Zaštita sigurnosti i privatnosti u okruženju 5G mobilnih mreža

Miletić, Dorian

SVEUČILIŠTE JOSIPA JURJA STROSSMAYERA U OSIJEKU
FAKULTET ELEKTROTEHNIKE, RAČUNARSTVA I INFORMACIJSKIH TEHNOLOGIJA OSIJEK

Sveučilišni studij

ZAŠTITA SIGURNOSTI I PRIVATNOSTI U OKRUŽENJU 5G MOBILNIH MREŽA

Završni rad

Dorian Miletić

Osijek, 2024.

FERIT
FAKULTET ELEKTROTEHNIKE, RAČUNARSTVA I INFORMACIJSKIH TEHNOLOGIJA **OSIJEK**

Obrazac Z1P: Obrazac za ocjenu završnog rada na sveučilišnom prijediplomskom studiju

Ocjena završnog rada na sveučilišnom prijediplomskom studiju

Ime i prezime pristupnika:	Dorian Miletić
Studij, smjer:	Sveučilišni prijediplomski studij Računarstvo
Mat. br. pristupnika, god.	R 4403, 13.10.2021.
JMBAG:	0165082232
Mentor:	prof. dr. sc. Krešimir Grgić
Sumentor:	
Sumentor iz tvrtke:	
Naslov završnog rada:	Zaštita sigurnosti i privatnosti u okruženju 5G mobilnih mreža
Znanstvena grana završnog rada:	**Telekomunikacije i informatika (zn. polje elektrotehnika)**
Zadatak završnog rada:	Mobilna 5G mreža postala je temeljna infrastruktura za brojne primjene i usluge. Kao takva, nužno mora pružiti sigurnost i privatnost korisnicima, unatoč izloženosti različitim kibernetičkim prijetnjama. Potrebno je sustavno istražiti i analizirati sigurnosne izazove, rizike i prijetnje u 5G mobilnim mrežama. Analizirati moguće protumjere i sigurnosne mehanizme koji se koriste za zaštitu sigurnosti i privatnosti korisnika, te istaknuti smjernice njihovog daljnjeg razvoja. Tema rezervirana za: Dorian Miletić

Datum prijedloga ocjene završnog rada od strane mentora:	18.09.2024.
Prijedlog ocjene završnog rada od strane mentora:	Izvrstan (5)
Datum potvrde ocjene završnog rada od strane Odbora:	25.09.2024.
Ocjena završnog rada nakon obrane:	Izvrstan (5)
Datum potvrde mentora o predaji konačne verzije završnog rada čime je pristupnik završio sveučilišni prijediplomski studij:	26.09.2024.

FERIT
FAKULTET ELEKTROTEHNIKE, RAČUNARSTVA I INFORMACIJSKIH TEHNOLOGIJA **OSIJEK**

IZJAVA O IZVORNOSTI RADA

Osijek, 26.09.2024.

Ime i prezime Pristupnika:	Dorian Miletić
Studij:	Sveučilišni prijediplomski studij Računarstvo
Mat. br. Pristupnika, godina upisa:	R 4403, 13.10.2021.
Turnitin podudaranje [%]:	1

Ovom izjavom izjavljujem da je rad pod nazivom**: Zaštita sigurnosti i privatnosti u okruženju 5G mobilnih mreža**

izrađen pod vodstvom mentora prof. dr. sc. Krešimir Grgić

i sumentora

moj vlastiti rad i prema mom najboljem znanju ne sadrži prethodno objavljene ili neobjavljene pisane materijale drugih osoba, osim onih koji su izričito priznati navođenjem literature i drugih izvora informacija.
Izjavljujem da je intelektualni sadržaj navedenog rada proizvod mog vlastitog rada, osim u onom dijelu za koji mi je bila potrebna pomoć mentora, sumentora i drugih osoba, a što je izričito navedeno u radu.

Potpis pristupnika:

SADRŽAJ

1. UVOD 1

1.1. Zadatak završnog rada 1

2. 5G MOBILNA MREŽA 2

2.1. Prethodne generacije mobilnih mreža 2

2.1.1. 1G mobilna mreža 2

2.1.2. 2G mobilna mreža 3

2.1.3. 3G mobilna mreža 3

2.1.4. 4G mobilna mreža 3

2.2. Arhitektura 5G mobilnih mreža 4

2.3. Internet Stvari (IoT) 5

3. SIGURNOSNE PRIJETNJE U 5G MREŽAMA 6

3.1. Korisnička oprema 6

3.1.1. Mobilni malware napadi na korisničku opremu 6

3.1.2. 5G Mobilni Botnetovi (eng. 5G Mobile Botnets) 7

3.2. Pristupne mreže 8

3.2.1. Napad na 4G pristupnu mrežu 8

3.2.2. HeNB Femtocell napadi 10

3.3. Jezgra mreže poslužitelja 13

3.3.1. DDoS napad ciljan na jezgru mreže mobilnog operatera 13

3.3.2. DDoS napadi ciljani na vanjske entitete preko jezgre mreže mobilnih operatora 15

3.4. Vanjske IP mreže 15

3.4.1. Ugrožene poduzetničke mreže 15

4. MJERE ZAŠTITE I SIGURNOSNI MEHANIZMI U 5G MREŽAMA 17

4.1. Kriptografski pristup i sigurnost fizičkog sloja 17

4.1.1. Kriptografija simetričnim ključem 17

4.1.2. Kriptografija javnim ključem 17

4.1.3. Sigurnost fizičkog sloja 18

4.2. Autentifikacija 18

4.2.1. Potreba za niskom latencijom 19

4.2.2. Podržavanje D2D komunikacije 20

4.2.3. Visoka efikasnost korištenja propusnosti i energije 20

4.2.4. Ograničene računalne mogućnosti uređaja 21

4.3. Dostupnost **21**

4.4. Povjerljivost podataka **23**

4.5. Upravljanje ključevima **23**

5. PRIVATNOST U 5G MREŽAMA **25**

5.1. Privatnost kod korisnika **25**

5.1.1. Privatnost podataka 25

5.1.2. Privatnost lokacije 25

5.1.3. Privatnost identiteta 26

5.2. Problemi privatnosti u 5G mrežama **26**

5.2.1. End-to-End privatnost podataka 26

5.2.2. Dijeljeno okruženje i gubitak vlasništva osobnih podataka 26

5.2.3. Problemi s različitim ciljevima povjerenja 27

5.2.4. Problem u prekograničnom protoku podataka 27

5.2.5. Problem treće strane u 5G mrežama 27

5.3. Regulatorni ciljevi u zaštiti privatnosti **27**

5.3.1. Promicanje jedinstvenog tržišta i ravnoteže interesa globalno 27

5.3.2. Promoviranje prenosivosti podataka 27

5.3.3. Definiranje propisa privatnosti na globalnom tržištu 28

5.3.4. Promoviranje odgovornosti podataka 28

5.4. Sigurnosni mehanizmi **28**

5.4.1. Anonimnost 28

5.4.2. Nepovezanost 28

5.4.3. Neotkrivenost 29

5.4.4. Neopažljivost 29

5.4.5. Pseudonimnost 29

ZAKLJUČAK **30**

LITERATURA **31**

SAŽETAK **33**

ABSTRACT **33**

1. UVOD

U današnjici Internet je svugdje oko nas. Isto tako gotovo svaki čovjek koristi mobilne uređaje gotovo svakodnevno. Samim time što puno vremena provodimo na Internetu, pogotovo putem mobilnih uređaja, naša sigurnost i privatnost naših podataka se dovodi u upit. Svakom novom generacijom tehnologijom i mreža mijenja se i sam način njihovog funkcioniranja te samim time i način na koji se omogućuje sigurna komunikacija. Mogući sigurnosni napadi i propusti u komunikaciji se zaštićuju raznim sigurnosnim protokolima i načinima same komunikacije. 5G mobilna mreža koja se koristi unazad nekoliko godina nam pruža i donosi nove standardne i načine zaštite podataka koji se dijele putem Interneta te načini pojedinih pristupa će se kasnije razraditi unutar ovog rada. Veliki fokus se mora staviti na zaštitu sigurnosti i privatnosti unutar 5G mobilnih mreža upravo zato što su one mobilne, tj. korisnici stalno mijenjaju svoje vlastito okruženje i samim time šanse za napad na njihovu privatnost i sigurnost se povećavaju jer je puno teže kontrolirati mrežu koja konstantno mijenja svoje točke prijema. 5G mobilna mreža shvaća ozbiljnost zaštite sigurnosti i privatnosti i to pokazuje u svojim raznim primjenama, te je nadogradnja prethodnih generacija mobilnih mreža.

1.1. Zadatak završnog rada

Mobilna 5G mreža postala je temeljna infrastruktura za brojne primjene i usluge. Kao takva, nužno mora pružiti sigurnost i privatnost korisnicima, unatoč izloženosti različitim kibernetičkim prijetnjama. Potrebno je sustavno istražiti i analizirati sigurnosne izazove, rizike i prijetnje u 5G mobilnim mrežama. Analizirati moguće protumjere i sigurnosne mehanizme koji se koriste za zaštitu sigurnosti i privatnosti korisnika, te istaknuti smjernice njihovog daljnjeg razvoja.

2. 5G MOBILNA MREŽA

Peta generacija mobilnih mreža (5G) je nova generacija mobilnih mreža koja omogućuje inovacije i progresivne promjene kroz različite primjene poput pametnih mreža (eng. *Smart Grid*) te kroz sve ciljeve unutar našega društva [1]. Druga definicija je da je 5G mobilna mreža modernija, bolja verzija prethodnih generacija koja koristi veću propusnost (eng. *Bandwidth*), ima veću brzinu i omogućuje puno više mogućnosti za budući razvoj komunikacije kakvu znamo. Najviše se temelji na IPv6 protokolu ali jezgra samog koncepta 5G mobilnih mreža se može staviti u tri tehnologije:

- Nanotehnologija
- Računarstvo u oblaku (eng. *Cloud Computing*)
- Svi uređaji imaju IP adresu (eng. All flat IP platform) [2].

Relativno novonastala tehnologija koja se nadovezuje na prethodne generacije i omogućuje kreiranje novih tehnologija, a jedna od najbitnijih koja je proizašla je Internet stvari (eng. *Internet of Things,* IoT). Osim vrlo velikih brzina, peta generacija nam omogućuje puno veći kapacitet prometa, smanjenu latenciju i sveukupno veći korišteni prostor frekvencija za komunikaciju.

2.1. Prethodne generacije mobilnih mreža

Prije samog razmatranja problema zaštite sigurnosti i privatnosti u 5G mobilnim mrežama važno je spomenuti kako je to izvedeno u prethodnim generacijama te koje sve probleme su uspjeli riješiti i sve one koje nisu.

2.1.1. 1G mobilna mreža

Prva generacija mobilnih mreža se pojavila početkom osamdesetih godina. Arhitektura je bila bazirana na analognim signalima. Korisnik je imao dugme za prijenos i dugme za prekid prijenosa. Tehnologija u to vrijeme nije podržavala istovremeno slušanje prijenosa i sam prijenos pa je šezdesetih uveden novi sistem pod nazivom Poboljšani Mobilni Telefonski Sistem (eng. *Improved Mobile Telephone System*, IMTS). Sada s dva komunikacijska kanala, omogućeno je i prijenos i slušanje istovremeno. Za komunikaciju mreža je koristila 23 kanala u rasponu od 150Mhz do 450Mhz. Glavna svrha je bila podijeliti geografski prostor u ćelije (eng. *Cells*) koji su onda međusobno komunicirali. Sigurnosni problemi kod prve generacije su bili veliki jer se

koristi analogni signali za komunikaciju te je bilo koja osoba s prijemnikom mogla prisluškivati razgovor [2].

2.1.2. 2G mobilna mreža

Druga generacija mobilnih mreža pak koristi digitalni signal za prijenos te se pojavila krajem 1980ih godina. Pruža znatno veći spektar korištenja, omogućuje korištenje SMS (eng. *Short Message Service*) poruka te po prvi puta se u komunikaciji koristi digitalna enkripcija. Sve je to 1991. godine pušteno u komercijalne svrhe na GSM (eng. *The Global System for Mobile Communications,* GSM) standardu [2]. Veće brzine i veći rasponi su standard za svaku od novonastalih generacija pa tako i u drugoj. 2G rješava dosta sigurnosnih problema prve generacije, no prelaskom na digitalni sustav su se pojavili novi sigurnosni problemi. Korištenjem digitalne enkripcije su se većina problema riješila no tijekom vremena i razvojem novih tehnologija, potreba za novim standardima i enkripcijom će biti nužna.

2.1.3. 3G mobilna mreža

Treća generacija koristi IMT-2000 (eng. *International Mobile Telecommunication,* IMT) standard za svoju komunikaciju. Treća generacija pridonosi puno novih inačica za korisnike, poput televizije na samome mobitelu, pristup Internetu, video pozivi i sl. UTMS (eng. *Universal Mobile Telecommunication System*, UMTS) je najbolji primjer korištenja 3G mobilnih mreža, gdje je glavna ideja bila korištenje 3G tehnologije putem cijeloga svijeta i u različite svrhe/ potrebe [2]. Pojavom mobilnog interneta zaštita sigurnosti i privatnosti se postavlja na veliku razinu, zbog puno većeg prometa informacija koji se svakodnevno prenosi. Jedan od najpoznatijih napada koji je i problem u današnjici, poznat kao Distribuirani napadi uskraćivanjem resursa (eng. *Distributed Denial of Service*, DDoS) [3].

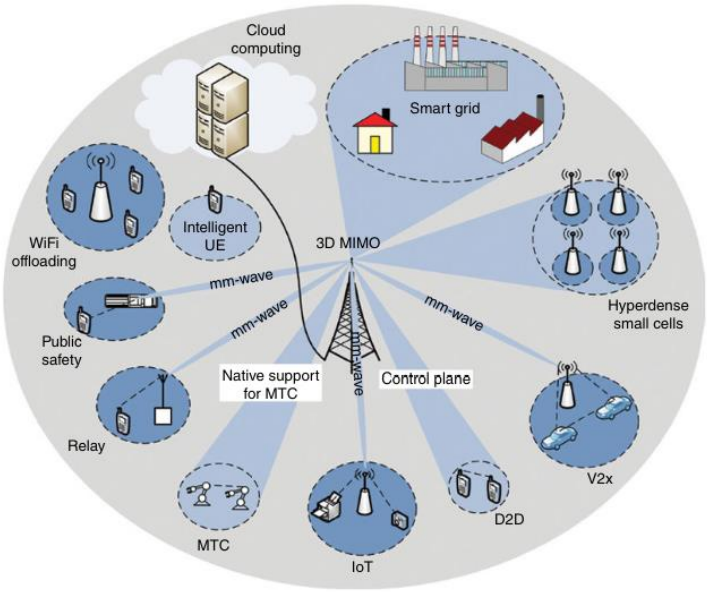
2.1.4. 4G mobilna mreža

Četvrta generacija po prvi put koristi LTE (eng. *Long Term Evolution*, LTE), što je zapravo standard za bežičnu komunikaciju za mobilne uređaje. Ona nam omogućuje mobilni pristup internetu, pozive putem interneta, razne računalne servise, televiziju visoke rezolucije na mobilnom uređaju i još mnogo toga [2]. S sve novijom tehnologijom, i napadi na sigurnost i

privatnost podataka postaju sve kompleksniji, pa isto tako i s ovom generacijom. Pošto 4G ima puno veću propusnost, to znači da možemo slati više podataka, no i napadači to mogu također zlouporabiti. Jedan od napada koji to iskorištava u svoju svrhu je napad na arhitekturu bežične privatne mreže (eng. *Wireless Architecturally Private Newtork Flooding*) [4].

2.2. Arhitektura 5G mobilnih mreža

Rastom novih tehnologija raste i broj korisnika, pa samim time sama arhitektura mreža mora isto tako se razvijati. Jedna analiza od strane Cisco kompanije u 2019. godini je iskazala da broj povezanih uređaja na internetu će porasti od 29 milijarde (aproksimiran za 2022. godinu) do 300 milijardi do 2030. godine. Također broj korisnika koji koriste Internet će se povećati za gotovo 3.5 milijarde [5]. To je značajni skok te mreža mora podržati sve te nove strukture i korisnike ali i novi način povezivanja mreže u pametnu mrežu. Prikaz izgleda arhitekture možemo vidjeti na slici 2.1 :



Slika 2.1 Arhitektura 5G mreže [6]

2.3. Internet Stvari (IoT)

Definicija IoT-a je već po prvi puta korištena 1999. godine kada je britanski znanstvenik Kevin Ashton opisao kao sistem koji objekte u fizičkome svijetu povezuje sa internetom putem senzora. Danas možemo reći da IoT su međusobno povezane mreže i računalna snaga povezano zajedno koje se šire u objekte, senzore i svakodnevne stvari koje normalno ne smatramo računalima i gdje omogućujemo tim stvarima da stvaraju, šalju i koriste podatke uz minimalnu ljudsku intervenciju. No konkretna definicija za IoT ne postoji [6]. Međusobno povezivanje stvari nam pruža puno novih prilika za razvoj novih tehnologija i za unaprjeđenje kvalitete života ali samim time što dodajemo stvari na Internet koje su međusobno povezane, povećavamo rizik od napada na sve te uređaje te komunikaciju između njih.

3. SIGURNOSNE PRIJETNJE U 5G MREŽAMA

Kao i sa svakom od prethodnih generacija, sigurnosne prijetnje su uvijek prisutne. Što se tehnologija više razvija, tako se i paralelno razvijaju metode napada i raznorazne sigurnosne prijetnje. Većina napada su zapravo već viđene u prethodnim generacijama no prisustvom novih resursa i tehnologija, mnogi od napada se ponovno mogu iskoristiti. Neke od napada i meta napada ćemo navesti i pobliže objasniti, no napadi se najčešće dijele u sljedeće kategorije: [7].

1. Korisnička oprema
2. Pristup mreži
3. Jezgra mreže poslužitelja
4. Vanjske IP mreže

3.1. Korisnička oprema

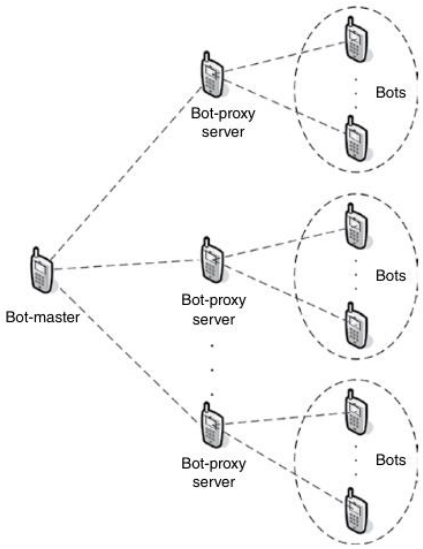
U današnjici, pametni mobiteli i pametni uređaji su svugdje oko nas. Omogućuju nam da povećavamo kvalitetu života sa svojim širokim primjenama. S rastom prometa i s velikim brojem podrške za povezivanje (poput 2G/3G/4G, IEEE 802.11, Bluetooth), raste i broj mogućih ranjivosti za kibernetičke napade. Također napadi zlonamjernih programa (eng. *Malware*) poput virusa i crva su puno lakše izvedivi upravo radi povećanog prometa i povećanog broja uređaja. Otvoreni operacijski sustavi će omogućavati instalaciju programa od povjerenih i ne povjerenih izvora, što puno aplikacija poput video igrica će moći zloupotrijebiti. Mobilni *malware* može biti dizajniran da omogući napadačima pristup osobnim podacima korisnika ili pak napad na druge uređaje (poput DDoS napada), što onda predstavlja prijetnju za sam uređaj i korisnika ali i prijetnju za cijelu 5G mobilnu mrežu koju koriste [7].

3.1.1. Mobilni malware napadi na korisničku opremu

U budućnosti korištenje korisničke opreme će biti kao osobni uređaj koji će pohranjivati sve od kontakata do informacija o bankarstvu. Korisnik će uređaj imati pored sebe gotovo uvijek te će zapravo predstavljati njegov identitet. To čini osobni uređaj savršenu metu za napad jer ako napadač dobije pristup uređaju, praktički ima cijeli identitet korisnika. Napadač instaliranjem malicioznog softwarea na krajnji uređaj korisnika mu može omogućiti pristup cijelom uređaju, ali i također daje pristup hardwareu uređaja gdje napadač može računsku moć uređaja koristiti za bespotrebno trošenje energije ili pak može koristiti uređaj za napad na ostale korisnike. Napad mobilnih botova upravo koristi tu mogućnost kako bi automatizirao napad za financijsku dobit, gdje upravo prednosti 5G mobilne mreže to omogućuju [7].

3.1.2. 5G Mobilni Botnetovi (eng. 5G Mobile Botnets)

U 5G komunikacijskom okruženju, mobilni *botnetovi* su u porastu korištenja, jer su mobilni uređaji odlični uređaji za udaljeno korištenje. 5G mobilni uređaji podržavaju više različitih načina povezivanja i uz povećanu propusnost, kao rezultat daje uređaj koji će gotovo uvijek biti povezan na Internet. Napadači će moći kreirati mobilne bot mreže na puno različitih i efikasnih načina [8]. Nove *bot* mreže za 5G mobilnu mrežu će biti mreže koje sadrže zaražene mobilne uređaje koji su pod kontrolom napadača pod nazivom *Bot-Masters*. Prikaz centralizirane 5G mobilne *bot* mreže gdje napadač dobiva pristup putem *Command and Control* servera je prikazana na slici 3.1 .



Slika 3.1 Centralizirana 5G mobilna *bot* mreža [8]

- *Bot-master*: će biti maliciozni korisnik koji ima pristup i upravljanje bot mreže koje se vrši udaljeno putem *bot-proxy* servera. *Bot-master* je odgovoran za odabir mobilnih uređaja koji će biti zaraženi *malwareom* i koji će postati *botovi*. On koristi sigurnosne ranjivosti u operacijskim sustavima i u samoj konfiguraciji mobilnih uređaja kako bi ih zarazio. Radi na vrlo sličan način kako i radi s osobnih računalima (eng. *Personal Computer*, PC) ali koristi i tehnike koje su specifične za mobilne uređaje poput SMS poruka. Pošto 5G korisnički uređaji nude veliki raspon opcija za povezivanje, moguće je da u budućnosti bot-masteri će moći koristiti dodatne tehnike za upravljanje i kontrolu ostalih uređaja.

- *Bot-proxy* serveri: Oni se koriste kao sredstvo za komunikaciju koju će *bot- master* koristiti za upravljanje i kontrolu ostalih *botova*.
- *Botovi*: uređaji koji će biti programirani od strane bot-mastera da izvode razne maliciozne zadatke poput DDoS napada na druge elemente mobilnih mreža, distribucija spam poruka, krađa i kopiranje osjetljivih podataka ili pak širenje *malwarea* na druge mobilne uređaje.

3.2. Pristupne mreže

U 5G komunikaciji, pristupne mreže su vrlo kompleksne, uključuju razne tehnologije radijskog pristupa i ostale pristupne sheme poput femtoćelija (eng. *Femtocells*), tako da pristupačnost servisa je zagarantirana. Primjerice, ako nema prisutnosti 4G mobilne mreže, korisnički uređaji će pokušavati uspostaviti vezu putem 2G ili 3G mobilne mreže. Samim time što 5G mobilna mreža podržava puno različitih načina pristupa mrežama, to dovodi do nasljeđivanja svih sigurnosnih rizika pristupa mrežama koje ona objedinjuje [9]. Tijekom razvoja komunikacije kroz generacije mobilnih mreža, fokus uvijek treba biti na poboljšanju sigurnosnih mehanizama najnovije generacije jer ako prepoznamo vrstu napada u starijim generacijama, onda rješenje možemo primijeniti i na noviju generacijom. Napadi poput napad pristupnim 4G mrežama i napad na HeNB (eng. *Home eNodeB*) femto ćelije se moraju razmotriti jer bi upravo oni mogli biti potencijalni napadi na 5G mobilnu mrežu.

3.2.1. Napad na 4G pristupnu mrežu

Neki od napada na 4G pristupnu mrežu mogu biti prošireni i za 5G mobilne mreže, pa njihova rješenja za takve napade je bitno proučiti i prikazati.

1. Praćenje lokacije korisničke opreme (eng. *User Equipment Location Tracking)*
   Praćenje prisustva korisničke opreme u određenim ćelijama ili kroz više ćelija je sigurnosni problem za LTE mreže koji može ozbiljno ugroziti korisnikovu privatnost. Koriste se dvije tehnike za napad te se one zasnivaju na Cell Radio Network Temporary Identifieru (C-RNTI) i na paketu sekvencijalnih brojeva.
   - Praćenje lokacije korisničke opreme na temelju C-RNTI
     C-RTNI sadrži unikatni i privremeni identifikator korisničke opreme na razini ćelija. Onda se pridodaje od strane mreže putem RRC (eng. *Radio Resource Control*) signala kada korisnička oprema je povezana s ćelijom. C-RNTI je

prenesen u L1 kontrolnom signalu u obliku običnog teksta. Time bi napadač mogao odrediti da li je uređaj s dobivenim C-RNTI-om još uvijek u istoj ćeliji ili ne. Po [10], periodička C-RNTI re-alokacija predstavlja potencijalno rješenje. Ona za uređaje koji su u istoj ćeliji dugi period vremena može napraviti da je puno teže napadačima doći do informacije da li se oni nalaze u ćeliji ili ne. Također dolazak novog uređaja u isto vrijeme kada se C-RNTI osvježi može predstaviti još težim zadatkom za napadača. Praćenje lokacije korisničkog uređaja može se postići i praćenjem kombinacije C-RNTI s *handover* signalima. Tom kombinacijom se omogućuje praćenje kroz više ćelija. Tijekom *handover* procesa, novi C-RNTI se daje uređaju putem *Handover Command* poruke. U tom slučaju, ako alokacija samog C-RNTI nije dobro zaštićena, napadač može novi C-RNTI povezati u *Handover Command* poruci s starim C-RNTI u L1 kontrolnom signalu [10]. Kako bi izbjegli ovu vrstu napada, potrebno je napraviti enkripciju na poruke poput *Handover Command* i *Handover Confirm* poruka, kako napadač ne bi mogao povezati navedene poruke s C-RNTI unutar *handover* procesa.

- Praćenje lokacije korisničke opreme na temelju paketa sekvencijalnih brojeva:
  Korištenje konstantnih paketa sekvencijalnih brojeva za korisničke i kontrolne pakete prije i poslije *handovera* omogućuje napadaču da poveže stari i novi C-RNTI [10]. Također se može primijeniti na *ideal-to-active* način rada tranzicije ako sekvencijalni brojevi se drže kontinuirano. Onda napadač može povezati uređaj na temelju kontinuiranog paketa sekvencijalnih brojeva u komunikaciji paketa. Jedan od prijedloga za problem jest da sekvencijalni brojevi putem radija budu ne kontinuirani u *handover* procesu i ako je moguće u promijeni stanja između aktivnog i pasivnog načina rada. Također korištenje novih ključeva za svaki eNB, koji omogućuje postavljanje sekvencijalnih brojeva na bilo koju nasumičnu vrijednost te samim time ih napravi ne kontinuirane.

2. Napadi temeljeni na lažnom izvješću *buffer* statusa

   U LTE mrežama, napadač može iskoristiti izvješća *buffer* statusa koji su korišteni kao ulazna informacija za raspored paketa, balansiranje tereta i odabir kontrolnih algoritama, za izvršavanje svojih malicioznih namjera. Napadač može poslati lažno izvješće *buffer* statusa u ime legitimnog korisničkog uređaja kako bi promijenio ponašanje algoritama na eNBu i kako bi uzrokovao probleme prema legitimnom korisničkom uređaju [10]. Promjenom ponašanja algoritma raspodijele paketa napadač je u mogućnosti ukrasti *bandwidth*. Kako bi uspio u tome, on mora koristiti C-RNTI drugih legitimnih uređaja i

poslati lažno izvješće. Zatim će eNB smatrati da je legitiman uređaj nema podatke za prijenos. Pa će samim time algoritam u eNB-u pridijeliti više resursa za napadačev uređaj i manje ili vrlo malo resursa za ostale uređaje, što je zapravo napad uskraćivanjem resursa. Također promjenom ponašanja algoritama za balansiranje paketa i odabir kontrolnih algoritama unutar eNB, DoS mogu iskusiti i novi uređaji koji su unutar ćelije. Kako bi napadač postigao to, on šalje izvješće sa raznih različitih uređaja u kojim piše da imaju više podataka za poslati nego što zapravo imaju. Zatim eNB smatra da unutar ćelije se nalazi puno podataka pa kada se novi uređaji žele spojiti, on ih odbije. Za rješenje ovakvog napada, koristi se jednokratni tokena unutar MAC razine [10]. Svaki uređaj će morati pokazati token eNB-u kako bi dobio pravo pristupa. Svaki token je različit za svako izvješće poslano tijekom DRX (eng. *Discontinuous Reception,* DRX) perioda.

3. Napad ubacivanjem poruke (eng. *Message Insertion Attack*)

   Ovakav napad je napad na LTE mreže koji je dodatno opisan u [10]. U LTE mrežama, korisnički uređaj je dopušteno da ostane u aktivnom modu rada ali ako isključi radio primatelj radi uštede energije. To je moguće napraviti kroz DRX period ali kroz dugi DRX period, uređaj može slati pakete jer uređaj možda ima važan promet za slanje. Ta mogućnost je sigurnosna prijetnja jer napadač može ubrizgati pakete kontrolnog protokola u sistem tijekom DRX perioda kako bi kreirao DoS napad protiv novi uređaja. Rješenje za ovaj problem je zahtjev za kapacitet kroz izvješće *uplink buffer* statusa.

3.2.2. HeNB Femtocell napadi

Fizička veličina, kvaliteta materijala, jeftine komponente i IP sučelje HeNB femto-ćelija čini ih više sklonim napadima u usporedi s eNB. U ovome dijelu rada ćemo razmotriti glavne kategorije potencijalnih napada vezane za HeNB femto ćelije. Također protumjere za te napade ćemo također razmotriti, a za detaljnu listu svih mogućih napada vezane uz HeNB femtoćelije može se pronaći u reference [11].

1. Fizički napad na HeNB

   Fizičko miješanje s HeNB-om je napad gdje maliciozni napadač može modificirati ili zamijeniti HeNB komponente. S ovakvim tipom napada, moguće je utjecati na krajnje korisnike i mobilne operatore. Primjerice, modificirana RF komponenta HeNB-a može utjecati na druge bežične uređaje *u eHealth* tele-monitorskom sistemu u okruženju pacijenta bolnice i učinit ih neuporabljivim. To može utjecati za zdravlje pacijenta. Također, HeNB s modificiranim RF komponentama može utjecati negativno na

okruženje makro mreži. Očito je da HeNB mora biti fizički osiguran kako bi spriječili zamjenu komponenti sustava. Također treba koristiti provjerene računalne tehnike za otkrivanje kada se dogodila zamjena kritičnih komponenti na HeNB-u. Isto tako podizanje HeNB sustava s modificiranim malicioznim softwareom također može biti na štetu krajnjih korisnika i mobilnih operatora. To se može postići u HeNB pomoćnom korisničko pristupačnom kodu za polazne programe. Kao rezultat dobivamo prisluškivanje komunikacije i krađu identiteta kao potencijalne prijetnje za koje krajnji korisnik mora svjestan. DoS napadi su također prisutni te rješenje ovih problema je osigurati proces podizanja polaznih programa putem kriptografije, korištenjem primjerice TPM-a (eng. *Trusted Platform Module*).

2. Napad na vjerodajnice (eng. *Credentials*) HeNB-a

   Kod ovakvih napada, komprimirana autentifikacija vjerodajnice HeNB-a se koristi. Napadač dobiva kopiju autentifikacijskih vjerodajnica od mreža za zadani HeNB. Onda bilo koji maliciozni uređaj može ih koristiti i predstavljati se kao zadani HeNB. Time, napadač može koristiti maskirane napade protiv krajnjeg korisnika i mobilnih operatora. Uspjeh dobivanja kopije autentifikacijske vjerodajnice ovisi o njenoj samoj implementaciji. Vjerodajnice bi trebale biti pohranjene u zaštitnoj domeni poput TPM modula kako bi osigurali da napadač ne može olako doći do njih.

3. Konfiguracijski napad na HeNB

   Mogući napad unutar ove kategorije je kriva konfiguracija na ACL-u (eng. *Access Control List,* ACL) zadanog HeNB-a. Prvenstveno napadač mora dobiti pristup ACL-u, uključujući i CSG (eng. *Closed Subscriber Group,* CSG) listi. Onda može modificirati ACL tako da nelegitimne uređaji mogu pristupiti mreži. Također napadač može i modificirati ACL da zabrani legitimnim uređajima pristup mreži ili pak promijeniti razinu pristupa određenim uređajima. Kao rezultat dobivamo da legitimni krajnji korisnici dobivaju efekte DoS napada dok neki maliciozni krajnji korisnici mogu koristiti servise besplatno. Time je vrlo bitno osigurati sigurno stvaranje, održavanje i spremanje ACL lista.

4. Napadi protokola na HeNB

   Napadi protokola uključuju čovjek u sredini napade (eng. *Man-in-the-middle attacks*) na HeNB prvu mrežu pristupa, gdje može uzrokovati veliku štetu krajnjim korisnicima.

HeNB je ranjiv na ovaj tip napada kada nemaju jedinstveni autentifikacijski vjerodajnice. U takvim slučajevima, tijekom prvog kontakta s ciljanim HeNB do jezgre mreže preko interneta, operator nije u mogućnosti prepoznati ga. Napadač na internetu može presresti sav promet koji je izašao iz HeNB-a i dobiva pristup privatnim informacijama koje može koristiti po volji. Za napad čovjeka u sredini, autentifikacijske vjerodajnice morale bi se koristiti prvi prvom kontaktu s zadanim HeNB-om. Korištenjem UICC (eng. *Universal Integrated Circuit Card*, UICC) ili certifikata je moguće potencijalno riješiti problem. U slučaju korištenja UICC, on se postavlja u HeNB od strane prodavača ili korisnika, i zajednička autentifikacija između HSS (eng. *Home Subscriber Server*, HSS) i UICC se uspostavlja. Za rješenja koja koriste certifikate , on mora biti pohranjen na HeNB u fazi stvaranja samog HeNB-a i mora biti korišten za zajedničku autentifikaciju između prvog kontaktnog čvora i HeNB-a.

5. Napad na jezgru mreže mobilnog operatora

   DoS napadi mogu biti pokrenuti kroz zlonamjerni promet kreiran od strane zaraženih HeNB-sa protiv elementa jezgre mreže. Dvije kategorije DoS napada koji direktno napadaju jezgru mreže ali ne i HeNB-a su: IKEv2(eng. Internet Key Exchange Version 2, IKEv2) napad koji može biti pokrenut protiv inicijalne postave IKEv2 tunela između HeNB i sigurnosnog gatewaya te druga vrsta napada su slojevi 5,6 i 7 napadi i IKEv2 napad gdje je visoka količina signaliziranog prometa ili gdje IKEv2 tunel postavlja promet koji će preplaviti infrastrukturu. Za smanjenje ovakvih napada, sigurnosni gateway mora ostati siguran i dostupan kao prva točka pristupa u jezgri mreže. Isto tako u ovakvu grupa napada smatra se i promjena HeNB lokacije bez izvješća. Napadač može premjestiti HeNB i napraviti da lokacijska informacija bude netočna. Kao rezultat ovo može dovesti prijenosa hitnih poziva preko premještenog HeNB-a koji neće točno ili pouzdano povezati se na točan hitni centar. Zakonita presretanje izvješća pozicije je nemoguće. Mehanizam za zaključavanje lokacije je jedan od mogućih rješenja zadanog problema.

6. Napad na korisničke podatke i privatnost identiteta

   Prisluškivanje E-UTRAN (eng. *Evolved Universal Terrestrial Radio Access Network*, E-UTRAN) podatke drugog korisnika je vrlo štetan napad jer narušava privatnost korisnika. Napadač postavi vlastiti HeNB i konfigurira ga da bude otvoren. Zatim korisnik koristi ugroženi HeNB za pristup jezgri mreže bez da on zna da je on zapravo ugrožen. Time napadač može prisluškivati sav promet koji prolazi između korisnika i

mreže. Taj napad iskorištava ne zaštićenost korisničkog prometa u nekim dijelovima HeNB. Iz tog razloga ne zaštićeni promet korisnika nikada ne smije izaći iz sigurne domene unutar HeNB-a kako bi spriječili prisluškivanje. Krajnji korisnici bi trebali biti obavješteni kada se povezuju na zatvoreni ili otvoreni tip HeNB-a.

7. Napad na radio resurse i upravljanje
   Diranje upravljanja radio resursima je napad gdje HeNB priloži nepravilnu informaciju o radio resursima. Kako bi postigao to, napadač mora imati pristup HeNB-u i mora modificirati aspekte upravljanja resursima. Barem bi trebao moći modificirati snagu kontrolnog dijela HeNB-a. Rezultat ovog napada je povećani *handover* te samim time bi konfiguracija sučelja HeNB-a trebala biti osigurana.

3.3. Jezgra mreže poslužitelja

Zbog otvorene arhitekture zasnivane na IP-u, 5G mobilni sustavi su ranjivi na napade zasnivane na IP-u koji su često korišteni na Internetu. DoS napadi, koji su jedan od glavnih prijetnji današnjice, će također biti prisutni u 5G komunikacijskim sustavima koji će ciljati entitete na jezgri mreže mobilnih operatera. Isto tako je 5G jezgra mreže mobilnih operatera meta i DDoS napada koji ciljaju vanjske entitete ali svoj zlonamjerni promet šalju preko nje. Neki od napada uključuju sljedeće napade:

3.3.1. DDoS napad ciljan na jezgru mreže mobilnog operatera

DDoS napadi su vrlo ozbiljan problem koji može utjecati na dostupnost jezgre mobilnih mreža. Pošto 5G mobilna mreža je korištena od strane miliona korisnika, posljedice DoS i DDoS napada na jezgru mreže su velike. U 5G komunikacijskom okruženju, DDoS napad može biti pokrenut sa strane *botneta* koji uključuje veliki broj zaraženih mobilnih uređaja. Unutar ove potkategorije dva predstavnika DDoS napada protiv 4G jezgre mreže mobilnih operatora su prisutan, te se i njihovi napadi mogu primijeniti na 5G jezgru mreže.

1. Pojačanje signala
   Napad pojačanjem signala (eng. *Signalling Amplification*) je izveden uz pomoću *botneta* od nekoliko zaraženih mobilnih uređaja unutar same ćelije kako bi potrošili resurse mreže i doveli do lošijeg servisa. Ovaj napad iskorištava opterećenje signalizacije potrebno za postavljanje i puštanje određenih radio nositelja u LTE mreži. Time veliki broj zahtjeva određenih nositelja će se inicijalizirati istovremeno, i time natjerati druge entitete mreže da

prate veliki signal aktivacije određenih nositelja za svaki od nositelja. Nakon dobivanja određenog nositelja, *botovi* ih neće koristiti i nakon isteka vremena za neaktivnost nositelja, oni će se deaktivirati što također prouzrokuje snažan signal. Onda, maliciozni uređaji *botneta* će izvršiti iste korake u krug kako bi povećali razinu napada i smanjili performanse mreže. Tehnika za otkrivanje ovakvih napada je temeljna na značajkama poput internog vremena za postavljanje te broj aktiviranja i deaktiviranja nositelja u minuti. Postavljanje niske granice za interno vrijeme postavljanja određuje performanse tehnike za otkrivanje. Visoka granična vrijednost za interno vrijeme postavljanja bi mogla uzrokovati puno lažno pozitivnih primjera. U drugu ruku, niska granična vrijednost može dovesti do puno neuhvaćenih slučaja. Visoki broj aktivacije i deaktivacije nositelja po minuti govori o zlonamjernoj aktivnosti i trebala bi biti otkrivena i zaustavljena sa strane operatora [12].

2. HSS Zasićenost (eng. *Saturation*)

   Potencijalni DDos napad na 5G jezgru mobilne mreže operatora je HSS zasićenost koja je za 4G mreže opisana u referenci [12].

   HSS je zapravo čvor EPC-a (eng. *Evolved Packet Core*, EPC), pošto se sastoji od glavne baze podataka za pojedinog korisnika i sadrži informacije o pretplaćivanju do podrške mrežnim entitetima koji održavaju ćelije/sesije. HSS također nudi podršku funkcionalnostima u korisničkoj autentifikaciji i pristup autorizaciji. Bazna mreža može sadržavati jedan ili više HSS-a temeljeno na broju mobilnih pretplatnika, kapacitetu opreme i organizaciji same mreže [13]. Time, DDoS napadi protiv ovog ključnog čvora može potencijalno smanjiti dostupnost jezgre mobilne mreže značajno. Unutar reference [14], opisana je u istraživanju mogućnost preopterećenja HLR (eng. *Home Location Register*, HLR), što je ključna komponenta u HSS, koristeći *botnet* mobilnih uređaja. Rezultat istraživanja pokazuje da smanjenje propusnosti je ovisno o veličini *botneta*. Svakako je bitno spomenuti da kod ovog tipa napada, legitimni korisnici čiji su mobilni uređaji zaraženi neće ni biti svjesni napada, jer su ti napadi izvršeni tihim slanjem zahtjeva mrežnih servisa, a ne kroz val poziva mobitela. U konačnici, istraživanje predlaže osnovne filtere i ljuštenje (eng. *Shedding*) kao dva moguća rješenja smanjenja takvih napada. Implementacija mehanizama dovoljno pametnih za odgovor na više dinamičke napade ostaje i dalje izazovni problem. Osobito je teško pružatelju usluga raspoznati napade od običnog prometa jer je vrlo velika količina konteksta izgubljena jer se poruke šalju između mobilnih uređaja i HLR. Isto tako filtriranje jezgre mreže se može dogoditi prekasno da zaustavi legitimne korisnike od DoS napada zbog velikog preopterećenja vezano uz prvi skok komunikacije unutar mobilnih mreža [14].

3.3.2. DDoS napadi ciljani na vanjske entitete preko jezgre mreže mobilnih operatora

Nadolazeće 5G mreže mogu služiti i kao *gateway* za DDoS napade protiv meta iz ostalih vanjskih mreža spojenih na jezgru mobilne mreže. U tom slučaju, *botnet* mobilnih uređaja može biti korišten za generiranje visoke količine prometa i prijenos na žrtve, koji se nalaze u vanjskoj infrastrukturi mreže, putem jezgre mobilne mreže. Iako mete ovih napada neće biti sama jezgra mreže, činjenica da one unose veliku količinu prometa u jezgru mreže može znatno utjecati na performansu mreže. Nedavni DDoS napadi protiv Spamhausa preko Interneta su dokazali kako visoki volumen napada prometa može utjecati na dostupnost komunikacijske mreže zadužene za prijenos do zadane mete [9].

3.4. Vanjske IP mreže

U 5G komunikacijskim sustavima, vanjske IP mreže mogu također biti žrtve DDoS napada, gdje mobilni *botnetovi* generiraju visoki volumen prometa te ga prenosi do žrtve putem jezgri mobilnih mreža. Također, vanjske IP mreže poput poduzetničkih mreža mogu također biti meta kroz *malware* koji se širi putem mobilnih uređaja koji ih koriste. Sljedeći slučaj, baziran na [15], način na koji poduzetnička mreža može biti ugrožena od zaraženih 5G mobilnih uređaja zaposlenika.

3.4.1. Ugrožene poduzetničke mreže

Trenutno široko prihvaćeni pametni uređaji su već razlog većine zaposlenika da nose vlastite pametne mobilne uređaje u radno okruženje i da ih koriste za dobivanje informacija putem izoliranih poduzetničkih mreža ili poduzetničkih mreža sa strogom kontrolom pristupa. Ovaj trend se očekuje da će se nastaviti i ubrzati kroz vrijeme. Puno sigurnosnih problema će biti prisutno za poduzetničke mreže pristupane od strane zaposlenikovih pametnih mobitela zbog potencijalne osjetljivosti pametnih mobitela na mobilni *malware* [15]. Potencijalne ranjivosti moguće je iskoristiti od strane napadača za ugrožavanje inače sigurnih poduzetničkih mreža. Mobilni *malware* poput *Dream Droida* [15], koji je nedavno zarazio Android Market, moguće je iskoristiti za neovlašteni pristup poduzetničkoj mreži od strane pametnih mobitela zaposlenika. Još jedan način na koji će se napadač moći pristupiti poduzetničkoj mreži je putem same raznovrsnosti povezivanja samog mobilnog uređaja. Ne samo da pametni mobitel podržava komunikacijske

tehnologije (2G/3G/4G/5G), već podržava i ostale tehnologije poput WiFi, *Bluetooth*, NFC (eng. *Near Field Communication*, NFC) i USB (eng. *Universal Serial Bus*, USB) Sve te tehnologije se mogu iskoristiti kao kanali za širenje mobilnog malware od strane napadača. Drugim riječima, pametni mobiteli zaposlenika služe kao most za napadača između vanjskog svijeta i poduzetničke mreže. Zaposlenikov pametni mobitel može biti ugrožen kroz mobilni komunikacijski kanal ili kroz kratko široki komunikacijski kanal i može postati prolaz do ciljanje poduzetničke mreže ili može pridonijeti zlonamjerni promet direktno kroz drugi komunikacijski kanal podržan od strane pametnog mobitela. U slučaju napada, možemo pretpostaviti da je zaposlenikov mobitel povezan na osobno računalo putem USB-a te je PC povezan direktno na unutarnju poduzetničku mrežu. Onda *bot-maste*r se može spojiti kroz *backdoor* na zaposlenikov mobitel putem WiFi ili 4G mobilne mreže i ubaciti zlonamjerni paket podataka u unutarnju poduzetničku mrežu kroz USB konekciju. Kako bi izbjegli sigurnosna probijanja u poduzetničkoj mreži od strane korištenja zaposlenikovog pametnog uređaja unutar radnog okruženja, vrlo učestali pristup je povremeno provjeravanje svih pametnih mobitela zaposlenika uz pomoć *anti-malware* softwarea. Iako ovaj pristup je nametljiv i skup u smislu energije. Nova rješenja moraju pružati balans između sigurnosne potrebe i efikasnosti troška. U referenci [15], strateško uzrokovanje je predloženo kao metoda za rješenje ovog problema, putem identificiranja i periodičkog uzrokovanja sigurnosnih potreba pametnih mobitela. Time su uređaji provjereni za *malware*. Sigurnost pametnih mobitela zaposlenika se mjeri po njegovom interesu i zapisu logova na njihovim uređajima. Vjerojatnosti korištene za metode za strateško uzrokovanje su izvedene od loto stabla koje se odnosi na sigurnosnu reprezentativnost kod pametnih mobilnih uređaja [15].

4. MJERE ZAŠTITE I SIGURNOSNI MEHANIZMI U 5G MREŽAMA

Unutar ovog poglavlja će biti objašnjeni sigurnosni mehanizmi i mjere zaštite unutar 5G mreža. Dotaknuti ćemo se pojmova poput autentifikacije, dostupnosti, povjerljivosti podataka i upravljanjem ključevima. Ove mehanizme možemo podijeliti u dvije skupine pristupa: kriptografija s novim mrežnim protokolima i sigurnost fizičkog sloja [16].

4.1. Kriptografski pristup i sigurnost fizičkog sloja

Kriptografske tehnike se koriste unutar sigurnosnih mehanizama unutar 5G mrežama i tipično su implementirane u višim slojevima uz korištenje novih mrežnih protokola. Moderna kriptografija sastoji se od kriptografije simetričnim ključevima i kriptografije javnim ključevima. Simetrična kriptografija se odnosi na enkripcijske metode unutar kojih se tajni ključ dijeli između primatelja i pošiljatelja. Kriptografija javim ključem, također poznata kao asimetrična kriptografija, koristi dva para ključa: javni ključ za enkripciju i privatni ključ za dekripciju. Ukratko ćemo vidjeti rad navedenih mehanizama kriptografije i spomenuti par pristupa sigurnosti na fizičkom sloju [16].

4.1.1. Kriptografija simetričnim ključem

Ona se odnosi na bilo koju kriptografski algoritam koji koristi dijeljeni tajni ključ za enkripciju i dekripciju podataka. Pruža cjelovitost, povjerljivost i autentičnost podataka. Često se koristi kako bi osigurali povjerljivost podataka za komunikaciju ili pohranu. Uz samu simetričnu enkripciju, MAC (eng. *Message Authentication Code,* MAC) i *hash* funkcije se također koriste kako bi osigurali autentifikaciju i integritet samih poruka. Kriptografija simetričnim ključem je zasnivana na pretpostavci da pošiljatelj i primatelj mogu sigurno razmijeniti i pohraniti tajni ključ K. Taj ključ se može razmijeniti putem centra za distribuciju ključa (eng. *Key Distribution Center,* KDC), koji je povjerljiv sa strane primatelja i pošiljatelja. KDC koristi unaprijed poslan ključ sa svakim korisnikom povezanim s njime. KDC generira zaseban ključ potreban za komunikaciju dvaju korisnika, i podijeli ih tajno njima kako bi osigurali komunikaciju tih dvaju korisnika za svaku sesiju.

4.1.2. Kriptografija javnim ključem

Ona koristi par ključeva, javni ključ i privatni kako bi osigurali povjerljivost, autentičnost, integritet i neoporicanje. Ovaj algoritam miče potrebu za sigurnim putem dijeljenja ključa između korisnika. Kriptografija javnim ključem također može biti korištena za digitalni potpis, koji nam služi kako bi znali da je osoba s kojom komuniciramo zapravo ona koja tvrdi da jest. Kriptografija

javnim ključem najčešće se koristi za distribuciju tajnog ključa i pruža neporecivost, što nije moguće kod kriptografije simetričnim ključem.

4.1.3. Sigurnost fizičkog sloja

Cilj sigurnosti fizičkog sloja (eng. *Physical Layer Security*, PLS) je korištenje fizičkih svojstava komunikacijskih kanala za uspostavljanje sigurne komunikacije. Kako bi poboljšali sigurnost komunikacije na fizičkom sloju u bežičnim mrežama, nekoliko metoda se koristi te su one podijeljene u pet većih kategorija: teorijska sigurnost kapaciteta, kanala, kodiranja, snage i sl. PLS tehnike se fokusiraju na sprječavanju prisluškivanja i napade na sam signal. Teoretska sigurnost kapaciteta istražuje primarno centre oko analize tajnosti kapaciteta, gdje su razlike u brzini prijenosa podataka između autoriziranih i ne autoriziranih korisnika. PLS se sastoji od tri jedinstvena pristupa:

- Kanalski pristupi koriste jedinstvene karakteristike u komunikacijskim kanalima kako bi poboljšali sigurnost. Ove metode se mogu kategorizirati u tri tipa: Otisak radijskih frekvencija, dekompozicijsko multipleksiranje za algebarski kanal te nasumičnost MIMO-a (eng. *Multilpe-input and multiple-output*, MIMO) transmisijski koeficijenti.
- Pristup kodiranja: gdje su korišteni za poboljšanje otpornosti na prisluškivanje i blokiranje signala. Kodiranje za ispravljanje grešaka i kodiranje širom spektra su dvije najčešće korištene metode za pristup kodiranja.
- Pristup snage: poboljšava sigurnost podataka. Napredak u sklopovlju i programskom svijetu unutar 5G su omogućili korištenje tehnika poput usmjerenih antena, umjetno ubrizgavanje šuma te kontrolu snage kako bi smanjili prisluškivanje i blokiranje signala u komunikaciji. Usmjerene antene omogućuju legitimnom korisniku da dobiva podatke iz određenog smjera, dok napadači nisu u mogućnosti primiti signal. Umjetno ubrizgavanje šuma omogućuje sigurnu komunikaciju kroz smanjenje omjera signala i šuma.

4.2. Autentifikacija

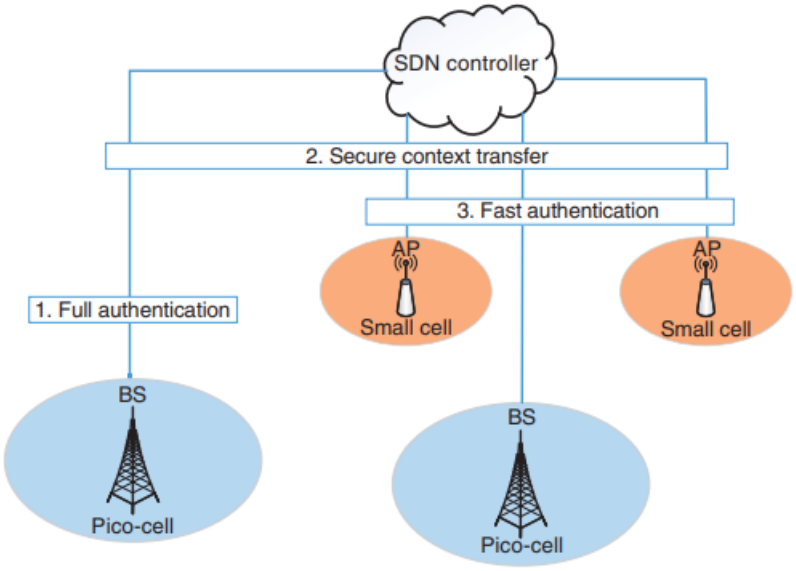
Autentifikacija je važni sigurnosni servis unutar 5G bežičnih mreža. U prethodnim generacijama, autentifikacija se zasnivala na kriptografiji simetričnih ključeva dok autentifikacija u 5G mrežama donosi niz izazova i problema poput potrebne za niskom latencijom, podržavanje D2D (eng. *Device-to-device*, D2D) komunikacije, osiguravanje efikasnog korištenja propusnosti i

energije, rješavanje ograničenih računalnih mogućnosti uređaja i razmatranje za nove sigurnosne servise [16].

4.2.1. Potreba za niskom latencijom

Zbog potrebe za niskom latencijom u 5G mrežama, shema autentifikacije mora biti više efikasna nego ikada. Kako bi iskoristili prednosti softverski definiranog umrežavanja (eng. *Software-Defined Networking,* SDN), predložena je nova shema koja koristi mjerene informacije sigurnim kontekstom (eng. *Secure-Context-Information,* SCI) prenošene kao ne kriptografski sigurna tehnika kako bi poboljšali efikasnost autentifikacije prilikom čestih prelazaka u HetNet, kako bi se riješila potreba za niskom latencijom. Predložen je brzi autentifikacijski protokol od strane Duan i Wang u radu iz 2016. godine, koji uključuje punu autentifikaciju i mjereni SCI prijenos zasnivan na njoj. Nakon prve pune autentifikacije u jednoj ćeliji, može se lako primijeniti na druge ćelije uz korištenje verifikacije MAC adrese, za koju je potrebno samo lokalno procesiranje. Štoviše, puna autentifikacija može čak biti provedena bez ometanja komunikacije korisnika. Valjani parametar vremenskog trajanja koristi se za fleksibilno podešavanje sigurnosne razine. Za razliku od kriptografskih metoda autentifikacije, predložena metoda je manje osjetljiva na ugrožavanje jer se odnosi u korisnikove atribute na fizičkome sloju. SCI koristi više karakteristika fizičkih slojeva kako bi unaprijedila pouzdanost autentifikacije za aplikacije koje zahtijevaju visoku razinu sigurnosti. SDN kontroler koristi model za nadgledanje i predviđanje korisnikove lokacije (prikazano na slici 4.1) i omogućava da potrebne ćelije se pripreme prije nego korisnik uopće dođe u blizinu i s time se postiže neprimjetni prijelaz. Atributi fizičkog sloja se koriste kako bi pružili jedinstvene otiske korisnika i kako bi pojednostavili autentifikacijski postupak. Tri tipa atributa fizičkog sloja se koriste kao otisak za pojedinog korisnika. Kada je autentifikacija dovršena, validirani početni atributi su zapisani. SDN kontroler neprestano prikuplja opažanja kroz uzimanje uzoraka raznih atributa fizičkog sloja kroz primljene pakete kako bi validirao originalne atribute. Originalna datoteka i rezultati zapažanja oboje sadrže srednju vrijednost i varijancu odabranih atributa. Onda pomak srednje vrijednosti atributa se može izračunati po originalnim validiranim atributima i promatranim atributima. Ako je pomak atributa manji od prije definirane granice, korisnikova oprema se smatra legitimnom. Za procjenu performanse metode autentifikacije, SDN mrežni model koji koristi prioritet pristupa je predložen. Sav nadolazeći promet je modeliran koristeći Pareto distribuciju. Odgoda u autentifikaciji se uspoređuje kroz više scenarija korištenja mreže. Rezultati simulacije uspoređuju odgodu performanse SDN korištene brze autentifikacije sa standardnom kriptografskom metodom

autentifikacije. Korištenjem svih prednosti koje pružaju 5G mreže, korištenje SDN-a za brzu autentifikaciju se uspostavilo najbrže i najefikasnije.



Slika 4.1 SDN autentifikacijski model [16]

4.2.2. Podržavanje D2D komunikacije

Kako bi smanjili sigurnosne probleme koji potiču iz nedostatka sigurnosne infrastrukture koji koristi D2D komunikacija, predložen je sigurnosni mehanizam bodovanja temeljen na kontinuiranoj autentičnosti. Ovaj pristup koristi koncept uzoraka legitimnosti za implementaciju kontinuirane autentičnosti, koja omogućava otkrivanje napada i mjerenje sigurnosnih rezultata sustava. Uzorak legitimacije uključuje dodavanje redundantnog niza bitova u paket kako bi lakše prepoznali pokušaj napada. Rezultati simulacije prikazuju efikasnost predloženog mehanizma, te je uzet u obzir i tehnički i ljudski aspekt koji bi mogao daljnje poboljšati performanse.

4.2.3. Visoka efikasnost korištenja propusnosti i energije

Unutar svoga rada [Dubrova et al, 2015], autori predlažu novi mehanizam autentifikacije poruke zasnivan na cikličkoj provjeri redundancije (eng. *Cyclic Redundancy Check*, CRC) koji bi povezao visoku razinu sigurnosti i vrlo efikasnu upotrebu propusnosti i energije koje su moguće u 5G mrežama. Ova shema omogućuje detekciju dvobitnih grešaka unutar jedne poruke, i time poboljšava pouzdanost i točnost autentifikacijskog procesa. CRC bazirane kriptografske hash

funckije su definirane. Linearni registar pomaka s povratnom informacijom (eng. *Linear Feedback Shift Register*, LFSR) se koristi za efikasnu implementaciju CRC kodiranja i dekodiranja. Algoritam proizvodi autentifikacijsku oznaku zasnivanu na tajnome ključu i poruci. Sigurnosna pretpostavka na kojoj se temelji ova shema je da korisnik posjeduje obitelj hash funkcija, ali nema pristup specifičnom polinomu g(x) i popunjenju s koji su korišteni za stvaranje autentifikacijske oznake. Generator polinoma se mijenja periodički na početku svake sesije, popunjenje s se mijenja svaku poruku. Nova familija kriptografskih *hash* funkcija temeljena na CRC kodiranju s generatorom polinoma g(x)=(1+x)p(x) je predstavljen, gdje je p(x) primitivan polinom.

4.2.4. Ograničene računalne mogućnosti uređaja

Identifikacija radio frekvencijom (eng. *Radio Frequency Identification*, RFID) ima široku primjenu kroz razne industrije i aplikacije. Zbog ranih ograničenja u jeftinim RFID oznakama, enkripcijski algoritmi i autentifikacijski mehanizmi u RFID sustavima moraju biti jako efikasni. Ako koristimo jednu RFID oznaku za više primjena, moramo uzeti u obzir mogućnosti opoziva u autentifikacijskoj shemi. Nova shema je predložena koja koristi hash funkcije i nasumični broj koji su korišteni za kreiranje zadanog modula kroz mehanizam izazov-odgovor. Čitač sadrži pseudo-nasumičan generator brojeva, dok server ima hash funkciju i bazu podataka. Server zatim uspostavi bazu oznaka za svaku legitimnu oznaku i grupu odgovarajućih zapisa. Kada dobije autentifikacijski zahtjev, oznaka generira drugi nasumičan broj, te se računaju dvije hash autentifikacijske poruke, te uz pomoću XOR funkcije dobijemo vrijednost, koja služi za prihvaćanje ili odbijanje zahtjeva. Predloženi sigurnosni sustav nudi puno bolju zaštitu i na istoj je razini kompleksnosti kao već postojeće sheme.

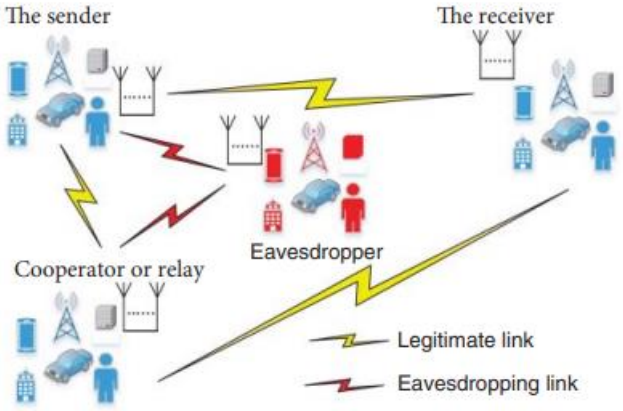
4.3. Dostupnost

Dostupnost je ključna kako bi osigurali visoku razinu pouzdane komunikacije unutar 5G mreža. Kroz emitiranje nasumičnih bežičnih šumova, blokirajući uređaji mogu znatno naštetiti performansama mobilnih korisnika te čak i u potpunosti blokirati pristup servisa. Blokiranje (eng. *Jamming*) je jedan od uobičajenih mehanizam koji se koriste u DDoS napadima. Većina mehanizama protiv blokiranja koristi tehnike preskakivanja frekvencija unutar kojih korisnici skaču kroz više kanala kako bi izbjegli blokiranje i kako bi mogli koristiti svoje usluge ili servise. Glavni izazov je poboljšati dostupnost u 5G mrežama sa svim tehnologijama koje nam one pružaju. Predložena je tajna shema koja bi usvojila preskakivanje frekvencija kao moguću tehniku protiv DoS napada za platforme unutar 5G sistemima. Predložen je estimator stope pogreške u

bitovima (eng. *Bit Error Rate*, BER) zasnivan na informacijama fizičkog sloja koja bi odlučivala blokiranje frekvencija pod DoS napadima. Dinamički spektar koji korisnici koriste možda neće biti efektivan kod tehnike preskakivanja frekvencija zbog visoke razine promjene i vjerojatnosti za blokiranje jer joj je potrebno više kanala za komunikaciju. Kako bi smanjili potrebu za mijenjanjem kanala i vjerojatnost blokiranja samog signala, predložen je pseudo nasumična shema koja bi koristila vremensko skakanje i metode protiv blokiranja za korisnike koji koriste 5G mrežu. Kognitivni omotač sa ograničenim resursima je uključen u model za analizu utjecaja dinamičkog spektra performansi za mobilne korisnike. Vjerojatnost blokiranja signala je smanjena kada omotač ima ograničen pristup samome kanalu. Usporedi s sistemom skakanjem frekvencija, vremensko skakanje se ispostavilo puno bolje, gdje je vjerojatnost greške puno manja za istu uloženu energiju. No na nekim razinama energije, performanse stagniraju. Predlaže se korištenje ove metode za D2D veze u 5G mrežama zbog njihove vrlo snažne performanse vezane uz efikasnost energije i spektra. Za tehniku vremenskog skakanja i protublokiranja potreban je ključ koji je unaprijed dijeljen. Kako bi zaštitili čvorove sa ograničenim računalnim sposobnostima od napada blokiranja, fuzijski centar je predstavljen. Kada je jedan od čvorova napadnut, centar šalje instrukcije da poveća svoju prijenosnu snagu kako bi jačina signala ostala nepromijenjena. Simulacije su pokazale kako su performanse značajno bolje kada koristimo fuzijski centar za prijavu takvih napada.

4.4. Povjerljivost podataka

Kako bi smanjili napade prisluškivanja, servisi za povjerljivost podataka su potrebni. Općeniti sustav koji se koristi prikazan je na slici 4.2. Kod povjerljivosti podataka, neke od bitnih pojmova koji nam pomažu u zaštiti su kontrola snage, relej, umjetni šumovi, obrada signala i kriptografske metode koje se koriste. Većinu od ovih pojmova smo do neke razine spomenuli u prethodnim poglavljima te se praktični sve zasniva na tome se pokušamo obraniti od napadača kako bi naši podaci ostali povjerljivi, tj. kako bi ostali zaštićeni od drugih izvora, koristeći razne metode, koje su od nekih navedene.



Slika 4.2. Općeniti sustav kod napada prisluškivanja. [16]

4.5. Upravljanje ključevima

Upravljanje ključevima se odnosi na sam proces zaštićenog stvaranja, čuvanja , dijeljenja i uništavanja kriptografskih ključeva koje koristimo unutar kriptografskih sustava. Oni se koriste za enkripciju i dekripciju informacija, za provjeru digitalnih potpisa i nude autentifikaciju u raznim primjenama poput sigurne komunikacije, pohrane podataka i online transakcija. Predložena su tri nova protokola za razmjenu ključeva, svi koji imaju drugačiju razinu računalnog vremena, kompleksnosti i sigurnosti, za korištenje u D2D komunikaciji, koji se zasnivaju na Diffie-Hellman shemi. Razne analize su napravljene kako bi procijenili efikasnost sigurnosnih sistema, koje uključuju povjerljivost, integritet, autentifikacija i neoporicanje. Analiza je zasnivana na kombinaciji teoretske evaluacije i praktičkih eksperimenta te se uspostavila njihova korisnost. U

slučaju D2D komunikacije, mehanizam upravljanja grupnog ključa (eng. *Group Key Managment*, GKM) je predložen za sigurnu razmjenu D2D poruka tijekom faze otkrivanja i komunikacije. Pet sigurnosnih stavki je predloženo za GKM sustav, a to su:

1. Proslijeđena tajnost-korisnici koji su izašli iz grupe nemaju pristup budućim ključevima.
2. Vraćena tajnost-novi korisnici koji su ušli u sesiju ne smiju imati pristup starim ključevima.
3. Sloboda od tajnih dogovora-lažni korisnici ne mogu predvidjeti trenutni kriptirani promet.
4. Neovisnost ključa-ključevi jedne grupe ne smiju moći vidjeti ključeve druge grupe.
5. Odnos povjerenja- korisnici ne smiju otkrivati ključeve drugima unutar domene ili van nje.

Shema kriptografije ID-u (eng. *ID-based Cryptography*, IBC) zasnivane na kriptografiji eliptične krivulje (eng. *Eliptic Curve Cryptography*, ECC) je predstavljena. Koraci protokola uključuju stvaranje tajnog ključa, algoritam potpisa na eliptičnoj krivulji, verifikacija samog potpisa, procedura formiranja grupa, generiranje ključa, te procese za ulazak i izlazak. Generiranje glavnog i privatnog ključa se zasniva na IBC i ECC shemi. Prostor za komunikaciju, ponovno korištenje ključa za poruke i pohranu ključa su uključene.

5. PRIVATNOST U 5G MREŽAMA

5G mreže obećavaju krajnjim korisnicima korištenje pametnih servisa, što donosi brigu za privatnost samih tih korisnika. Servisi koji pruža 5G mreža će se koristiti osnovne podatke (poput identiteta, lokacije ili pozicije i privatne podatke) o svojim korisnicima. Kako će ti podaci biti spremljeni i na koji način će pojedini podaci biti dostupni drugim kompanijama, 5G mreže naglašavaju važnost problema u curenju privatnih podataka. Razmatrati ćemo razne tehnike i metode koje 5G mreža uključuje kako bi riješila prethodno navedene probleme privatnosti podataka kod korisnika [17].

5.1. Privatnost kod korisnika

Tri bitne kategorije se smatraju kod privatnosti korisnika, a to su privatnost podataka, lokacije i identiteta [18].

5.1.1. Privatnost podataka

5G mreže dopuštaju korisnicima korištenje pametnih i podatkovno zahtjevnih servisa kroz heterogene pametne uređaje. Kako bi pružali takve servise, oni će možda spremati i koristiti privatne podatke pojedinaca bez njihovog znanja. Spremljeni podaci će možda biti dijeljeni s ostalim dionicima kako bi mogli koristiti podatke za analizu koristeći strojno učenje kako bi mogli naći nove trendove za njihove pojedine proizvode koji bi više odgovarali korisnicima. Primjerice, nedavna istraživanja su otkrila da pametni mjerači podataka mogu otkriti osobne informacije poput da li je kuća u kojoj se nalazi prazna, ili pak ekonomski status korisnika. Kako bi smanjili takve probleme kod privatnosti, pružatelji usluga moraju jasno objasniti korisniku kako se i gdje spremaju njegovi podaci, te kako će oni biti korišteni.

5.1.2. Privatnost lokacije

Unutar 5G mreža, većina uređaja koristi sveprisutne usluge temeljene na lokaciji (eng. *Location-Based Services*, LBS). LBS koristi podatke o lokaciji od pametnih mobilnih uređaja kako bi dostavili servise korisnicima. Korištenje LBS-a je znatno povećalo u određenim područjima, poput logistike, zdravstva, usluge dostavljanja hrane i sl. LBS znatno olakšava život korisnicima ali i donosi puno problema vezano uz privatnost, jer su konstantno praćeni. U nekim slučajevima, pojedinci možda nisu ni svjesni rizika koje donose takve tehnologije i implikacije kako su računaju njihov položaj lokacije i tko ima pristup tim podacima. Samim time, LBS može biti potencijalni rizik za privatnosti korisnika.

5.1.3. Privatnost identiteta

Privatnost identiteta se odnosi na zaštitu informacija vezanih za identitet uređaja, servisa ili samog korisnika protiv napada. Kako sve više i više uređaja je povezano na Internet, postoji veća vjerojatnost za krađom identiteta. Napadači mogu otkriti identitet korisnika kroz razne metode, presretanjem paketa je najčešći oblik napada. Krađa identiteta se može smatrati kao jedan od najvećih rizika kod 5G mreža i općenito kod IoT. Stoga je jako bitno dizajnirati siguran i efikasan mehanizam za upravljanjem identiteta za privatnost identiteta unutar 5G mreža.

5.2. Problemi privatnosti u 5G mrežama

5G mreže imaju široku primjenu u mrežama koju koriste dionici, razne nove tehnologije, poslovni sustavi, sastoji se od puno regulacija i na kraju i samih korisnika. Razmatranje problema privatnosti kod svakog dionika je kompleksan zadatak jer postoje više interesa sa svih strana. Neki od problema privatnosti ćemo istaknuti iz računarstva u oblaku jer su njegovi koncepti bitni za same 5G tehnologije jer ih vrlo često i koristi [18].

5.2.1. End-to-End privatnost podataka

5G mreže podržavaju nekoliko dionika poput operatora, pružatelji usluga, kompanija i nove tehnologije uz nove poslovne modele. Većina dionika koriste računarstvo u oblaku za pohranu, korištenje i procesiranje osobnih informacija od korisnika. Osobni podaci korisnika će biti procesirani i podijeljeni drugim dionicima za njihovu svrhu, i samim time dolazi do kršenja privatnosti. Samim time, 5G mreže moraju postaviti zaštićen pristup za krajnje korisnike kako bi osigurali privatnost korisnika.

5.2.2. Dijeljeno okruženje i gubitak vlasništva osobnih podataka

5G mreže bi nudile dijeljenu mrežnu infrastrukturu ili virtualne mreže kako bi mogli koristiti kontrolirati više aplikacija, poput zdravstva i pametne mreže. Takve dijeljene mrežne infrastrukture mogu predstavljani neautorizirani pristup podacima i njihovu izmjenu. Kako bi to spriječili, efikasna rješenja su potrebna koja bi mogla ponuditi dijeljenju infrastrukturu bez narušavanja privatnosti korisnika. Ako se u dijeljenoj mrežnoj infrastrukturi izgube privatni podaci, tko će biti odgovoran za to, što je također velika briga kod korisnika. Stoga, vlasništvo ili licenca privatnih informacija mora biti dodijeljena između dionicima poput operatora mobilnih mreža, pružateljima usluga i trećim stranama kako bi znali tko je odgovoran u slučaju gubitka osobnih podataka.

5.2.3. Problemi s različitim ciljevima povjerenja

U tipičnim 5G mrežama, mobilni operatori i komunikacijski servisi mogu surađivati i migrirati dio svoje mreže na oblak. U takvim slučajevima, dionici mogu imati različite ciljeve ili prioritete povjerenja prema vlastitim politikama i pravilima. Samim time, možda ne uzmu u obzir sve dijelove privatnosti podataka njihovih korisnika.

5.2.4. Problem u prekograničnom protoku podataka

Zbog globalne digitalizacije, osobni podaci su krvotok modernog tržišta i svojevoljno će prelaziti razne granice. Kako podaci svojevoljno prolaze, vrlo je važno za pristanak pojedinca ili vlade za prijenos podataka uključujući kako je informacija procesirana i gdje se pohranjuje preko granice.

5.2.5. Problem treće strane u 5G mrežama

5G sa IoT donosi novu inovaciju za developere aplikacija da dizajniraju više interaktivne aplikacije za servise koje koriste takve komunikacijske protokole. Kao dizajner aplikacija, pristup 5G mrežama je uobičajeno dopušten, te su u mogućnosti prodati pojedine dijelove privatnih podataka drugim sudionicima, što može narušiti našu privatnost kao korisnici. Pravilo dijeljenja informacija putem računarstva u oblaku je također jedan od problema kod privatnosti podataka.

5.3. Regulatorni ciljevi u zaštiti privatnosti

Regulatorni ciljevi su najvažniji za postizanje privatnosti u 5G mrežama. U početku istraživanja 5G mreža, nije puno direktnih ciljeva definirano za privatnost od strane regulacijskih organizacija, no kasnije nekoliko ciljeva je usvojeno od strane računarstva u oblaku te su primijenjene u 5G mreže [17].

5.3.1. Promicanje jedinstvenog tržišta i ravnoteže interesa globalno

Promicanje jedinstvenog tržišta se odnosi na sve bitne regulatorne ciljeve ili zakonodavne prakse kojima je cilj ojačati i uspostaviti globalne privatne politike bez nekih unutarnjih granica i regulatornih prepreka. Osim toga, propisi o privatnosti bi trebali uravnotežiti interes različitih dionika uključujući potrošače kako bi ostvarili sve prednosti 5G tehnologija i njezinih aplikacija.

5.3.2. Promoviranje prenosivosti podataka

Princip za prenosivost podataka omogućava pojedincima ili tvrtkama da promijene svoje osobne informacije od jednog pružatelja usluga do drugog, ili iz jedne države u drugu bez primjene propisanih standarda, te time je jako bitno promovirati prenosivost podatak u 5G mrežama.

5.3.3. Definiranje propisa privatnosti na globalnom tržištu

U kontekstu globalnog tržišta, nove regulacije privatnosti podataka su potrebne za osiguravanje interoperabilnosti i kompatibilnosti u 5G zasnivanim tehnologijama. Globalno, drugačija regulativna tijela moraju međusobno surađivati i razviti zahtjeve za nove propise o privatnosti.

5.3.4. Promoviranje odgovornosti podataka

Kako se nekoliko korisnika uključuje u 5G mrežu, odgovornost podataka je vrlo bitna. Odgovornost uključuje različite dionike obaveza kako i kada koristiti pojednine osobne podatke I koja će se pravila pridržavati kada su podaci dostupni drugim dionicima. Stoga, svi dionici moraju imati značajne i odgovarajuće mjere koje mogu dokazati odgovornost za osobne podatke.

5.4. Sigurnosni mehanizmi

Prateći novu opću uredbu EU-a o privatnosti podataka (eng. *EU General Data Privacy Regulation,* GDPR), privatnost pojedinca važno je pitanje za sve dionike koji okupljaju i korsite pojedne osobne podatke. Vrlo je važno koristiti efikasne algoritme,sheme i protokole koji će zaštititi što više korisničkih informacija. Sa strane 5G mreža, puno distribucijskih aplikacija i uređaja izmjenjuje poruke putem mreže kroz komunikacijske tehnologije i protokole. Takve aplikacije i uređaji imaju vrlo visok broj poruka koji izmjenjuju preko Interneta. Glavno pitanje je kako se te poruke skupljaju, spremaju i koriste bez otkrivanja privatnih podataka pojedinaca. Neke od ključnih svojstava privatnosti mogu biti korištene u 5G mrežama poput:

5.4.1. Anonimnost

U ovome svojstvu objekt nije sposoban da bude identificiran među ostalim objektima. Anonimnost od kraja do kraja (eng. *End-to-End*) cilja na identitet entiteta da bude sakriven od drugih, čak i u istom anonimnoj grupi.

5.4.2. Nepovezanost

U nepovezanosti, informacije pojedinaca su uobičajno nepovezani između dva ili više korisnika u sistemu. U 5G mrežama, nepovezanost je vrlo važna i može biti postavljena na različite domene 5G mreža, poput SDN-a, VPN (eng. *Virtual Private Network,* VPN), usmjeravanju i krajnim serverima,

5.4.3. Neotkrivenost

U 5G mrežama, nekoliko objekata poput strojeva, aplikacija i korisnika, komuniciraju i razmjenjuju informacije međusobno. Ali napadač može otkriti promet putem prisluškivanja kod razmjene informacija ili podataka. Stoga, objekti i informacije moraju biti skriveni od napadača unutar 5G mreža kako bi osigurali sigurnu i privatnu komunikaciju među njima.

5.4.4. Neopažljivost

U ovome svojsstu, napadač ne bi mogao biti u mogućnosti promatrati da li dva ili više entiteta komuniciraju. Drugačije rečeno, ako entitet je poslao poruku preko komunikacijskog kanala, onda napadač ne smije promatrati ciljanog korisnika te gledati kakve je on informacije slao.

5.4.5. Pseudonimnost

Pseudonim je instance objekta koji je drugačiji od stvarnih imena objekata. U 5G mrežama, obično je uključeno nekoliko dionika. Budući da ti dionici imaju pristup osobnim podacima, pametni objekti moraju imati nekoliko instanci. Te instance moraju biti samo poznati uključenim entitetima koji razmjenjuju informacije sa pametnim objektima.

ZAKLJUČAK

5G mreže se razvijaju vrlo velikom brzinom. Samim time se i razvijaju protokoli i sigurnosni mehanizmi koji čine komunikaciju sigurnom. No također se i razvijaju razne vrste novih napada koji nisu postojali u prošlim generacijama ili su pak unaprijeđene za nove potrebe. Neke od sigurnosnih prijetnji opisano je kroz prethodna poglavlja te kako oni rade i koja je njihova funkcionalnost . Spomenuti su i sigurnosni mehanizmi i mjere sigurnosti koje služe da upravo takvi napadi se ne dogode i da omoguće sigurnu komunikaciju unutar 5G mreža. Privatnost je također jako bitan pojam u komunikacijama te se 5G mreže posebno moraju pozabaviti tim pojmom jer razvijanjem novih tehnologija i metoda stavlja privatnost korisnika i privatnost njihovih podataka i informacija na mjesto gdje vrlo lako mogu biti ugrožene. Spomenuta je i njihova važnost, kako se one implementiraju u svakodnevnu i ne svakodnevnu komunikaciju te na što sve posebno administrator neke mreže mora pripaziti. Sama dinamika mobilnih mreža je vrlo dinamična i sve se često mijenja. Isto tako uz svaku novu generaciju ili dolazak novih tehnologija i vremena (poput IoT), mreže moraju biti spremne za adaptaciju i unaprjeđenja. Moraju biti spremne na sve nove mogućnosti što nam nove tehnologije donose ali i izazove koje dolaze s njima. Ipak zaštita sigurnosti i privatnosti na Internetu i u komunikacijama je najbitnija i mora se staviti vrlo visoko na prioritetu važnosti kod implementacije novih mreža i tehnologija. Upravo korištenje prethodno navedenih protokola i sigurnosnih metoda može se ostvariti sigurna komunikacija u 5G mobilnim mrežama. Privatnost podataka se može postići na razne načine, ovisno o razini sigurnosti privatnih podataka koja je potrebna za neku određenu komunikaciju. 5G mobilna mreža koja koristi spoj svega navedenoga u prethodnim poglavljima se može smatrati poprilično sigurnom mrežom u kojoj korisnici mogu komunicirati i sigurno i privatno.

LITERATURA

[1] S. E. Elayoubi, J. S. Bedo, M. Filippou et al., “5G innovations for new business opportunities,” in Mobile World Congress, 5G Infrastructure association, Mobile World Congress, Barcelone, Spain, 2017.

[2] Frauendorf, José Luiz, and Érika Almeida de Souza. "The different architectures used in 1G, 2G, 3G, 4G, and 5G networks." *The Architectural and Technological Revolution of 5G*. Cham: Springer International Publishing, 2022. 83-107.

[3] Peng, Xuena & Wen, Yingyou & Zhao, Hong. (2011). JNW. 6. 823-830. 10.4304/jnw.6.5.823-830.

[4] Asmare, F. M., & Ayalew, L. G. (2023).. *Cogent Engineering*, *10*(1). https://doi.org/10.1080/23311916.2023.2166214

[5]El-Shorbagy, Abdel-moniem. "5G Technology and the Future of Architecture." *Procedia Computer Science* 182 (2021): 121-131.

[6] Rose, Karen, Scott Eldridge, and Lyman Chapin. "The internet of things: An overview." *The internet society (ISOC)* 80.15 (2015): 1-53.

[7]Rodriguez, Jonathan. *Fundamentals of 5G mobile networks*. John Wiley & Sons, 2015.

[8] Arabo, A. and Pranggono, B., ‘Mobile malware and smart device security: trends, challenges and solutions’, Control Systems and Computer Science (CSCS), 2013 19th International Conference on (pp. 526–531). IEEE

[9] Piqueras Jover, R., ‘Security attacks against the availability of LTE mobility networks: Overview and research directions’, Wireless Personal Multimedia Communications (WPMC), 2013 16th International Symposium on (pp. 1–9). IEEE

[10] Forsberg, D., Leping, H., Tsuyoshi, K. and Alanara, S., ‘Enhancing security and privacy in 3GPP E- UTRAN radio interface’, Personal, Indoor and Mobile Radio Communications, 2007. PIMRC 2007. IEEE 18th International Symposium on (pp. 1–5). IEEE.

[11] 3GPP TR 33.820 V8.3.0. 3rd Generation Partnership Project; Technical Specification Group Service and System Aspects; Security of H(e)NB (Release 8), December 2009.

[12] Bassil, R., Chehab, A., Elhajj, I. and Kayssi, A., ‘Signaling oriented denial of service on LTE networks’, Proceedings of the 10th ACM International Symposium on Mobility Management and Wireless Access (pp. 153–158). ACM.

[13] EPC (2014). 3GPP-The Evolved Packet Core. http://www.3gpp.org/technologies/keywords-acronyms/100-the-evolved-packet-core (last accessed 11 December 2014).

[14] Traynor, P., Lin, M., Ongtang, M. et al., 'On cellular botnets: measuring the impact of malicious devices on a cellular network core', Proceedings of the 16th ACM Conference on Computer and Communications Security (pp. 223–234). ACM

[15] Li, F., Peng, W., Huang, C. T. and Zou, X., 'Smartphone strategic sampling in defending enterprise network security', Communications (ICC), 2013 IEEE International Conference on (pp. 2155–2159). IEEE.

[16] DongFeng Fang, Yi Qian, Rose Qingyang Hu, "5G Wireless Network Security and Privacy"

[17] Khan, Rabia, et al. "A survey on security and privacy of 5G technologies: Potential solutions, recent advancements, and future directions." *IEEE Communications Surveys & Tutorials* 22.1 (2019): 196-248.

[18] M. Liyanage, J. Salo, A. Braeken, T. Kumar, S. Seneviratne, and M. Ylianttila, "5G Privacy: Scenarios and Solutions," in IEEE 5G World Forum (5GWF). IEEE, 2018.

SAŽETAK

5G mobilne mreže se koriste svakodnevno, te kako bi ta komunikacija ostala sigurna i privatna, potrebno ju je zaštititi. Bilo to putem same korisničke opreme koja se koristi ili jezgre mrežnih poslužitelja. Napadači uvijek pokušavaju doći na razne načine do privatnih informacija korisnika, poput DDoS napada ili *HeNB Femtocell* napada. Kako bi osigurali mrežu, moraju se koristiti sigurnosne mjere poput kriptografije na fizičkom sloju, autentifikacija. Servisi moraju uvijek biti dostupni, podaci moraju ostati ne promijenjeni te se na siguran način treba obaviti razmjena ključeva. U slučaju privatnosti, koriste se razne tehnike kako bi ju osigurali. Prvenstveno se privatnost korisnika mora osigurati, zatim privatnost same 5G mreže koju koriste. Na kraju se implementiraju sigurnosni mehanizmi poput anonimnosti i nepovezanosti kako bi komunikacija bila i ostala privatna i zaštićena od razne vrste napada na korisnike i njihove podatke.

Ključne riječi: autentifikacija , mobilne mreže, privatnost, protokoli, sigurnost.

ABSTRACT

5G mobile networks are used every day, and in order for this communication to remain secure and private, it needs to be protected. Be it through the user equipment itself being used or the core of the network servers. Attackers always try various ways to get private information of users, such as DDoS attacks or HeNB Femtocell attacks. In order to secure the network, security measures must be used such as cryptography on the physical layer, authentication. Services must always be available, data must remain unchanged and key exchange must be done in a secure manner. In the case of privacy, various techniques are used to ensure it. First of all, the privacy of users must be ensured, then the privacy of the 5G network they use. Finally, security mechanisms such as anonymity and disconnection are implemented so that communication is and remains private and protected from various types of attacks on users and their data.

Keywords: authentication, mobile networks, privacy, protocols, security.