Sigurnost u radijskim mrežama pete generacije

Musulin, Toni

SVEUČILIŠTE U DUBROVNIKU
ODJEL ZA ELEKTROTEHNIKU I RAČUNARSTVO

TONI MUSULIN

SIGURNOST U RADIJSKIM MREŽAMA PETE GENERACIJE

DIPLOMSKI RAD

Dubrovnik, rujan 2020.

SVEUČILIŠTE U DUBROVNIKU
ODJEL ZA ELEKTROTEHNIKU I RAČUNARSTVO

SIGURNOST U RADIJSKIM MREŽAMA PETE GENERACIJE

DIPLOMSKI RAD

Studij: Diplomski studij
Studijski smjer: Elektrotehničke i komunikacijske tehnologije u pomorstvu
Kolegij: Mobilne brodske komunikacijske mreže
Mentor: izv. prof. dr. sc. Adriana Lipovac
Student: Toni Musulin, univ. bacc. ing. el.

Dubrovnik, rujan 2020.

SAŽETAK

Razvojem radijske mreže pete generacije (5G) omogućeno je povezivanje gotovo svih aspekata života putem mreže s većom brzinom prijenosa podataka, niskom latencijom te boljim povezivanjem u svim dijelovima svijeta. Nadolazeća peta generacija sve je češća tema među društvom, a uskoro će postati i stvarnost. Omogućit će se povezivanje velikog broja uređaja u mrežu koja se naziva Internet stvari, ali imat će i mnoštvo drugih primjena u pametnim gradovima i autonomnim vozilima.

Skup sigurnosnih prijetnji u 5G-u enormno je porastao zbog proporcionalnog porasta vrsta usluga i broja uređaja koji pružaju te usluge. Stoga, sigurnosna rješenja, ako još nisu razvijena, moraju biti osmišljena na način kako bi se mogla nositi s različitim prijetnjama različitih usluga, novim tehnologijama i povećanim brojem informacija koje korisnik dobiva putem dostupne mreže.

Tematika ovog rada odnosi se na sigurnosni aspekt 5G mreže. Opisane su sigurnosne ranjivosti 5G mrežne infrastrukture, prijetnje u novim tehnološkim konceptima, te rješenja za te prijetnje i buduće upute za rješavanje tih sigurnosnih izazova.

Ključne riječi: 5G, radijska mreža, korisnik, informacija, sigurnosne prijetnje, sigurnosna rješenja, sigurnosni izazovi

ABSTRACT

The development of the fifth generation network (5G) enabled the connection of almost all aspects of life through a network characterised by a higher speed of data transfer, low latency and better connectivity in all parts of the world. The forthcoming fifth generation is an increasingly common topic in society which will soon become reality. The connection of a large number of devices in a network named the Internet of things will be enabled, but it will also have numerous other applications in smart cities and autonomous vehicles.

The set of security threats in the 5G network increased enormously due to the proportional rise in the types of services and number of devices offering them. Therefore, security solutions, if not yet developed, have to be conceived so as to be able to deal with the various threats of different services, new technologies and the elevated number of information a user obtains through an accessible network.

The topic of this paper relates to the security aspects of the 5G network. The security vulnerabilities of the 5G network infrastructure have been described, as well as the threats to the new technological concepts, solutions to those threats and guidelines for the solution of such security challenges in the future.

Keywords: 5G, radio network, user, information, security threats, security solutions, security challenges

SADRŽAJ

1. UVOD

Sigurnosni rizici postoje u bilo kojoj radijskoj tehnologiji. Neki od tih rizika slični su onima u žičnim mrežama, a neki se pogoršavaju radijskim povezivanjem. Najznačajniji izvor rizika u radijskim mrežama je taj što je komunikacijski medij otvoren uljezima. Mobilni radijski uređaji ograničeni su s resursima (npr. vijek trajanja baterije) pa stoga takvi uređaji imaju ograničenu snagu prijenosa i mogu koristiti slabije kriptografske mehanizme za uštedu energije, što ih čini lakšim metama za moćne protivnike. Samo-konfiguriranje heterogenih mreža može upotrebljavati različite razine sigurnosti, a donje zaštićene veze mogu predstavljati kršenje za cijeli sustav. Izravna posljedica ovih rizika je gubitak povjerljivosti i integriteta podataka te prijetnja uskraćivanjem usluge (DoS) na radijskoj komunikaciji. Neovlašteni korisnici mogu dobiti pristup sustavu i informacijama, oštetiti podatke, smanjiti performanse mreže, pokretati napade koji onemogućavaju ovlaštenim korisnicima pristup mreži ili koristiti resurse za pokretanje napada na druge mreže. Sigurnost radijskih sučelja danas je presudna za mnoge aplikacije: širokopojasni Internet, e-trgovina, plaćanje radio-terminala, bankovne usluge, komunikacija stroja sa strojem, udaljene usluge u zdravstvu / bolnici itd.

Sigurnosne metode koje se najčešće koriste oslanjaju se na kriptografske tehnike, bilo asimetrične (temeljene na javnim i privatnim ključevima) ili simetrične (zasnovane na zajedničkoj tajni koju drugi ne znaju), a nalaze se na gornjim slojevima radijske mreže. Šifriranje ne štiti od neželjene demodulacije informacija napadačima, već samo od prikaza podataka kao smislenih riječi. Kriptografski protokoli svoju sigurnost temelje na činjenici da je, statistički gledano, vrijeme za obavljanje analize dešifriranja ogromno. Vrijeme za proboj kodne riječi povezano je s računskom snagom napadača, tj. kriptografija fundamentalno pretpostavlja da prisluškivač ima vremenski ograničenu količinu mogućnosti za računanje. Nedavni napori akademske zajednice i industrije da povećaju količinu operacija digitalnih procesora u sekundi čine ovu pretpostavku sve slabijom. Uobičajena praksa dodavanja autentifikacije i enkripcije postojećim protokolima na raznim komunikacijskim slojevima dovela je do neučinkovitih udruživanja sigurnosnih mehanizama. Budući da je sigurnost podataka važna, razumno je tvrditi da se mjere sigurnosti trebaju provoditi na svim razinama gdje se to može učiniti na ekonomičan način.

Prvi dio rada opisuje općenito sigurnost u radijskim mrežama, uvjete koje treba postići kako bi se osigurala mreža te su navedene metode osiguranja mrežne sigurnosti.

Opisana je sigurnost u ranijim generacijama radijskih mreža, karakteristike 5G mreže, dizajn i arhitektura.

Težište rada stavljeno je na sigurnost u 5G mrežama, gdje su definirani sigurnosna arhitektura i dizajn mreže te mogući problemi i nedostatci. Također, u nastavku je detaljno opisana privatnost korisnika, identiteta te da li kao korisnici imamo povjerenje u 5G mrežu.

Kao zaključak ovog rada navedena su rješenja za te prijetnje i buduće upute za rješavanje tih sigurnosnih izazova te je prikazan utjecaj na zdravlje 5G mreže u svijetu.

2. SIGURNOST I ZAŠTITA PRIVATNOSTI

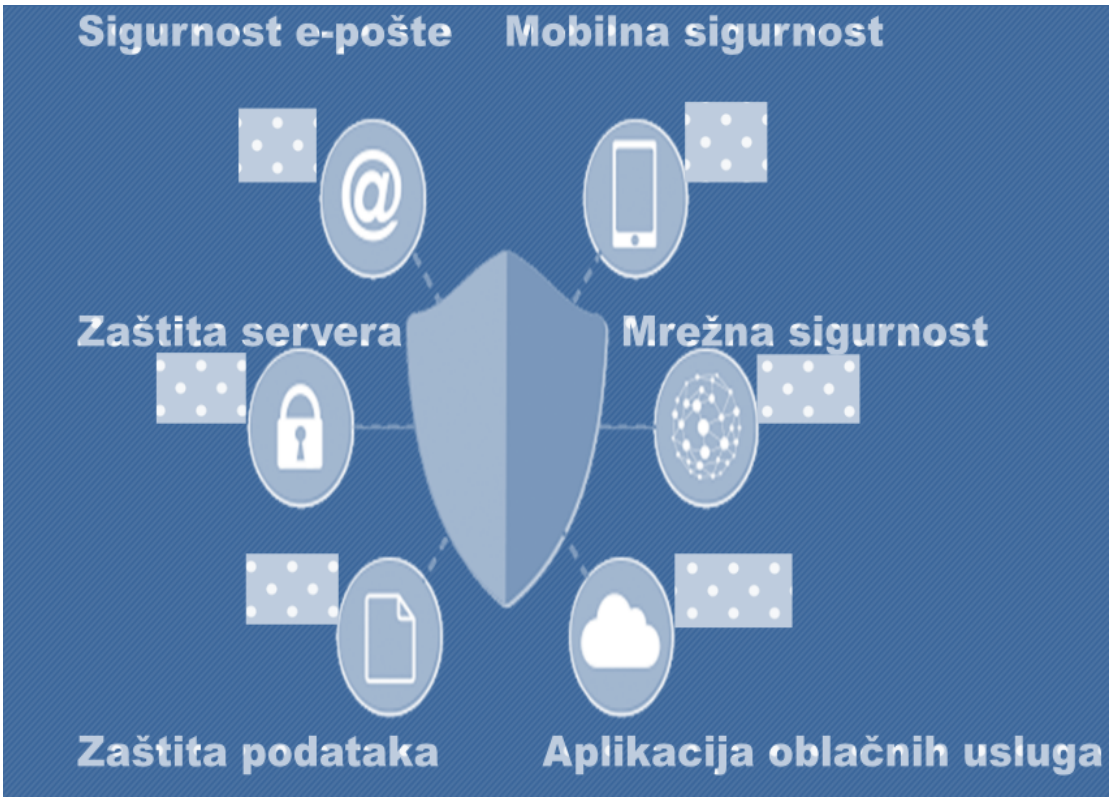
Sigurnost podataka i zaštita privatnosti sve više dobivaju na važnosti u poslovanju jer se povećava zabrinutost potrošača zbog moguće zlouporabe njihovih osobnih podataka. Iz tog razloga doneseni su novi zakoni i pravila ponašanja za one koji ne poštuju pravila privatnosti i sigurnosti. Da bi internetska infrastruktura postala pouzdana i sigurna, treba je opremiti mogućnostima kontrole pristupa, provjere autentičnosti, autorizacije, zaštite integriteta uređaja i podataka, zaštite privatnosti, povjerljivosti, revizije transakcija itd. Slično tome, pristupnici mogu provesti strogu sigurnosnu mjeru za izoliranje mreže korisničkih prostora (npr. mreža područja tijela koja se koristi za zdravstvo) iz nepouzdane vanjske domene. [3]

2.1 Sigurnost u radijskim mrežama

U posljednjem desetljeću, radijska komunikacijska infrastruktura i usluge povećavali su se u skladu s traženim zahtjevima korisnika. Prema najnovijim istraživanjima gotovo 60 % svjetske populacije trenutno koristi Internet. Isto tako, sve veći broj radijskih uređaja zlostavlja se putem nezakonitog *cyber* kriminala, uključujući zlonamjerne napade, hakiranje računala, krivotvorenje podataka, krađu financijskih informacija, internetska maltretiranja / provaljivanja i slično. Stoga, od najveće važnosti jest poboljšanje sigurnosti radijske komunikacije za borbu protiv *cyber* kriminala, posebno zato što sve više ljudi koristi radijske mreže (npr. mobilne mreže i *Wi-Fi*) za internetsko bankarstvo i osobne *e-mailove*, zahvaljujući raširenoj upotrebi pametnih telefona. [1]

Kao što je vidljivo na slici 2.1.1 metodologija sigurnosti u radijskim mrežama se dijeli na:

- Mobilna sigurnost
- Mrežna sigurnost
- Aplikacija oblačnih usluga
- Zaštita podataka
- Zaštita servera
- Sigurnost e-pošte



Slika 2.1.1 Metodologija sigurnosti u radijskim mrežama [8]

2.2 Uvjeti za sigurnost u radijskim mrežama

U radijskim mrežama, informacije se razmjenjuju između ovlaštenih korisnika, ali taj postupak je ranjiv na različite zlonamjerne prijetnje zbog same prirode prijenosa putem radijskog medija. Sigurnosni zahtjevi radijskih mreža postavljeni su da zaštite bežični prijenos od bežičnih napada, kao što su napad prisluškivanja, DoS napadi, napad falsificiranja podataka, i slično. Na primjer, održavanje povjerljivosti podataka tipičan je sigurnosni zahtjev, koji se odnosi na sposobnost ograničavanja pristupa podacima samo ovlaštenim korisnicima, istovremeno sprečavajući prisluškivače da presreću informacije.

Općenito govoreći, sigurna radijska komunikacija treba zadovoljiti zahtjeve autentičnosti, povjerljivosti, integriteta i dostupnosti, kako je detaljnije opisano u nastavku.

- Autentičnost: Odnosi se na potvrđivanje istinskog identiteta mrežnog čvora radi razlikovanja ovlaštenih korisnika od neovlaštenih korisnika. U radijskim mrežama par komunikacijskih čvorova prvo bi trebao izvršiti uzajamnu provjeru autentičnosti prije uspostavljanja komunikacijske veze za prijenos podataka. Mrežni čvor obično je opremljen karticom sučelja radijske mreže i ima jedinstvenu MAC adresu, koja se može koristiti u svrhu provjere autentičnosti. Opet, osim MAC provjere autentičnosti,

postoje i druge metode radijske provjere autentičnosti, uključujući provjeru autentičnosti na mrežnom sloju, provjeru autentičnosti na transportnom sloju i provjeru autentičnosti na razini aplikacije.

- Povjerljivost: Odnosi se na ograničavanje pristupa podacima samo namijenjenim korisnicima, istovremeno sprečavajući otkrivanje podataka neovlaštenim subjektima. Ako se uzme u obzir tehnika simetričnog šifriranja ključa kao primjer, izvorni čvor najprije šifrira izvorne podatke (često nazvane *plaintext*) koristeći algoritam šifriranja uz pomoć tajnog ključa koji se dijeli samo s predviđenim odredištem. Zatim se šifrirani otvoreni tekst šalje na odredište koje zatim dešifrira primljeni šifrirani tekst pomoću tajnog ključa. Budući da prisluškivač nema saznanja o tajnom ključu, neće se moći prikazati otvoreni tekst na temelju teksta sakrivene šifre. Tradicionalno, klasični protokol dogovora o ključu *Diffie-Hellman* koristi se za postizanje razmjene ključeva između izvora i odredišta.
- Integritet: Integritet informacija koje se prenose u radijskoj mreži trebao bi biti točan i pouzdan tijekom cijelog životnog ciklusa predstavljajući izvorne informacije bez falsificiranja i izmjene od strane neovlaštenih korisnika. Cjelovitost podataka može biti narušena vanjskim napadima, kao što su, na primjer, napadi kompromitiranih čvorova. Točnije, legitimni čvor koji napadač mijenja i kompromitira naziva se kompromitirani čvor. Kompromitirani čvor može nanijeti štetu integritetu podataka pokretanjem zlonamjernih napada, uključujući ubacivanje poruka, lažno prijavljivanje, izmjenu podataka itd. Općenito, izazovno je otkrivati napade kompromitiranih čvorova, jer ovi kompromitirani čvorovi koji imaju zlonamjerne kodove i dalje imaju važeći identitet. Obećavajuće rješenje za otkrivanje kompromitiranih čvorova jest korištenje automatskog ažuriranja i obnavljanja koda, što osigurava da su čvorovi periodično zatvoreni i da se kompromitirani čvor može otkriti ako se ne uspije zatvoriti. Ugroženi čvorovi mogu se popraviti i vratiti kroz postupak obnavljanja koda.
- Dostupnost: Podrazumijeva da ovlašteni korisnici doista mogu pristupiti radijskoj mreži bilo kada i bilo gdje na zahtjev. Kršenje dostupnosti, koje se naziva uskraćivanje usluge, rezultirat će time da ovlašteni korisnici onemoguće pristup radijskoj mreži, što zauzvrat rezultira nezadovoljavajućim korisničkim iskustvom. Na primjer, bilo koji neovlašteni čvor može pokrenuti DoS aktivnost na fizičkom sloju zlonamjerno generirajući interferencije za ometanje željenih komunikacija između zakonitih korisnika, što je poznato i kao napad ometanja. Da bi se suzbili napadi ometanja, postojeći radijski sustavi obično razmatraju primjenu tehnika raširenog spektra,

uključujući rješenja DSSS i FHSS. Da bude jasnije, DSSS koristi PN sekvencu za širenje spektra izvornog signala na široku frekvencijsku širinu. Na ovaj način, napad koji djeluje bez znanja PN sekvence mora raspršiti mnogo veću snagu za ometanje zakonitog prijenosa, što u praksi možda neće biti izvedivo zbog njegove realne snage prijenosa ograničenja. Kao alternativa, FHSS kontinuirano mijenja središnju frekvenciju prenesenog valnog oblika koristeći određenu funkciju skakanja frekvencije, tako da napadač ne može nadzirati i prekinuti zakonite prijenose. [1]

Tablica 2.2.1 Sažetak radijskih sigurnosnih zahtjeva [1]

Uvjet sigurnost	Specifičan cilj koji treba postići
Autentičnost	Razlikovati ovlaštene korisnike od neovlaštenih korisnika.
Povjerljivost	Ograničiti pristup povjerljivim podacima samo namijenjenim korisnicima.
Integritet	Osigurati točnost poslanih informacija bez ikakvog krivotvorenja.
Dostupnost	Osigurati da ovlašteni korisnici mogu pristupiti izvorima radijske mreže u bilo koje vrijeme i bilo gdje na zahtjev.

2.3 Metode osiguranja mrežne sigurnosti

Postoji niz metoda osiguranja mrežne sigurnosti kojima se osnažuju obrambeni mehanizmi. To su:

- Kontrola pristupa: Ova metoda se uvodi radi ograničavanja ili ukidanja nelegitimnih uređaja za pristup mreži neke organizacije. Korisnici kojima je dopušten pristup mreži također su ovlašteni za pristup određenom skupu resursa.
- Anti-*Malware*: Zlonamjerni softver uključuje računalne crve, viruse i trojance koji pokušavaju zaraziti cijelu mrežu i tjednima mogu ostati na zaraženim računalima. Sigurnosni sustav trebao bi provoditi značajnije tehnike kako bi spriječio infekciju i odmah uklonio zlonamjerni softver.
- Sigurnost aplikacija: Nisu sve aplikacije originalne i bez zlonamjernog softvera. Napadači koriste zlonamjerne i nesigurne aplikacije kao mamac za pristup mrežama organizacija. Stoga će trebati učinkovita integracija softvera, hardvera i sigurnosnih procesa kako bi se ograničile sumnjive aplikacije.
- Bihevioralna analitika: Važna je analiza mreže da bi se razumjelo njeno ponašanje. Ovo će pomoći da se uoči ako mreža prolazi kroz neko nenormalno ponašanje i stoga djelovati pomoću bilo koje odgovarajuće zaštitne metode.
- Sprečavanje gubitka podataka: Važno je primijeniti metode i tehnike koje ograničavaju zaposlenike i ostale korisnike da namjerno ili nenamjerno šalju povjerljive podatke izvan mreže organizacije.
- Sigurnost e-pošte: Napadači koriste tzv. *phishing* (mrežna krađa identiteta) *e*-poštu kako bi dobili pristup mreži. Treba primijeniti sigurnosne metode *e*-pošte kako bi se omogućila zaštita od takvih *phishing* e-poruka.
- Vatrozid: Ovo definira skup pravila koja trebaju biti onemogućena ili omogućena internetskom prometu pristup vašoj mreži. Otkrivanje i sprečavanje provale: Ovo omogućava skeniranje prometa na mreži radi otkrivanja i zaustavljanja napada.
- Segmentacija mreže: Segmentacija koja je povezana sa softverom pomoći će da se organizira različita kategorija, pa će provedba sigurnosnih politika biti lakša.
- Web Sigurnost: Upravlja internim osobljem koje upotrebljava Internet radi zaustavljanja napada temeljenih na webu iz iskorištavanja potencijalnih preglednika kao vektora kako bi se dobio pristup vašoj mreži. [2]

2.4 Sigurnost radijskih mreža i faktor dizajna

Radijske mreže općenito prihvaćaju arhitekturu OSI protokola koja sadrži aplikacijski sloj, transportni sloj, mrežni sloj, MAC sloj i fizički sloj. Sigurnosne prijetnje i ranjivosti povezane s ovim slojevima protokola najčešće se štite odvojeno na svakom sloju kako bi se zadovoljili sigurnosni zahtjevi, uključujući autentičnost, povjerljivost, integritet i dostupnost. Na primjer, kriptografija se široko koristi za zaštitu povjerljivosti prijenosa podataka sprečavanjem otkrivanja informacija neovlaštenim korisnicima. Iako kriptografija poboljšava komunikacijsku povjerljivost, zahtijeva dodatnu računsku moć i nameće kašnjenje, jer je potrebno određeno vrijeme i za šifriranje podataka i za dešifriranje. Da bi se osigurala autentičnost pozivatelja ili primatelja, postojeće radijske mreže obično koriste više pristupa za provjeru autentičnosti istovremeno na različitim slojevima protokola, uključujući provjeru autentičnosti na MAC sloju, provjeru autentičnosti na mrežnom sloju i provjeru autentičnosti transportnog sloja. Da bi bili specifični, u MAC sloju treba MAC adresu korisnika ovjeriti kako bi se spriječio neovlašteni pristup. U mrežnom sloju, WPA i WPA2 dva su najčešće korištena protokola provjere autentičnosti mrežnog sloja. Uz to, prepoznavanje transportnog sloja uključuje SSL i njegovog nasljednika, pod nazivom TLS protokol. Postaje očigledno da je upotreba više mehanizama provjere autentičnosti na različitim slojevima protokola iz razloga poboljšanja radijske sigurnosti. Kao što je prikazano na slici 2.4.1, glavna radijska sigurnosna metodologija uključuju provjeru autentičnosti, autorizacije i enkripcije za bilo koji različiti faktor dizajna, npr. razina sigurnosti, složenost implementacije i kašnjenje komunikacije moraju biti uravnoteženi. [1]

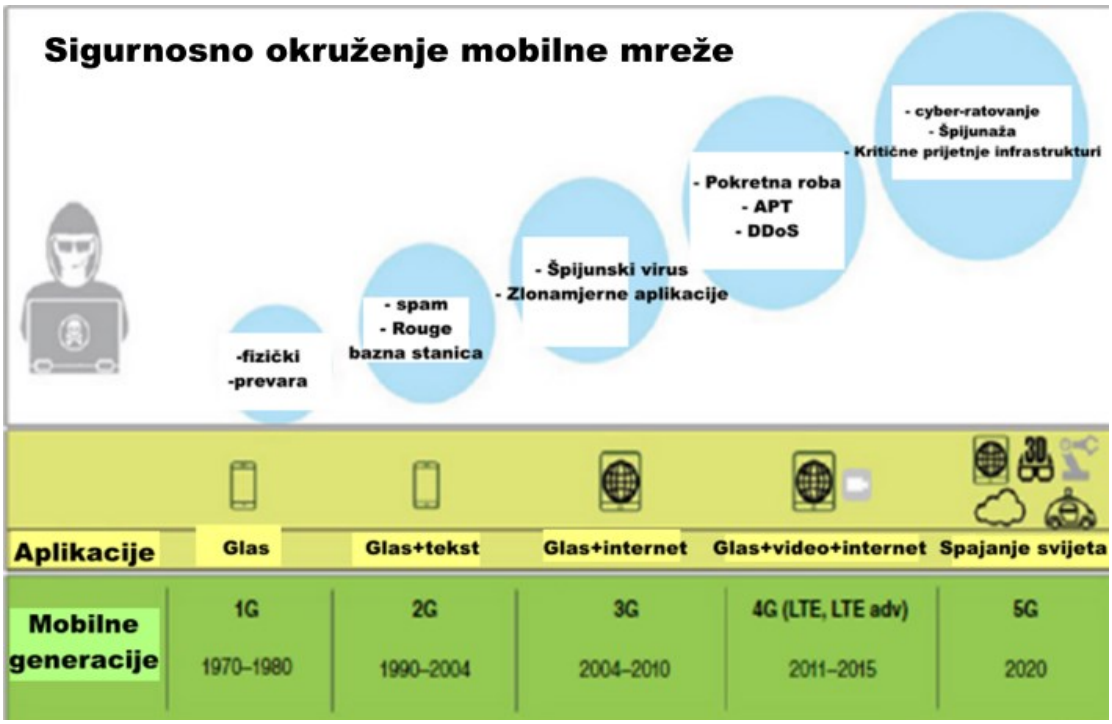
Slika 2.4.1 Sigurnost radijskih mreža i faktor dizajna [1]

3. SIGURNOST U MOBILNIM RADIJSKIM MREŽAMA

Budućnost društava i velikih gospodarstava, poput Europe, u velikoj se mjeri oslanjaju na mobilnu infrastrukturu gdje neposredni financijski i ekonomski utjecaj industrije IKT (informacijske i komunikacijske tehnologije) rezultira s približno 5 % BDP-a ili stotinama milijardi eura [13]. Mobilno stanovništvo doseći će 5, 5 milijardi korisnika do službenog pokretanja 5G-a ove godine [32]. To će značiti veću povezanost, više stvaranja i dijeljenja informacija putem mobilnih radijskih mreža. Kao rezultat telekomunikacijskog preporoda i njegove važne uloge u cjelokupnom javnom i gospodarskom zdravstvu, ova će industrija uskoro postati glavna meta za antidržavne i kriminalne aktere koji žele iskoristiti ovu platformu da naruše njen rast i zauzvrat je iskoriste za pokretanje napada na širu bazu korisnika mobilnih radijskih mreža.

Kršenja podataka u novijoj generaciji povezanog svijeta ima ogroman broj, kao što se nedavno dogodilo u slučaju velikog *Yahoo-a,* kada je zbog kršenja podataka u jednom napadu utjecala na milijardu korisnika ili slučaj *LinkedIn* 2016. godine kada je zbog kršenja podataka imalo utjecaj na 117 milijuna korisnika, što je rezultiralo propuštanje osjetljivih osobnih i profesionalnih podataka [33]. Sigurnost mobilne mreže postepeno se razvijala paralelno s razvojem telekomunikacijske industrije. Iz tog razloga u ovom poglavlju obuhvatit će se cjelokupno okruženje sigurnosnih prijetnji mobilnih mreža kako se razvijao s različitim generacijama mobilnih mreža. Također, raspravljat će se i o povijesti mobilnih sigurnosnih prijetnji, relativnim mehanizmima zaštite i utjecaja na mobilne mreže te je prikazan sigurnosni pristup životnog ciklusa, kako bi se ponudio učinkovit i sveobuhvatan mehanizam zaštite za suvremene mobilne uređaje i mreže.

Sigurnosno okruženje mobilne mreže kao što slika 3.1 prikazuje treba promatrati u svjetlu razvoja različitih generacija mobilnih mreža. Izravna je povezanost između evolucije tehnologije mobilne mreže i relativne povezanosti razvoja sigurnosnih prijetnji u smislu tehnološke arhitekture, tehničkih mogućnosti, ponuđenih usluga i pridruženih vektora prijetnji.



Slika 3.1 Sigurnost mobilnih mreža kroz generacije [5]

Mobilne mreže počele su svjedočiti ozbiljnim prijetnjama i izazovima odmah nakon uvođenja prve generacije mobilne tehnologije i nastavile su rasti kao složen i izazovan krug prijetnji. 1G je primarno predstavljen kako bi ponudio mobilnost za glasovne korisnike. Potrošači su počeli svjedočiti slobodi javljanja i upućivanja poziva preko mobitela dok su u pokretu. Zločinci su otkrili priliku i metode za počinjenje mobilnih prijevara i lažno se predstavljali kao legalni pretplatnici da im hakiraju mobitel za besplatne pozive. Kloniranje mobitela postalo je industrija stvaranjem i prodajom ilegalnih kloniranih telefona. Neki su hakeri identificirali nove načine otmice i prisluškivanja poziva tijekom upućivanja te slušali privatne razgovore iz različitih loših razloga.

S 2G-om, u svijetu mobilnih uređaja došlo je doba neželjenih poruka. *Spam* se koristio kao rašireni napad za ubacivanje lažnih podataka ili slanje neželjenih marketinških reklama mobilnim korisnicima. Spremnici pošte bili su zauzeti neželjenim porukama koje ciljaju određenu grupu ili širu zajednicu. Prevaranti su koristili mobilne neželjene sadržaje u svrhu vlastitog interesa. Izmišljene su bazne stanice za presretanje mobilnog prometa nudeći lažnu mrežnu provjeru identiteta.

Kako korisnički uređaji postaju pametni i snalažljivi, aplikacije za prijenos podataka i Internet postali su ključne usluge koje se nude davateljima mobilnih usluga u novim 3G mrežama. Prosječna brzina veze za prijenos podataka u 3G-u bila je negdje između 500 i 700 kb/s, dovoljna da omogući povezivanje aplikacija preko Interneta. Vektor prijetnje u 3G-u ciljao je

korisničke telefone, računalni sustav i njegov operativni sustav. Iskorištene su ranjivosti mobilnog OS-a jer su mobilne aplikacije ubacivale zlonamjerni kod radi neovlaštenog pristupa osjetljivim osobnim podacima, poput, zaporke i podacima o lokaciji. Kako se povećavala brzina podataka, povećala se i vrsta napada u obliku zlonamjernog softvera i špijunske mreže.

LTE se pojavio prvi put kad je mobilna mreža prebačena na cjelokupnu IP temeljenu arhitekturu. Pomagao je pružateljima usluga mobilne mreže u brzini inovacija, ponudio nove usluge, a također i povećao vektor prijetnji za 4G mreže. DDoS (distribuirano uskraćivanje usluge) i APT (unaprijed trajne prijetnje) nove su prijetnje za mobilnu mrežu. Napadači su postali organiziraniji i počeli su pratiti sustavni pristup mreži. Postalo je teže otkriti njihovu prikrivenu prisutnost u mobilnoj mreži, zaštititi je, s prosječnim napadom koji je trajao mjesecima.

5G napreduje s obećanjem povezivanja milijardi uređaja preko vrlo pouzdane, široko propusne mreže, brze i bez greške sadržane mrežne infrastrukture, koja će služiti mnogim sektorima i industrijama. Ključni slučajevi upotrebe za 5G su IoT, pametni gradovi i povezani svijet. S ovim slučajevima upotrebe, 5G će biti idealna meta za napadače koji će možda htjeti izazvati velike ekonomske i socijalne poremećaje u minimalnom vremenskom roku. Prijetnje za 5G mrežu sastojat će se od financijske i politički motivirane dobiti, koju izvršavaju skupine profesionalaca i kriminalaca sa širokim tehnološkim znanjem i resursima. Okvirni plan prijetnji za 5G bit će dinamičan i temeljit će se na sofisticiranim i složenim prijetnjama, poput *Stuxneta* i *malwarea*. [5]

3.1 Funkcije životnog ciklusa sigurnosti mobilnih mreža

Funkcije životnog ciklusa sigurnosti za mobilne uređaje i mreže razvijene su u svrhu zaštite s jednog kraja na drugi kraj sigurnosnog položaja mobilnih sustava i mreža. Zadatak tih funkcija jest sigurnost na pojedinim fazama mobilnog pružanja usluga, konfiguracija, procjena i nadzor sigurnosti. Funkcije životnog ciklusa utječu na sigurnosne sustave, alate i procese koji su potrebni za zaštitu povjerljivosti, integriteta i dostupnosti mobilnih uređaja i mreža.

Budući da će 5G mreže uvesti nove alate za provođenje mobilne e-trgovine i nove slučajeve poslovne upotrebe mobilnih telefona, kao što su IoT i širokopojasni pristup, takva poduzeća posebno će se zalagati za dobro definiran sustav upravljanja sigurnošću i upravljanja za svoje krajnje korisnike mobilnih uređaja, sve u cilju kako bi dodatno zaštitio njihove važne podatke

i aplikacije koje se nalaze na osobnim mobilnim uređajima krajnjih korisnika kao proširenje korporativne mreže, kao u slučaju BYOD. [5]

Ključni sigurnosni propusti u takvim slučajevima su: [34]

- nedosljedna sigurnosna politika,
- curenje u zajedničkim medijima,
- minimalno upravljanje uređajima,
- čitljivi podaci koji se nalaze u odloženim uređajima,
- curenje podataka među aplikacijama.

Životni ciklus sigurnosti, kako je prikazano na slici 3.1.1, može pomoći u rješavanju gore navedenih i ostalih uobičajenih sigurnosnih izazova i umanjiti rizike u različitim fazama mobilnog uređaja tijekom njegova sudjelovanja u mreži. Ključne faze životnog ciklusa sigurnosti mobilnih uređaja su opskrba mobilnim uređajima, konfiguracija, upravljanje i nadzor. U odjeljcima u nastavku detaljno će se prikazati funkcije životnog ciklusa sigurnosti za mobilne sustave i mreže.

Slika 3.1.1 Funkcije životnog ciklusa sigurnosti mobilnih mreža [5]

Sigurno upravljanje uređajima

Iako MSP (pružatelj mobilnih usluga) ima ograničenu kontrolu nad sigurnošću mobilnih uređaja, on nudi osnovnu provjeru autentičnosti i autorizaciju mobilnih uređaja za pristup mreži. Međutim, poduzeća koja koriste BYOD za korporativni pristup osobnim mobilnim uređajima zahtijevaju unaprijed mogućnost upravljanja i koriste alate poput MDM-a (*Mobile Device Management*) za središnje upravljanje i zaštitu mobilnih uređaja koje koriste njihovi

zaposlenici. MDM pomaže organizacijama da provedu sigurnosnu politiku, zaštite se od zlonamjernih prijetnji i ograniče neovlašteni pristup mobilnim uređajima. Mobilni uređaji moraju se registrirati s centraliziranim MDM-om poduzeća prije nego što preuzmu sigurnosnu politiku, konfiguraciju i kontrolu kako bi zaštitili taj uređaj. Takve politike mogu primijeniti mehanizme zaštite za mobilne uređaje, poput primjene složenih alfanumeričkih lozinki, definiranja postavki mobilnog automatskog zaključavanja ili pristupa odabranim aplikacijama.

Upravljanje mobilnim uređajima i aplikacijama

Dobavljač mobilnog OS-a (operativnog sustava) redovito objavljuje nadogradnje i ažuriranja kako bi zatvorio poznate ranjivosti i rupe u petlji svog softvera što može dovesti do kompromitacije uređaja ili neke veće slučajeve narušavanja sigurnosti uređaja. Napadači često traže prilike da se počnu boriti s tim ranjivostima i iskoriste ih za neovlašteni pristup mobilnim uređajima. Za korisnike je najvažnije da redovito nadograđuju svoje mobilne uređaje s kojima se koriste. Davatelji mobilnih usluga često objavljuju savjete za svoje korisnike da ažuriraju određene aplikacije i nadogradnje kako bi izbjegli sigurnosni propust. Slično tome, programeri aplikacija također redovito ažuriraju svoje mobilne aplikacije kako bi popunili sve nesigurne značajke ili kodove koji se nalaze u njihovim aplikacijama. Ažuriranja i nadogradnje aplikacija neovisne su o ažuriranjima OS-a i mobilni korisnici ih moraju posebno obraditi. Dobavljač mobilnih uređaja često ovaj postupak pojednostavljuje kroz trgovine aplikacija, a za instalacije prilagođenih aplikacija potrebno je samostalno ažuriranje tih aplikacija.

Analiza i procjena sigurnosnih prijetnji

5G mreže će se u velikoj mjeri oslanjati na mrežne komunikacije i protokole temeljene na IP-u i koristit će nove softversko definirane mobilne mreže (SDMN). 5G planira iskoristiti prednosti SDMN-a za odvajanje upravljačke ravnine i podatkovne razine mobilnih mreža radi pojednostavljenja mreža te ponuditi nove i poboljšane usluge korištenjem novih programskih mreža. SDMN sa svojim mogućnostima nudi nove sigurnosne izazove i može uzrokovati ranjivosti na različitim ravninama (upravljanje, kontrola i podaci) mreže. Prijetnje za mreže temeljene na 5G-u i SDMN-u složene su i mogu dinamički uvoditi nedostatke u mreži na različitim točkama mobilnih mreža. Tradicionalne sigurnosne procjene i tehnike analize prijetnji temelje se na statičkoj i jednostavnoj prirodi tradicionalnih mobilnih mreža i ne bave se izazovima uvedenim s dinamičkim ponašanjem temeljenim na 5G i SDMN. Procjena

sigurnosti za SDMN mreže mora obuhvatiti i adresirati sve komponente i slojeve mobilne mreže. Preporučuju se novi pristupi procjeni sigurnosti koji se usredotočuju na dinamičnu prirodu SDMN-ova. [35].

Nadzor sigurnosti

S razvojem mobilnih mreža od LTE-a do LTE-a *Advanced* i sada su 5G, mobilni RAN i osnovne mrežne tehnologije također su evoluirali i zamjenjuju ih novim tehnologijama poput *Cloud* RAN, NFV i SDMN. Za mobilne operatere je izuzetno važno da imaju sveobuhvatnu mrežu vidljivost i znanje za njihove mrežne operatore u stvarnom vremenu, ne samo da bi pružili bolje osiguranje usluga, već i zaštitili njihovu važnu mrežnu infrastrukturu od sigurnosnih prijetnji. Naslijeđena rješenja za nadzor sigurnosti u mobilnim uređajima koja nisu dizajnirana za zaštitu mreža temeljenih na SDN-u ili NFV-u nisu imala ili su imala ograničenu sposobnost integracije s modernim tehnološkim komponentama mobilne mreže te ih je potrebno zamijeniti rješenjima za nadzor sigurnosti koja nude veće performanse, skalabilnost i sposobnost integriranja i rada s tim novim mobilnim tehnologijama. Rješenja za sigurnosni nadzor za LTE i 5G mreže trebala bi pružiti mogućnost praćenja i pregledavanja signalizacije i podatkovnog prometa u više mrežnih točaka, počevši od UE do RAN-a, pa sve do komponenti unutarnje mreže LTE / 5G. Rješenje treba moći ne samo provjeravati IPv4 i IPv6, već ponuditi vidljivost i ostalim protokolima kao što su TCP, UDP, GRE itd. 5G mreže mogu također utjecati na SDN kontrolu i razdvajanje podataka te mogu izvoditi centralizirano nadgledanje prometa protoka mreže radi dublje vidljivosti i korelacije prolaska prometa unutar mreže.

Nadzor sigurnosti mobilne mreže mora ponuditi neke unaprijed sigurnosne usluge kao što su:

- testovi ranjivosti,
- redovita sigurnosna provjera zdravlja za cijelu mrežu,
- vidljivost mreže temeljena na protoku,
- sustav upravljanja sigurnosnim upozorenjima,
- nadzor i inspekcija prometa.

4. SIGURNOST U RANIJIM GENERACIJAMA RADIJSKIH MREŽA

U ovom poglavlju opisano je promjenjivo okruženje prijetnji mobilnim mrežama, počevši od 1G kada su mobilne usluge nudile samo govorne usluge i kada su se sigurnosne prijetnje uglavnom vrtjele oko financijske dobiti kloniranjem mobilnih telefona pa sve do uvođenja podatkovnih usluga i mobilnih uređaja takozvani pametni telefoni. Mobilnim mrežama izgrađenim preko IP jezgre, sigurnosne prijetnje također su se značajno proširile. Napadi koji su nekoć bili usmjereni na računala bili su ublaženi i ponovo korišteni za mobilne uređaje, a cilj je sada izvan financijske dobiti, jer su uvedene nove prijetnje poput špijunaže i DoS napada. Mobilni uređaji bili su glavni izvor prenošenja špijunskog softvera, crva i zlonamjerne mreže, a svakodnevno se otkrivala nova ranjivost u mobilnim operativnim sustavima, jer su milijuni uređaja dobili pristup nesigurnim aplikacijama. Planirane 5G mreže prenose naslijeđe prethodnih mreža i služit će kao važna infrastruktura za poslovanje te će ponuditi nove mogućnosti kao što su aplikacija oblačnih usluga, IoT i ultra širokopojasni pristup koji će se suočiti s jedinstvenim izazovima i postati meta sofisticiranih sigurnosnih prijetnji poput *ransomwarea* i *Botnetsa*. Detaljno su razmotrene različite faze mobilnih uređaja i njegovo sudjelovanje u mreži. Slijedom životnog ciklusa „s kraja na kraj“ može pomoći izgraditi sigurnosni zid oko nadolazećih mreža, poput LTE i 5G.

Tijekom proteklih godina zahtjevi za mobilnim mrežama su prešli iz prilično jednonamjenskih mreža (govorne usluge) u višenamjenske mreže (podatke). U nastavku su obrađene trenutno aktivne generacije mreža.

4.1 Prva generacija (1G)

Glavni programeri prve generacije (1G) mobilne mreže bili su Sjedinjene Države, Japan i neki dijelovi Europe. Temeljila se na analognoj modulaciji za pružanje govornih usluga. 1979. godine je komercijalni mobilni sustav implementirao Nippon *Telephone* i Telegrafska kompanija (NTT) u Japanu. Nordijski mobilni telefon (NMT-400) je sustav razvijen 1981. godine te podržava međunarodni *roaming* i automatsku primopredaju. Neke su europske zemlje u to vrijeme provele ovaj sustav. Pretplatnici NMT-400 mogli su putem automobilskih telefona prenijeti do 15 W snage. Šest zemalja - točnije Finska, Švedska, Norveška, Austrija, Španjolska i Danska - usvojile su NMT-400.

Napredna usluga mobilne telefonije (AMPS) i alternativni komunikacijski sustavi s potpunim pristupom (ETACS i NTACS) bili su uspješniji za 1G. Sa stajališta radija navedeni su sustavi bili identični, glavna razlika bila je širina kanala. [5]

Sigurnost i prijetnje u 1G

Mobitelski sustav prve generacije (1G) koristio je analognu komunikaciju, kao što je prethodno rečeno. S obzirom na ranjivu prirodu analogne obrade signala, bilo je teško pružiti učinkovite sigurnosne usluge za 1G. Na primjer, prisluškivanje je predstavljalo vječnu brigu za 1G telefone, jer je bilo moguće da netko sluša privatnu komunikaciju između dva korisnika. Sve što je bilo potrebno jest jednostavan prijemnik koji radi na sličnim frekvencijama. U komunikaciji u 1G mrežama nije postojala nikakva povjerljivost.

Također, identitet mobitela mogao bi se lako kopirati, a svi troškovi poziva s dupliciranog telefona mogli bi se usmjeriti na izvornog vlasnika. Budući da je mreža bila mala, a mali broj korisnika trebao se servisirati, 1G mobilne mreže su imale ograničen rizik od masovnog kloniranja mobilnih uređaja. Iako su probani u potpunosti riješiti se kloniranja mobilnih uređaja, pokazalo se da nisu bili uspješni. Iako se podaci o biranom broju mogu šifrirati, glavni problem bio je prijenos putem zraka, jer se signali lako mogu primiti bilo kojim FM prijemnikom, budući da se u prijenosu koristi frekvencijska modulacija. [5]

4.2 Druga generacija (2G)

GSM (2G, *Global System for Mobile Communications*) je prvi digitalni mobilni komunikacijski sustav. Dizajniran je za prijenos glasa. Koristi se u spojenom rasporedu u kojem su dodijeljeni fiksni čvorovi prijenosa putem zraka i na mrežnim komponentama. *General Packet Radio Service* (GPRS) je paketna, radijska podatkovna komunikacijska usluga projektirana da zamijeni usluge s prijenosom kanala dostupne u GSM mrežama druge generacije kao i u TDMA mrežama. [4]

Poboljšanje procesnih sposobnosti hardverskih platformi omogućilo je daljnji razvoj 2G radijskih sustava. Shema digitalne modulacije provedena je u 2G-u, usmjeravajući na glasovno tržište. Zbog toga se ukupna učinkovitost sustava brzo poboljšala do prelaska s analogne na digitalnu shemu modulacije. Ukupni kapacitet u 2G-u poboljšan je korištenjem digitalnih govornih kodova, provođenjem vremenske podjele i tehnika *Code Division Multiplexing* (CDM) za multipleksiranje više korisnika pomoću jednog kanala. U 2G-u su

uvedeni i jači sigurnosni sustavi primjenom algoritama za šifriranje koji nisu bili prisutni u 1G-u.

Još jedna atraktivna značajka druge generacije, u suradnji s ostalim novim aplikacijama, bila je usluga kratkih poruka (SMS). Prvi SMS poslan je putem Vodafone GSM mreže 3. prosinca 1992. godine u Ujedinjenom Kraljevstvu. Postupno su neke europske zemlje primijenile ovu uslugu kako bi obavijestile korisnike o govornoj pošti. Nokia je izdala svoj prvi mobilni telefon koji podržava SMS, a koji je mogao slati SMS od jednog korisnika do drugog. Danas preko 50 milijardi SMS poruka se dnevno šalje preko mobilnog operatera u cijelom svijetu. 2G sustavi razvili su se za podršku paketnih usluga, dok je prethodna metoda bila podatkovna usluga s komutacijskim krugom, koja je bila slična u konceptu *dial-up* modema. Uveden je protokol radijskog pristupa (WAP) radi pružanja internetskog sadržaja ručnim uređajima. [5]

Sigurnost i prijetnje u 2G

2G mobilna mreža razvijena je zbog sve veće potrebe za poboljšanom kvalitetom, kapacitetom i pokrivenosti prijenosa. Napredak u tehnologiji poluvodiča i mikrovalnim uređajima omogućio je digitalni prijenos u mobilnoj komunikaciji. 2G mobilna mreža uključila je podatkovnu komunikaciju, za razliku od 1G, među druge vrste digitalnih usluga poput tekstualnih poruka, slikovnih poruka i MMS-a (multimedijske poruke).

S digitaliziranim uslugama u procesu, povjerljivost podataka i sigurnost postali su glavna briga. 2G ćelijski sustavi se općenito sastoje od GSM, digitalnih AMPS (D-AMPS), CDMA i osobne digitalne komunikacije (PDC). GSM je najuspješniji i najčešće korišteni standard u mobilnoj komunikaciji širom svijeta, kao dio 2G mobilne mreže. Sadrži GSM900, GSM-željeznicu (GSM-R), GSM1800, GSM1900 i GSM400. 2G telefoni koji koriste GSM prvi su put predstavljeni oko 1990. godine. Prvi put su korišteni u Finskoj u srpnju 1991. godine IS-95 ili CDMAONE, druga tehnologija pod pokroviteljstvom 2G, utemeljena na CDMA, za razliku od GSM-a, temeljenog na vremenskoj podjeli s višestrukim pristupom (TDMA). Međutim, upotreba GSM-a znatno je veća od IS-95. Nasljednik GSM-a je širokopojasni CDMA (W-CDMA), dok je nasljednik IS-95 CDMA 2000. Kako bi se razumjele sigurnosne mjere u 2G mobilnim mrežama, najprije se mora razumjeti sigurnost u GSM-u. Dopunski kodni kanal (SCH) uveden je u verziji IS-95B. Poznat je i kao paketni način prijenosa radi veće učinkovitosti. [5]

4.3 Treća generacija (3G)

UMTS (3G, Univerzalni mobilni telekomunikacijski sustav) je osmišljen radi sve veće potražnje korisnika za prijenosom podataka. Sljedeća generacija optimizirana je za prijenos podataka na radijskom sloju. Uz to, UMTS je dodao nove sigurnosne značajke kao što su međusobna provjera autentičnosti i novi algoritmi za enkripciju. Iako je mreža u svojoj jezgri uključena u paket, glasovni i SMS prijenosi i dalje se nude kao različite mrežne usluge. [4]

Sustavi treće generacije (3G) pružali su veće brzine podataka uz veći kapacitet za prijenos glasa, a i naprednih značajki poput aplikacija i multimedije. Planiranje za 3G započelo je početkom 1990-ih, na poziv prijedloga Međunarodne unije za telekomunikacije (ITU) poznate kao IMT-2000. Započeli su sa istraživanjem spektra za ove sustave. Cilj je bio provesti specifikacije za globalnu harmoniju mobilne komunikacije, koja je u stanju pokrenuti globalnu unutarnju komunikativnost pružajući niže troškove.

ITU je postavio kriterij za IMT-2000:

- u brzini prijenosa podataka lokalno ili okruženju od 2 Mb/s,
- za urbane sredine od 384 kb/s,
- za šira okruženja od 144 kb/s.

Osim gore navedenih zahtjeva, 3G sustavi trebali su osigurati i bolju kvalitetu usluge (QoS) za govornu telefoniju i interaktivno igranje putem Interneta, pregledavanja e-pošte i strujanja multimedijskih aplikacija. [5]

Sigurnost i prijetnje u 3G

Kao što je gore spomenuto, mobilne mreže treće generacije uvele su usluge kao što su video, audio i multimedijski programi. Također je uvela video telefoniju i video produkciju komunikacijom putem mobilnih mreža. Bilo je to privlačno obilježje mobilnih mreža, kada se pogledala evolucija kroz koju je prolazila. Objektivno od ograničenja mobilne mreže 1. generacije, bio je svojevrsni orijentir. CDMA 2000 i UMTS CDMA našli su se u sklopu 3G-a. 3G ili UMTS (*Universal Mobile Telecommunications*), posebno IMT-2000, pružili su jedinstveni kompatibilni standard za mobilne mreže koji se može koristiti širom svijeta za sve mobilne aplikacije. [5]

4.4 Četvrta generacija (4G)

LTE (4G, *Long Term Evolution*) koristi potpuno redizajnirani radijski sloj i strogu paketno-preklopljenu arhitekturu koja se temelji na IP-u sa osiguranim klasama usluge (QoS). Za razliku od svojih prethodnika, prijenos glasa i SMS-a više nije mrežna usluga, već se nudi kao IP-usluga (SIP, VoIP) na vrhu opće namjenske IP mreže podataka. Međutim, rezervne opcije postoje za telefone ili operatere koji ne podržavaju *Voice over* LTE (VoLTE).

Nazivi i skraćenice za ekvivalentne mrežne komponente i koncepte razlikuju se u različitim generacijama mreža. Sve u svemu, generacije se trude opstati i pristupiti tehnologijama. Ako trebamo posebno razlikovati različite pojmove, označit ćemo ih 2G za GSM, 3G za UMTS i 4G za LTE. [4]

4G je četvrta generacija mobilne telekomunikacijske tehnologije. Zahtjeve 4G sustava definirao je ITU u IMT *Advanced*-u.

Uvjeti su:

- visok stupanj dijeljenja ima značajke širom svijeta, što treba podržati širokim spektrom usluga i aplikacija s troškovnom učinkovitošću,
- kompatibilnost s mrežnim mrežama unutar IMT-a, ali i s ostalim radio pristupnim mrežama,
- kompatibilnost usluga s fiksnom i IMT mrežom,
- mobilni uređaji visoke kvalitete,
- mogućnost *roaminga* u cijelom svijetu,
- oprema, usluge i aplikacije prilagođene korisnicima,
- 100 Mb/s za visoku mobilnost i 1 Gb/s za uređaje razmjerno male mobilnosti za podršku naprednih usluga. [5]

Sigurnost između 3G i 4G mobilnih mreža

Mobilne mreže četvrte generacije obećavaju da će omogućiti veće korisničke brzine podataka, niže vrijeme čekanja te potpunu mrežnu arhitekturu zasnovanu na internetskom protokolu (IP). Glavna razlika između 3G i 4G mobilne mreže je ta što 4G djeluje u potpunosti na IP protokolu i arhitekturi. Iz tog razloga, WiMAX se također smatra dijelom 4G mreža. Dok se raspravlja izvan 3G tehnologija, glavna podloga koja se koristi je LTE. Iako se sličnost između LTE i WiMAX može izvući, zbog protokola i arhitekture temeljenog na IP-u oni se međusobno razlikuju u mrežnoj arhitekturi i sigurnosti. Sva infrastruktura utemeljena na IP-u povećava sigurnosna pitanja u usporedbi sa tehnologijama prethodne generacije. Zbog toga se u 4G mrežama očekuje provođenje dodatnih sigurnosnih mehanizama koji će pružiti sigurnost za pouzdanu komunikaciju.

Sigurnost i prijetnje u 4G

Glavna briga u sigurnosti 4G mreža uključuje to da korisnik koji želi pristupiti mreži mora biti prepoznat u suradnji s uređajem koji će biti spojen na mrežu. Iz tog razloga se za provjeru autentičnosti koriste sigurnosne vjerodajnice, identitet, potvrde, korisničko ime i lozinka. Ako napravimo usporedbu, počevši od 2G kada se sigurnost počela uzimati kao glavna briga u mobilnim mrežama, na SIM kartici u 2G-u koristio se jedinstveni ID. Dok se u 3G-u i 4G-u LTE koristi privremeni ID i dodatna apstrakcija za ograničavanje mogućnosti bilo kakve provale. U 4G-u uvodi se daljnja sigurna signalizacija između UE i MME (Entitet za upravljanje mobilnim uređajima), a poduzimaju se i sigurnosne mjere između 3GPP i nepovjerljivih korisnika koji nisu 3GPP. Kao što je već spomenuto, zbog korištenja otvorene arhitekture zasnovane na IP-u, sigurnost ostaje važna briga u 4G mobilnoj mreži. Važno je naglasiti da su LTE- i LTE-*Advanced* iste tehnologije. Oznaka "*Advanced*" prvenstveno je dodana kako bi se naglasila veza između izdanja LTE 10 (LTE-*Advanced*) i ITU / IMT *Advanced*. Time se LTE-*Advanced* ne razlikuje od LTE-a. [5]

5. 5G MREŽA

5.1 Što je 5G?

Pojam "5G" koristi se za označavanje pete generacije mobilnih radijskih tehnologija, koja je nastala analognom mobilnom telefonijom krajem osamdesetih i napredovala je do točke kad se svi ljudi i stvari mogu povezati na Internet. Svaka generacija mobilne tehnologije imala je za cilj povezivanje bilo gdje i bilo kada. Međutim, temeljni tehnološki ciljevi i mogućnosti mreže nastavili su se mijenjati u novu generaciju svakih 7 do 10 godina, s tim da je svaka generacija dizajnirana tako da služi društvenim potrebama u trajanju od 2 do 3 desetljeća na tržištima širom svijeta. Utjecaj tih generacija na način na koji komuniciramo može se promatrati u različitim dimenzijama.

Tu spadaju:

- ponuda usluga,
- zračna sučelja,
- brzina prijenosa podataka,
- rasponi spektra i
- performanse.

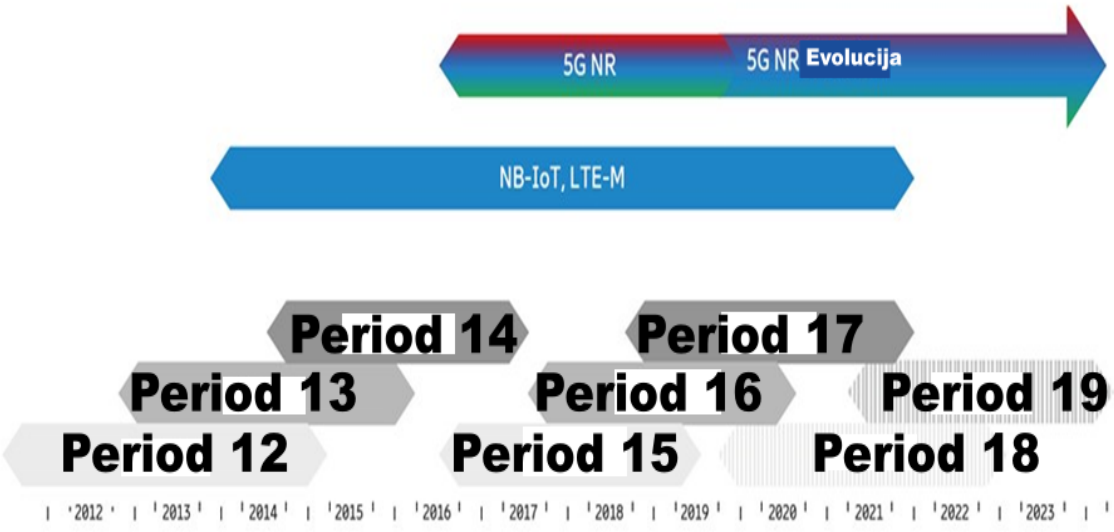
Ranije generacije započele su sa samo telefonskim razgovorima, dok su se kasnije one razvile u digitalnu komunikaciju podataka i sofisticiraniju arhitekturu usluga. U skladu s tim, fokus u prošlim generacijama bio je dosljedno na radu u širim rasponima spektra i s većom stopom podataka i mogućnostima prometa. Ti su ciljevi i dalje važni i danas, jer će 5G moći raditi u mnogo širem rasponu frekvencijskih opsega nego ikad prije. Najviše pozornosti privlači masovna IoT podrška, razvoj podrške važnim uslugama i ponovno osmišljavanje funkcionalnosti središnje mreže.

Kombinacija mobilnih tehnologija kao što su 5G NR, *Long-Term Evolution* (LTE) i NB-IoT (*Narrowband Internet of Things*) bave se širokim dosegom mobilnih komunikacija, obuhvaćajući javne telekomunikacijske usluge kao i energiju, promet i pametne gradove. 5G NR nudi podršku važnim uslugama koje postavljaju ekstremne zahtjeve za kašnjenje i pouzdanost veze, dok LTE za komunikaciju putem stroja (MTC) (aka LTE-M) i NB-IoT rješavaju ogroman broj IoT uređaja koji se često koriste kao senzori i pokretači s ograničenjima energije i snage.

Sustav 5G izgrađen je na radio pristupnim čvorovima, distribuiranim i centraliziranim podatkovnim centrima, omogućavajući fleksibilnu raspodjelu radnog opterećenja. Ti su čvorovi i podatkovni centri povezani preko programibilnih prometnih mreža, koji su povezani preko matičnih čvorova koji prenose informacije iz pristupnih čvorova u podatkovne centre, gdje se pohranjuje većina podataka i upravlja sama mreža. Uz to, upravljanje aplikacijama, oblakom, transportnim i pristupnim resursima može se dodijeliti centralno u podatkovnom centru ili se prema potrebi fleksibilno dodijeliti.

5G sustavi imat će značajnu ulogu, ne samo u evoluciji komunikacija, već u razvoju poslovanja i društva u cjelini. Sustav 5G osmišljen je za upravljanje nevjerojatnim povećanjem prometa iz prethodnih godina na način na koji dionici mogu uhvatiti vrijednost s minimalnim utjecajem na neto troškove potrošača. Na kraju 2019. godine Ericssonovo izvješće o mobilnosti bilježi razinu globalnog prometa s 38 egzabajta mjesečno, s projiciranim četverostrukim porastom na 160 eksabajta mjesečno do 2025. godine.

Kao i prethodnih generacija, 5G radio pristupne tehnologije leže u srcu 5G sustava, pružajući radijsku povezanost za širok spektar novih aplikacija i slučajeva korištenja, od kojih najvažnije uključuju industrije poput automobilske industrije, logistike, javne sigurnosti, medija i proizvodnje. Kao rezultat, ubrzao je razvoj i provedbu IoT-a. [6]



Slika 5.1.1 Vremenski plan 5G i 3GPP [6]

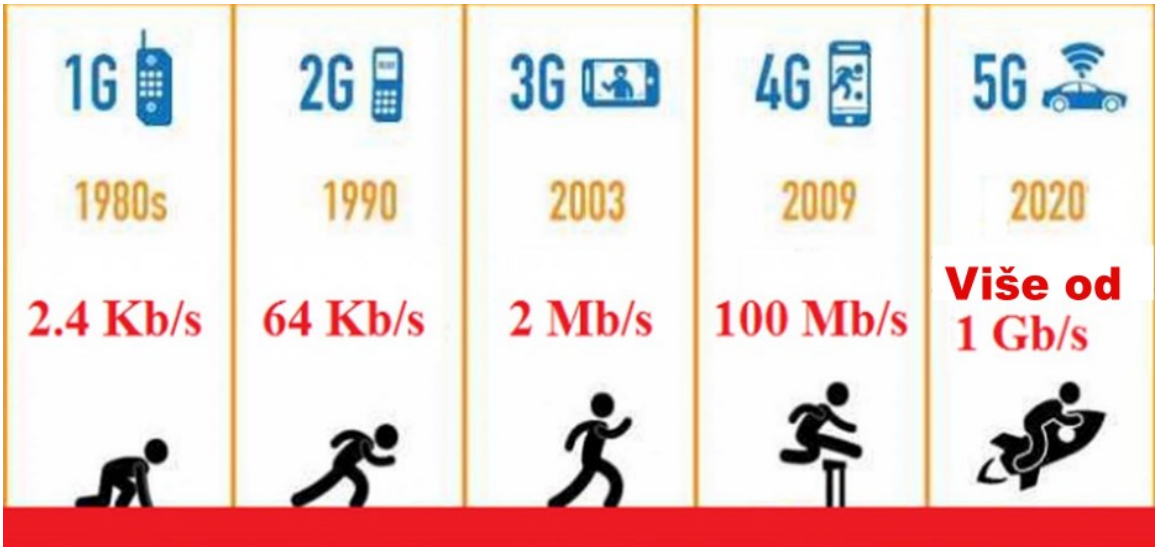
Promatrajući sliku 5.1.1 može se vidjeti da vremenski plan 5G i 3GPP zahvaća izdanja 12 do 19. NB-IoT i LTE-M razvijaju se u izdanju 3GPP-a 17. Preklapanja između prikazanih izdanja 3GPP nastaju zbog činjenice da izdanja počinju uslugama i sistemskim aspektima (SA) otprilike godinu dana prije početka RAN specifikacija.

5.2 Što je novo s 5G?

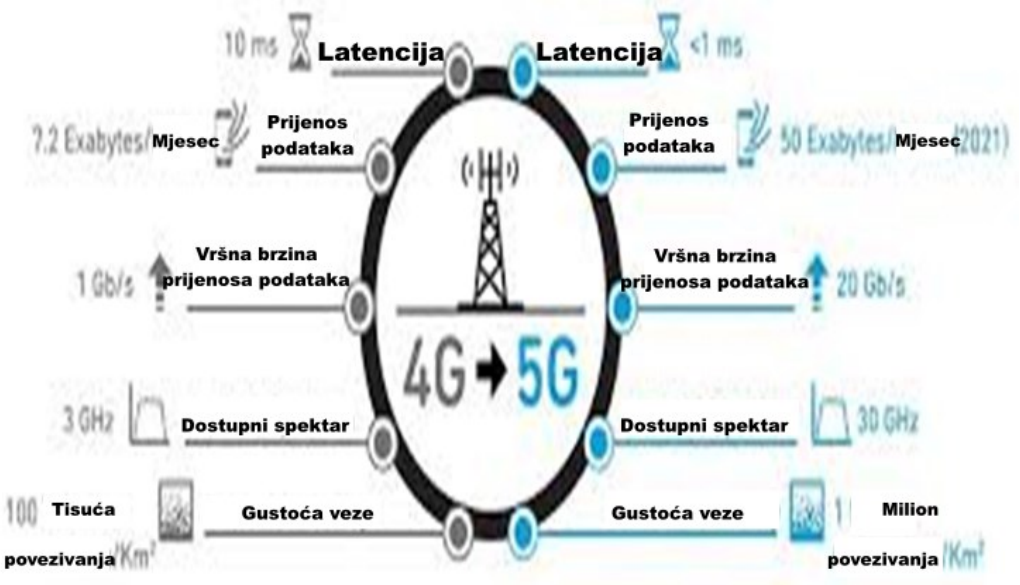
5G je sljedeća generacija 3GPP tehnologije nakon 4G / LTE definirana za radijsku mobilnu podatkovnu komunikaciju. Počevši s izdanjem 3GPP-a od 15. nadalje, 3GPP je započeo s definiranjem standarda za 5G. Definira se radijska i paketna jezgra koja zadovoljava potrebe 5G mreža.

Ispod su navedeni neki od ključnih krajnjih ciljeva 5G:

- Vrlo visoka propusnost (1-20 Gb/s),
- Ultra niska latencija (<1ms),
- 1000 x širine pojasa po jedinici površine,
- Masivna povezanost,
- Visoka dostupnost,
- Gusta pokrivenost,
- Mala potrošnja energije,
- Do 10 godina trajanja baterije za komunikaciju na stroju. [7]



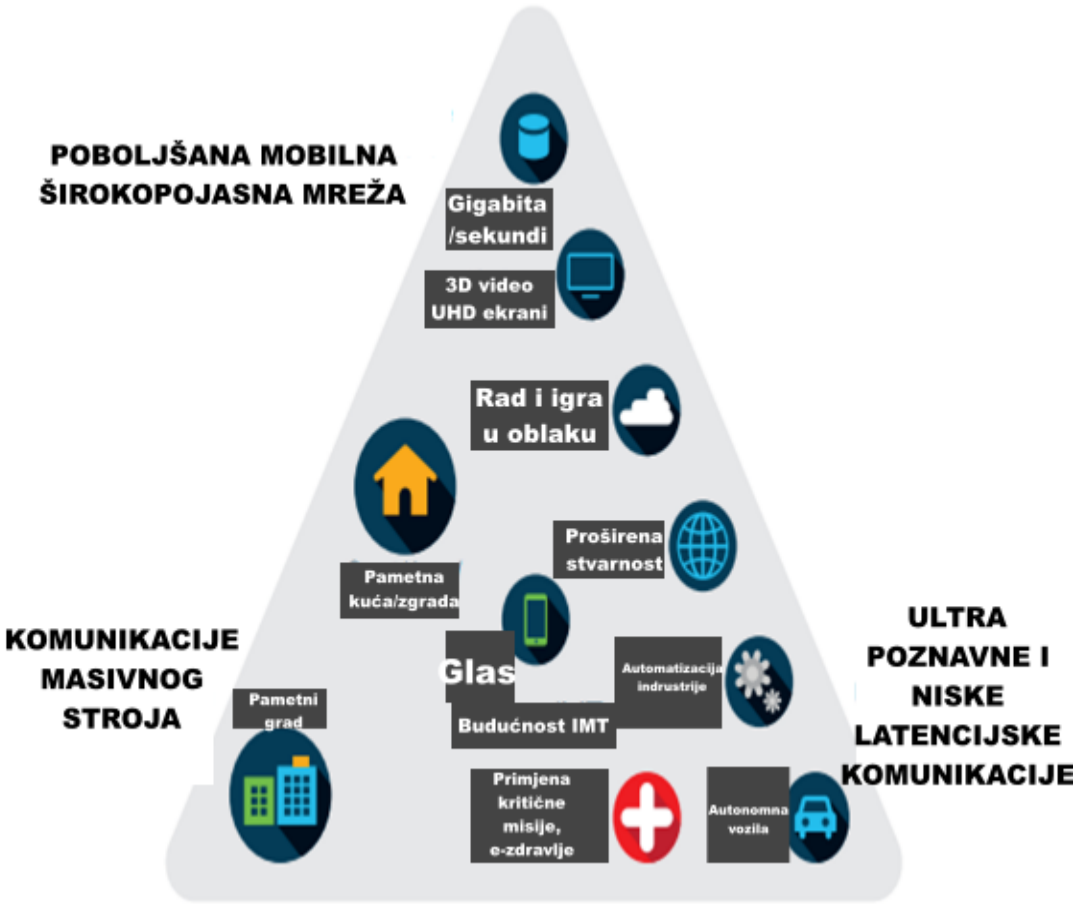
Slika 5.2.1 Prikaz brzine prijenosa podataka u radijskim mrežama [10]



Slika 5.2.2 Usporedba četvrte i pete generacije mobilnih mreža [10]

5.3 Upotreba 5G sustava

Ispod je grafikon koji ilustrira široke kategorije slučajeva korištenja 5G:



Slika 5.3.1 Kategorije korištenja 5G

Ispod su navedene 3 različite kategorije koje će pokriti sve slučajeve uporabe.

- *Enhanced Mobile broadband* (eMBB): 5G poboljšana širokopojasna mreža (eMBB) pretplatniku donosi obećanje o brzoj i širokopojasnoj mreži. S gigabitnim brzinama, 5G nudi alternativu tradicionalnim fiksnim uslugama. Fiksni radijski pristup utemeljen na mmWave radio tehnologijama omogućuje gustoću podržavanja usluga velike propusnosti poput video zapisa preko 5G radijske veze. Da bi podržao slučajeve korištenja eMBB, mobilna jezgra mora podržavati potrebnu gustoću performansi, skalabilnost i sigurnost. [7]
- *Massive Machine Type Communications*: Ovaj se scenarij upotrebe odnosi na velik broj povezanih uređaja koji obično prenose relativno malu količinu podataka kao što su senzori i pomoćna brojila. Potrebno je da ovi uređaji budu jeftini i imaju dugo trajanje baterije. Neki tipični primjeri 5G usluga u ovoj kategoriji su kontrola zaliha, pametni grad, pametno mjerenje, video nadzor itd.
- *Ultra-reliable low latency Communications* (*Robotics, Factory Automation*): Ovaj scenarij upotrebe govori o mogućnostima pružanja određene usluge strogim zahtjevima u pogledu ultra-niske latencije, ultra visoke pouzdanosti i dostupnosti, kao i velike propusnosti. Neki tipični primjeri 5G usluga u ovoj kategoriji su automobili s autonomnom vožnjom, pametne mreže, *e*-zdravlje, taktilni Internet, daljinska kirurgija, industrijska automatizacija i kontrola itd. [5]

5.4 5G za Internet stvari (IoT)

Mnoge industrije već upotrebljavaju prednosti mobilne povezanosti, na primjer, u elektronici, automobilskoj industriji, željeznici, rudarstvu, komunalnim uslugama, zdravstvu, poljoprivredi, proizvodnji i prometu. U 2020. postoji preko milijardu mobilnih internetskih veza (IoT), a Ericsson predviđa oko 5 milijardi veza do 2025. godine. Gotovo svaka industrija istražuje potencijal 5G za temeljnu transformaciju svog poslovanja.

Slika 5.4.1 5G za Internet stvari (IoT) [6]

Radijsko povezivanje u različitim industrijama može se grupirati u četiri različita skupa zahtjeva. Za rješavanje ovih zahtjeva, Ericsson je definirao četiri segmenta IoT povezivanja: *Massive* IoT, širokopojasni IoT, važni IoT i industrijska automatizacija IoT-a. Svaki segment povezivanja IoT je višenamjenski i bavi se sa više slučajeva uporabe u više industrija.

- *Massive* IoT rješava ITU-R mMTC zahtjev s NB-IoT i kategorijama M ili Cat-M uređajima (serija uređaja niske složenosti definirana kao dio LTE-M). LTE-M / NB-IoT može učinkovito funkcionirati s 5G NR u istom spektru i ispuniti sve 5G ogromne MTC zahtjeve, kako je utvrđeno u IMT-2020 i 3GPP standardima, u pogledu pokrivenosti, kašnjenja, brzine prijenosa podataka, dugog vijeka trajanja baterije i gustoće veze.
- Širokopojasni IoT povezivanjem prihvaća mogućnosti eMBB za IoT u smislu pružanja velikih količina prijenosa podataka, puno veće brzine podataka i nižih kašnjenja od *Massive* IoT-a, istovremeno omogućava dodatne mogućnosti za IoT kao što su produženi vijek trajanja baterije, proširena pokrivenost i velike brzine prijenosa

podataka. Od 2020. postoji više od 500 milijuna korisnika širokopojasnog IoT-a. Komercijalnom uporabom danas dominiraju osobni automobili, komercijalna vozila, vlakovi, nosive opreme, uređaji, kamere, senzori itd.

- Važna IoT povezanost namijenjena je vremenski važnoj komunikaciji. Omogućuje ultra pouzdanu i / ili ultra nisku latencijsku komunikaciju pri različitim brzinama prijenosa podataka. Za razliku od širokopojasnog IoT-a koji postiže nisku latenciju na osnovi prosječnog i najboljeg napora, *Critical* IoT može isporučiti podatke unutar zadanih granica kašnjenja s traženom razinom garancije, čak i u jako opterećenim mrežama. Takvi vremenski važni slučajevi upotrebe postoje u gotovo svakoj industriji.
- Industrijska automatizacija IoT ima za cilj omogućiti izraženu integraciju stanične povezanosti u žičnu industrijsku infrastrukturu koja se koristi za naprednu automatizaciju u stvarnom vremenu. Uključuje mogućnosti za integriranje 5G sustava s industrijskim protokolima temeljenim na *Ethernetu* i vremenski osjetljivim mrežama. [6]

5.5 Dizajn i arhitektura 5G mreže

Tijekom proteklih desetljeća, mobilne komunikacije su napredovale od isključivo prijenosa glasa, do današnjih „uvijek uključenih“ komunikacija. Velik napredak je vidljiv i u individualnim komunikacijama. U ranim danima ona se mogla isključivo obavljati od čovjeka do čovjeka, a danas je moguće komunicirati s jednim mobilnim uređajem prema svima, odnosno prema fiksnim ili mobilnim (autonomnim ili upravljanim od strane ovlaštene osobe) komunikacijama, uključujući usluge bazirane u aplikacijskom oblaku.

Percepcija mobilnih uređaja u potpunosti se promijenila. U nastajanju mobilnih mreža, težilo se da korisnik bude u centru odvijanja komunikacija, a danas je to slučaj sa sadržajem. Sadržaj je u centru odvijanja komunikacija te nam može ponuditi mnogo usluga vezanih uz naš uređaj. Glavni izazov svih mobilnih operatera u stvaranju mobilne mreže pete generacije (5G) upravo će biti postavljanje sadržaja potrebnog korisnicima u oblak. Takav način komunikacije bi korisnicima dao potpuno nove mogućnosti u korištenju mobilne mreže.

Mobilna mreža pete generacije neće biti samo evolucija širokopojasne mreže, već jedinstvena mreža s potpuno novim uslužnim mogućnostima. Kao prvo, osigurat će korisniku vrlo velike brzine prijenosa podataka u slučaju visoke mobilnosti (npr. vožnja automobilom po autoputu) ili u područjima manje naseljenosti, novim tehnologijama. Kasnije, novim verzijama i

nadogradnjama, 5G mreža će biti ključ u povezivanju svih uređaja u jednu cjelinu, zvanu Internet stvari (engl. *Internet of Things – IoT*).

5G mreža pružit će korisniku niz poboljšanja performansi u smislu povećanja kapaciteta mreže, manjeg vremena čekanja (latencije), više mobilnosti te povećanje pouzdanosti i sigurnosti mreže. Omogućit će bolju povezanost uređaja na istu baznu stanicu, produljit će vijek trajanja baterija uređaja i pomoći korisnicima u upravljanju vlastitim podacima.

Dizajn mreže osiguravat će veću fleksibilnost, a sama mreža bit će temeljena na uslužnom pristupu (engl. *service approach*), što znači da će svi podaci i alati biti pohranjeni u oblaku i uvijek biti dostupni korisniku na bilo kojem mjestu. Mreža će se brzo prilagođavati raznim zahtjevima korisnika pružajući mogućnost kontrole bilo kojeg resursa iz područja IT (engl. *Information Technology*) tehnologija.

Arhitektura 5G mreže, prikazana na slici 5.5.1, drastično će se promijeniti u usporedbi s prijašnjim generacijama, u cilju postizanja željenih performansi, osobito smanjenja vremena kašnjenja i pouzdanosti te podrški novim poslovnim modelima. Arhitektura će težiti podrški širokom opsegu aplikacija kao što je mobilni Internet visokim brzinama (engl. *multi-Giga-biper-second*) pa sve do direktne komunikacije između dva ili više susjedna uređaja (engl. *Device to Device – D2D*) ili komunikacije vozila s okolinom (engl. *Vehicle to X or Vehicle to Vehicle – V2X or V2V*) što će uvelike pomoći pri izbjegavanju zagušenja u prometu, nezgoda na cesti i smanjenju ispušnih plinova. [42]

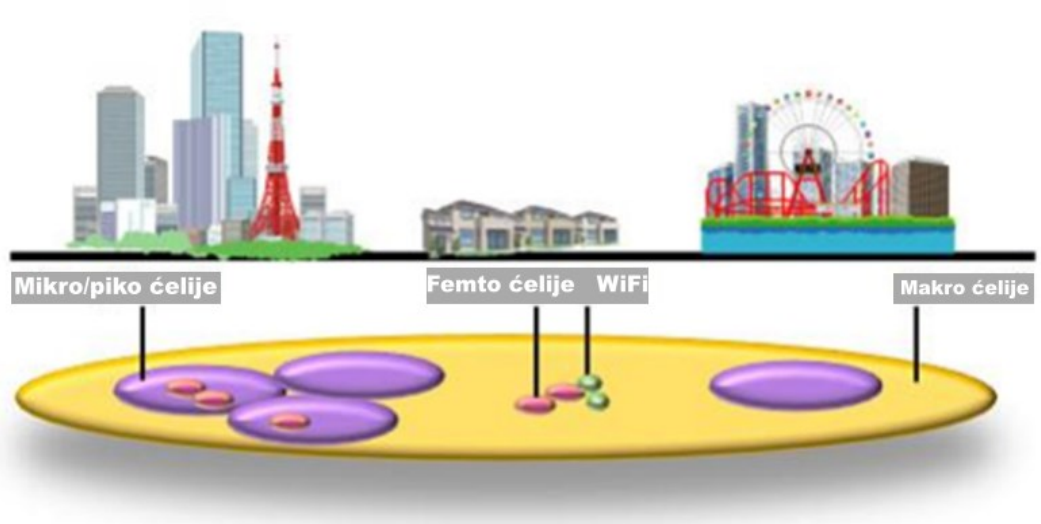
Slika 5.5.1 Arhitektura 5G mreže [43]

Računarstvo u oblaku (engl. *Cloud computing*) temelji se na pružanju računalnih resursa kao usluge umjesto kao proizvoda. Usluga se krajnjim korisnicima dostavlja preko Interneta, a korisnik plaća uslugu onoliko koliko je koristi. Osnovna ideja ovog servisa je pružanje računalnih sadržaja po potrebi u bilo koje vrijeme na bilo kojem mjestu, uz jedini uvjet, Internet vezu. Glavna karakteristika ovog servisa je pružanje usluge na zahtjev, što omogućuje veliku elastičnost mreže. Dijeljenje sadržaja pohranjenog u oblaku može se odvijati isključivo iz jednog oblaka ili više oblaka koji su povezani, udruživanjem resursa. Stupanj i vrijeme dostupnosti svakog privatnog sadržaja u oblaku kontrolira korisnik te postavlja sigurnosne postavke kome će taj sadržaj biti vidljiv, a kome ne. [43]

MIMO antenske konfiguracije su nužne za tehnologiju pete generacije. U svakoj baznoj stanici implementirat će se masivna MIMO tehnologija (engl. *Massive MIMO technology*) što znači da će svaka bazna stanica sadržavati vrlo velik broj antena u svrhu povećanja brzine podataka i kapaciteta mreže. Masivna MIMO tehnologija omogućit će posluživanje puno većeg broja korisnika istovremeno u istom frekvencijskom opsegu uz znatnu uštedu energije,

uporabom jednostavne sheme upravljanja snagom. *Smart grid* tehnologija je još jedna u nizu zanimljivih aplikacijskih rješenja predviđenih za 5G, a temelji se na upotrebi naprednih informacijskih i telekomunikacijskih tehnologija koje omogućuju lakše i učinkovitije upravljanje električnom energijom u smislu uštede. [45]

Predviđa se nadogradnja postojećih pristupnih mreža s potpuno novom tehnologijom, koja radi u iznimno visokim frekvencijama. Takva tehnologija će omogućiti revoluciju u mobilnoj industriji, ne samo zbog velike širine slobodnog frekvencijskog pojasa, nego i mogućnosti smanjenja veličine antena koje se ugrađuju u uređaje. Visoke frekvencije su vrlo kratkog dometa (oko 1 kilometar), pa se ćelijske konstrukcije moraju postaviti na manjoj udaljenosti kako bi cijelo područje prekrivanja bilo prekriveno signalom. Takav način postavljanja ćelija naziva se razvoj manjih ćelija visoke gustoće (engl. *Hyperdense small-cell deployment*) te smanjuje udaljenost bazne stanice od uređaja na minimum. Manje ćelije se još dijele na: mikro ćelije, piko ćelije i femto ćelije, poredane po veličini snage raspršivanja signala, od najjače do najslabije. Razvoj tehnologija poput ove, omogućuje mreži pete generacije izvršenje svog cilja k povećanju kapaciteta od 1000 puta u odnosu na prethodnu mrežu. Uobičajene bazne stanice, poput današnjih, dobit će ulogu makro ćelija i bit će zadužene za upravljanje nad manjim ćelijama kao što je vidljivo na slici 5.5.2. [43]



Slika 5.5.2 Razlike u snazi signala različitih veličina ćelija [43]

Ljubičastom bojom označena je snaga mikro i piko ćelije, crvenom bojom snaga femto ćelije i žutom bojom snaga makro ćelije.

6. SIGURNOST 5G MREŽE

U ovom će se odjeljku obraditi sigurnosna arhitektura, definirati glavni koncept naše predložene sigurnosne arhitekture i njezine primjene. Također, navodimo ciljeve koje bi 5G sigurnosna arhitektura trebala ispuniti. Kroz zadnji odjeljak navode se potencijalni problemi i nedostatci sigurnosti u 5G-u.

5G razvija se s novim konceptima i mogućnostima kako bi novi poslovni modeli mobilnim operaterima omogućili pružanje poboljšanih aplikacija i usluga pretplatnicima mobilne mreže. Da bi se osiguralo da 5G ispuni svoje obećanje, potrebno je riješiti sva sigurnosna pitanja koja prate 5G arhitekturu. [15]

5G pružit će širokopojasne usluge, omogućiti povezivanje ogromnog broja uređaja u obliku IoT-a te omogućiti korisnicima i uređajima velike mobilnosti na vrlo pouzdan i pristupačan način. Razvoj prema komunikaciji zasnovanoj na IP u 4G-u već je pomogao razvoju novih poslovnih prilika, međutim, 5G smatra se novim ekosustavom koji povezuje gotovo sve aspekte društva; vozila, kućanske aparate, zdravstvo, industriju, poduzeća itd., na mrežu. Međutim, ovaj će razvoj donijeti nove prijetnje i sigurnosne ranjivosti koje će predstavljati veliki izazov kako sadašnjim tako i budućim mrežama. Stoga se sigurnost 5G-a i sustava spojenih putem 5G-a mora razmotriti odmah od faza dizajna. Da bismo razvili sigurnosne implikacije u 5G-u, principi dizajna 5G-a ukratko su dolje razrađeni. [26]

6.1 Pregled sigurnosnog dizajna 5G mreže

Slika 6.1.1 Pregled sigurnosnog dizajna 5G mreže [26]

S novim vrstama usluga i uređaja te novim zahtjevima korisnika u pogledu niskog kašnjenja, veće propusnosti i pokrivenosti, javlja se potreba za novim načelima dizajna za 5G. Principi dizajna 5G-a opisani u NGMN, prikazani na slici 6.1.1, ističu potrebu za visoko elastičnim i robusnim sustavima. Radijski dio mreže treba ogromnu efikasnost spektra, isplativo gusto raspoređivanje, učinkovitu koordinaciju, poništavanje smetnji i dinamične radio topologije. Na primjer, zajednička sastavna jezgra će koristiti SDN i NFV za razdvajanje korisničke i upravljačke ravnine i omogućavanje dinamičkog postavljanja mrežnih funkcija. Ovaj je cilj usmjeren na minimiziranje naslijeđenih mreža i uvođenje novih sučelja između osnovne i radio pristupne tehnologije (RATs).

5G mrežna arhitektura mora podržavati provedbu sigurnosnih mehanizama i funkcija (npr. Virtualnih zaštitnih zidova) kad god je to potrebno u bilo kojoj mrežnoj ravnini. Kao što je prikazano na slici 6.1.1, potrebno je pojednostaviti rad i upravljanje. Najistaknutija tehnologija za pojednostavljenje upravljanja mrežom je SDN. SDN razdvaja upravljačku mrežu od ravnine prosljeđivanja podataka. Upravljačka ravnina je logično centralizirana da nadgleda cijelu mrežu ispod i kontrolira mrežne resurse putem programibilnih aplikacijskih programskih sučelja (API-ja). Međutim, centraliziranjem mrežne kontrole i uvođenjem programibilnih API-ja u mrežnu opremu također se otvaraju rupe za sigurnosne ranjivosti.

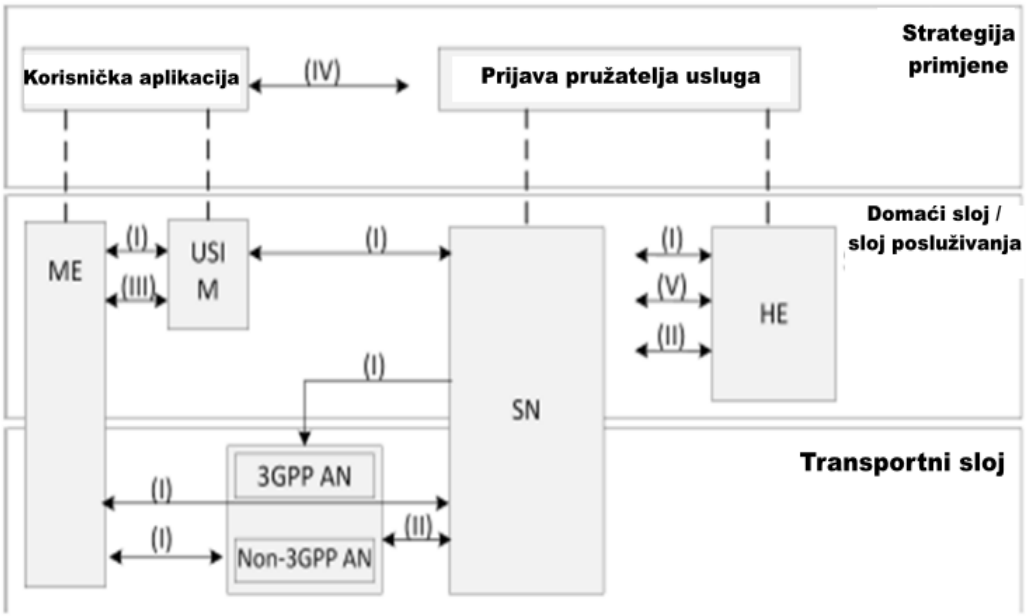
Stoga se mora analizirati sigurnosni izazov povezan sa SDN-om. Stoga, sigurnosni izazovi povezani sa svim tehnologijama koje koristi 5G trebaju biti istraženi na pravi način. U sljedećem pododjeljku daje se kratki pregled sigurnosne arhitekture 5G, usredotočujući se uglavnom na sigurnosne domene definirane u 3GPPP. [26]

6.2 Pregled sigurnosne arhitekture

Prema ITU-T, sigurnosna arhitektura dijeli sigurnosne značajke na posebne komponente. To omogućava sustavni pristup cjelovitoj sigurnosti novih usluga koji olakšava planiranje novih sigurnosnih rješenja i procjenu sigurnosti postojećih mreža. Sigurnosna arhitektura 5G definirana je u najnovijem izdanju tehničke specifikacije 3GPP s različitim domenama.

Sigurnosna arhitektura prikazana je na slici 6.2.1, osim domene (VI) ima sljedeće glavne domene:

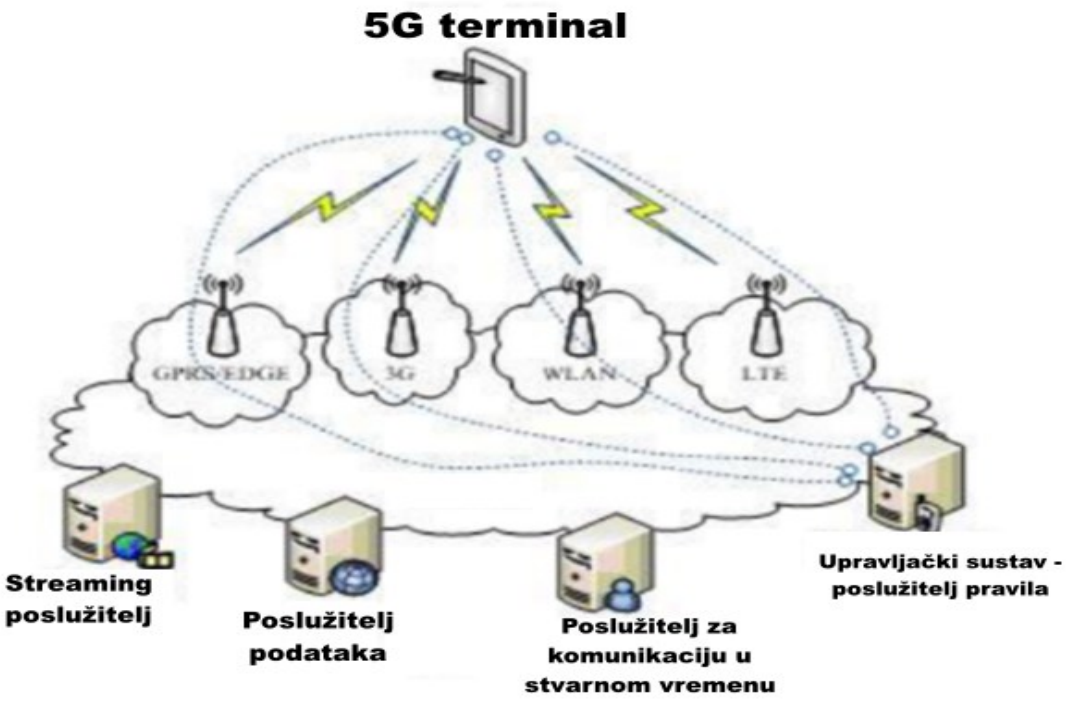
- Sigurnost mrežnog pristupa (I): sastoji se od skupa sigurnosnih značajki koje omogućuju UE sigurno provjeravanje autentičnosti i pristupa mrežnim uslugama. Sigurnost pristupa uključuje sigurnost 3GPP i ne-3GPP pristupnih tehnologija i isporuku sigurnosnog konteksta iz SN-a u UE.
- Sigurnost mrežne domene (II): sastoji se od skupa sigurnosnih značajki koje mrežnim čvorovima omogućuju sigurnu razmjenu podataka u signalnoj i korisničkoj ravnini.
- Sigurnost korisničke domene (III): sastoji se od sigurnosnih značajki koje omogućuju siguran pristup korisniku UE.
- Sigurnost domene aplikacija (IV): uključuje sigurnosne značajke koje omogućuju aplikacijama (domenama korisnika i dobavljača) da sigurno razmjenjuju poruke.
- Sigurnost domene zasnovana na servisnoj arhitekturi (V): Sadrži sigurnosne značajke za registraciju, otkrivanje i autorizaciju mrežnih elemenata, kao i sigurnost za sučelja utemeljena na usluzi.
- Vidljivost i podesivost sigurnosti (VI): uključuje sigurnosne značajke koje informiraju korisnike da li sigurnosne značajke rade ili ne. [26]



Slika 6.2.1 Pregled sigurnosne arhitekture [26]

Sama sigurnosna arhitektura 5G-a ne definira određene sigurnosne prijetnje i rješenja za te prijetnje. Međutim, postoje određena definirana sigurnosna rješenja ili dolaze iz prethodnih generacija s modifikacijama za poboljšanja ili su novo definirana u skladu s 5G-om. LTE sigurnosni koncepti su polazišta, ali se smatraju referentnim vrijednostima za sigurnost budućih radijskih mreža. U svakom slučaju, vizija visoke razine sigurnosti 5G-a temelji se na: visoko ugrađenoj sigurnosti, fleksibilnim sigurnosnim mehanizmima i automatizaciji. [26]

Na slici 6.2.2 prikazan je model sustava koji predlaže dizajn mrežne arhitekture za 5G mobilne sustave, a sve su bazirane na IP-u modelu. Sustav se sastoji od korisničkog terminala (koji ima presudnu ulogu u novoj arhitekturi) i niza neovisnih, autonomnih tehnologija radijskog pristupa. Unutar terminala svaka se tehnologija pristupa radiju smatra IP vezom s vanjskim internetskim svijetom. Međutim, trebalo bi postojati različito radio sučelje za svaku tehnologiju radio pristupa (RAT) u mobilnom terminalu. Na primjer, ako želimo imati pristup četiri različita RAT-a, moramo imati četiri različita pristupačna sučelja u mobilnom terminalu i da svi budemo istodobno aktivni, s ciljem da ova arhitektura bude funkcionalna. [11]



Slika 6.2.2 Funkcionalna arhitektura za 5G mobilne mreže [11]

6.3 Problemi i nedostatci

U današnje vrijeme, sve više uređaja ima mogućnost spajanja na Internet i sudjelovanja u razmjeni podataka s ostatkom mreže. Od servera velikih IT korporacija do automobila i hladnjaka otvaraju se mogućnosti za neželjene upade i krađu povjerljivih informacija. Nova tehnologija donosi i nove sigurnosne prijetnje. Navedeni su neki od razloga zbog kojih 5G mreža može predstavljati sigurnosni rizik. [26]

- Radi se o novoj tehnologiji čije su komponente nedovoljno testirane,
- 5G omogućuje kretanje i pristup velikoj količini podataka što rezultira širom pozadinom za izvođenje napada,
- Dolazi do većeg problema naspram 4G mreže u pogledu osjetljivih podataka kao što je primjena u zdravstvu.

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. [27]

7. PRIVATNOST KORISNIKA, IDENTITET I POVJERENJE U 5G

Ovo se poglavlje prije svega fokusiralo na izazove privatnosti, identiteta i povjerenja korisnika u budućim 5G sustavima. Svi se subjekti i akteri koji sudjeluju u tehnologiji 5G nesumnjivo slažu da će se 5G bez ispravnog rukovanja privatnošću suočiti s većim preprekama na putu potpunog prihvaćanja, usvajanja i uspjeha među svojim korisnicima. Sa stajališta korisnika, podaci, lokacija i privatnost identiteta osnovni su elementi koje treba uzeti u obzir. U 5G sustavu značajke privatnosti moraju se uzeti u obzir od faze dizajniranja i neke od njih treba ugraditi u sustav. Nadalje, sustav bi trebao biti dovoljno inteligentan i u skladu s tim može usvojiti privatnost prema stupnju važnosti usluga. Aplikacije i usluge koje imaju kontekst također će zahtijevati usmjerenija rješenja o privatnosti. 5G bit će pokretačka snaga mnogih drugih tehnologija, poput IoT-a i zato bi ogroman broj korisnika i pametnih uređaja došao u napast. Potrebno je imati siguran mehanizam upravljanja identitetom i za pretplatnika i za uređaj. Privatnost ponekad ima sukob s povjerenjem, jer više povjerenja u davatelja usluga može povećati rizik od kršenja privatnosti. Budući sustavi 5G uvest će nove poslovne modele koji će s vremenom povećati broj sudionika, stoga će ključna povezanost među njima biti od presudne važnosti. 5G tehnologija mogla bi upotrijebiti neke slične koncepte s postojećim modelima povjerenja, zajedno s dodavanjem nekoliko novih aktera i entiteta. [5]

5G sustavi sljedeći su glavni prijelaz na putu buduće mobilne komunikacije. Porast novih poslovnih modela, arhitekture i tehnološke promjene u 5G-u donijet će nove izazove privatnosti korisnika. Zahtjevi za privatnost jedan su od ključnih elemenata koji treba uzeti u obzir u raspravi o 5G tehnologiji jer je od najveće važnosti uravnotežiti zahtjeve korisnika o privatnosti s obzirom na ponuđene usluge. U tijeku mobilne mreže uglavnom razmatraju četiri sigurnosna aspekta, a to su; autentičnost, integritet, povjerljivost i dostupnost. Budući da će 5G proizvoditi nove i složene aplikacije, stoga je od osobitog značaja razmotriti karakteristike privatnosti s gledišta arhitekture, kao što su promatranje, anonimnost, nepovezanost i lažno predstavljanje. Ovo će također osigurati snažan povjerljiviji odnos potrošača s mobilnim operaterima i s trećim stranama, koje pružaju različite usluge. Također, ne mogu se uključiti svi aspekti privatnosti tijekom rješavanja arhitekture mreže, zbog zakonitih pravila o reguliranju privatnosti. [5]

5G tehnologija predviđa viziju "uvijek dostupnog", gdje su usluge korisnicima dostupne bilo kada i bilo gdje. Ova 24 / 7 veza s drugim uređajima može stvoriti brojne napade kao što su lažno predstavljanje, odbacivanje usluge (DoS) i ponovni napadi između ostalog. 5G

tehnologija se također smatra ključnom tehnologijom koja ima mogućnost povezivanja pametnih objekata. Impresivna iskustva, poput usluga svjesnih konteksta, proširene stvarnosti i koncepata svega kao personalizacije usluge i korisnika bit će glavna vitalna snaga iza masovnog usvajanja 5G tehnologije. 5G je također glavni pokretač aplikacija utemeljenih na Internetu stvari (IoTs), gdje su stvari povezane ovom tehnologijom i usluge će se isporučiti učinkovitijim i bržim sredstvima. To znači da 5G zahtijeva posebno razmatranje zahtjeva o privatnosti iz različitih perspektiva tehnologija i usluga. [6, 16]

Nadalje, zahvaljujući nedavnom napretku u senzornim i komunikacijskim tehnologijama kao što su pametni telefoni, povećala se opća svijest o privatnosti u trenutnom društvu, a to potiče veću zaštitu korisničkih meta podataka i komunikacija. Mehanizam privatnosti orijentiran prema uslugama bio bi poželjniji način zaštite privatnosti. Također se, u slučaju 5G, rješenja koja se temelje na sigurnosti i privatnosti moraju usmjeriti ispočetka. Dakle, on mora dodati značajke sigurnosti i privatnosti ugrađene u dizajn sustava od početka. Poboljšanja tehnologija mobilne komunikacije također zahtijevaju unapređenje tehnika upravljanja identitetom. 5G tehnologija će okupiti ogroman broj korisnika i uređaja i oni će biti povezani, stoga je presudno zaštititi identitet pretplatnika i uređaja. Važno je osigurati da nijedan protivnik ili treća strana ne može ukrasti stvarni identitet pretplatnika bez njegovog pristanka. Slični sigurni pristupi potrebni su za izgradnju i održavanje snažnog odnosa povjerenja među pretplatnicima i različitim sudionicima, poput pružatelja usluga, poduzeća itd. Ovo poglavlje uglavnom ističe potencijalne izazove privatnosti, identiteta i povjerenja za buduću 5G tehnologiju sa stajališta korisnika. [5]

7.1 Sigurnost i privatnost u ranijim generacijama

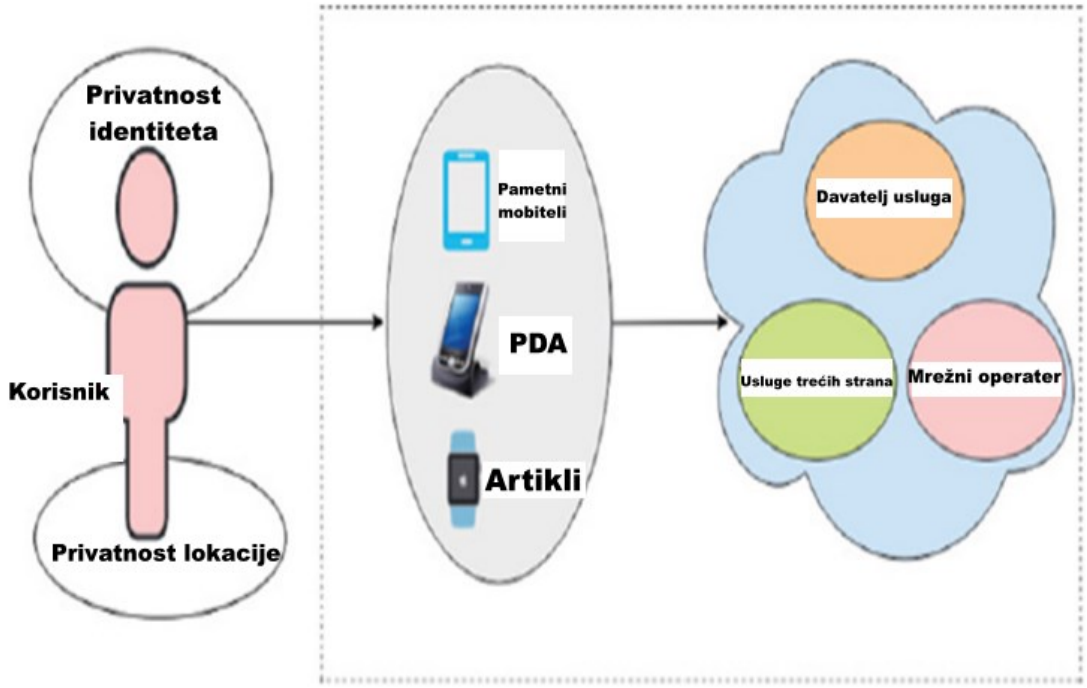
Tijekom posljednja dva desetljeća pametni uređaji poput pametnih telefona i tableta pružali su potrošačima sve prisutnije i uvjerljivije vrste usluga. Pokretanje sustava mobilne komunikacije, počevši od Globalnog sustava za mobilne komunikacije druge generacije (2G / GSM) koje vodi prema trećoj generaciji Univerzalnih mobilnih telekomunikacijskih sustava (3G / UMTS), široko se proširilo na sve dijelove svijeta. Sljedeći veliki prijelaz je ta evolucija najnovije generacije, „*Long Term Evolution*“ (4G / LTE) sustava, koji se široko primjenjuju. Od samog početka, brojne su prijetnje s kojima se suočavaju 2G sustavi, poput mehanizama međusobne provjere autentičnosti između korisnika mobilnih telefona i mreža. To znači da je s tim ograničenim resursima napadač mogao lako pokrenuti lažnu baznu stanicu i uvjeravati mobilne uređaje da je to valjana bazna stanica i da se može povezati s njom. Lažne bazne stanice mogu također biti napadači međunarodnog identiteta mobilnog pretplatnika (IMSI)

zbog nedostatka mehanizama za provjeru autentičnosti te se tako mogu koristiti za praćenje i nadzor korisnika. Sljedeći veliki prijelaz je 3GPP (Partnerski projekt treće generacije), koji je povećao razinu sigurnosti u odnosu na 2G sustave. Sigurnosne specifikacije u 3GPP-u također su uključivale mehanizme međusobne provjere autentičnosti. Nadalje, s porastom količine mobilnih podataka, zajedno s razvojem novih aplikacija, porasla je motivacija za prelazak s 3GPP-a prema četvrtoj generaciji. LTE je dizajniran tako da omogućava snažne mehanizme kriptografije, enkripcije i međusobne provjere autentičnosti. [17, 18]

Zbog visokih sigurnosnih zahtjeva tehnike rješavanja izazova upravljanja identitetom ključni su dio 5G-a. Prijetnje poput hvatanja međunarodnog mobilnog pretplatničkog identiteta (IMSI) također su raspravljane tijekom standardizacije 3G-a i 4G-a i stoga se također smatra središnjom točkom u 5G sustavima. Još nema dostupnih cjelovitih ili točnih dokumenata / specifikacija (barem ne u tehničkoj specifikaciji za 3GPP) koji se odnose na modele povjerenja za stalne mobilne mreže (2G-4G). Ali s obzirom na trend sigurnosnih zahtjeva, koji je evoluirao od 2G-4G, može se analizirati i trenutni model povjerenja za mobilne mreže. Međutim, u slučaju 5G mreža, model povjerenja među različitim sudionicima bio bi još složeniji, jer će se uključiti i dodatni subjekti. [5]

7.2 Privatnost korisnika

5G tehnologija omogućit će nekoliko novih aplikacija koje će potencijalno otvoriti vrata za veliki broj industrija. To nas dovodi do činjenice da će se velika količina osobnih podataka provoditi preko 5G mreža. Uvođenjem tehnike kopanja podataka lakše je dohvatiti podatke o privatnosti podataka, pa su podaci pod velikim rizikom. 5G sustav mora osigurati sigurnosne mehanizme za zaštitu različitih pouzdanih informacija, kako ljudi, tako i korisnika računala (npr. identitet, pretplaćene usluge, informacije o lokaciji / prisutnosti, obrasci mobilnosti, itd.). 5G tehnologija također bi ponudila prilagođene mrežne usluge za potrošače ostvarivanjem karakteristika pojedinih usluga. Stoga zahtjevi privatnosti u mreži 5G-a mogu se provoditi od usluge do usluge. Na primjer, zdravstvene informacije korisnika u određenim aplikacijama za zdravstvo zahtijevat će veći stupanj privatnosti. Također, u slučaju nekih važnih industrijskih zadataka, potrebna je podjednako viša razina zaštite privatnosti. Ali aplikacije poput pretraživanja neke vrste informacija o lokaciji mogu zahtijevati manji stupanj privatnosti. Radi usredotočenijeg razumijevanja, koncepte privatnosti korisnika podijelili smo u tri dijela, to su; privatnost podataka, lokacije i identiteta. [5]



Slika 7.2.1 Različiti elementi u privatnosti korisnika [5]

7.3 Privatnost podataka

Bit će gomila pametnih i heterogenih uređaja povezanih 5G tehnologijom, pa su šanse za propuštanje osobnih podataka korisnika vrlo velike. Davatelji usluga / tvrtke pohranjuju i koriste privatne podatke potrošača bez njihovog dopuštenja. U nekim slučajevima davatelj usluga pohranjuje korisničke podatke te ih kasnije dijeli s drugim tvrtkama kako bi mogli analizirati podatke i pronaći neke trendove koji od njihovih vlastitih proizvoda je prikladniji za tog određenog korisnika. U nekim je slučajevima čak korisno uzeti neke osobne podatke korisnika, a na temelju toga tvrtka može graditi nove proizvode i usluge. No, tvrtke / davatelji usluga moraju pružiti jasnije objašnjenje u vezi s kojom se svrhom koriste njihovi podaci. Oni također moraju odgovoriti na pitanja poput podataka koji su uzeti i kako i gdje su ih pohranili. Nekoliko aplikacija za pametne telefone, na primjer, android, pitaju za određene informacije prije instalacije. Podaci, za koje aplikacija želi dozvolu, uglavnom nemaju neposredne veze s uslugom te aplikacije. Ovi se podaci mogu koristiti u druge svrhe koje su definirali programeri aplikacija [19]. Danas su web lokacije društvenih medija najčešći načini razmjene javnih i privatnih podataka među različitim korisnicima. To su česti načini ažuriranja drugih o trenutnim aktivacijama, dijeljenje / prijenos osobnih slika, dijeljenje *live* teksta, audio i video razgovori. 5G bi trebao omogućiti ovakvu vrstu komunikacije pouzdano i kontinuirano. No, još uvijek mnogi ljudi postavljaju sumnju u curenje svojih osobnih podataka raznim sredstvima, koja predstavljaju stvarnu brigu za naše trenutačno društvo. IoT sustavi koji se

temelje na 5G-u ključni su dio budućih tehnologija za pružanje brojnih digitalnih usluga. To će s vremenom stalno stvarati ogromne količine podataka. Budući da IoT postaje aktualan, velike količine podataka stupaju na snagu. 5G će osigurati povećanje brzine prijenosa podataka i tako imati veći rizik od zlonamjernih napada. Na sličan način prenosivi uređaji proizvode veliku količinu podataka, jer senzori / čipovi pričvršćeni za nosive uređaje kontinuirano nadziru i prikupljaju osobne podatke korisnika, kao što su kalorije, puls, rad srca itd. Te podatke može analizirati treća strana koja može izdvojiti iz njih druge značajke bez traženja odobrenja korisnika. Rizici za privatnost podataka nastaju kada treća strana / pružatelj usluga ili bilo koji zlonamjerni napadač želi pristupiti korisnikovim osobnim podacima bez njegovog pristanka. Na primjer, praćenjem aktivnosti nekoga tko koristi njegove osobne podatke, lako se može predvidjeti svakodnevna aktivnost tog određenog potrošača. To može biti štetno u nekim slučajevima, jer ako netko želi promatrati / nagađati aktivnosti neke osobe, to lako može učiniti. Drugi bitan primjer može biti zdravstvena zaštita, gdje su zdravstveni podaci vrlo povjerljivi i osjetljivi.

U mnogim slučajevima pacijent želi ograničiti neke određene informacije na određene ljude poput liječnika, određenih članova obitelji ili prijatelja. Zlonamjerni korisnici ili neovlaštene osobe mogu pristupiti informacijama i koristiti ih u neetičke svrhe. Drugi takav primjer kršenja privatnosti može biti stalna kupovina bilo čega, poput bilo koje određene vrste hrane koja može otkriti religiju ili zdravstvene podatke. U 5G mrežama za mnoge slučajeve zahtjevi za zaštitu privatnosti također ovise o korištenju određene tehnologije pristupa. Budući da će element heterogenosti biti dostupan po mnogo većim putovima, zajedno s pristupnim tehnologijama koristit će se za dobivanje potrebnih usluga. Korisnički podaci će se kretati u različitim pristupnim mrežama u 5G-u, a različiti dobavljači pružit će funkcionalne cjeline za mrežu. Kao mogućnost, pomoću metodologije kopanja podataka, treća strana može dobiti osobne podatke korisnika analizom podataka o raspršivanju korisnika, koji bi mogli biti dostupni u bilo kojem dijelu mreže. Zbog rizika takvih scenarija potrebni su stroži programi zaštite privatnosti podataka za 5G mreže [20]. Važno je formulirati snažne mehanizme zaštite podataka dok se razgovara o standardizaciji i izradi politika za 5G tehnologiju. Davatelji usluga moraju objasniti načine prikupljanja podataka i njihovu upotrebu za razne usluge. Trebala bi postojati ravnoteža između privatnosti korisnika i podataka koje koriste pružatelji usluga, tako da tvrtke mogu graditi nove i korisne aplikacije za korisnika, a istodobno se ne smije utjecati na privatnost korisnika. Trebali bi biti uključeni mehanizmi odgovornosti kako bi nadzor pojedinih akcija od strane različitih entiteta bio lagan. Tehnike minimiziranja

podataka također bi trebale uzeti u obzir tako da tvrtke / pružatelji usluga / treće strane ograničavaju podatke koje prikupljaju i čuvaju i odlažu nakon što im više nisu potrebni. [5]

7.4 Privatnost lokacije

Danas nekoliko pametnih telefona, tableta i nosivih uređaja, koji posjeduju snažne mogućnosti računanja i pohrane, zajedno s tehnologijom pozicioniranja, mogu zatražiti usluge u bilo koje vrijeme i na bilo kojem mjestu. Lokacijske usluge (LBS) popularno se koriste s obzirom na razvoj buduće radijske tehnologije. Uvođenjem 5G-a koji će omogućiti besprijekornu i kontinuiranu dostupnost usluga, u takvim se slučajevima kontinuirano nadzire i lokacija korisnika. Kako bi pružile poboljšane usluge, razne tvrtke su počele pratiti i trenutnu lokaciju korisnika. Iz tih informacija, oni stalno prate navike i rutinu korisnika. S jedne strane, ova vrsta usluge praćenja pomaže tvrtkama u poboljšanju svojih usluga i izgradnji novih usluga prilagođenih korisnicima. Međutim, s druge strane izaziva ozbiljnu zabrinutost zbog privatnosti korisnika. Također, mnoge mrežne aplikacije na mobilnim uređajima zahtijevaju informacije o lokaciji zajedno s njihovim osobnim podacima. U nekim se slučajevima uzimaju informacije o lokaciji korisnika, bez obzira na to treba li se koristiti ili ne. Ove internetske aplikacije žele sve više i više informacija sa svakim njihovim ažuriranjem. Danas aplikacije na društvenim mrežama poput *Facebooka* također imaju opciju "*check-in*" gdje korisnici dijele svoje trenutne lokacije. To će izazvati zabrinutost zbog praćenja kretanja korisnika stalnim promatranjem informacija o lokaciji. U posljednje vrijeme prenosivi uređaji također se aktivno koriste u svrhu praćenja, poput praćenja djece i kućnih ljubimaca. Ovi mobilni uređaji prate svakog korisnika svakog sekunda, što također predstavlja velike probleme oko privatnosti. Postojeće tehnike za očuvanje privatnosti lokacije mogu biti korisne u kontekstu zaštite privatnosti lokacije u 5G tehnologiji. Uobičajene metode koje se koriste za zaštitu privatnosti korisnika mogu uključivati anonimnost, promjenu podataka i poremećaj putanja [21]. Potrebni su i regulatorni pristupi kako bi se mogli oblikovati snažni propisi i zakoni za pravilno korištenje mreže, stavljajući u obzir svijest o specifičnostima Interneta i sigurnosti mreže [22]. Tehnike temeljene na šifriranju između ostalih su načina za zaštitu privatnosti korisnika. Korisnik šifrira poruku prije slanja davatelju usluga LBS. Nakon što dobavljač LBS-a primi poruku, dešifrirat će se. Ovaj pristup uključuje veći intenzitet anonimnosti, ali ima velike računske i komunikacijske troškove, što je jedan od nedostataka korištenja ovog pristupa [22]. Pristupi temeljeni na anonimnosti skrivaju stvarni identitet korisnika i zamjenjuju ga lažnim imenima. U ovom se slučaju pouzdan srednji softver koristi za generiranje lažnih podataka koji se zatim šalju davatelju LBS-a za određenu lokacijsku

uslugu. Postoji i drugi pristup, u kojem se kvaliteta podataka o lokaciji korisnika smanjuje kako bi se sačuvala privatnost lokacije, što je poznato kao zamračenje. Na primjer, formulirana je jedna tehnika koja se temelji na prostornom skrivanju koja proširuje lokaciju lokacije korisnika na regiju zvanu ASR koja sadrži lokaciju korisnika, gdje se uglavnom koristi tipična tehnika k-anonimnosti. Tada pouzdana treća strana šalje ASR davatelju LBS-a da ispuni LBS upit. I na kraju, potrebni su neki pristupi zasnovani na politici privatnosti kako bi se osiguralo da se može ograničiti zlouporaba podataka o lokaciji na određene načine, na primjer, zaštitom privatnosti korisnika metodama pretraživanja informacija. [22]

7.5 Privatnost identiteta

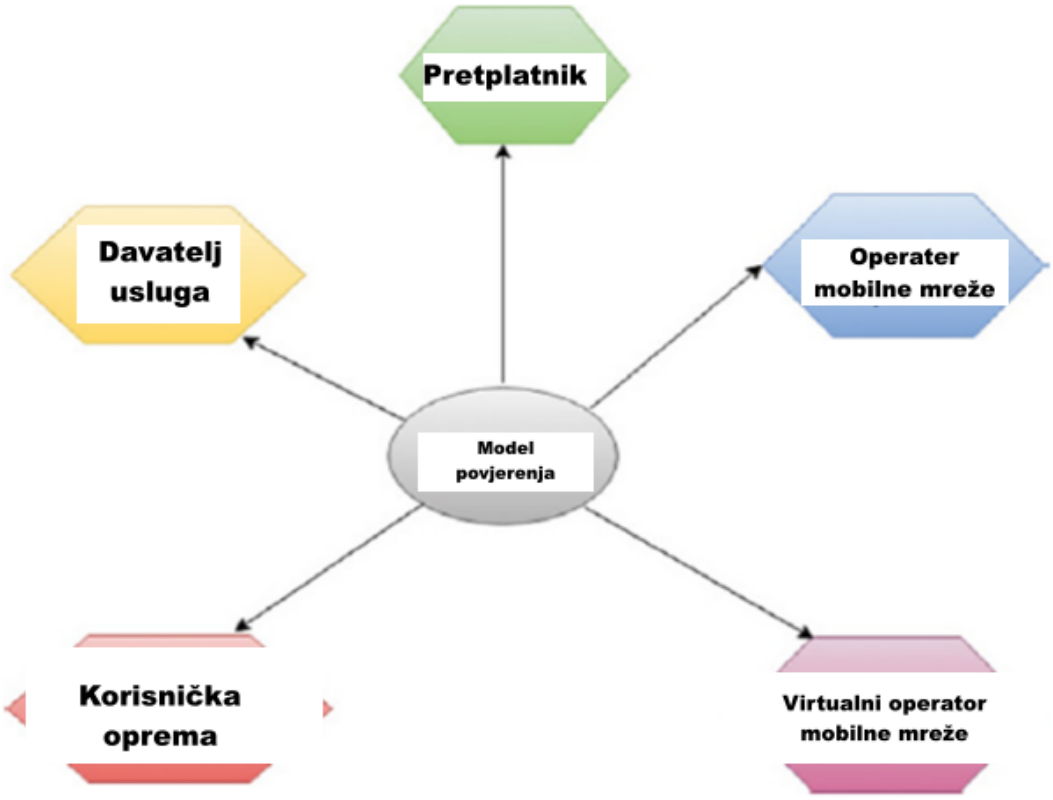
Tijekom kupnje digitalnih usluga u određenim prilikama, potrošači ne žele otkriti svoj izvorni identitet drugim korisnicima ili davateljima usluga. Na primjer, kada postavljaju bilo kakve upite putem Interneta ili daju povratne informacije o web stranicama tvrtki, korisnici radije ostaju anonimni. U nekim situacijama korisnici mogu koristiti privremeni ili lažni identitet i odbaciti ih kada je ispunjen potrebni zadatak. Poznavanje trajnog identiteta korisnika može omogućiti protivniku da prati i skuplja profile o pojedincima. Trend krađe internetskih identiteta danas je češći. Postoje brojne internetske aplikacije kao što su kupovina i bankarstvo koji bi zahtijevali internetske načine plaćanja putem kreditnih kartica. Te informacije mogu dovesti do otkrivanja stvarnog identiteta i mogu uzrokovati moguće rizike za privatnost korisnika. Za skrivanje stvarnog identiteta obično se koriste pristupi temeljeni na anonimnosti. Privatnost identiteta može se dalje podijeliti na privatnost identiteta pretplatnika i uređaja:

- Privatnost pretplatničkog identiteta: u ovom slučaju mogu se pojaviti prijetnje ako korisnici prate ili nadziru pretplatnikov identifikator ili mogu biti preko privremene identifikacijske isprave. Korisnici također obično ne žele nikakvu vezu između identiteta svog pretplatnika i identiteta uređaja. Moguće rješenje zaštite privatnosti pretplatničkog identiteta bilo bi šifriranjem IMSI-a i korištenjem poboljšanog pseudo-identifikatora. Kako bi se osigurala neispravnost identifikatora pretplatnika i uređaja, sustav anonimnosti mogao bi biti jedan od potencijalnih pristupa koje treba razmotriti.
- Privatnost identiteta uređaja: Ranjivosti koje mogu postojati u vezi s privatnošću identiteta uređaja su da pretplatnici ne žele da ih prate njihovi UE identifikatori. Isto tako, kao i kod privatnosti pretplatničkog identiteta, korisnici također ne žele povezivanje svojih identifikatora pretplatnika s identifikatorima uređaja. To se može riješiti proučavanjem mogućih pristupa anonimnosti od početka do kraja koji pružaju

zaštitu od neovlaštenog praćenja uređaja i čuvaju otkrivanje identiteta uređaja. 5G također osigurava da samo putem povjerljive zaštićene poruke treba poslati međunarodni identitet mobilne opreme (IMEI). [23]

7.6 Povjerenje u 5G mrežu

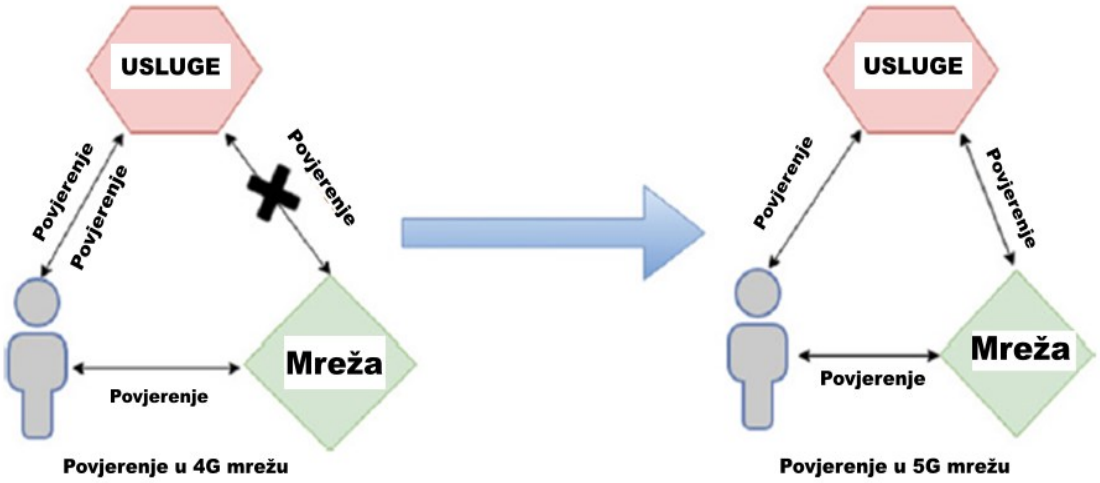
Povjerljivi modeli se mijenjaju s obzirom na vrijeme i poboljšanja tehnologije. Ranije se za tvrtke smatralo da su mobilni uređaji svih korisnika pouzdaniji, jer ih je izdao i upravljao njihov vlastiti IT odjel. Ali u posljednje vrijeme svaki korisnik u tvrtki / poduzeću želi svoje osobne uređaje, što na kraju može dovesti do brojnih sigurnosnih prijetnji uređajima tvrtke [6]. Povjerenje uključuje mogućnosti kao što su sigurnost, upravljanje identitetom i privatnost. Čak i do danas, nema standardnih pouzdanih modela za trenutne mreže (2G-4G). Postojeći (2G-4G) model povjerenja uglavnom se sastoji od entiteta, poput korisnika (pretplatnika), davatelja usluga, mrežnog operatora, operatora virtualne mobilne mreže (VMNO) i proizvođača opreme, među ostalim, kao što je prikazano na slici 7.6.1. [24]



Slika 7.6.1 Subjekti u modelu povjerenja [5]

Obično pretplatnici zadržavaju povjerenje nad pružateljem usluga i pretpostavljaju da se moraju poštovati pravila i propisi napisani u ugovoru o naplati usluga / naplate, a to povjerenje dalje razvija na temelju iskustva, ugleda i pravnog okvira. Pretpostavlja se da su čvorovi između pretplatnika i pružatelja usluga osigurani tijekom bilo kakve komunikacije (može biti i glasovna), a korisnici vjeruju da su njihovi važni podaci sigurni kod operatora. Davatelj usluga odgovoran je za pružanje potrebnih usluga pretplatnicima putem nekog korisničkog uređaja ili opreme, poput mobilnog telefona ili tableta. Povjerenje koje davatelji usluga uglavnom traže od pretplatnika je da moraju biti u mogućnosti da naplate obračunsku / naplatu ili pretplatu u unaprijed zadanom roku. Iako davatelji usluga nemaju puno povjerenja u to da će pretplatnici zadržati snažne lozinke za autentifikaciju usluge te stoga, u svrhu sigurne provjere autentičnosti, pretplatniku nudi UICC. Mrežni operator je poznat kao središnji element i pruža vezu s povjerenjem raznim drugim elementima u mreži. Na primjer, operateri mobilne mreže (MNO) ili operateri satelitske mreže (SNO) obavljaju operacije poput raspoređivanja, održavanja i upravljanja mrežom pomoću satelita. Do sada ne postoje dostupni takvi standardizirani sigurnosni postupci koji bi mogli istaknuti mrežne operatore koji dijele određene podatke. U trenutnom scenariju, odnos povjerenja među različitim mrežnim operaterima je jak i reguliran ugovorom. Međutim, mogu postojati nepouzdani mrežni operatori koji mogu zloupotrijebiti osobne podatke i to može biti ozbiljna prijetnja takvim mrežama [24]. VMNO se temelji na jednom od posebnih oblika mrežnog operatera. Ne sadrži mobilnu mrežu, već umjesto toga posuđuje neki virtualni prostor iz baze podataka tog mrežnog operatora. Stoga slijedi gotovo isti model povjerenja i entiteta koji su dodijeljeni mrežnim operatorima. Čuva povjerenje između VMNO-a i njeni infrastrukturni elementi mogu koristiti razne resurse kako je ugovoreno u obje strane. Što se tiče (UE), pretpostavljeno je da ovaj entitet ne treba biti uključen u modele povjerenja, jer je mrežni operator onaj koji bira koji je proizvođač pouzdan i koju opremu treba koristiti. Postoje slučajevi kao što je USIM proizvođač, gdje je potrebno razmotriti višu razinu povjerenja zbog posebnih zahtjeva za USIM / UICC [23]. Iz perspektive mrežnog operatora, mobilna mreža nove generacije (NGMN) [25] predstavila je tri vrste poslovnih modela, odnosno davatelja sredstava, pružatelja povezanosti i pružatelja usluga partnera. Za *Asset* su najvažniji *XaaS* i modeli dijeljenja mreže. Pružatelj povezivanja oslanja se na dva poslovna modela, osnovni (projekcija trenutnog 4G poslovanja) i poboljšani. Postoje i dva poslovna modela za pružatelje usluga partnera. Prvi je "ponuda operatora obogaćena od strane partnera", koja se bavi uslugama koje pruža operator mobilne mreže koristeći jedinstvene mogućnosti trećih resursa. Drugi je "partnerska ponuda obogaćena od strane operatora", gdje se jedinstvene mogućnosti

operatera koriste za isporuku usluga izravno pretplatnicima. Postojeći modeli povjerenja možda nisu u potpunosti primjenjivi za 5G mreže, kao u slučaju gdje će biti dodatni entiteti i akteri koji će djelovati kako bi pružili i podržali brojne nove usluge. Stoga izgradnja modela povjerenja neće biti jednostavna i uključivat će daleko više složenosti nego što se ikada moglo zamisliti. Na primjer, jedna od mogućnosti mogla bi biti uvođenje novog entiteta, poput vanjske oblačne infrastrukture. To je zato što kroz radijsko umrežavanje mrežni operatori mogu izvoditi neke operacije i aplikacije mreže na vanjskom oblaku. Nadalje, ovi vanjski oblaci također mogu imati različite svoje podatkovne centre nadležnosti. Ostale mogućnosti za poboljšanje pružanja usluga u 5G-u su pronalaženje nekih mrežnih funkcionalnosti, koje može obaviti treća strana. Kako pružatelji mrežne distribucijske mreže (CDN) integriraju ulove u mrežnog operatora, presudno je uzeti u obzir činjenicu da dodavanje ovih novih funkcionalnosti ne bi trebalo utjecati na mrežu. U tradicionalnoj arhitekturi mobilne komunikacije, telekomunikacijske vlasti odgovorne su za pristup važećim korisnicima samo za određene mreže. Ne postoji model povjerenja između provjere autentičnosti korisnika s njihovim uslugama. Međutim, u 5G mrežama ovaj bi nedostatak također bio riješen, jer mreže mogu ovjeriti pružatelje usluga da imaju još sigurnije i učinkovitije upravljanje identitetom, kao što je prikazano na slici 7.6.2. [20]



Slika 7.6.2 Evolucija u modelu povjerenja [5]

Dakle, IMSI i IMEI koriste se za otkrivanje pokušaja napada od strane ili protiv sudionika. Stoga pretplatnici i davatelji usluga vjeruju proizvođačima domena USIM i mobilne opreme (ME). Operatori opreme uglavnom su odgovorni za njegovo ponašanje, dok proizvođač ima manje odgovornosti. U nekim slučajevima, ugovori odražavaju povjerenje različitih sudionika, poput sporazuma o *roamingu* pružatelja usluga s drugim pružateljima usluga *roaminga*, koji korisnicima mogu omogućiti povezivanje na njihove domene. I pružatelji

usluga i *roaming* moraju imati ugovore s drugim pružateljima usluga za uspostavljanje komunikacijskog puta za pretplatnike. U mreži 5G-a (4G-a), povjerljivi odnosi postoje između različitih sudionika, ali može doći do određenih napada u kojima pouzdanost opreme možda neće ostati u skladu s očekivanjima [24]. Tablica 7.6.1 ističe takve vrste prijetnji.

Tablica 7.6.1 Potencijalne prijetnje među sudionicima [5]

Vrste prijetnja	Detalji
Zlonamjerni sudionici	Jedan sudionik može raditi protiv interesa drugih
Ne zlonamjerne radnje	Uzrok djelovanja tehnoloških posrednika sudionika, pogreške korisnika
Zlonamjerni napadi	Vanjski napadač može potkopati tehnologiju sudionika, što dovodi do djelovanja protiv drugih sudionika
Unutarnji kvarovi	Uzrokovane unutarnjim greškama u sustavu vode na štetu sudionika
Vanjske katastrofe	Uzrokuju ga vanjski izvori, poput prirodne katastrofe
Prijetnja sudionicima	Sudionik nastavlja s povjerenjem i upotrebom sustava
Prijetnja nepovjerenju sudionika	Sudionik gubi povjerenje i povlači se iz sustava

8. SIGURNOSNE PREPORUKE I IZAZOVI

Vektori sigurnosnih prijetnji u 5G-u bit će višedimenzionalni, od fizičkih sučelja do aplikacijskih sučelja, usluga u oblaku i korisničkih podataka. 5G mreže povezivat će važnu infrastrukturu, međusobno povezati društva i industrije, pružiti bilo što kao uslugu i integrirati nove modele pružanja usluga.

Ekosustav 5G-a u ovom trenutku nije moguće u potpunosti vizualizirati zbog brzog razvoja i integracije novih uređaja i usluga. Međutim, glavne atrakcije 5G-a izvan proširene povezanosti, veće brzine podataka i manja kašnjenja bit će lako postavljanje i korištenje novih usluga i funkcija. To će također kompliciratи sigurnosni krug. Da bismo sigurnosni krug lakše razumjeli, dajemo raspravu o sigurnosti u dvije domene. Prvo, sigurnost pristupnih mreža, na primjer, radio pristupne mreže (RAN) koje mogu biti sastavni dijelovi višestrukih pristupnih tehnologija poput stanične mreže RAN koja obuhvaća male i velike bazne stanice i *Wi-Fi* itd. Drugo, sigurnost središnje mreže u kojoj mrežna kontrola ima usluge specifične za operatera i dobavljača. Sektor telekomunikacija Međunarodne unije za telekomunikacije (ITU-T) predložio je dimenzije sigurnosti telekomunikacijskih mreža koje se bave svim aspektima sigurnosti [36]. Stoga će se prvo dati kratki uvod u ove preporuke, a zatim će se razgovarati o različitim sigurnosnim izazovima na različitim područjima 5G mreža.

8.1 Sigurnosne preporuke od strane ITU-T-a

Sigurnosne veličine predlažu ITU-T u svojoj sigurnosnoj preporuci kako bi se pozabavili skoro svim aspektima mrežne sigurnosti. Sigurnosne dimenzije uključuju skup sigurnosnih mjera koje se mogu koristiti za zaštitu korisnika i mreže od svih većih sigurnosnih prijetnji.

Te su dimenzije:

- Kontrola pristupa: sigurnosne mjere koje osiguravaju samo ovlaštenom osoblju ili uređajima pristup mrežnim resursima.
- Provjera identiteta: sigurnosni mehanizmi koji osiguravaju identitet komunikacijskih strana i da korisnik ili uređaj ne pokušava maskirati ili neovlašteno reproducirati prethodne komunikacije.
- Ne reprodukcija: osigurava da određeni korisnik ili uređaj izvrši određenu radnju da se ne odbija. Pravilni identiteti koriste se za osiguravanje da autentični korisnik ili uređaj mogu pristupiti određenim uslugama i resursima.

- Povjerljivost podataka: sigurnosni mehanizmi za zaštitu podataka od neovlaštenog pristupa. Za osiguravanje povjerljivosti podataka koriste se šifriranje, mehanizmi kontrole pristupa i dopuštenja datoteka.
- Sigurnost komunikacije: osigurava da podaci prolaze između ovlaštenih krajnjih točaka i da se ne preusmjeravaju ili presreću između.
- Integritet podataka: osigurava ispravnost ili točnost podataka u prijenosu i štiti ih od neovlaštene izmjene, brisanja, stvaranja i replikacije.
- Dostupnost: osigurava da nema uskraćivanja autoriziranog pristupa mrežnim resursima i aplikacijama. Događaji koji utječu na mrežu, poput kvarova sustava, skalabilnosti i sigurnosnog kompromisa, ne smiju ograničavati pristup ovlaštenim korisnicima i uređajima.
- Privatnost: mehanizmi koji osiguravaju zaštitu informacija, a koje bi mogle proizaći iz promatranja mrežnih aktivnosti. [5]

8.2 Sigurnost na temelju standarda

Važno načelo u dizajniranju i izgradnji sigurnih sustava je odabir sigurnosnih algoritama i sigurnosnih protokola iz standardiziranih izvora, poput organizacija navedenih u nastavku. Trebat će razviti nove standarde, ali kad god je to moguće, oni bi se trebali koristiti i nadograditi na postojećim sigurnosnim standardima, preferirajući razvoj svojih.

ETSI

Europski institut za telekomunikacijske standarde (ETSI) neovisna je organizacija za standardizaciju neprofitne organizacije u telekomunikacijskoj industriji u Europi. ETSI proizvodi globalno primjenjive standarde za informacijske i komunikacijske tehnologije (ICT), uključujući fiksne, mobilne, radio, konvergirane, emitirane i internetske tehnologije. 3GPP je tijelo za standardi unutar ETSI-ja.

NIST

Nacionalni institut za standarde i tehnologiju (NIST) nacionalni je laboratorij, agencija za trgovinu Sjedinjenih Država koja osigurava razvoj tehnologije, mjerenja i standarda. Unatoč nacionalnom krugu, Federalni standardi obrade informacija NIST-a (FIPS) i posebne publikacije (SP) imaju svjetski utjecaj.

IETF

Radna grupa za Internet inženjering (IETF) glavno je tijelo za standardizaciju internetskih protokola i nekih pridruženih sigurnosnih algoritama. To je organizacija otvorenih standarda, bez formalnog članstva ili zahtjeva za članstvo za sudjelovanje. Podržava ga *Internet Society* (ISOC), međunarodna neprofitna organizacija osnovana radi vođenja u internetskim standardima, obrazovanju, pristupu i politici. ISOC ima članstvo u cijelom svijetu, uključujući organizacije i pojedince. Organizacijski odbor internetske arhitekture (IAB) također je dom organizacije koji pruža smjernice IETF na visokoj razini. Te organizacije razvijaju internetske standarde i povezane specifikacije koje se objavljuju kao Zahtjevi za komentare (RFC). IETF je odgovoran za standardizaciju mnogih najčešće korištenih internetskih protokola, npr. TLS, IPSec.

ITU-T

Međunarodna unija za telekomunikacije (ITU) međunarodna je organizacija koja je dio sustava Ujedinjenih naroda, gdje vlade i komercijalni subjekti sudjeluju u globalnoj koordinaciji i standardizaciji telekomunikacijskih mreža i usluga. Sektor za standardizaciju telekomunikacija ITU (ITU-T) jedan je od tri sektora ITU-a. Misija ITU-T je izrada standarda koji pokrivaju sva područja telekomunikacija. Međunarodni standardi koje proizvodi ITU-T poznati su kao preporuke.

ISO

Međunarodna organizacija za standardizaciju (ISO) globalna je federacija nacionalnih tijela za standardizaciju. ISO je nevladina organizacija koja promiče razvoj standardizacije i srodnih aktivnosti koje imaju za cilj olakšati međunarodnu razmjenu dobara i usluga i razviti suradnju u područjima intelektualne, znanstvene, tehnološke i ekonomske aktivnosti. Rad ISO-a rezultira međunarodnim sporazumima koji se objavljuju kao Međunarodni standardi. [15]

Pri dizajniranju sustava poput 5G-a, koji imaju veliku raznolikost, potreban nam je alatni okvir i upute koje nam omogućuju da sami modeliramo njegov sustav zajedno s njegovom sigurnošću i razradimo sigurnosna rješenja dizajniranog sustava od početka. Stoga, u ovom radu je definirana sigurnosna arhitektura kao metodologija za stvaranje sigurnih sustava, koja sadrži alat za sigurnosno modeliranje sustava, načela sigurnosnog dizajna i skup sigurnosnih funkcija i mehanizama za provedbu sigurnosnih kontrola potrebnih za postizanje sigurnosnih

ciljeva sustava. Ovaj je pogled sigurnosne arhitekture potkrijepljen sigurnosnom arhitekturom u ITU-T X.805.

Konkretno, X.805 kaže da "sigurnosna arhitektura dijeli složen skup cjelovitih značajki povezanih sa sigurnošću mreže na posebne arhitektonske komponente" i da "ovo razdvajanje omogućuje sustavni pristup cjelovitoj sigurnosti koja se mogu koristiti za planiranje novih sigurnosnih rješenja, kao i za procjenu sigurnosti postojećih mreža." [14]

8.3 Prijetnje sigurnosti i preporuke NGMN-a

Mobilne mreže nove generacije (NGMN) pružaju preporuke za 5G temeljene na trenutnim mrežnim arhitekturama i potrebne sigurnosne mjere koje se ne provode ili nisu dostupne. Preporuke naglašavaju upozorenja, ističu ograničenja u pristupnim mrežama i *cyber* napade u odnosu na mrežnu infrastrukturu. [37]

U nastavku se navode ključne točke u preporukama:

- *Flash* mrežni promet: Poznato je da će broj uređaja krajnjeg korisnika eksponencijalno rasti u 5G-u, tako da bi događaji velikih razmjera mogli uzrokovati značajne promjene u obrascu mrežnog prometa koje bi mogle biti slučajne ili zlonamjerne. Zbog toga se preporučuje da 5G sustavi moraju smanjiti velike promjene u prometnoj upotrebi i pružiti otpornost kad god se pojave takvi udari, održavajući prihvatljivu razinu performansi.
- Sigurnost tipki radijskog sučelja: U prethodnim generacijama, čak i u 4G-u, ključevi za šifriranje radio sučelja generiraju se u kućnoj mreži i šalju u posjećenu mrežu preko nesigurnih veza što uzrokuje jasno izlaganje tipki. Preporučuje se da se ključevi ili ne šalju preko tih veza ili da se pravilno osiguraju.
- Integritet korisničke razine: 3G i 4G ne pružaju zaštitu kriptografskog integriteta za ravninu korisničkih podataka, mada oni pružaju zaštitu nekim signalnim porukama. Preporučuje se pružiti zaštitu na transportnom ili aplikacijskom sloju koji završava izvan mobilne mreže. Izuzetak od ovoga može biti sigurnost na razini mreže za IoT ograničene resurse ili 5G uređaje i usluge osjetljive na kašnjenje. Aplikacijska razina sigurnosti E2E može uključivati prevelike troškove za prijenos podataka u zaglavljima paketa i rukovanju paketa.
- Omogućena sigurnost u mreži: postoje sigurnosna ograničenja sigurnosne arhitekture koja vode do neobavezne uporabe sigurnosnih mjera. Nažalost, ta ograničenja

potkopavaju sigurnosne pretpostavke o dimenzijama sustava i ne mogu se u potpunosti otkloniti. Izazov se povećava u scenarijima za više operatora kada jedan operator pati zbog neadekvatnih mjera drugog. Stoga se visoko preporučuje da se neka razina, ako ne i sve, moraju izložiti u 5G-u nakon odgovarajuće istrage kako bi se prepoznali najvažniji sigurnosni izazovi.

- Dosljednost u sigurnosnim pravilima na razini pretplatnika: Postoji potreba da se sigurnosni parametri korisnika ne mijenjaju zbog odlaska iz jedne mreže u drugu. U slučaju mobilnih korisnika, vrlo je moguće da se sve sigurnosne usluge ne ažuriraju često i po korisniku, dok se korisnik u slučaju *roaminga* kreće s mjesta na mjesto ili s jedne mreže na drugu. Kada se korisnik s jednog operatera prebaci na drugog i koristi usluge osjetljive na kašnjenje, usluge se mogu pružati preko ruba posjećene mreže operatora, kao što je *Mobile Edge Computing* (MEC). Hoće li se sigurnost usluge koja se koristi automatski ponuditi ili konfigurirati na novoj lokaciji? Zahtijeva dijeljenje sigurnosnih pravila među mrežnim operaterima na mnogo bržoj skali kako bi se osigurao korisnički promet u *roamingu*. Preporuka govori o mogućnosti korištenja tehnika radijskog umrežavanja u takvim situacijama koje mogu omogućiti konfiguraciju odsječka po korisniku da sigurnosne politike i usluge ostanu netaknuti kad god i gdje god se korisnik kreće.
- DoS napadi na infrastrukturu: DoS i distribuirani DoS (DDoS) napadi mogu zaobići rad uređaja koji kontroliraju važnu infrastrukturu poput energije, zdravlja, transporta i telekomunikacija, uzrokujući opasnosti po život s ogromnim gubicima od ljudi i kapitala. DoS napadi dizajnirani su tako da iscrpljuju fizičke i logičke resurse ciljanih uređaja. Izazov će biti prijeteći zbog mogućnosti napada sa strojeva koji su geografski gledano raspršeni na lokacijama i u ogromnom broju. Mreža mora biti sposobna servisirati sve veći broj veza uzrokovanih sve većom širinom povezanih uređaja (npr. IoT) s različitim radnim mogućnostima i ograničenjima. [5]

8.4 Ostali sigurnosni izazovi

Sigurnosni izazovi na visokoj razini mogu se razvrstati u tri domene, odnosno sigurnosni izazovi u pristupnoj mreži, DoS napadi i sigurnosni izazovi u osnovnoj mreži. U nastavku kratko se opisuje svaka od njih.

Izazovi sigurnosti u pristupnoj mreži

Sigurnost pristupa mreži omogućuje siguran pristup mreži i uslugama uz zaštitu od ranjivosti. Na primjer, korisniku se mora osigurati sigurnost od zlonamjernih mrežnih aktivnosti, a mreža mora biti zaštićena od zlonamjernog pristupa. 5G će koristiti razne pristupne tehnologije i integrirati različite vrste pristupnih mreža za veću pokrivenost, bolju propusnost i nisko kašnjenje. Da bi mreža nastavila raditi, 5G mora poboljšati robusnost sustava protiv napada ometanja radijskih signala i kanala. Nadalje, sigurnost malih ćelijskih čvorova mora se poboljšati zbog njihove geografske distribucije i lakoće pristupa. Jedan od ključnih izazova u 5G-u bit će prekomjerni čvorovi koji šalju podatke i primaju podatke istovremeno, praktički ometajući radijska sučelja. Taj izazov može biti pogoršan zlоćudnim čvorovima koji šalju pretjerano prometovanje signalom, što izaziva izazove dostupnosti ili, drugim riječima, dovodi do napada uskraćivanja usluge (DoS). Takav promet signala ili napadi moraju se prepoznati rano i zaustaviti prije zastoja u mreži. 3G i 4G pružali su zaštitu kriptografskog integriteta nekih signalnih poruka, ali ravnina korisničkih podataka još uvijek nije bila zaštićena.

Od 2G do 4G, ključevi za šifriranje radio sučelja računaju se u matičnoj osnovnoj mreži i prenose se u posjećenu radio mrežu preko signalnih veza SS7 ili *Diameterom*. [37]

Stoga bi trebali postojati dobro dizajnirani protokoli upravljanja ključem za 5G kako bi se smanjile prijetnje. Osnovne tehnike uključuju poboljšanje sigurnosti SS7 i promjera uvođenjem vatrozida [37]. Mogu se primijeniti i drugi pristupi, poput korištenja različitih sigurnih upravljačkih kanala za distribuciju ključeva.

DoS napadi

DoS i DDoS napadi koji potječu iz velikih skupova povezanih uređaja vrlo će vjerojatno predstavljati stvarnu prijetnju 5G mrežama. Ti napadi mogu biti protiv mrežne infrastrukture ili uređaja krajnjeg korisnika. Napadi na infrastrukturu osmišljeni su tako da iscrpe resurse mrežnih operatora koji služe korisnicima i uređajima. Iako je izvorna meta mreža operatora, na pretplatnike se to neizravno utječe. Napadi na korisnike / uređaje dizajnirani su tako da

iscrpe resurse korisnika i uređaja. U ovom su slučaju izravno ciljani pretplatnici i uređaji, ali to neizravno utječe na mrežnog operatora. Kompromitirani korisnički uređaji također se mogu koristiti za izazivanje napada na mrežnu infrastrukturu. [5]

Stoga se fokus može posvetiti sljedećim područjima:

1) signalna ravnina potrebna za provjeru autentičnosti, povezanosti i dodjelu propusne širine, te mobilnost 5G korisnika,
2) korisnički avion potreban za podršku dvosmjerne komunikacije uređaja,
3) upravljačka ravnina koja podržava konfiguraciju mrežnih elemenata koji podržavaju signalnu i korisničku ravninu,
4) sustavi podrške koji obavljaju račune za korisnike / uređaje,
5) radio resursi koji pružaju pristup korisničkim uređajima, i
6) fizički i logički resursi koji podržavaju mrežne oblake.

DoS napadi na korisničke uređaje ciljat će na fizičke resurse korisničkih uređaja kao što su memorija, baterija, procesne jedinice, radio i senzori itd. Ovi napadi mogu ciljati i na logičke resurse poput operativnih sustava, aplikacija, konfiguracijskih podataka i korisnički podaci itd.

Izazovi sigurnosti u upravljačkom sloju ili osnovnoj mreži

Masivan prodor IP protokola u kontrolne i korisničke ravnine u svim mrežnim funkcijama čini 5G središnju mrežu vrlo ranjivom. Stoga mreža mora biti sposobna osigurati dostupnost s poboljšanom otpornošću na prijetnje na temelju signalizacije.

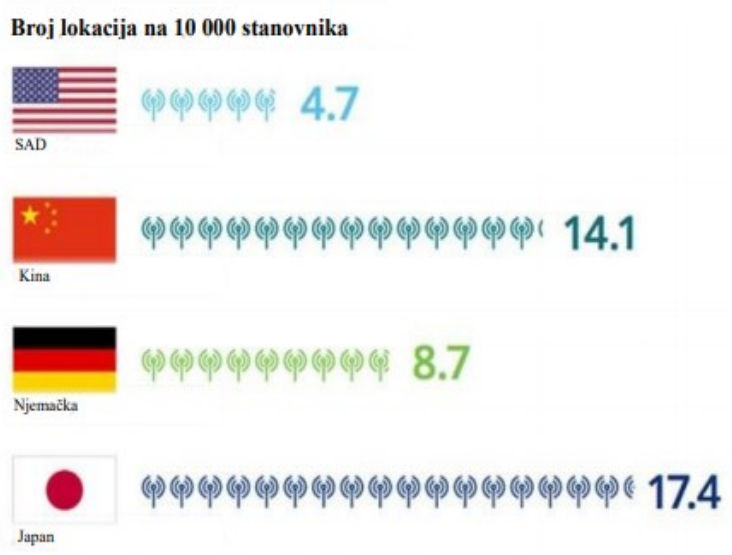
Za aplikacije osjetljive na kašnjenje i slučajeve uporabe moraju se ugraditi posebne sigurnosne značajke. Mreža također mora sadržavati sigurnosne zahtjeve definirane u 3GPP. Nadalje, 5G mreže trebale bi osigurati komunikaciju u izvanrednim situacijama, primjerice kada je dio mreže nepristupačan ili uništen. Preopterećenje signalne ravnine ogromnim brojem korisnika zaraženim IoT-om ili M2M uređaja, bilo kao pokušaj DoS napada ili dobiti pristup mreži, bit će još jedan gorući izazov u 5G mrežama [37]. IoT uređaji, u milijardama [38], bit će ograničeni resursima, čineći tako dvije vrste zahtjeva. Prvo, zbog ograničenih mogućnosti ovi uređaji će trebati resurse u oblacima da bi izvršili obradu, pohranu ili razmjenu informacija. Drugo, zbog svojih ograničenih mogućnosti, oni će biti laka meta maskiranja ili djelovanja u kompromitiranom okruženju za napade na mrežu u obliku DoS napada. Stoga će sve veći broj povezanih uređaja biti veliki izazov za signalnu ravninu ili

jezgru mreže 5G mreža. Primjer za to su zahtjevi za autentifikaciju i autorizaciju HSS-u koji potencijalno mogu učiniti HSS nepristupačnim za legitimne korisnike, drugim riječima, kompromitirati centralizirani entitet putem DoS napada ili napada zasićenja [39]. Sve veći raspon komunikacijskih usluga i uređaja dovodi do velike količine prometa u svrhu signalizacije, kao što su provjera autentičnosti i aktiviranje nositelja. Takvi prometni pragovi dovode do signalnog poremećaja koji mogu srušiti središnju mrežu [40]. Slično tome, signalizacijski postupci događaju se na NAS sloju 3GPP protokola koji uključuju dodavanje / odvajanje, aktivaciju nosioca, ažuriranje lokacije i provjeru autentičnosti. One tvore NAS-ove signalne poremećaje [40]. To može biti izazovnije za 5G, gdje će milijarde uređaja biti spojeno na istu centralnu mrežu. *Nokia Seimens Networks* objavio je da promet signala raste 50 % brže od podatkovnog prometa [41]. Male ćelije s velikim brojem povezanih uređaja koji su mobilni povećavat će mobilnost predavanja, povećavajući tako signalni promet. To ne samo da će povećati opterećenje signalizacije na entitetu za upravljanje mobilnošću (MME), već i na druge kontrolne jedinice kao što su HSS, mrežni prolaz javne mreže podataka (P-GW) i posluživanje *Gateway* (S-GW), radi održavanja kvalitete usluge (QoS). Nadalje, NAS-ov sloj 3GPP protokola za UE funkcije pridruživanja ili odvajanja, aktivaciju nosioca, ažuriranje lokacije i provjeru autentičnosti mogu uzrokovati signalne poremećaje [16]. 3GPP preporučuje upotrebu IPSec enkripcije za LTE sučelja, kao što su X2, S1-MME, S5 i S6, itd. Dakle, svaki eNB je potreban za podršku stotinama IPSec tunela, dok *backhaul* mora podržati tisuće tunela. Ovakav masivni uspon tunela ne samo da komplicira sigurnosnu mrežu, već i uvelike povećava opterećenje signala u mreži. Nadalje, postavljanje tunela ima statičku prirodu i definira ga administrator što dodatno remeti proces osiguranja upravljačkog prometa. Tuneli, statički uspostavljeni, možda se ne koriste, ali i dalje slanje informacija periodične kontrole također povećava opterećenje signalizacije. Stoga će korištenje trenutačno raspoređenih sigurnosnih arhitektura u 5G uzrokovati velike izazove skalabilnosti i dostupnosti i tako otvoriti put za DoS i DDoS napade. Za sigurnost sustava 5G potrebne su nove sigurnosne arhitekture kako bi se osigurala sigurnost korisnika i mreža zaštitila od zlonamjernih napada.

9. SIGURNOST 5G MREŽE U SVIJETU

Od prve generacije mobilnih mreža do posljednje, države koje su bile vodeće u razvoju tehnologije su uživale pogodnosti razvijenih inovacija. Biti lider razvoja 5G mobilne mreže rezultira otvaranjem novih industrija, zapošljavanjem nove radne snage, ali i prodajom potrebne opreme za implementaciju 5G mreže ostatku svijeta. Osim uspostavljanja tehnološke dominacije i ostvarivanja značajnog profita, prodaja opreme omogućuje postavljanje vlastitih uvjeta o načinu korištenja ove nove tehnologije. Trenutno se vodi trgovinski rat između dvije vodeće zemlje u razvoju 5G mobilne mreže, a jedan od glavnih razloga je i nastojanje da se stekne vodstvo u inovacijama vezanim za 5G mrežu. SAD strahuje da kineske telekomunikacijske korporacije prodaju opremu koja ima značajne sigurnosne propuste i omogućuje špijunažu nad korisnicima i državnim službenicima kao i krađu povjerljivih podataka.

Bez obzira na prijetnje sankcijama poput prestanka razmjene sigurnosnih informacija država partnera SAD-a poput Njemačke i Ujedinjenog Kraljevstva, većina razvijenih država ne može si priuštiti odugovlačenje vremena i odgađanje implementacije 5G mreže. Razlozi koji se navode zbog čega se Kina naziva liderom u razvoju 5G mreže su visoka ulaganja državnih fondova za razvoj inovacija i omogućavanje vodećim poduzećima monopolističko poslovanje na domaćem tržištu. Operateri u Republici Hrvatskoj pretežito nabavljaju opremu za 5G mrežu od Švedskog poduzeća Ericsson koji je sklopio ugovore s T-Mobile i A1.



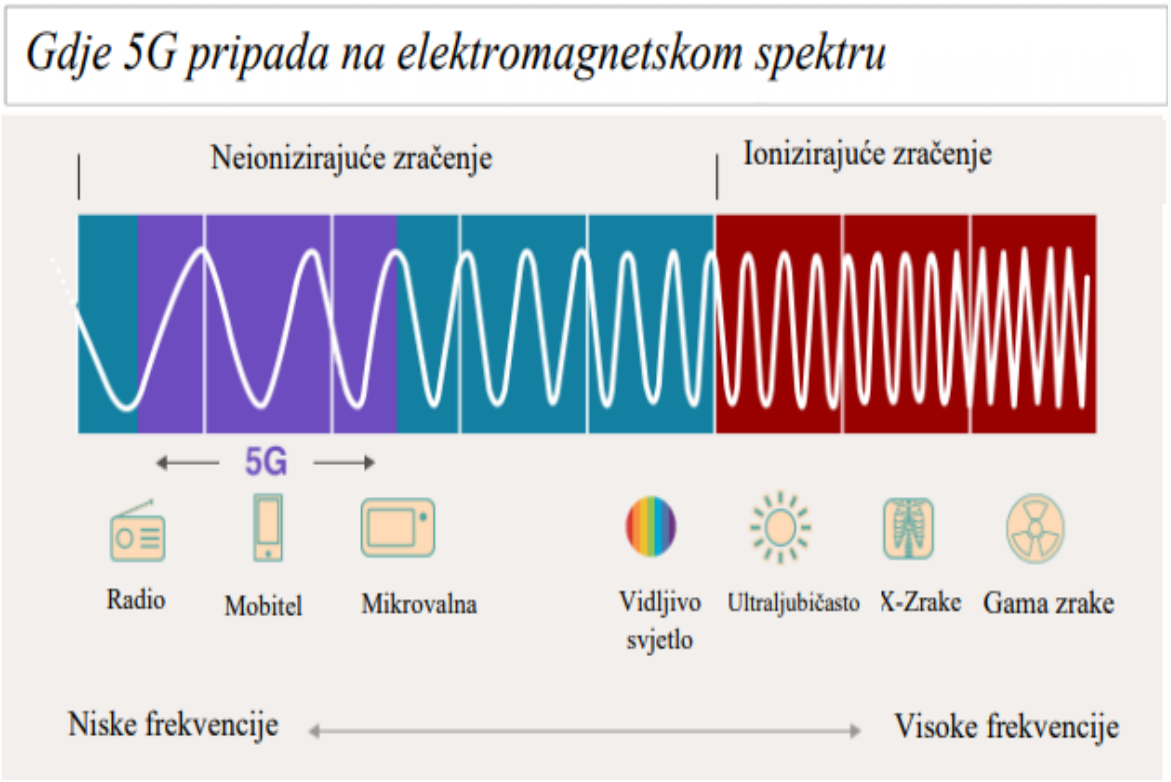
Slika 9.1 Broj lokacija na kojima se pruža 5G mreža u omjeru na 10 000 stanovnika [28]

Vodstvo u takozvanoj „5G utrci“” utječe na izravnu kompetitivnost u opremi i industriji komunikacijskih usluga, ali također indirektno i na ekonomski rast koji 5G omogućava. Ovo su zasebna, ali povezana razmatranja. Prvo treba uzeti u obzir indirektne koristi 5G mobilne mreže: Ova tehnologija je zamišljena kao platforma za značajno unaprjeđenje kompetitivnosti i inovativnosti u svakoj industriji u kojoj se primjenjuje, od proizvodnje i transporta do zdravstva i poljoprivrede. Drugačije rečeno, snaga državne 5G infrastrukture će se signifikantno odraziti na mogućnost poduzeća da razvijaju inovativne proizvode i usluge što će u konačnici imati snažan utjecaj na sveukupnu ekonomiju države. [29]

9.1 Utjecaj na zdravlje

Sve više se u svijetu špekulira o mogućnosti negativnog utjecaja na zdravlje novih tehnologija koje se javljaju u 5G mobilnoj mreži. U posljednje vrijeme može se primijetiti na društvenim stranicama i medijima upozorenja o štetnosti radijacije koja može oštetiti DNK kod pojedinca i uzrokovati rak, ubrzano starenje, uništavanje metabolizma pa čak i korištenje 5G mreže kao oružje. Ovakve objave i članci pozivaju stanovnike na prosvjede i uništavanje implementirane 5G infrastrukture. Nerijetko se i citiraju istraživanja priznatih organizacija poput Svjetske zdravstvene organizacije. Ovakva reakcija nije toliko iznenađujuća i neočekivana. Većina novih i kompleksnih tehnologija su također izazivale strah javnosti. Pojava električne struje bila je popraćena velikim prosvjedima i pozivima na uništavanje infrastrukture. U mnogim gradovima uništavala se gradska rasvjeta i sprječavao napredak. Kao najveći razlog zabrinutosti navodi se frekvencija na kojoj će 5G djelovati odnosno milimetarski radiovalovi. Zračenje se dijeli na ionizirajuće i neionizirajuće zračenje. Za razliku od ionizirajućeg zračenja koje ima dovoljno energije da uzrokuje promjene u energiji ili u sastavu atoma ili atomske jezgre, neionizirajuće zračenje ne posjeduje dovoljno energije po kvantu da može izazvati ionizaciju odnosno da ukloni elektron iz atoma ili molekule. U kategoriju imitacije neionizirajućeg zračenja spadaju tehnologije kao što su dalekovodi, radio, *Wi-Fi* i milimetarski radiovalovi. Emisija iz mobilnih telefona, uključujući i 5G tehnologiju, nije dovoljno snažna da prouzrokuje bio kakvu štetu. Ova neionizirajuća radijacija u najgorem slučaju može prouzrokovati vibraciju stanica koja se osjeti kao toplina. Ne ruši se struktura stanica i ne uzrokuje trajna šteta. [30]

Također, jedan od razloga sve veće zabrinutosti građana je i činjenica da se zbog manjeg dometa radiovalova postavljaju male ćelije na malim udaljenostima pa se stječe dojam da je 5G oprema posvuda. Zbog sve bržeg razvoja i implementacije 5G mreže, a nedovoljnog informiranja njenih korisnika, nije bilo neočekivano da će se zabrinutost stanovništva povećavati.



Slika 9.1.1 Razlika između ionizirajućeg i neionizirajućeg zračenja [31]

Do danas provedeno je više od tisuću istraživanja i nije dokazana nikakva povezanost između razvoja kancerogenih stanica i neionizirajućeg zračenja. Iako se nikada ne može u potpunosti dokazati da nova tehnologija neće imati nikakva štetna svojstva na čovjeka i prirodu, s trenutnim istraživanjima izgleda da ne postoji razlog za brigu.

10. ZAKLJUČAK

Radijske komunikacijske mreže razvijaju se sve od povezivanja preko jednostavnih mobilnih telefona u 1G do povezivanja gotovo svih i svega preko 5G mreže. Rad na petoj generaciji mobilnih mreža napreduje brže od očekivanog te će uskoro biti dostupan korisnicima diljem svijeta. Kako su istraživački projekti 5G-a, na primjer u okviru EU 5G javno-privatnog partnerstva, već započeli ili tek počinju, a aktivnosti 5G-a u tijelima za standardizaciju, posebno 3GPP, već su zakazane, važno je započeti rad na sigurnosnoj arhitekturi, kako bi se sigurnost ugradila u 5G mreže od samog početka. Važni koraci bit će razjašnjenje sigurnosnih zahtjeva, pregled postojećih sigurnosnih arhitektura, posebno sigurnosne arhitekture LTE, i konačno odabir sigurnosnih mjera 5G-a u uskoj interakciji s dizajnom opće 5G mrežne arhitekture. Te tehnologije imaju svoje vlastite sigurnosne izazove koji mogu dodatno kompliciratи mrežni sigurnosni krug. Stoga se temeljito razmatraju sigurnosni izazovi u različitim dijelovima i tehnologijama 5G mreža te su se iznijeli mogući sigurnosni principi, tehnike i prijedlozi za spomenute sigurnosne izazove. Budući da privatnost korisnika i korisničke informacije idu više u ruke vlasnika infrastrukture i operatora sustava, na primjer, u sustavima za pohranu u oblaku, privatnost je privukla veliku pažnju istraživanja. Stoga se navode i slabosti u privatnosti radijskih mreža i prikazuju se potencijalna rješenja za osiguranje privatnosti korisnika i podataka. Budući da će povezani sustavi u skoroj budućnosti biti složeni, okruženje sigurnosni prijetnji također će biti složeno, pa će stoga biti neizbježni i novi načini sigurnosnih operacija. Ukratko, velika je vjerojatnost da će se uz primjenu novih komunikacijskih tehnologija i usluga pojaviti nove vrste sigurnosnih prijetnji i izazova. Međutim, ako se uzmu u obzir ovi izazovi od početnih faza dizajna do faze implementacije, umanjit će se vjerojatnost gubitka sigurnosti i privatnosti.

LITERATURA

[1] Yulong Zou, Jia Zhu, Xianbin Wang, Lajos Hanzo, „A Survey on Wireless Security: Technical Challenges, Recent Advances, and Future Trends", dostupno na: https://ieeexplore.ieee.org/document/7467419

[2] „What is Network Security?", dostupno na: https://www.itarian.com/networksecurity.php

[3] „Internet of things standardization in ITU and prospective networking Technologies", IEEE Communications Magazine, September 2016

[4] David Rupprecht, Adrian Dabrowski, Thorsten Holz, Edgar Weippl, Christina Popper, „On Security Research Towards Future Mobile Network Generations", dostupno na: https://arxiv.org/pdf/1710.08932.pdf

[5] Madhusanka Liyanage, Ijaz Ahmad, Ahmed Bux Abro, Andrei Gurtov, Mika Ylianttila, „A Comprehensive Guide to 5G Security"

[6] „White papers", ericsson.com, dostupno na: https://www.ericsson.com/en/reports-and-papers/white-papers

[7] Michael Geller and Pramod Nair, „5G Security Innovation with Cisco", dostupno na: https://www.cisco.com/c/dam/en/us/solutions/collateral/service- provider/service-provider security-solutions/5g-security-innovation-with-cisco-wp.pdf

[8] „Nour global", dostupno na: http://nourglobal.com/network-security/

[9] Branislav Bubanja, „Sve o 5G tehnologiji: U petoj brzini!", dostupno na: https://pcpress.rs/sve-o-5g-tehnologiji-u-petoj-brzini/

[10] „Šta je 5G tehnologija (I dio)?", dostupno na: https://tekport.me/sta-je-5g-tehnologija-i-dio/

[11] Aleksandar Tudzarov, Toni Janevski, „Design for 5G Mobile Network Architecture",

[12] 5G Vision, „The 5G Infrastructure Public Private Partnership: the next generation of communication networks and services", dostupno na: https://5g-ppp.eu/wp-content/uploads/2015/02/5G-Vision-Brochure-v1.pdf

[13] 5G PPP, „The 5G Infrastructure Public Private Partnership", dostupno na: https://5g-ppp.eu/

[14] Ghada Arfaoui, Pascal Bisson, Rolf Blom, Ravishankar Borgaonkar, „A Security Architecture for 5G Networks"

[15] Mats Naslund, Gianluca Correndo, Seppo Heikkinen, Ghada Arfaoui, „5G-ENSURE D2.4: Security Architecture (draft)", October 2016

[16] Ijaz Ahmad, Suneth Namal, Mika Ylianttila, Andrei Gurtov, „Security in Software Defined Networks: A Survey“

[17] Altaf Shaik, Ravishankar Borgaonkar, N. Asokan, Valtteri Niemi, Jean- Pierre Seifert, „Practical Attacks Against Privacy and Availability in 4G/LTE Mobile Communication Systems“, dostupno na: https://arxiv.org/pdf/1510.07563.pdf

[18] N. Seddigh, B. Nandy, R. Makkar, J.F. Beaumont, „Security advances and challenges in 4G wireless networks“, dostupno na: https://ieeexplore.ieee.org/document/5593244

[19] Lene Tolstrup Sørensen, Samant Khajuria, Knud Erik Skouby, Department of Electronic Systems, „5G Visions of User Privacy“, dostupno na: https://vbn.aau.dk/en/publications/5g-visions-of-user-privacy

[20] „5G Security: Forward Thinking Huawei White Paper“, dostupno na: https://www.huawei.com/minisite/5g/img/5G_Security_Whitepaper_en.pdf

[21] Sadegh Farhang, Yezekael Hayel, Quanyan Zhu, „PHY-layer location privacy-preserving access point selection mechanism in next-generation wireless networks“, dostupno na: https://ieeexplore.ieee.org/document/7346836?reload=true&arnumber=7346836

[22] Ruiyun Yu, Zhihong Bai, Leyou Yang, Pengfei Wang, Oguti Ann Move, Yonghe Liu, „Ruiyun Yu ; Zhihong Bai ; Leyou Yang ; Pengfei Wang ; Oguti Ann Move ; Yonghe Liu“, dostupno na: https://ieeexplore.ieee.org/abstract/document/7593330

[23] 5G-ENSURE, „5G Enablers for Network and SystemSecurity and Resilience“

[24] Ghada Arfaoui, Jose Manuel Sanchez Vilchez, Jean-Philippe Wary, „Security and Resilience in 5G: Current Challenges and Future Directions“, dostupno na: http://www.5gensure.eu/sites/default/files/security-resilience-5g%2813%29_0.pdf

[25] NGMN 5G Initiative White Paper, „Next generations mobile networks“, dostupno na: https://www.ngmn.org/wp-content/uploads/NGMN_5G_White_Paper_V1_0.pdf

[26] Ijaz Ahmad, Shahriar Shahabuddin, Tanesh Kumar, Jude Okwuibe, Andrei Gurtovx, Mika Ylianttila,„ Security for 5G and Beyond“

[27] Marin Matijašević, „SIGURNOSNI ZAHTJEVI I IZAZOVI U 5G POKRETNIM MREŽAMA“, Završni rad

[28] GYT Analytics, „USA is lagging behind in 5G deployment, based on report by Deloitte“, dostupno na: http://gytanalytics.com/usa-lagging-behind-5g-deployment/

[29] Marko Opačak, „PRILIKE I PRIJETNJE 5G MOBILNE MREŽE U REPUBLICI HRVATSKOJ“, Završni rad

[30] Vodafone UK News Centre, „Is 5G safe?“, dostupno na: https://newscentre.vodafone.co.uk/5g/is-5g-safe/

[31] BBC News, „Does 5G pose health risks?“, dostupno na: https://www.bbc.com/news/world-europe-48616174

[32] Cisco, „Cisco Visual Networking Index: Global Mobile Data Traffic Forecast Update, 2015–2020“

[33] The wall street journal, „Yahoo Discloses New Breach of 1 Billion User Accounts“,

[34] Nima Zahadat, Paul Blessner, Timothy Blackburn, Bill A. Olson, „BYOD security engineering: A framework and its analysis“

[35] Shibo Luo, Mianxiong Dong, Kaoru Ota, Jun Wu, „A Security Assessment Mechanism for Software-Defined Networking-Based Mobile Networks“

[36] INTERNATIONAL TELECOMMUNICATION UNION, „Security architecture for systems providing end-to-end communications“

[37] NGMN – 5G Security, „5G security recommendations Package #1“

[38] Cheng-Xiang Wang, Fourat Haider, Xiqi Gao and Xiao-Hu You, „Cellular Architecture and Key Technologies for 5G Wireless Communication Networks“,

[39] Roger Piqueras Jover, „Security Attacks Against the Availability of LTE Mobility Networks: Overview and Research Directions“

[40] Mamta Agiwal, Abhishek Roy, Navrati Saxena, „Next Generation 5G Wireless Networks: A Comprehensive Survey“, dostupno na: https://ieeexplore.ieee.org/document/7414384

[41] Nokia, „Security challenges and opportunities for 5G mobile networks“

[42] Yasir I. A. Al-Yasir, „Fundamentals of 5G mobile networks“

[43] Sven Maček, „RAZVOJ I KARAKTERISTIKE MOBILNE MREŽE PETE GENERACIJE, Završni rad

[44] Hien Quoc Ngo, „Massive MIMO: Fundamentals and System Designs“

PRILOZI

Popis slika

Popis tablica

Popis i opis kratica

3GPP	3rd Generation Partnership Project
5G	5th generation
5G NR	5th generation New Radio
D2D	Device to Device
DoS	Denial of Service
DDoS	Distributed Denial of Service
DSSS	Direct Sequence Spread Spectrum
EDGE	Enhanced Data rates for GSM Evolution
FHSS	Frequency Hopping Spread Spectrum
GPRS	General Packet Radio Service
GSM	Global System for Mobile Communications
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
PLS	Physical Layer Security
SDN	Software Defined Networking
TCP	Transmission Control Protocol
UDP	User Datagram Protocol

IZJAVA

Izjavljujem pod punom moralnom odgovornošću da sam diplomski rad izradio samostalno, isključivo znanjem stečenim na Odjelu za elektrotehniku i računarstvo, služeći se navedenim izvorima podataka i uz stručno vodstvo mentorice izv. prof. dr. sc. Adriane Lipovac, kojoj se još jednom srdačno zahvaljujem.

Toni Musulin