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

SIGURNOSNI ZAHTJEVI I IZAZOVI U 5G POKRETNIM MREŽAMA

Završni rad

Marin Matijašević

Osijek, 2018.

FERIT
FAKULTET ELEKTROTEHNIKE, RAČUNARSTVA I INFORMACIJSKIH TEHNOLOGIJA OSIJEK

Obrazac Z1P - Obrazac za ocjenu završnog rada na preddiplomskom sveučilišnom studiju

Osijek, 16.09.2018.

Odboru za završne i diplomske ispite

Prijedlog ocjene završnog rada

Ime i prezime studenta:	Marin Matijašević
Studij, smjer:	Preddiplomski sveučilišni studij Elektrotehnika i informacijska tehnologija
Mat. br. studenta, godina upisa:	3937, 26.09.2017.
OIB studenta:	72726636341
Mentor:	Izv. prof. dr. sc. Krešimir Grgić
Sumentor:	
Sumentor iz tvrtke:	
Naslov završnog rada:	Sigurnosni zahtjevi i izazovi u 5G pokretnim mrežama
Znanstvena grana rada:	**Telekomunikacije i informatika (zn. polje elektrotehnika)**
Predložena ocjena završnog rada:	Izvrstan (5)
Kratko obrazloženje ocjene prema Kriterijima za ocjenjivanje završnih i diplomskih radova:	Primjena znanja stečenih na fakultetu: 2 bod/boda Postignuti rezultati u odnosu na složenost zadatka: 3 bod/boda Jasnoća pismenog izražavanja: 3 bod/boda Razina samostalnosti: 3 razina
Datum prijedloga ocjene mentora:	16.09.2018.
Datum potvrde ocjene Odbora:	26.09.2018.

Potpis mentora za predaju konačne verzije rada u Studentsku službu pri završetku studija:	Potpis:
	Datum:

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

IZJAVA O ORIGINALNOSTI RADA

Osijek, 26.09.2018.

Ime i prezime studenta:	Marin Matijašević
Studij:	Preddiplomski sveučilišni studij Elektrotehnika i informacijska tehnologija
Mat. br. studenta, godina upisa:	3937, 26.09.2017.
Ephorus podudaranje [%]:	7%

Ovom izjavom izjavljujem da je rad pod nazivom**: Sigurnosni zahtjevi i izazovi u 5G pokretnim mrežama**

izrađen pod vodstvom mentora Izv. 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 studenta:

Sadržaj

1. UVOD 1

1.1. Zadatak završnog rada 1

2. BEŽIČNA KOMUNIKACIJSKA TEHNOLOGIJA 2

2.1. Razvoj pokretnih mreža 3

3. POKRETNA MREŽA PETE GENERACIJE (5G) 5

3.2. Arhitektura 5G mreže 6

3.1.1. 5G Novi radio 7

3.1.3. mmWave 8

3.1.2. 5G NextGen Core Network 9

4. SIGURNOSNI ZAHTJEVI I IZAZOVI U 5G POKRETNIM MREŽAMA 10

4.1. Sigurnosne prijetnje 11

4.1.1. Pasivni i aktivni napadi 11

4.1.2. Prisluškivanje 12

4.1.3. Analiza prometa 12

4.1.4. Ometanje 13

4.1.5. DoS i DDoS 14

4.1.6. MITM 15

4.2. Sigurnosni mehanizmi u 5G mreži 16

4.2.1. Provjera autentičnosti 16

4.2.2. Povjerljivost 17

4.2.3. Dostupnost 19

4.2.4. Integritet 19

4.3. Sigurnost tehnologija primjenjenih u 5G pokretnim mrežama 20

4.3.1. HetNet 20

4.3.2. D2D komunikacija 21

4.3.3. Massive MIMO 22

4.3.4 SDN 23

4.3.6. Internet stvari (IoT) 25

4.4. Sigurnosna arhitektura pokretnih mreža pete generacije 27

4.4.1. Upravljanje identitetima 29

4.4.2. Fleksibilna provjera autentičnosti 29

4.4.3. Smanjenje kompleksnosti kontrolnih protokola 29

5. ZAKLJUČAK 31
LITERATURA 32
Popis i opis korištenih kratica 35
Sažetak 36
Abstract 36
Životopis 37

1. UVOD

Moderan način života zahtjeva automatizaciju gotovo svih aspekata života i povezivanje sve većeg broja uređaja u mrežu, tzv. Internet stvari. Radi se o mreži uređaja koja će omogućiti razvoj pametnih kuća, pametnih gradova, autonomnih vozila i dr. Da bi to bilo moguće ostvariti potrebna je nova peta generacija pokretnih mreža (5G) koja je trenutno u fazi istraživanja i razvoja tehnologija potrebnih za njenu realizaciju. Od pete generacije se očekuje ogroman kapacitet, izrazito mala kašnjenja pri komunikaciji, velike brzine prijenosa i mala potrošnja energije.

Razvoj budućih pokretnih komunikacijskih sustava ovisit će o arhitekturi 5G mreže koja mora biti dobro definirana i spremna nositi se s različitim izazovima. Također, bitan je i sigurnosni aspekt jer svaka nova tehnologija donosi i nove izazove i potencijalne prijetnje. Sigurnosni mehanizmi moraju biti efikasni i zauzimati malo prostora kako bi se mogla ostvariti spomenuta očekivanja.

1.1. Zadatak završnog rada

Napredna svojstva i primjene pete generacije pokretnih mreža postavljaju nove zahtjeve i izazove u području sigurnosne problematike. Potrebno je napraviti detaljan pregled i analizu sigurnosne problematike 5G mreža, prepoznati i opisati postojeće sigurnosne prijetnje, kao i moguće protumjere. Potrebno je vidjeti koji su preostali neriješeni problemi u ovom području, te koje su smjernice ka daljnjem razvoju i rješavanju ovih problema. Potrebno je se posebno osvrnuti na sigurnosnu problematiku u kontekstu 5G mreža kao heterogenih sustava, koji uključuju raznolike tehnologije i modele komunikacije (npr. D2D komunikacija, MIMO, SDN, IoT).

2. BEŽIČNA KOMUNIKACIJSKA TEHNOLOGIJA

Bežična komunikacija predstavlja prijenos informacija između dvaju ili više točaka kroz prostor bez korištenja električnih vodiča. Za ovakvu komunikaciju najčešće se koriste radio valovi na određenim frekvencijama koji putuju kroz prostor i nose informacije, a također se koriste i elektromagnetska bežična tehnologija i svjetlosna tehnologija. Ovisno o jačini odašiljača i prijamnika te načinu izrade razmak između točaka koje komuniciraju može biti mali (Bluetooth) ili jako velik (satelitska komunikacija).

Zbog svog načela prijenosa podatak kroz prostor bežične mreže predstavljaju najnesigurniji aspekt komunikacijskog sustava i jako je bitno na ispravan način osigurati bežičnu komunikaciju kako bi se zadržala funkcionalnost i sigurnost sustava. Sama problematika sigurnosti proizlazi iz činjenice da se bežični signali odašilju svugdje u prostor i dostupni su potencijalnim napadačima. Najčešći načini zaštite su MAC filtriranje, IP filtriranje i uporaba ključa za dekodiranje, međutim ni na ovaj način se ne može potpuno osigurati bežična komunikacija.

Bežična komunikacija ima razne primjene kod pokretnih komunikacija, upravljanja na daljinu, odašiljanja i primanja radio i televizijskog signala, bežičnih mreža računala i dr. U današnje vrijeme se sve više tehnologija bazira na bežičnoj komunikaciji zbog pokretnosti, praktičnosti i manjih troškova prilikom izrade uređaja jer nisu potrebni fizički električni vodiči. Također se sve više se priča i o Internetu stvari (IoT) koji bi trebao povezati svakodnevne uređaje u svrhu lakšeg i bržeg korištenja.

Razvoj bežičnih tehnologija doveo je do ubrzanog razvoja globalnih pokretnih mreža i život je postao gotovo nezamisliv bez mobilnih uređaja. Prema podacima Hrvatske regulatorne agencije za mrežne djelatnosti (HAKOM), u 2017 godini 81,44 posto stanovnika Hrvatske pristupilo je internetu putem pokretne mreže [1]. Sasvim je jasno da će u budućnosti taj postotak biti i veći pa je potreban konstantan razvoj pokretnih tehnologija kako bi se mogla zadovoljiti potražnja.

2.1. Razvoj pokretnih mreža

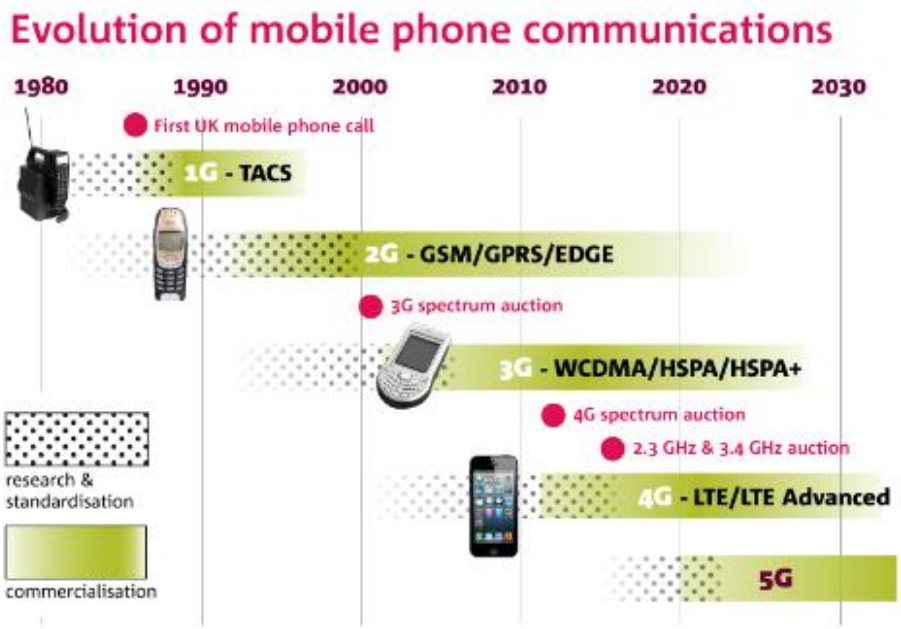
Pokretne komunikacije su se promijenile od sustava sposobnih za prijenos glasovnih razgovora za milijune korisnika diljem svijeta do sustava sposobnih za povezivanje trilijun uređaja za razmjenu podataka. Stoga ne treba posebno naglašavati važnost bežične komunikacije bez koje je život postao nezamisliv.Od pojave pokretnih mreža konstantno se povećavao broj korisnika i veličine podataka koji se prenose te su se i tehnologije tome prilagođavale. Tehnologije su razvijane u generacijama od prve generacije (1G) do četvrte generacije (4G). Svaka nova generacija bila je unaprijeđena prethodna generacija i prilagođena novim tehnologijama.

Prva generacija, 1G: Pojavljuje se krajem sedamdesetih godina prošlog stoljeća i donosi nam mobilne uređaje koji su bili analogni i bili su prvi mobilni telefoni ikad korišteni. Iako revolucionarni u svoje vrijeme, ponudili su malu efikasnost spektra i razinu sigurnosti. Počele su se koristiti bazne stanice preko kojih su korisnici mogli međusobno komunicirati i kretati se kroz prostor koji su pokrivale. Prva komercijalna mobilna mreža puštena je u rad 1979. godine u Japanu.

Druga generacija, 2G: Generacija je koja se bazira na digitalnoj tehnologiji i nudi puno veću spektralnu efikasnost, sigurnost i neke nove značajke kao što su tekstualne poruke. Digitalno kodiranje je također poboljšalo kvalitetu glasovnih razgovora i smanjilo šum. Globalno je lansirana preko GSM standarda u Finskoj 1991. godine. Prednosti ove generacije bili su digitalni signali koji su zahtijevali manju potrošnju energije pa su baterije mobilnih uređaja trajale duže. U razdoblju 2G pokretne mreže prvo je nastala GPRS tehnologija koja je pružala brzine prijenosa podataka od 56 kbit/s do 115 kbit/s , a zatim EDGE tehnologija koja je brzinu povećala na 384 kbit/s.

Treća generacija, 3G: Cilj ove generacije je bio pružiti velike brzine podatkovnog prometa. Predstavljena je 1998. godine i originalno je omogućavala brzine do 14 Mbit/s. Glavna razlika u odnosu na prijašnje generacije bila je početak korištenja komutacije paketa umjesto dosadašnje komutacije kanala za prijenos podataka. Početkom 2000. godine pojavljuje se HSDPA koji omogućuje brzine do 14 Mbit/s.

Četvrta generacija, 4G: Tehnologija potpuno bazirana na IP protokolu te omogućava brzine do 1 Gbps. Razvijena je 2008. godine s ciljem omogućavanja poziva preko internet protokola (IP), mobilne televizije visoke razlučivosti, 3D televizije i dr. Tehnologije bazirane na četvrtoj generaciji pokretnih mreža su WiMAX, LTE i VoIP. Brzine koje se postižu su do 128 Mbit/s.



Slika 2.1.1. Evolucija pokretnih mreža [2]

4G/LTE mreža će u sljedećih nekoliko godina biti na svom maksimumu i neće moći zadovoljiti komunikacijske potrebe. Stoga će se morati osmisliti nova tehnologija i arhitektura mreže kako bi se udovoljilo novim zahtjevima.

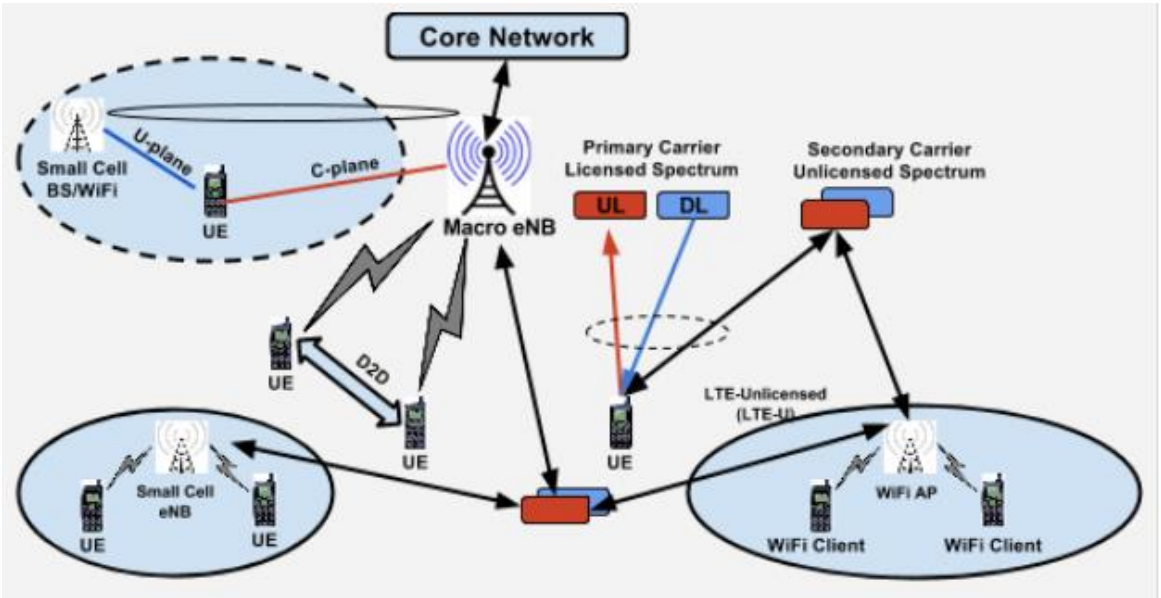
Logično je naslutiti da će sljedeća nadogradnja biti pokretna mreža pete generacije (5G). Ona će morati osigurati značajne napretke u odnosu na prethodne generacije kako bi mobilni operateri uložili sredstva u razvoj novih sustava baziranih na 5G tehnologiji. Postrojenja povezana 5G tehnologijom pružit će puno veći nivo povezanosti i pokrivenosti. Pojavljuje se i termin „WWWW“ koji je skraćenica od „*World Wide Wireless Web*“ što vjerno dočarava ambicije mreže pete generacije koja bi dodatno trebala povezati svijet u kojem živimo.

Da bi 5G tehnologija mogla postići od nje očekivane ciljeve morat će riješiti probleme koje dosadašnje generacije nisu uspjele riješiti. Nove metode povezivanja bit će potrebne jer jedan od glavnih nedostataka prethodnih generacija bio je problem s pokrivenosti signalom, prekidanje komunikacije i slabije performanse na rubu područja koje pokriva signal [3].

3. POKRETNA MREŽA PETE GENERACIJE (5G)

Pokretni komunikacijski sustav pete generacije omogućava daleko bolje performanse nego prijašnje generacije mobilnih komunikacijskih sustava. Nova 5G tehnologija nije samo sljedeća generacija pokretnih mreža, nego je zapravo bitno drugačija. Za razliku od prijašnjih generacija obuhvaća puno više primjena kao što su autonomni automobili, pametni gradovi, Internet stvari, kontrola na daljinu skoro bez ikakvog kašnjenja i mnoge druge stvari. Novi 5G mobilni sustav omogućit će veće brzine prijenosa, ogroman kapacitet, veliku pokrivenost i bolju povezanost [3]. Skratit će se udaljenosti na koju su signali odašiljani i smanjit će se kašnjenja u prijenosu. Očekuje se da kašnjenje bude manje od 1 milisekunde što je poboljšanje s dosadašnjih 25 milisekundi koje su bile kod 4G tehnologije. Ovaj aspekt je bitan za razvoj tehnologija koje zahtijevaju komunikaciju u stvarnom vremenu.

Također za razliku od ostalih mrežnih nadogradnji, 5G će raditi preko manjih antena koje se mogu montirati na stupove javne rasvjete, zgrade i sl. , umjesto velikih antenskih tornjeva koji su bili potrebni do sada. Da bi ovo bilo moguće potrebno je izgraditi heterogenu mrežu koja će međusobno povezati različite odašiljačke tehnologije (Slika 3.1.).

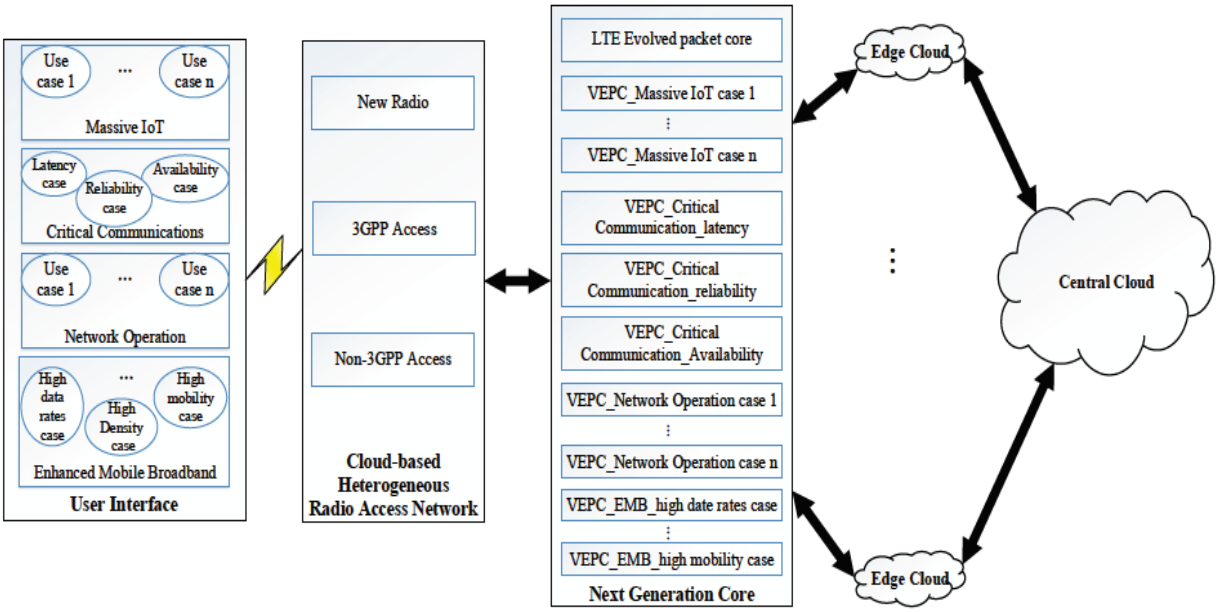


Slika 3.1. Heterogena mreža [4]

Trenutno je razvoj 5G tehnologije u ranoj fazi. Mnoge kompanije istražuju tehnologije koje bi se mogle iskoristiti za stvaranje ovakvog komunikacijskog sustava. Sveučilišta diljem svijeta sve više vremena ulažu u razvoj 5G tehnologije jer je sad potpuno jasno da je ona budućnost.

3.2. Arhitektura 5G mreže

Pokretna mreža pete generacije suočit će se s dosad neviđenim izazovima i stoga će njezina arhitektura biti pravo čudo moderne tehnologije. Mreža će se općenito sastojati od korisničkog sučelja (*User Interface*), heterogene radio pristupne mreže bazirane na virtualnom oblaku (*Cloud-based Heterogeneous Radio Access Network*), jezgre nove generacije (*Next Generation Core*), rubnih oblaka (*Edge Cloud*) i centralnog oblaka (*Central Cloud*) (Slika 3.2.1.).



Slika 3.2.1. Generalna arhitektura za 5G mrežu [6]

Jezgra nove generacije će biti bazirana na oblaku koji koristi slaganje mreže (*Network slicing*), softverski definirano umrežavanje (SDN - *Software Defined Networking*) i virtualizacija mrežnih funkcija (NFV - *Network Functions Virtualisation)* kako bi podržao razne primjene. SDN i NFV će se koristiti kao virtuala paketna jezgra (VEPC - *Virtual Evolved Packet Core*) koja se sastoji od modularizirane mrežne funkcije i novi je oblik EPC-a bazirana na slaganju mreže. Očekuje se da će jezgra nove generacije biti samostalna, te takvo odvajanje kontrole i korisnika je važno za ostvarivanje fleksibilne i prilagodljive arhitekture.

Heterogena radio pristupna mreža može kombinirati virtualizaciju, centralizaciju i koordinaciju za efektivnu i fleksibilnu raspodjelu resursa. Ovdje će se uz 3GPP pristup i ne 3GPP pristup (*non-3GPP*), dodat još i nove radio tehnologije kako bi se što efikasnije iskoristio spektar. Nove radio tehnologije mogu podržavati razne nove primjene u 5G mreži kao što su masivno polje antena (mMIMO), heterogena mreža (HetNet) i izravna komunikacija između uređaja (D2D). Rubni oblak je podijeljen kako bi usluga bila poboljšana, a pogotovo da bi se smanjilo kašnjenje. Dok centralni oblak može implementirati globalno dijeljenje podatka i centraliziranu kontrolu [5].

3.1.1. 5G Novi radio

5G novi radio (5G NR) je nova odašiljačka tehnologija koja će biti primijenjena u 5G mreži. Razvoj 5G NR je ključan za rad pete generacije mobilnih komunikacijskih sustava i razvijen je na temelju potreba koje 5G mreža mora zadovoljiti. Sastoji se od različitih elemenata koji su puno fleksibilniji i imaju mogućnosti prilagođavanja izazovima koji se konstantno mijenjaju. 5G NR koristi modulaciju, valne oblike i pristupne tehnologije kako bi sustavu omogućili veću brzinu, malo kašnjenje i bolju energetsku učinkovitost. Postoji nekoliko bitnih tehnika za realizaciju 5G NR:

Novi radio spektar: Spektar frekvencija koje će biti najviše korištene u ranijoj fazi je između 3.3 GHz – 3.8 GHz i 4.4 GHz – 5.0 GHz dok će se kasnije spektar proširiti do čak 86 GHz. Prednost visokih frekvencijskih pojasa je njihova širina spektra koja će omogućiti puno veće brzine prijenosa podataka, a nedostatak je manji domet.

Usmjeravanje signalnih snopova: Tehnologija koja omogućava da snop signala iz bazne stanice bude usmjeren direktno prema mobilnom uređaju. Na ovaj način optimalni signal može biti prenesen do mobilnog uređaja dok se ujedno izbjegava interferencija s drugim uređajima.

Tehnike dijeljenog spektra: Dobar dio frekvencijskog spektra nije efikasno iskorišten, stoga se metodom dijeljenja spektra može bolje iskoristiti potencijal mreže. Na ovaj način se poboljšava iskorištenost dostupnog frekvencijskog spektra i samim time se smanjuje kašnjenje i povećavaju brzine prijenosa podataka.

Sitne ćelije (*Small Cells*): Zbog povećanja potreba za gustoćom mreže kako bi se povezao veliki broj uređaja predlaže se korištenje velikog broja malih baznih stanica. Mreža sitnih ćelija je

grupa baznih stanica niske snage odašiljanja koje koriste milimetarske valove u svrhu povećanja ukupnog mrežnog kapaciteta. Ovakva mreža radi na način da se koordiniraju grupe malih baznih stanica koje međusobno komuniciraju i tako smanjuju utjecaj fizičkih zapreka, slabljenja signala i ostalih poteškoća.

Primjenom ovih tehnika 5G novi radio omogućiti će novoj generaciji pokretne mreže mogućnosti koje do sada nisu bile moguće i donijet će revoluciju u načinu upravljanja komunikacijskim signalima [7].

3.1.3. mmWave

Milimetarski valni spektar predstavlja raspon frekvencijskog spektra između 30 GHz i 300 GHz. Smješten je između infracrvenih valova i mikrovalova te može biti upotrijebljen za bežičnu komunikaciju s velikim brzinama prijenosa. Smatra se da će mmWave uvesti 5G mrežu u budućnost tako što će joj omogućiti veći frekvencijski spektar, veće brzine prijenosa, bolju kvalitetu video sadržaja i multimedije kao i ostalih usluga.

Prije samo par godina mmWave se nije ni razmatrao kao spektar koji se može iskoristiti učinkovito jer je samo mali broj elektroničkih komponenata mogao primati milimetarske valove. Danas, zahvaljujući novim tehnologijama na rubu je da postane ključan za novu generaciju pokretne mreže.

Frekvencije milimetarskog valnog spektra se već koriste za primjene kao što su prijenos video sadržaja visoke kvalitete na pokretne uređaje, ali postoje problemi s visokim frekvencijama. Ti problemi su veliki gubici prilikom širenja prostorom, osjetljivost na prepreke kao što su zgrade i apsorpcija u kapljicama kiše. Ove probleme je moguće riješiti s 5G arhitekturom koja se sastoji od velikog broja malih baznih stanica.

Kratki prijenosni putevi i veliki gubitci prilikom širenja dopuštaju da spektar bude ponovno iskorišten sa smanjenom količinom interferencije između susjednih ćelija smatra profesor Robert Heath sa Sveučilišta u Austinu u Teksasu. Nadalje, gdje su potrebni duži prijenosni putevi, ekstremno kratke valne duljine milimetarskih valova omogućuju malim antenama da koncentriraju signale u usmjerene snopove s jakim pojačanjem da se nadvladaju gubitci širenja u prostor. Kratke valne duljine milimetarskih valova također omogućavaju da se izrade male antene koje stanu u male uređaje [8].

3.1.2. 5G NextGen Core Network

Iako će u početku 5G mreža koristiti LTE i čak 3G mrežnu jezgru cilj je osmisliti novu mrežnu jezgru koja će moći podnijeti veće kapacitete prijenosa podataka uz malo kašnjenje, puno veći broj korisnika i zahtjeva te će morati biti energetski efikasnija. Da bi se sve ovo moglo ostvariti morat će se koristiti neke nove tehnike koje mogu zadovoljiti tražene zahtjeve.

Tehnike koje će se koristiti u novoj jezgri mreže:

SDN (*Software Defined Networking*) – upravljanje mrežom pomoću softvera umjesto hardvera. Ovako će se poboljšati fleksibilnost i efikasnost.

NFV (*Network Functions Virtualisation*) – Koristeći softversku mrežu postojeći hardver se može rekonfigurirati tako da pruži drugačije funkcije.

Slaganje mreže (*Network Slicing*) – S ciljem smanjivanja kašnjenja i bolje efikasnosti mreža se može podijeliti u više slojeva koji obavljaju određene zadatke te se s obzirom na potrebe korisnika koriste.

Svojstva potrebna za realizaciju 5G nove mrežne jezgre su definirana od strane NGMN (*Next Generation Mobile Network Alliance*). NGMN je telekomunikacijsko udruženje mobilnih operatera, dobavljača, proizvođača i razvojnih instituta čije je cilj na temelju iskustva u pokretnim komunikacijama razviti novu generaciju pokretne mreže. Slično kao i 5G NG, nova jezgra će morati zadovoljiti zahtjeve koji se stavljaju pred buduću pokretnu mrežu [9].

4. SIGURNOSNI ZAHTJEVI I IZAZOVI U 5G POKRETNIM MREŽAMA

Uz prednosti koje donosi komunikacijski sustav pete generacije, dolaze i mane u sigurnosnom području. Zbog načina izvedbe s rasprostranjenim odašiljačima i prijamnicima te ograničenom širinom frekvencijskog pojasa, moguće je da se jave neki sigurnosni problemi te je tada teže zadržati autentičnost, integritet i povjerljivost komunikacije. Obujam komunikacije bit će ogroman s velikim brojem uređaja koji međusobno komuniciraju te će i to biti dodatan sigurnosni izazov.

Od 5G mreže očekuje se da zadovolji određene standarde kao što su mala potrošnja, komunikacija u stvarnom vremenu s izrazito malim kašnjenjem, velika pokrivenost područja i dr. i s time su ograničene mogućnosti sigurnosnih rješenja. Za rješavanje ovih problema potrebno je osmisliti nova sigurnosna rješenja koja će biti integrirana u 5G mrežu od samog početka. Također je potrebno razviti fleksibilne sigurnosne mehanizme koji se mogu prilagođavati potencijalno opasnim situacijama. Treba voditi računa i o tome da sigurnosni mehanizmi ne opterećuju sustav previše i da su energetski efikasni zbog prijenosnih uređaja koji imaju ugrađene baterije i s time ograničeno napajanje.

U dosadašnjim generacijama bežičnih mreža dosta se uspješno rješavalo sigurnosne probleme pomoću kodiranja poruka, obostrane autentifikacije pošiljatelja i primatelja i kroz hijerarhiju ključeva (privatni i javni ključ). Međutim pred 5G mrežu se stavljaju veliki izazovi stoga se sigurnosni mehanizmi moraju prilagoditi tome.

Zbog načina na koji se signali odašilju u prostor i lako su dostupni javljaju se različite sigurnosne prijetnje.Neke sigurnosne prijetnje opisane su u ovom poglavlju, a to su prisluškivanje, analiza prometa, ometanje, DoS, DDoS i MITM napad. Također su i navedene sigurnosne usluge koje će pomoći pri zaštiti od navedenih sigurnosnih prijetnji.

4.1. Sigurnosne prijetnje

Zbog same prirode pokretne mreže pete generacije, velikog broja uređaja i obujma komunikacije ovakva mreža je osjetljiva na različite prijetnje i kompromitirajuće radnje kojima se može ugroziti njezin integritet i povjerljivost. Stoga je potrebno prepoznati moguće slabe točke i mane kako bi se primijenile odgovarajuće sigurnosne tehnike.

Prilikom razmatranja mogućih sigurnosnih nedostataka, fokusirat ćemo se fizički sloj i MAC podsloj gdje je ključna razlika u sigurnosti između bežične i žične mreže.

4.1.1. Pasivni i aktivni napadi

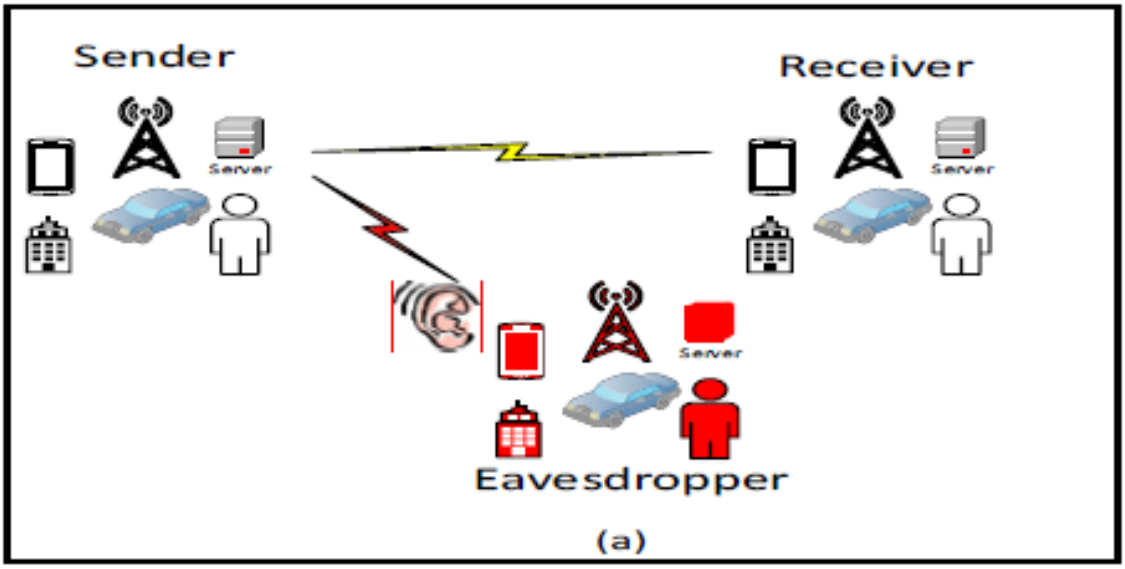
Sigurnosni napadi se mogu podijeliti na pasivne i aktivne. Pasivni napad je pokušaj dolaska do korisnih informacija od korisnika, bez da se utječe na samu mrežu. Cilj pasivnih napada je kršenje povjerljivosti i privatnosti korisnika. Popularni pasivni napadi u mobilnoj mreži su prisluškivanje i analiza prometa. Za razliku od pasivnih napada, aktivni napadi mogu uključivati i promjene povjerljivih podatka ili prekidanje legitimne komunikacije. Tipični aktivni napadi uključuju MITM napad, DoS napad i DDoS napad**.**

Za borbu protiv sigurnosnih napada koriste se dvije kategorije obrambenih mehanizama: kriptografija s novim mrežnim protokolima i sigurnost fizičkog sloja (*Physical Layer Security - PLS*). Kriptografske tehnike su najčešće korišteni sigurnosni mehanizmi, koji će se primijenjeniti na višim slojevima 5G pokretne mreže uz korištenje novih protokola. Moderna kriptografija se sastoji od metoda simetričnog ključa i javnog ključa. Metoda simetričnog ključa se odnosi na metode kodiranja u kojima je tajni ključ poznat pošiljatelju i primatelju te se pomoću njega dešifriraju kodiranje poruke koje su poslane.Metoda javnog ključa ili asimetrična kriptografija, koristi dva različita ključa, jedan se koristi kao javni ključ za kodiranje, a drugi je tajni ključ koji se koristi za dešifriranje poruke.

Razina sigurnosti ovisi o dužini ključa i složenosti algoritma za dekodiranje. Upravljanje i dijeljenje simetričnog ključa je dobro osigurano u dosadašnjim mobilnim mrežama. Zbog kompleksnosti protokola i heterogene mrežne arhitekture u 5G mreži moglo bi doći do težeg upravljanja i dijeljenja ključeva [10].

4.1.2. Prisluškivanje

Prisluškivanje je presretanje poruke između pošiljatelja (*sender*) i primatelja (*receiver*) (Slika 4.1.1.) kako bi se došlo do sadržaja poruke. Radi se o pasivnom napadu koji ne utječe na komunikaciju i teško ga je otkriti. Najčešće korišten način za borbu protiv prisluškivanja je kodiranje. Jačina kodiranja ovisi o jačini algoritma korištenog u kodiranju, ali i o sposobnostima treće strane koja prisluškuje. Tako se može dogoditi da treća strana koristi napredniju tehnologiju i u mogućnosti je prevesti kodiranu poruku. Neke tehnologije koje će biti primijenjene u 5G mreži kao što je HetNet mogu dodatno povećati opasnost od prisluškivanja.



Slika 4.1.1. Prisluškivanje [11]

4.1.3. Analiza prometa

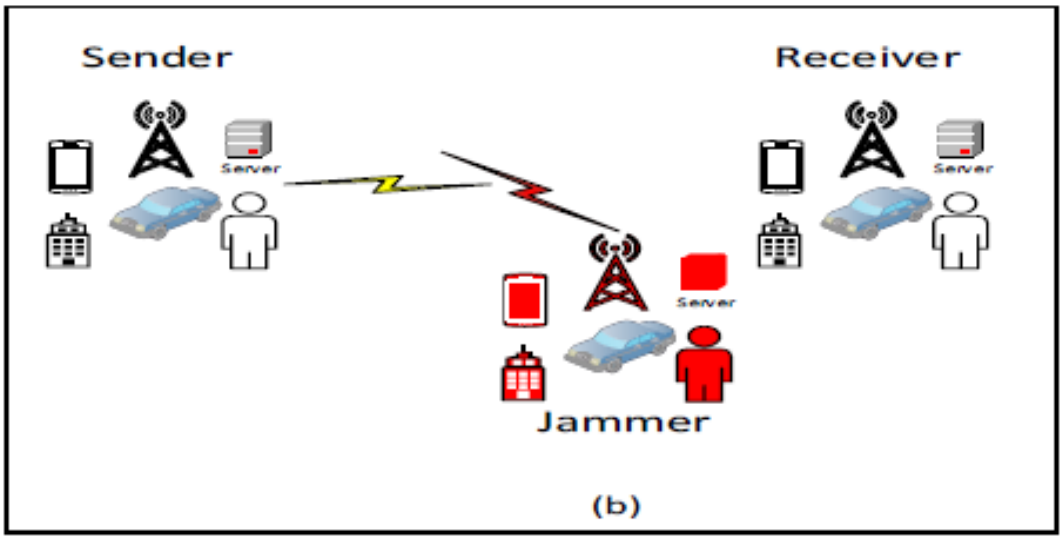
Analiza prometa još je jedan primjer pasivnog napada, kod kojeg je cilj doći do informacija kao što su lokacija ili identitet osoba koje komuniciraju tako što se analizira njihov internet promet. Za analizu prometa često se koriste računalni programi koji nadgledaju komunikaciju i na temelju zakonitosti rekonstruiraju npr. lozinke korisničkih računa, bankovnih kartica itd. U ovom slučaju kodiranje nije nužno rješenje jer se opet može koristi analiza prometa za prepoznavanje pravilnosti u komunikaciji te se tako može doći do traženih informacija.

4.1.4. Ometanje

Za razliku od prisluškivanja i analize prometa ometanje je aktivni napad te služi za ometanje ili potpuno onemogućavanje komunikacije. Ometanje se izvršava preko izvora signala koji se interferira s korisnim signalom komunikacije i onemogućava komunikaciju (Slika 4.2.). Cilj ometanja je onemogućiti komunikaciju i izazvati smetnje u radu nekih uređaja.

Bluetooth, WiFi i slični protokoli imaju ugrađene detektore koji omogućavaju komunikaciju samo kada je kanal slobodan, pa tako bilo kakav prijenos preko kanala onemogućava komunikaciju i na taj način se ometa komunikacija. Neki drugi uređaji za ometanje analiziraju komunikacijske pakete i ovisno o njihovom odredištu, selektivno odašilju šum preko kraja poruke i tako kvare komunikaciju.

Rješenja za ovakve napade se često baziraju na detekciji i otklanjanju izvora smetnje, a mogu se prijemjeniti i metode proširenja spektra izravnim slijedom (*DSSS – Direct Sequence Spread Spectrum*) i proširenja spektra poskakivanjem frekvencija (*FHSS – Frequency Hopping Spread Spectrum*). Ove metode se temelje na proširivanju snage signala na široki frekvencijski pojas te postoji mogućnost da ovakav način zaštite neće odgovarati zahtjevima u 5G pokretnim mrežama.



Slika 4.1.2. Ometanje [11]

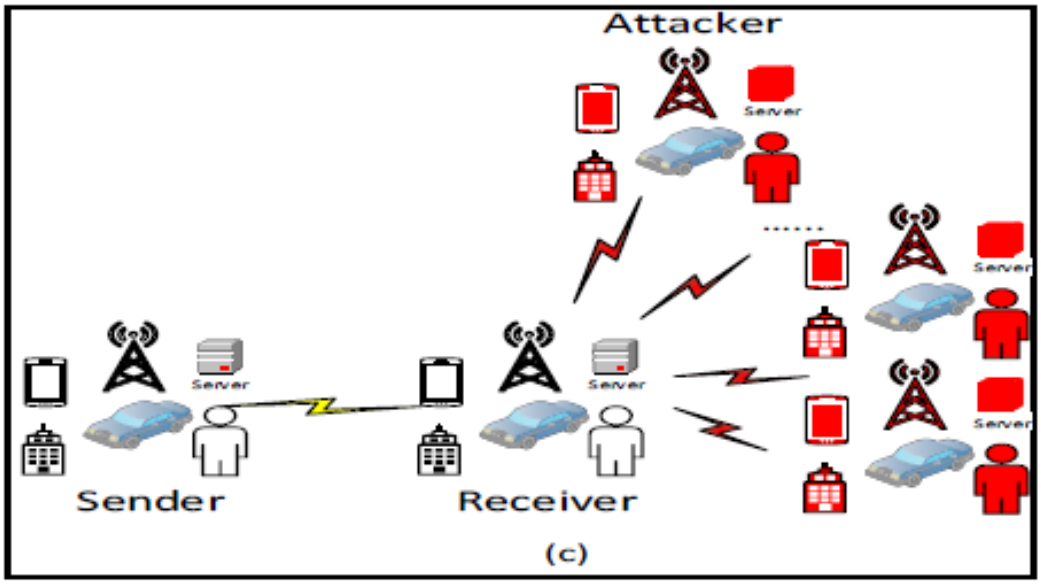
4.1.5. DoS i DDoS

DoS (*Denial of Service*) je napad na mrežu iz jednog izvora koji preplavi server neželjenim paketima (TCP/UDP) s ciljem da preoptereti mrežne resurse. Tako mrežni poslužitelj postaje nepristupačan korisnicima jer su blokirani svi mrežni sadržaji.

DDoS (*Distributed Denial of Service Attack*) je sličan DoS napadu, ali rezultati su puno drugačiji. DDoS napad se vrši preko puno izvora koji su često na različitim lokacijama te ih je teško zaustaviti (Slika 4.3.). Ovakav napad može potpuno srušiti mrežu i puno je opasniji od DoS napada.

DoS i DDoS napadi su aktivni napadi i mogu biti primijenjeni na različitim slojevima mreže. Zbog velikog broja uređaja u 5G mreži DoS i DDoS napadi imaju veliku šansu postati ozbiljne sigurnosne prijetnje za operatere [12].

Detektiranje mogućih napada je trenutno najkorištenija metoda za obranu od DoS i DDoS napada.



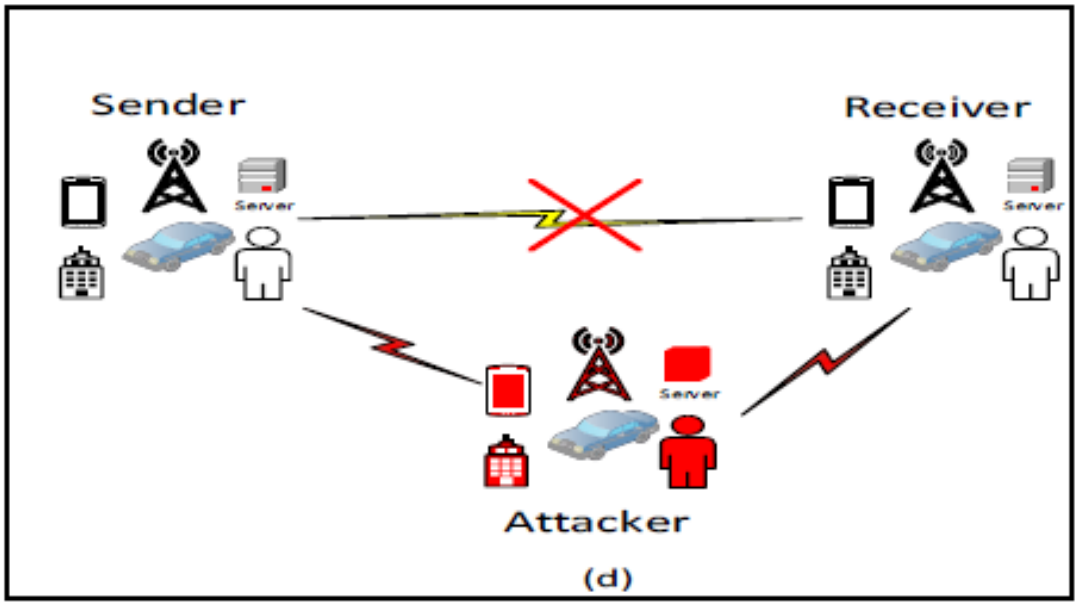
Slika 4.1.3. DDoS napad [11]

4.1.6. MITM

MITM (*Man-In-The-Middle*) napad je napad u kojem napadač tajno preuzima kontrolu nad komunikacijskim kanalom između dvije strane koje komuniciraju (Slika 4.4.). Radi se o jednom od najčešćih oblika napada na povjerljivost komunikacije. Napadač može presresti, izmijeniti i zamijeniti poruku te tako ugroziti sigurnu komunikaciju.

Jedan od načina kako MITM napad može ugroziti komunikaciju je taj da napadač presretne poruku od pošiljatelja, izmjeni je i zatim proslijedi dalje primatelju. Primatelj ne može znati da je poruku poslao napadač i na ovaj način se može doći do osjetljivih podataka kao što su šifre kreditnih kartica, bankovnih računa, internet računa i sl.

Ovo je samo jedan od puno mogućih načina za ugrožavanje komunikacije jer MITM napad je aktivni napad koji se može dogoditi na različitim slojevima mreže. Za osiguravanje od MITM napada predlaže se obostrana provjera autentičnosti primatelja i pošiljatelja kako bi se znalo da poruku nije presrela treća strana.



Slika 4.1.4. MITM napad [11]

4.2. Sigurnosni mehanizmi u 5G mreži

Radi ostvarivanja sigurnosnih zahtjeva navedenih u prethodnom poglavlju potrebno je unaprijediti postojeće sigurnosne mehanizme i osmisliti nova rješenja koja će biti prilagođena primjeni u mreži pete generacije. Nova arhitektura, tehnologija i primjena zahtijevaju poboljšane sigurnosne protokole, malo zauzeće memorije te brzu obradu podataka kako bi se smanjilo kašnjenje u komunikaciji. Sigurnosni mehanizmi također moraju biti efikasni i fleksibilni da bi se mogli prilagoditi različitim sigurnosnim prijetnjama.

Sigurnosne tehnike koje će podići razinu sigurnosti u petoj generaciji pokretnih mreža se sastoje od provjere autentičnosti, održavanje povjerljivosti komunikacije, osiguranja dostupnosti usluge i zadržavanja integriteta.

4.2.1. Provjera autentičnosti

Postoje dvije vrste provjere autentičnosti, a to su provjera osobe i provjera poruke. Provjera osobe služi kao potvrda da su strane koje komuniciraju one za koje se predstavljaju, dok provjera poruke ovjerava poruku koja je poslana. Provjeru je moguće provesti na tri načina: provjerom same mreže, provjerom pružatelja usluge i provjerom i mreže i pružatelja usluge [13]. Ove metode će imati važnu ulogu u 5G mreži kako bi je zaštitili od napad koji joj prijete. Stoga ih je potrebno prilagoditi zahtjevima koje peta generacija mobilnih mreža mora ispuniti.

U prijašnjim generacijama mobilnih mreža provjera autentičnosti se obavljala uglavnom preko metode simetričnog ključa prije nego komunikacija započne između dvije strane koje komuniciraju, ali u 5G mreži zbog nove arhitekture provjera će se morati vršiti i između trećih strana kao što su davatelji usluge. Zbog toga je potrebno osmisliti hibridni fleksibilni sustav provjere autentičnosti.

U softverskoj mreži (SDN) preporučuje se brza provjera autentičnosti koja ne koristi kriptografiju kako bi se povećala efikasnost prilikom velikog broja zahtjeva. Ovu metodu je u usporedbi s digitalnom kriptografijom teško potpuno kompromitirati. Sastoji se od više sigurnosnih slojeva pa je i nivo sigurnosti veći [14].

4.2.2. Povjerljivost

Povjerljivost se sastoji od dva aspekta, povjerljivost podataka i privatnost. Povjerljivost podataka štiti podatke u prijenosu od pasivnih napada tako što ograničava pristup samo na ovlaštene korisnike. Privatnost pak sprječava kontroliranje i utjecanje na informaciju, tj. sprječava se dolazak analitičkih podataka do mogućeg napadača.

Kodiranje podataka najčešća je metoda zaštite povjerljivosti i privatnosti podatka. Ono onemogućuje neovlašten pristup podacima i njihovo neovlašteno korištenje. Metoda simetričnog ključa je često korištena za kodiranje poruka. Njen princip se zasniva na tome da svaka strana koja komunicira ima privatni ključ kojim se dešifrira poruka. Taj ključ se mora sigurno distribuirati kako komunikacija nebi bila kompromitirana. Ova metoda je relativno sigurna dok god napadač ima limitirane računalne mogućnosti i ne može probiti šifru.

Privatnosti u 5G mreži morat će se pridodati puno više pažnje zbog velikog broja spojenih uređaja i osjetljivosti podataka. U mnogim slučajevima odljev podataka može uzrokovati ozbiljne posljedice, npr. zdravstvene informacije mogu otkriti osjetljive podatke ili se podaci o kretanju vozila mogu iskoristiti za praćenje [14].

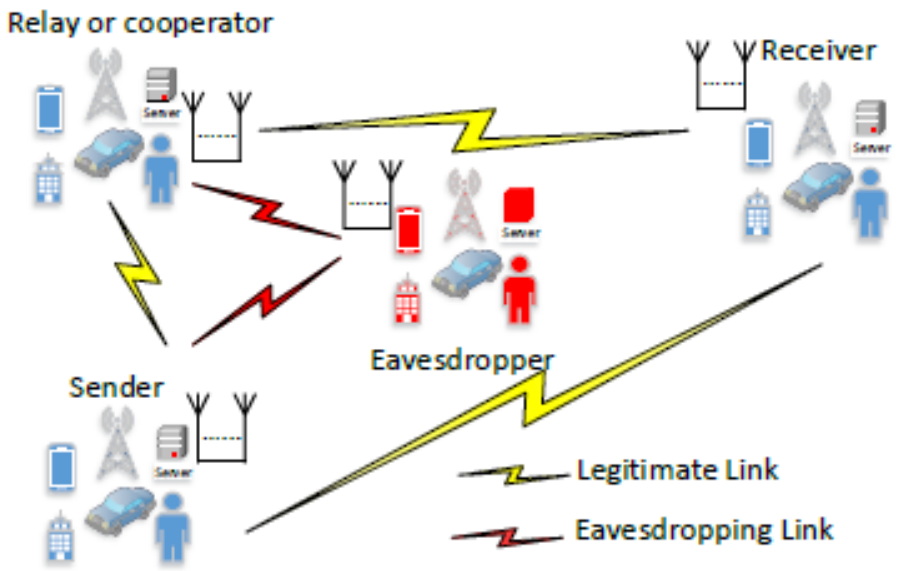
Kako bi se postigao veliki nivo povjerljivosti podataka koji se razmjenjuju u komunikaciji potrebne su sljedeće metode:

Upravljanje snagom

Upravljanje snagom signala bitno je kako bi se otežalo ili onemogućilo rekonstruiranje signala komunikacije te se tako izbjeglo presretanje i prisluškivanje komunikacije neovlaštenim osobama. Snaga signala se prilagođava smjeru komunikacije i cilj je da signal nosioc podataka dođe do uređaja kojem je namijenjen. Na ovaj način se može značajno smanjiti količina podataka dostupnih neovlaštenim osobama.

Sigurnosni relej

Komunikacija između dvije osobe može se odvijati preko posrednika odnosno releja koji pomaže pošiljatelju da sigurno prenese podatke do primatelja (Slika 4.2.1.).



Slika 4.2.1. Sigurnosni relej [15]

Umjetni šum

Generiranje umjetnog šuma je jedna od metoda koje se mogu iskoristiti kao zaštita podataka od neovlaštenog pristupa. Umjetni šum se generira zajedno s korisnim signalom kako bi se eventualnom napadaču otežao pristup podacima.

Obrada signala

Modulacija signala najčešći je oblik obrade signala u predajniku kako bi se povećao nivo sigurnosti i prilagodilo signal prijenosu kroz određeni medij. U postupku modulacije mijenja se jedan ili više parametara prijenosnog signala. Može se mijenjati amplituda, frekvencija ili faza signala ovisno o potrebama. Na prijemnoj strani se vrši inverzan proces koji se naziva demodulacija i služi za rekonstruiranje originalnog signala.

Kao metoda se može koristiti i rotacija parametra signala gdje se signal komunikacije obradom također može zaštiti tako da se primjeni rotacija npr. faze signala. Bazna stanica u ovom slučaju izmjenjuje fazu signala koji se šalje. Primatelj zna pravilo izmjene faza te ih tako rekonstruira. Napadaču je gotovo nemoguće doći do podataka ukoliko ne zna pravilo izmjene faza.

4.2.3. Dostupnost

Dostupnost se definira kao stupanj koji govori dali je usluga dostupna korisnicima i gdje je dostupna. Dostupnost ocjenjuje robusnost sustava u slučaju raznih napada. Glavni napad na dostupnost je DoS napad koji može onemogućiti korištenje usluga koje mreža pruža. Ometanje također utječe na dostupnost mreže tako što otežava komunikaciju. Veliki broj čvorova 5G mreže potrebnih za IoT predstavljaju veliki izazov u sprječavanju ometanja i DDoS napada kako bi se osigurala dostupnost mreže [14].

4.2.4. Integritet

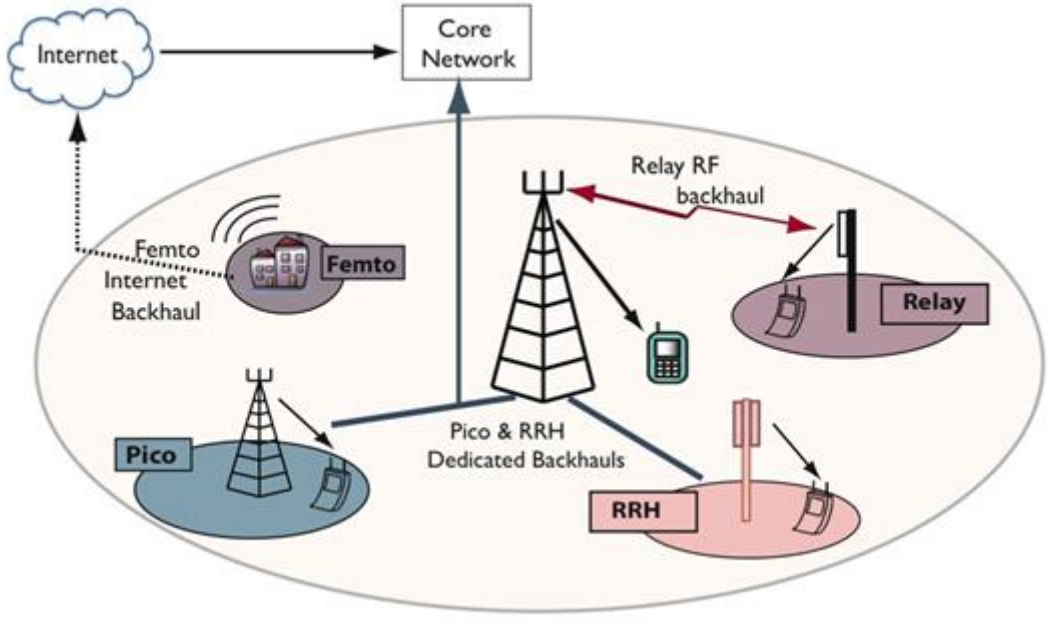
Iako se vrši provjera autentičnosti poruke čija je zadaća provjeriti dali je izvor poruke legitiman, još uvijek je potrebno provjeriti dali je poruka u međuvremenu izmijenjena ili duplicirana. Stoga je bitno uvesti dodatni sigurnosni mehanizam koji će provjeravati integritet poruke. Cilj je spriječiti nepotrebno umnožavanje poruke koja guši sustav ili aktivne napade na komunikaciju čiji je cilj izmijeniti poslanu poruku. Potpuni integritet se može osigurati tako da se obavi obostrana provjera s ključem koji je namjenjen za provjeru integriteta.

4.3. Sigurnost tehnologija primjenjenih u 5G pokretnim mrežama

Mnoge tehnologije će svoju primjenu naći s dolaskom pete generacije pokretnih mreža. Omogućiti će povezivanje raznih svakodnevnih uređaja te će se tako olakšati njihova primjena i poboljšati nivo upravljivosti. Kako bi to bilo moguće moraju se primijeniti komunikacijski i sigurnosni mehanizmi sposobni podržati izrazito veliki broj uređaja povezanih u mrežu. Upravo o njima bit će riječ u ovom poglavlju.

4.3.1. HetNet

HetNet (*Heterogeneous Network*) je tehnika čija je zadaća pružiti veliku pokrivenost bežične mreže i visoku propusnost u 5G sustavu. Radi se o višeslojnom sustavu koji se sastoji od makro, piko ili femto ćelija koje omogućavaju visoku pokrivenost signalom od otvorenog prostora do zgrada, kuća i podzemnih područja (Slika 4.3.1). Upotrebom ove tehnike poboljšat će se kapacitet mreže, širina pokrivenosti, energetska efikasnost i iskoristivost spektra.
HetNet ima i svojih mana u odnosu na jednoslojnu mobilnu mrežu pa su tako korisnici izloženiji prisluškivanju. Kako bi se izbjeglo prisluškivanje predlaže se ograničavanje snage signala koji se odašilje, ali snaga signala mora biti dovoljno jaka kako bi mobili uređaji ostali aktivni. Također, zbog velike gustoće malih ćelija, informacije kao što su njegova lokacija se mogu lako otkriti.



Slika 4.3.1. Heterogena mreža [16]

4.3.2. D2D komunikacija

D2D (*Device-to-device*) je vrsta komunikacije izravno između dva ili više uređaja bez korištenja resursa mreže. Kod dosadašnjih generacija je bila potrebna upotreba baznih stanica za komunikaciju i tako je mreža gubila na efikasnosti. Stoga ovaj način komunikacije omogućava efikasniju upotrebu spektra u 5G mreži. Osim izravne komunikacije između dva uređaja D2D će omogućiti scenarije u kojima uređaji komuniciraju preko drugih uređaja na njihovom pravcu komuniciranja i tako povećati doseg [17]. Ovaj način će također smanjiti potrošnju energije i kašnjenje jer neće biti potrebno komuniciranje preko posrednika (bazne stanice) nego će informacije teći izravno između uređaja.

Međutim nedostatak sigurnosti u D2D komunikaciji čini ovakvu vrstu komunikacije manje sigurnom od uobičajene mrežne komunikacije. U prijašnjim načinima komunikacije informacije su se štitile od prisluškivanja, napada, izmjene informacija i dr. kodirajući poruku koja se šalje i zatim dekodirajući je s dogovorenim ključem. Ključ se dijeli između dvije strane koje komuniciraju, može biti simetrični ili javni. Distribucija ključa se obavljala preko bazne stanice ili neke pouzdane treće strane. Međutim u D2D komunikaciji, strane komuniciraju izravno bez posredstva mreže i bit će teže podijeliti ključ na siguran način. Zbog velikog broja mobilnih uređaja, raznih proizvođača i standarda teško je skriveni ključ ugraditi u uređaje prije same komunikacije [18**].**

Kako bi se poboljšala efikasnost spektra koristi se tehnika dinamičkog pristupa spektru (*DSA – Dynamic Spectrum Access*). Suradnja između dva D2D čvora je popularan način za osiguravanje komunikacije od prisluškivanja. Odašiljači koji surađuju i koji imaju zajedničkog primatelja također međusobnom suradnjom povećavaju i pouzdanost komunikacije. Ova sigurnosna metoda se može primijeniti za razne scenarije u D2D komunikaciji pošto nema nekih specijalnih zahtjeva [19].

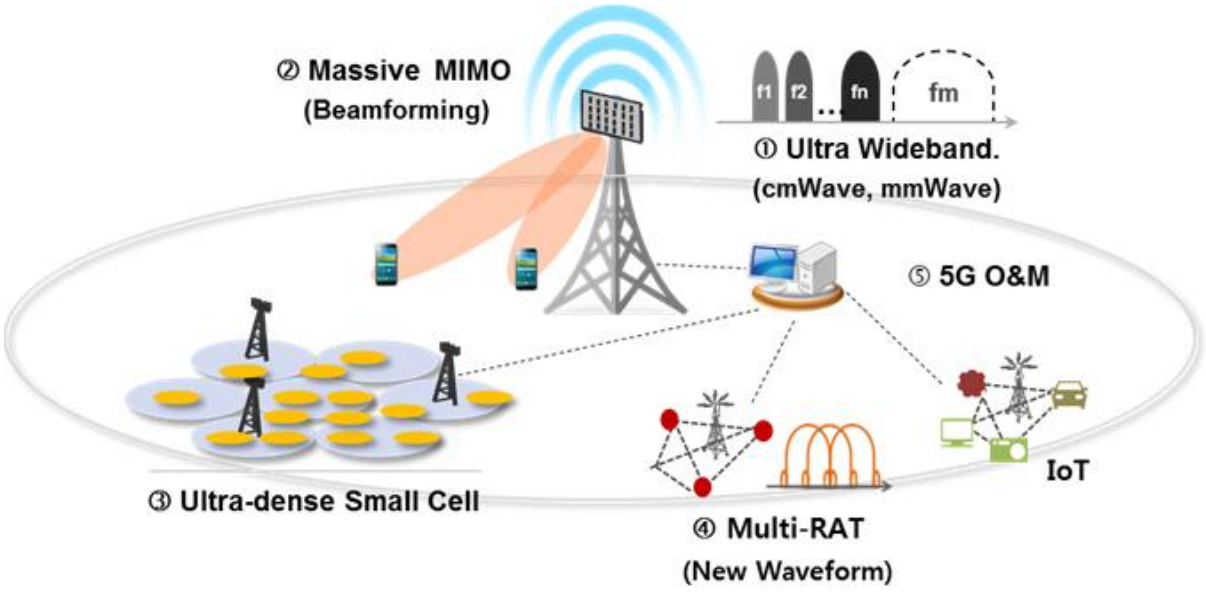
Uz suradnju, kontrola potrošnje energije i pristup kanalu su također bitni za sigurnost D2D komunikacije. Optimalna potrošnja energije i pristup kanalu D2D veze pridonijet će povećanju broja korisnika mobilnih usluga i sigurnosti fizičkog sloja [20].

4.3.3. Massive MIMO

MIMO (*Multiple-Input Multiple-Output*) je polje antena koje se trenutni koristi, ali se sastoji od nekoliko antena. U budućoj 5G mreži pojavljuje se pojam massive MIMO (mMIMO) koji označava polje antena s tisućama manjih antena koje su raspoređene u prostoru (Slika 4.3.2.). Zasad je zbog mobilnih frekvencija valna duljina takva da antene moraju biti dosta velike i ne praktične za masovno postavljanje. Kako bi riješili ovaj problem morat će se povećati frekvencije kako bi se smanjila valna duljina, a s time i veličina antena.

Ova tehnologija će povećati efikasnost komunikacijskog kanala, povećati brzinu i veličinu prijenosa podataka te smanjiti potrošnju energije tako što će se moći odašiljati i primati signali manje snage. Antene će biti pokretne i moći će se prilagođavati objektu s kojim komuniciraju.

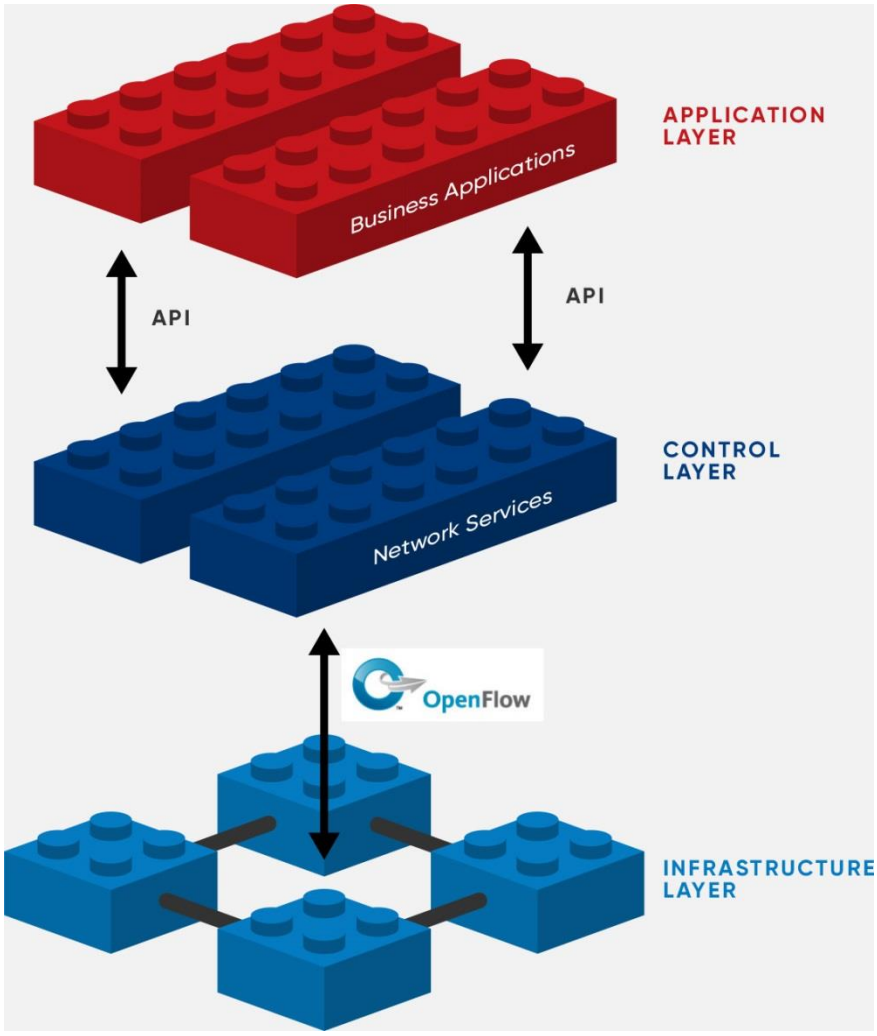
Dosad je feding bio glavni uzrok kašnjenja u telekomunikacijama. On nastaje kada je uređaj iza prepreke te potrebna promjena prijenosnog kanala kako bi se komunikacija uspješno obavila, a to uzrokuje kašnjenje. Kako bi izbjegli fading mMIMO antene se mogu pomicati i prilagođavati situaciji, moguće okrenuti antenu prema zgradi ili nekom drugom objektu te tako reflektirati signal u prostor koji antena inače ne bi mogla pokriti zbog prepreka.



Slika 4.3.2. mMIMO [21]

4.3.4 SDN

SDN (*Software-defined networking*) je tehnologija koja softverski upravlja mrežom kako bi se poboljšalo kontroliranje i svojstva mreže. SDN je za razliku od tradicionalnih mrežnih tehnologija, koje su decentralizirane i složene, puno fleksibilniji i lakša za održavanje. Svrha ove tehnologije je centraliziranje mrežnih resursa odvajanjem kontrolnog od podatkovnog sloja (Slika 4.3.3.). Međutim, centralizacija ima i neke mane kad je riječ o sigurnosti.



Slika 4.3.3. Softverski definirana mreža [22]

Prednosti SDN mreže su globalni pregled mreže koji omogućava centralizaciju i prikupljanje podataka o mrežnom prometu te se tako povećava kontrola nad mrežom. Na ovaj način se lakše detektiraju pogreške i potencijalno opasne situacije koje se mogu izbjeći pravovremenim djelovanjem.

S druge strane postoje sigurnosni problemi kao što su DDoS napadi, MITM napadi i napadi na kontrolni sustav. Centralizacija mreže nosi sa sobom i potencijalne probleme kao što su mogući napadi na kontrolni sustav kojima se kompromitira cijela mreža. Isto tako ogroman broj zahtjeva i korisnika koji će koristiti ovu mrežu predstavljaju veliki sigurnosni izazov koji će morati biti uspješno riješen kako bi se zadržao integritet i funkcionalnost.
Moguće rješenje za napade na kontrolni sustav je repliciranje kontrolera kako bi se potencijalnim napadačima otežao pronalazak onog pravog. Na ovaj način kontrolni sustav će barem donekle biti zaštićen, ali potrebni su naravno i drugi sigurnosni mehanizmi koji će povećati pouzdanost ovakve arhitekture.
Nadalje, osiguravanje paketa u SDN mreži vrši se uz pomoć kodiranja, ali ni to neće biti dovoljno ako se radi o DoS napadima čiji je cilj preopteretiti mrežu s velikim brojem zahtjeva tako da je potrebno uvesti i vremenske oznake preko kojih će se moći prepoznati ovu vrstu napada [23].

4.3.5. NFV

NFV (Network Functions Virtualization) je virtualizacija mrežnih funkcija što znači da se tradicionalne hardverske mrežne funkcije zamjenjuju s računalima čiji softveri pružaju istu funkcionalnost. Koristeći NFV, mreža se lakše proširuje, prilagođava i u mogućnosti je pružiti veću fleksibilnost. Također se smanjuju troškovi održavanja mreže i povećava se energetska učinkovitost.

NFV koristi tradicionalnu serversku virtualizaciju, ali i dodatno proširuje koncept. Na ovaj se način koristi jedan ili više virtualnih uređaja s različitim softverima koji vrše različite procese i tako se ubrzava proces obavljanje mrežnih funkcija. Primjeri funkcija koje mogu biti virtualizirane su: virtualni balans tereta, vatrozidi, uređaji za detekciju upada, ruteri, kontrola pristupa i kontrola naplate.

Mreža koja koristi NFV može se podijeliti na elemente:

VNF (*Virtualized Network Functions*) – Virtualizirane mrežne funkcije uključuju softvere korištene za njihovu virtualizaciju kako bi mogli obavljati potrebne funkcije. One se primjenjuju na hardver koji se naziva infrastruktura virtualiziranih mrežnih funkcija (*Network Function Virtualization Infrastructure*). NFV infrastruktura se može nalaziti na nekoliko fizičkih lokacija te tako operateri mogu postaviti mrežne centre na prikladne lokacije.

NFV-MANO (*Network Functions Virtualization Management and Network Orchestration*) – se sastoji od različitih funkcijskih blokova koji omogućavaju razmjenu, manipulaciju i spremanje informacija potrebnih za upravljanje mrežom na efikasan način.

NFVI i NFV-MANO dijelovi mreže su ugrađeni u NFV platformu koja koristi značajke za upravljanje mrežom, nadgledanje različitih komponenti, oporavak od kvarova i pružanje sigurnosti.

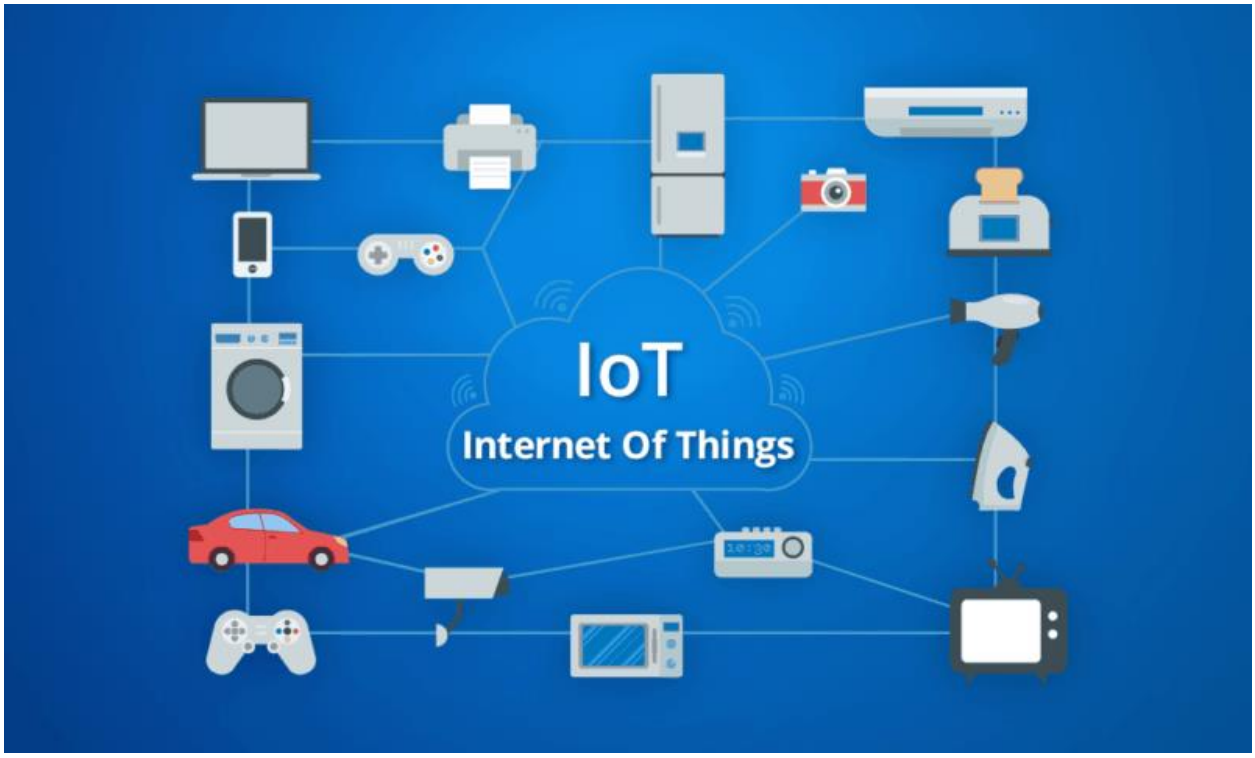
Često se poistovjećuju pojmovi SDN i NFV, ali zapravo se radi o različitim tehnologijama. SDN zamjenjuje standardne mrežne protokole s programiranom centraliziranom mrežnom kontrolom te tako pojednostavljuje složene mrežne protokole. S druge strane NFV razdvaja mrežne funkcije od privatnih hardvera . Stoga ove dvije tehnologije mogu biti primijenjene u istoj mreži u isto vrijeme [24].

4.3.6. Internet stvari (IoT)

Internet stvari (IoT) nadolazeća je vrsta mreže koja bi trebala povezati objekte i olakšati međusobnu interakciju raznih uređaja („stvari“) (Slika 4.3.4.). IoT će pretvoriti naše gradove, kuće, vozila u pametne i međusobno povezane. Sa svime će se moći upravljati na daljinu i bit ćemo svjesni svega što se događa te ćemo moći efikasnije i racionalnije raspolagati mrežnim resursima. Procjenjuje se da će u budućnosti 200 milijardi uređaja biti međusobno povezano u mrežu stvari [25]. Internet stvari će donijeti brojne prednosti i u industriju pa će se tako povećati produktivnost strojeva i zaposlenika, lakše će se nadgledati proizvodnja, uštedjet će se vrijeme i novac, proizvodnja će biti efikasnija i povezat će se različite grane proizvodnje.
Nakon svega navedenog sasvim je jasno da je cilj što prije izgraditi mrežu koja može podnijeti Internet stvari i zato se puno ulaže u razvoj novih tehnologija.

Zbog ograničene računalne moći IoT čvorova, sigurnosna usluga 5G uređaja mora biti efikasna i zauzimati malo prostora. Prosljeđivanje (*relaying*) se razmatra kao efikasni mehanizam u IoT mreži za uštedu energije i proširenja pokrivenosti prijenosa [23].
IoT sustav je ranjiv na ometanje (*jamming*) koje utječe na trajanje baterija ili potrošnju energije uređaja koji su izloženi ometanju i tako se smanjuje njihova radna efikasnost. Također ometanje može dovesti i do DoS napada koji je najčešći napad na bežičnu mrežu.

Postoji nekoliko rješenja protiv ometanja koja se mogu primijeniti u IoT mreži, međutim većina njih nije prikladna za ovu vrstu mreže zbog dva glavna razloga. Prvo, IoT uređaji nemaju velike procesorske resurse, prostor za pohranu je ograničen te nisu sposobni prilagoditi se kompleksnim sigurnosnim mehanizmima i protokolima. Nadalje kao drugi razlog navodi se heterogena priroda mreže s različitim čvorovima čije karakteristike otežavaju primjenu univerzalnih sigurnosnih mehanizama. Kao rješenje ovog problema moguće je uvesti više razina važnosti pojedinih čvorova te bi se oni prilagođavali važnosti posla koji obavljaju. Tako bi važniji čvorovi mogli upotrijebiti više energije od ostalih kako bi nadvladali ometanje korištenjem jačih signala [27].



Slika 4.3.4. Internet stvari [26]

4.4. Sigurnosna arhitektura pokretnih mreža pete generacije

Sigurnosna arhitektura mora se prilagoditi mrežnoj arhitekturi kao i izazovima koji su stavljeni pred 5G mrežu. Stoga je potrebno osmisliti efikasnu sigurnosnu strukturu koja ne opterećuje mrežu i prilagođava se trenutnim potrebama. Potrebno je da sigurnosna arhitektura bude otporna na razne prijetnje i radnje koje će ugroziti sigurnost korisnika i podataka koji se razmjenjuju.

Pošto se od pokretne mreže pete generacije očekuje da podržava veliki broj korisnika i uređaja i taj aspekt se mora uzeti u obzir prilikom osmišljavanja sigurnosnih mehanizama koji će se primjeniti. Mreža pete generacije povezivat će do sada neviđen broj uređaja i korisnika te i sigurnosni mehanizmi moraju biti napredniji od dosadašnjih. U obzir se mora uzeti i potreba za malim kašnjenjem zbog sustava kao što su pametni automobili te i sigurnosni mehanizmi moraju biti brzi i efikasni.

Predlaže se razdvajanje kontrolnog sloja od podatkovnog kako bi se podaci mogli kodirati da budu fleksibilniji. Na ovaj način se može bolje upravljati mrežom i mrežnim prometom te se ubrzati proces provjere sigurnosnih aspekata.

Glavne mrežne funkcije koje se nalaze u kontrolnom sloju su:

AMF (*Access and mobility management function*): funkcija koja upravlja pristup i mobilnost u LTE pokretnoj mreži. Ova funkcija ovisi o različitim primjenama te funkcija upravljanja mobilnosti nije potrebna u fiksnim primjenama.

SMF (*Session management function*): funkcija je koja upravlja sjednicama. Za jedan AMF više funkcija koje upravljaju sjednicama mogu upravljati različitim sjednicama jednog korisnika.

UDM (*Unified data management*): upravlja korisnikovim podacima i profilima za fiksni i mobilni pristup u mreži nove generacije.

PCF (*Policy control function*): ova funkcija omogućava roaming i upravljanje mobilnošću , kvalitetu usluge i slaganje mreže. PCF kontrolira AMF i SMF.

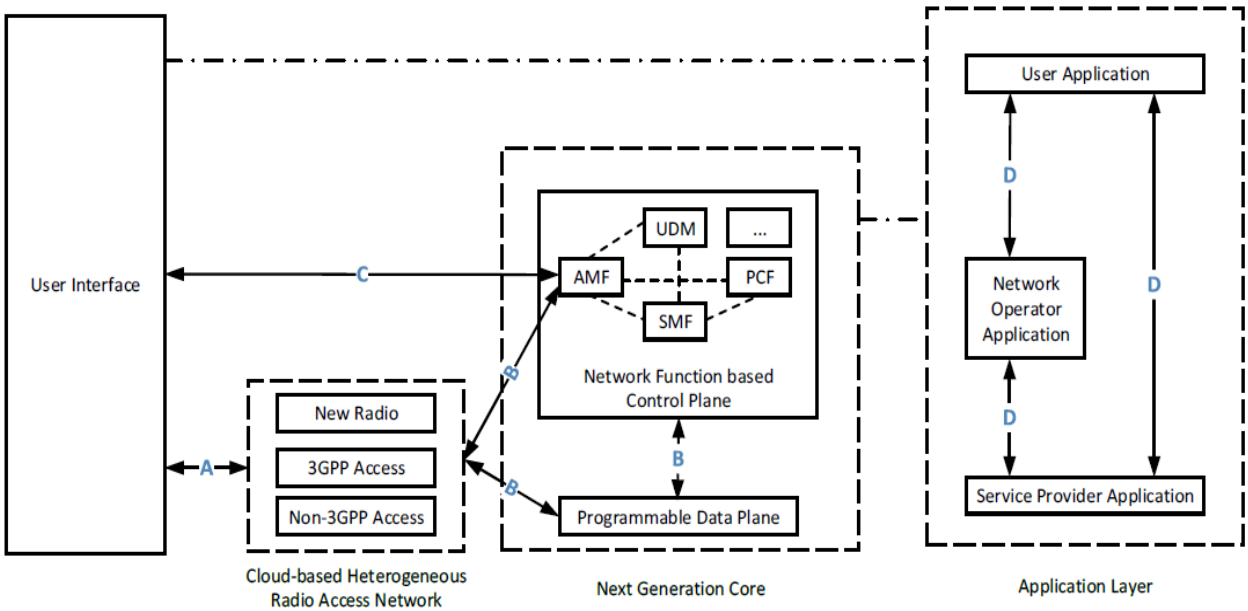
Slično kao i u prijašnjim generacija mreža postoje četiri sigurnosne domene koje su označene na slici 4.4.1. kao A,B,C,D.:

Sigurnost pristupa mreži (A) se sastoji od sigurnosnih značajki koje omogućavaju korisniku pristup mreži sigurno i zaštićeno od različitih napada. Kako se u novom fizičkom sloju koriste tehnologije kao MIMO, HetNet, D2D i ostale stvaraju se i novi sigurnosni zahtjevi koje je potrebno riješiti.

Sigurnost mrežne domene (B) sastoji se od sigurnosnih značajki koje štite od napada na žični dio mreže i onemogućuju razmjenu podataka na siguran način. Ovaj nivo sigurnosti nalazi se između radio-pristupne mreže i jezgre nove generacije, kontrolnog sloja i korisničkog sloja. Provjera autentičnosti osobe , povjerljivost podataka i integritet podataka su glavne sigurnosne usluge na ovom nivou sigurnosti.

Sigurnost korisničke domene (C) se sastoji od sigurnosnih značajki koje omogućavaju obostranu provjeru između korisničkog sučelja i jezgre nove generacije prije nego kontrolni sloj pristupi korisničkom sučelju. Provjera autentičnosti je glavni cilj ovog sigurnosnog nivoa.

Sigurnost domene primjene (D) je skup sigurnosnih značajki koje osiguravaju sigurnost poruka koje se izmjenjuju između zahtjeva na korisničkom sučelju, između korisničkog sučelja i pružatelja usluge kao i između korisnika i mrežnog operatera [28].



Slika 4.4.1. Predložena sigurnosna arhitektura [29]

4.4.1. Upravljanje identitetima

U prijašnjim generacijama pokretnih mreža, upravljanje identiteta se vršilo preko USIM kartica. Međutim u 5G pokretnoj mreži postojat će mnogi uređaj koji ne podržavaju USIM kartice. Također u 5G mreži anonimnost uređaja je potrebna zbog moguće zlouporabe pa će i s tog aspekta upravljanje identitetima biti drugačije nego do sada.

S velikim brojem povezanih uređaja i raznim primjenama efikasno upravljanje identitetima bit će potrebno kako bi se osigurala učinkovitost usluge. Dosadašnji način upravljanja koji je vršila mreža neće se moći primijeniti kod nekih uređaja kao što su uređaji u pametnim kućama. Moguće rješenje ovog problema je korisnički-bazirano upravljanje identitetima što znači da jedan korisnik može imati više uređaja te sam bira kojem je uređaju dopušten pristup mreži i uslugama

Osim identiteta uređaja koji je unikatan za pojedini uređaj postoji i identitet usluge koji se dodjeljuje od strane mrežnog poslužitelja. Nadalje za provjerene usluge može se uvesti ujedinjeno upravljanje identitetima kako bi se ubrzao i pojednostavio proces identifikacije i poboljšao doživljaj korisnika.

4.4.2. Fleksibilna provjera autentičnosti

Fleksibilna provjera autentičnosti je potrebna u 5G pokretnoj mreži kako bi se osigurala sigurnost i kvaliteta usluge u isto vrijeme. Obostrana provjera autentičnosti se dosad obavljala između korisnika i mreže, međutim u 5G mreži neke primjene mogu zahtijevati i provjeru pružatelja usluge i korisnika stoga je jasna bitnost fleksibilne provjere autentičnosti.

4.4.3. Smanjenje kompleksnosti kontrolnih protokola

Smanjenje kompleksnosti protokola u svakom slučaju doprinosi povećanju efikasnosti. Čak i kod jednostavnih prijenosa podataka, potrebni su protokoli koji osiguravaju da podaci budu uspješno preneseni. Kontrolni paketi se pri komunikaciji šalju između baznih stanica i uređaja. Ovi paketi čine 46 posto prenesenih paketa i značajan su teret za mrežu. Stoga smanjenje istih predstavlja veliki napredak u efikasnosti posebno kod IoT uređaja i D2D

komunikacije. Konstantno komuniciranje malih uređaja koji ovise o energiji iz vlastitih baterija s baznom stanicom samo zbog kontrolnih paketa nije energetski efikasno. Stoga je potrebno konfigurirati kada i kako će uređaji komunicirati kako bi se izbjegli nepotrebnu potrošnju energije.

Višestazni TCP protokol je jedno od rješenja koje dopušta uređajima da iskoriste jedan komunikacijski put koji je dostupan umjesto da stalno stvaraju nove puteve i ispituju njihovu sigurnost. Pojednostavljivanje protokola također povećava brzinu prijenosa podataka zato što je zauzeće komunikacijskog kanala manje.

Smanjenje kompleksnosti kontrolnih protokola pomoći će petoj generaciji pokretnih mreža da zadovolji od nje tražene ciljeve pa je važno da se ovaj aspekt ozbiljno shvati i primjeni.

5. ZAKLJUČAK

Sasvim je jasno da su pokretne mreže pete generacije i Internet stvari buduće tehnologije koje će promijeniti komunikaciju i upravljanje uređajima. Razviti će se pametni gradovi, pametne kuće, autonomna vozila te će svijet postati još povezaniji negoli je bio do sada. Prijenos podataka bit će brži i skoro bez kašnjenja, pokrivenost signalom nadvladat će sve dosadašnje sustave, a upravljanje mrežom bit će jednostavnije i sigurnije. Uz sve navedeno sigurnosni sustavi morat će zadovoljiti zahtjeve koji se od njih očekuju kako bi ovakva mreža bila ostvariva. Ovaj rad se bavi upravo sigurnosnom problematikom i potencijalnim rješenjima problema nastalih u ovom području kao i odgovora na moguće napade na mrežu. Prvo su navedene prijašnje generacije pokretnih mreža od prve (1G) do četvrte (4G) i njihova obilježja, a zatim je riječ bila o petoj generaciji pokretnih mreža. Opisana je arhitektura 5G pokretne mreže i ključne tehnologije za njezinu realizaciju. Detaljno su opisane sigurnosne prijetnje kao i protumjere kojima se mreža može zaštiti i zadržati integritet, povjerljivost i autentičnost. Zatim su navedene tehnologije koje će biti primijenjene u 5G pokretnoj mreži kao što su D2D komunikacija, HetNet, SDN i njihova sigurnost. Naposljetku je opisana sigurnosna arhitektura nastala na temelju potreba koje se nameću i koja može biti primijenjena u budućoj pokretnoj mreži pete generacije.

Sigurnost predstavlja veliki izazov za pokretnu mrežu pete generacije koja je trenutno u procesu razvoja i testiranja tehnologija potrebnih za njezinu realizaciju. Međutim ne treba sumnjati da će se pronaći prava sigurnosna rješenja te će pokretna mreže pete generacije biti primijenjena.

LITERATURA

[1] HAKOM , Prikupljanje i analiza podataka, dostupno na : https://www.hakom.hr/default.aspx?id=60

[2],„Laying the foundations for 5G mobile“, dostupno na: https://ytd2525.wordpress.com/2015/01/23/laying-the-foundations-for-5g-mobile/

[3],„5G Mobile Wireless Technology“, dostupno na: https://www.electronics-notes.com/articles/connectivity/5g-mobile-wireless-cellular/technology-basics.php

[4] OpenAirInterface, „5G software alliance for democratising wireless innovation“, dostupno na: http://www.openairinterface.org/? page_id=458

[5] Dongfeng Fang, Yi Qian, Rose Qingyang Hu, „Security for 5G Mobile Wireless Networks“, IEEE, August 2017., str. 17.

[6] Dongfeng Fang, Yi Qian, Rose Qingyang Hu, „Security for 5G Mobile Wireless Networks“, IEEE, August 2017.,Figure 15. , str. 18.

[7] 5G NR New Radio, dostupno na: https://www.electronics-notes.com/articles/connectivity/5g-mobile-wireless-cellular/5g-nr-new-radio.php

[8] „What is mmWave and how does it fit into 5G?“, Phillip Tracy, kolovoz 2016., dostupno na: https://www.rcrwireless.com/20160815/fundamentals/mmwave-5g-tag31-tag99

[9] 5G NextGen Core Network, dostupno na: https://www.electronics-notes.com/articles/connectivity/5g-mobile-wireless-cellular/5g-ng-nextgen-core-network.php

[10] W. Stallings, “Cryptography and Network Security Principles and Practice Sixth Edition”, PEARSON, 2014.

[11] Dongfeng Fang, Yi Qian, Rose Qingyang Hu, „Security for 5G Mobile Wireless Networks“, IEEE, August 2017., Figure 5. , str. 5.

[12] DoS vs DDoS – What is the difference? , dostupno na: http://www.security-faqs.com/dos-vs-ddos-what-is-the-difference.html

[13] “5G Security: Forward Thinking Huawei White Paper”, HUAWEI WHITE PAPER, 2015.

[14] Dongfeng Fang, Yi Qian, Rose Qingyang Hu, „Security for 5G Mobile Wireless Networks“, IEEE, August 2017.,str. 5 - 6.

[15] Dongfeng Fang, Yi Qian, Rose Qingyang Hu, „Security for 5G Mobile Wireless Networks“, IEEE, August 2017., Figure 12., str. 15

[16] Robert W. Heath Jr., „Heterogeneous Networks“ , University of Texas at Austin, dostupno na: http://www.profheath.org/research/heterogeneous-networks/

[17] Steve Bergren, „Design Considerations for a 5G Network Architecture“, Oklahoma State University, Stillwater, str. 7 - 8.

[18] M. J. Wang, Z. Yan, "A Survey on Security in D2D Communications", Mobile Networks and Applications, vol. 22, no. 2, pp. 195-208, 2017.

[19] Dongfeng Fang, Yi Qian, Rose Qingyang Hu, „Security for 5G Mobile Wireless Networks“, IEEE, August 2017.,str. 14.

[20] Y. Luo, L. Cui, Y. Yang, B. Gao, "Power control and channel access for physical-layer security of D2D underlay communication", 2015

[21] „Innovative service in the upcoming era of 5G“, dostupno na: https://developers.sktelecom.com/content/tech/Network/techDetail/?techId=40

[22] „Software-Defined Networking (SDN) Definition“, dostupno na: https://www.opennetworking.org/sdn-definition/

[23] Dongfeng Fang, Yi Qian, Rose Qingyang Hu, „Security for 5G Mobile Wireless Networks“, IEEE, August 2017.,str. 16.

[24] „What is NFV: network functions virtualization basics“ , dostupno na: https://www.electronics-notes.com/articles/connectivity/nfv-network-functions-virtualisation/what-is-nfv-basics.php

[25] Kent Mundle, „Home Smart Home: Domesticating the Internet of Things“, dostupno na: https://www.toptal.com/designers/interactive/smart-home-domestic-internet-of-things

[26] Ferguson O'Sullivan, „What Is The Internet Of Things?“, 2018, dostupno na: https://www.cloudwards.net/what-is-the-internet-of-things/

[27] Nima Namvar, Walid Saad, Niloofar Bahadori, Brian Kelley, „Jamming in the Internet of Things: A Game-Theoretic Perspective“, December 2016.

[28] Dongfeng Fang, Yi Qian, Rose Qingyang Hu, „Security for 5G Mobile Wireless Networks“, IEEE, August 2017.,str. 17 - 18.

[29] Dongfeng Fang, Yi Qian, Rose Qingyang Hu, „Security for 5G Mobile Wireless Networks“, IEEE, August 2017.,Figure 16, str. 18.

Popis i opis korištenih kratica

3GPP	3rd Generation Partnership Project
5G	5th generation
5G NR	5th generation New Radio
AMF	Access and mobility management function
D2D	Device to Device
DoS	Denial of Service
DDoS	Distributed Denial of Service
DSA	Dynamic Spectrum Access
DSSS	Direct Sequence Spread Spectrum
EDGE	Enhanced Data rates for GSM Evolution
EPC	Evolved Packet Core
FHSS	Frequency Hopping Spread Spectrum
GPRS	General Packet Radio Service
GSM	Global System for Mobile Communications
HDSPA	High-Speed Downlink Packet Access
HetNet	Heterogeneous Network
IP	Internet Protocol
IoT	Internet of Things
LTE	Long Term Evolution
MAC	Medium Access Control
MIMO	Multiple-Input Multiple-Output
MITM	Man-In-The-Middle
NFV	Network Functions Virtualisation
PCF	Policy control function
PLS	Physical Layer Security
SDN	Software Defined Networking
SMF	Session Management Function
TCP	Transmission Control Protocol
UDM	Unified Data Management
UDP	User Datagram Protocol
USIM	Universal Subscriber Identity Module
VNF	Virtualized Network Functions

Sažetak

Nadolazeća peta generacija pokretnih mreža sve je češća tema, a uskoro će postati i stvarnost. Omogućit će povezivanje ogromnog broja uređaja u mrežu koja se naziva Internet stvari, ali imat će i mnoštvo drugih primjena u pametnim gradovima i autonomnim vozilima. U ovom radu su opisane neke od tehnologija kao i njihova sigurnosna tematika. Tehnologije koje su obrađene su D2D komunikacija, SDN, HetNet, Internet stvari i MIMO. Opisani su sigurnosni izazovi i dana su moguća rješenja. Predložena je sigurnosna arhitektura 5G mreže i moguće tehnologije za postizanje ciljeva koji su pred petom generacijom pokretnih mreža.

Ključne riječi: 5G, sigurnost, internet stvari, pokretna mreža, heterogena mreža, sigurnosna arhitektura

Abstract

Security Requirements and Challenges in 5G Networks

Emerging fifth generation of mobile networks is soon to become reality. It will enable connection of a huge number of devices into the network called Internet of Things but will also have plenty other applications in smart cities and autonomous vehicles. In this thesis are described some of the technologies and their security issues. Technologies that are described are D2D, SDN, HetNet, IoT and MIMO. It is given possible solution for each security problem. It is also proposed security architecture of 5G network and possible technologies to overcome challenges that are put in front of the fifth generation of mobile networks.

Keywords: 5G, security, Internet of Things, mobile network, heterogeneous network, security architecture

Životopis

Marin Matijašević rođen je 30.6.1995. godine u Rijeci. Živio je u gradu Krku gdje je završio osnovnu školu Fran Krsto Frankopan. Nakon završene osnovne škole preselio se u Vinkovce gdje upisuje Tehničku školu Ruđera Boškovića, smjer elektrotehničar. Nakon završene srednje škole upisuje Fakultet elektrotehnike, računarstva i informacijskih tehnologija u Osijeku, te na drugoj godini studija odabire smjer komunikacije i informatika.

_____

(Potpis)