden yhteyksien vuoksi. Laitteet kuitenkin tarvitsevat ensin yhteisen avaimen toimiakseen keskenään. (Fang, Qian ja Hu 2017)



Kuvio 3. Verkon resurssien jakaminen verkkosolmuihin palvelunestohyökkäysten torjumiseksi (Fang, Qian ja Hu 2017)

4.4 Avaintenhallinta

Avaintenhallinnalla tarkoitetaan salaisen avaimen jakamista ja käsittelyä yhdistettyjen laitteiden välillä yhteyksien jatkuvan autentikoidun ja turvallisen yhteyksien ylläpitämiseksi. Mobiiliverkoissa avaimia jaettaessa on usein huomioitava laitteiden attribuutteja erilaisten turvallisten hallintaratkaisujen vuoksi. Monet näistä ratkaisuista ovat hierarkkisia laiteryhmiä, joista ylin on vastuussa avaimen jakamisesta muille laiteryhmän jäsenille. (Zhang, Wang ja Zhou 2019)



Kuvio 4. Erilaisia avaintenhallintajärjestelmiä (Fang, Qian ja Hu 2017)

5 Yhteenveto

5G-yhteyksien tietoturva on edellisten sukupolvien mobiilitiedonsiirtoteknologioiden tapaan paranneltu versio edellisestä. Useiden käyttötapausten, uusien ominaisuuksien ja erilaisen verkkoarkkitehtuurin vuoksi 5G-yhteydet vaativat uudenlaisia ratkaisuja tietoturvaongelmiin, minkä vuoksi onkin todennäköistä että 5G-yhteyksien luottamusmallit tulevat mukautumaan eri käyttötapausten mukaisesti. Esimerkiksi URLLC-tyyppisten käyttökohteiden suojausalgoritmit ovat jatkuvasti kehityksen kohteena mahdollisimman tehokkaan toiminnan takaamiseksi ja edeltävän sukupolven teknologioita kattavamman datan siirtämisen turvaamiseksi. Erityisesti D2D-yhteydet vaativat vielä jatkotutkimusta ja -suunnittelua turvallisen kommunikoinnin takaamiseksi. Useista esitetyistä ratkaisuista huolimatta toistaiseksi ei ole löydetty ratkaisua joka olisi sekä tehokas että suojaisi suorat laitteidenväliset yhteydet tarpeeksi hyvin. Lisäksi IoT-ympäristössä D2D-teknologioiden tietoturva vaatii lisäsuunnittelua vähäisten resurssien vuoksi. Näiden seikkojen ja esineiden internetin monimuotoisuuden vuoksi D2D-yhteyksien standardointi on ollut melko hidasta ja useat käytännön seikat, kuten käyttäjän yksityisyydenturva, ovat vielä kehitteillä.

Tässä tutkielmassa tietoturvaa tarkastellaan melko pintapuolisesti, eikä esimerkiksi algoritmeja tai niiden toimintaa eritellä perusteellisesti. Toisaalta teknologioiden standardisoinnin puutteen vuoksi algoritmien erittely lienee liian aikaista tässä vaiheessa eikä siksi vielä ole tarpeellista.

Lähteet

3GPP. 2020. “3GPP”. Viitattu 30. huhtikuuta 2020. https://www.3gpp.org/.

Cao, J., M. Ma, H. Li, R. Ma, Y. Sun, P. Yu ja L. Xiong. 2020. “A survey on security aspects for 3GPP 5G networks”. Cited By 0, *IEEE Communications Surveys and Tutorials* 22 (1): 170–195. doi:10.1109/COMST.2019.2951818.

Fang, D., Y. Qian ja R.Q. Hu. 2017. “Security for 5G Mobile Wireless Networks”. Cited By 40, *IEEE Access* 6:4850–4874. doi:10.1109/ACCESS.2017.2779146.

Hussain, R., F. Hussain ja S. Zeadally. 2019. “Integration of VANET and 5G Security: A review of design and implementation issues”. Cited By 3, *Future Generation Computer Systems* 101:843–864. doi:10.1016/j.future.2019.07.006.

Ji, X., K. Huang, L. Jin, H. Tang, C. Liu, Z. Zhong, W. You ym. 2018. “Overview of 5G security technology”. Cited By 14, *Science China Information Sciences* 61 (8). doi:10.1007/s11432-017-9426-4.

Zhang, S., Y. Wang ja W. Zhou. 2019. “Towards secure 5G networks: A Survey”. Cited By 1, *Computer Networks* 162. doi:10.1016/j.comnet.2019.106871.