Ispitivanje sigurnosti Wi-Fi mreže u javnom okruženju

Medur, Kristijan

Master's thesis / Diplomski rad

2022

Degree Grantor / Ustanova koja je dodijelila akademski / stručni stupanj: **University of Zagreb, Faculty of Transport and Traffic Sciences / Sveučilište u Zagrebu, Fakultet prometnih znanosti**

Permanent link / Trajna poveznica: https://urn.nsk.hr/urn:nbn:hr:119:033863

SVEUČILIŠTE U ZAGREBU
FAKULTET PROMETNIH ZNANOSTI

Kristijan Medur

ISPITIVANJE SIGURNOSTI WI-FI MREŽA U JAVNOM OKRUŽENJU

DIPLOMSKI RAD

Zagreb, 2022.

Sveučilište u Zagrebu
Fakultet prometnih znanosti

DIPLOMSKI RAD

ISPITIVANJE SIGURNOSTI WI-FI MREŽA U JAVNOM OKRUŽENJU

TESTING WI-FI NETWORK SECURITY IN PUBLIC ENVIRONMENT

Mentor: izv. prof. dr. sc. Ivan Grgurević

Student: Kristijan Medur

JMBAG: 0119031276

Zagreb, rujan 2022.

SVEUČILIŠTE U ZAGREBU
FAKULTET PROMETNIH ZNANOSTI
POVJERENSTVO ZA DIPLOMSKI ISPIT

Zagreb, 23. svibnja 2022.

Zavod: **Zavod za informacijsko komunikacijski promet**
Predmet: **Planiranje telekomunikacijskih mreža**

DIPLOMSKI ZADATAK br. 6947

Pristupnik: **Kristijan Medur (0119031276)**
Studij: Promet
Smjer: Informacijsko-komunikacijski promet

Zadatak: **Ispitivanje sigurnosti Wi-Fi mreže u javnom okruženju**

Opis zadatka:

Opisati tehničko-tehnološke značajke Wi-Fi mreža. Strukturirati elemente sigurnosti Wi-Fi mreža. Analizirati primjenu i razvoj javnih i privatnih Wi-Fi mreža. Sustavno analizirati i prikazati postojeća istraživanja iz područja sigurnosti Wi-Fi mreža u javnom okruženju. Izraditi studiju slučaja (case study) na temelju ispitivanja sigurnosti Wi-Fi mreža u javnom okruženju grada Trogira. Ispitivanjem sigurnosti Wi-Fi mreža u javnom okruženju grada Trogira utvrditi postojeće stanje Wi-Fi mreža i osviještenost korisnika o sigurnosti korištenja.

Mentor:

izv. prof. dr. sc. Ivan Grgurević

Predsjednik povjerenstva za diplomski ispit:

SAŽETAK

U današnjem svijetu bežične lokalne mreže postale su nezaobilazan dio svakodnevice. Pri tome najveću ulogu igraju upravo Wi-Fi mreže. Kroz pojavu pametnih telefona, tableta i ostalih uređaja koji imaju mogućnost bežičnog spajanja na Internet putem Wi-Fi-ja, još više je porasla popularnost te tehnologije. No kod Wi-Fi tehnologije i dalje postoje sigurnosni rizici, i to veći nego ikad prije zbog njene rasprostranjenosti. Većina ljudi nije svjesna načina na koji se Wi-Fi može iskoristiti kako bi se došlo do povjerljivih podataka. Danas je iznimno važno obratiti pažnju na to. U radu se provela anketa kojom se saznaje koliko su ljudi svjesni rizika koji su prisutni na Wi-Fi mrežama. Osim toga, korišten je i programski alat Vistumbler koji omogućava skeniranje Wi-Fi mreža u blizini te se skeniranjem Wi-Fi mreža u gradu Trogiru saznaje kakvo je stanje na terenu, odnosno kakvo je stanje Wi-Fi mreža u gradu što se tiče sigurnosnog aspekta.

KLJUČNE RIJEČI: Sigurnost, Wi-Fi, IEEE 802.11, Vistumbler

SUMMARY

In today's world, wireless local networks have become an indispensable part of everyday life. Wi-Fi networks play the biggest role in this. Through the appearance of smartphones, tablets and other devices that have the ability to wirelessly connect to the Internet via Wi-Fi, the popularity of this technology has grown even more. But there are still security risks with Wi-Fi technology, greater than ever before due to its prevalence. Most people are unaware of the ways in which Wi-Fi can be exploited to access confidential data. Today it is extremely important to pay attention to it. In the paper, a survey was conducted to find out how much people are aware of the risks lurking on Wi-Fi networks. In addition, the Vistumbler tool was also used, which enables scanning of Wi-Fi networks in the vicinity, and by scanning Wi-Fi networks in the city of Trogir, it is known what the situation is on the ground, that is, what is the state of Wi-Fi networks in the city as far as the security aspect is concerned.

KEYWORDS: Security, Wi-Fi, IEEE 802.11, Vistumbler

SADRŽAJ

1. Uvod

Ubrzan razvoj bežičnih mreža u današnjem svijetu učinio je Wi-Fi ljudskom svakodnevicom. Gotovo svi korisnici računala, ali i pametnih telefona koriste Wi-Fi kao glavnu tehnologiju za spajanje na Internet. Putem Wi-Fi tehnologije obavljaju se videopozivi, koristi Internet bankarstvo, konzumiraju multimedijski sadržaji te svi ostali sadržaji koji su dostupni na Internetu. Gotovo svatko tko posjeduje pametni telefon, koristi i Wi-Fi kao glavnu tehnologiju spajanja na Internet.

Nažalost, kao i sa svakom novom tehnologijom u svijetu telekomunikacija, i kod Wi-Fi-ja prijete mnogi sigurnosni rizici. Samim time što je to bežična mreža, postoji mogućnost da se netko neovlašteno spoji na nečiju mrežu te iskorištava to kako bi došao do povjerljivih podataka. Iako se od začetka Wi-Fi tehnologije uvode sigurnosni protokoli i standardi kako bi se njeno korištenje što više osiguralo, i dalje postoje mnogi rizici i načini upada u tuđu mrežu, unatoč tome što se kontinuirano radi na uvođenju novih i naprednijih sigurnosnih standarda.

Glavna motivacija za izradu ovog rada je upravo sigurnosni aspekt Wi-Fi mreža, to jest sigurnosni rizici koji prijete svakom korisniku Wi-Fi tehnologije, a pogotovo one koji nisu educirani u tom području te nisu svjesni opasnosti koje postoje pri spajanju na Wi-Fi mreže, ponajprije one koje su javne i dostupne velikom broju ljudi. U radu će se stoga obaviti istraživanje kako bi se saznalo koliko su korisnici svjesni rizika Wi-Fi mreža te kakvo je stanje u gradu Trogiru što se tiče sigurnosnog aspekta Wi-Fi mreža. Grad Trogir je iznimno popularno turističko odredište, te se većina turističkih posjetitelja spaja na Wi-Fi mreže koje su dostupne u apartmanima u kojima odsjedaju. Zato je potrebno saznati kakvo je stanje sigurnosti Wi-Fi mreža u gradu, jer ih koristi velik broj ljudi te zbog toga i kućne mreže na neki način imaju obilježja javnih Wi-Fi mreža.

Cilj rada je pomoću programskog alata Vistumbler, koji ima mogućnost skenirati Wi-Fi mreže u okruženju terminalnog uređaja prikupiti osnovne informacije o njima, poput naziva mreže, snage odašiljanja, korištenom sigurnosnom mehanizmu i dr. Osim toga, obavit će se i anketa kojom će se anketirati građane i turističke posjetitelje kako bi se saznalo koliko su korisnici Wi-Fi mreža educirani i svjesni rizika te tehnologije.

Svrha diplomskog rada je provedba analize o svjesnosti korisnika rizicima uslijed korištenja Wi-Fi tehnologije te dati uvid u trenutno stanje sigurnosti Wi-Fi mreža u gradskom okruženju, i to u okruženju grada Trogira. Na taj način mogu se dati preporuke kako korisnici mogu bolje zaštititi svoju mrežu, te kako biti oprezniji pri spajanju na druge Wi-Fi mreže u javnom prostoru.S ciljem postizanja navedenog, rad je strukturiran u sedam poglavlja:

1. Uvod
2. Tehničko-tehnološke značajke Wi-Fi mreža
3. Elementi sigurnosti Wi-Fi mreža
4. Primjena i razvoj javnih i privatnih Wi-Fi mreža
5. Pregled postojećih istraživanja iz područja sigurnosti Wi-Fi mreža u javnom okruženju
6. Studija slučaja: ispitivanje sigurnosti Wi-Fi mreža u javnom okruženju grada Trogira
7. Zaključak

Nakon uvoda, u drugom poglavlju opisuju se tehničko-tehnološke značajke Wi-Fi tehnologije te se stvara temelj na kojem se daljnji rad može zasnovati. U tom poglavlju opisana je tehnička pozadina Wi-Fi tehnologije te način njenog funkcioniranja. Nadalje, u trećem poglavlju opisuju se i elementi sigurnosti Wi-Fi mreža kako bi se dao uvid u sigurnosni aspekt te tehnologije.

U četvrtom poglavlju prikazan je razvoj Wi-Fi mreža, kako javnih, tako i privatnih, kako bi se stekao uvid u povijest razvoja i primjene Wi-Fi mreža. Nakon toga, u petom poglavlju je napravljen osvrt na postojeća istraživanja iz ovog područja u svijetu, što pomaže nadalje razumjeti sigurnosne trendove ove tehnologije i istraživanje tog područja.

U šestom poglavlju opisano je ispitivanje korisnika putem anketnog upitnika i skeniranje mreža u gradu Trogiru, te su prikazani dobiveni rezultati i njihova analiza.

U sedmom poglavlju - zaključku su skupljene sve informacije dobivene izradom ovog rada te su dane preporuke i zaključci izvedeni iz obavljenog.

2. Tehničko-tehnološke značajke Wi-Fi mreža

Princip rada Wi-Fi mreža zasnovan je na žičnim lokalnim mrežama, ponajprije zbog toga što su se Wi-Fi mreže razvile upravo iz njih. Kako bi se bolje razumjeli principi rada Wi-Fi mreže, pa i bežičnih lokalnih mreža općenito, potrebno je prvo definirati neke osnovne pojmove u lokalnim računalnim mrežama. Osim osnovnih pojmova koji se upotrebljavaju u kontekstu Wi-Fi mreža, potrebno je i poznavati arhitekturu Wi-Fi mreže, te samim time shvatiti i princip funkcioniranja mreža.

Također, postoji nekoliko različitih standarda same Wi-Fi mreže, koji su se unaprjeđivali s vremenom, usporedno s razvojem tehnologije. Prema [1], odbor za standarde instituta inženjera elektrike i elektronike (engl. *Institute of Electrical and Electronics Engineers* – IEEE) 802 izdao je 1997. godine prvi standard bežičnih lokalnih mreža, te je on nazvan IEEE 802.11. Trenutno je aktualan standard 802.11ax, s time da je već u razvoju idući, 802.11ay.

2.1. Arhitektura Wi-Fi mreže

Wi-Fi mreže, kao i svaka druga računalna mreža, mogu se objasniti arhitekturom mreže. Fizička arhitektura mreže predstavlja sve tipične uređaje koji se koriste u mreži, te ih prikazuje u skladu s njihovom ulogom u mreži. Drugim riječima, ona prikazuje mrežu u stvarnom, fizičkom svijetu. S druge strane, logička arhitektura prikazuje logičku stranu mreže, neopipljivu, te objašnjava što se događa u dijelu mreže koji se ne vidi, dakle kako putuju podaci, kako su organizirani, te kako je sama mreža logički organizirana. U logičku arhitekturu spada i opis mreže pomoću referentnog modela za otvoreno povezivanje sustava[1] (engl. *Open Systems Interconnection model* – OSI model).

2.1.1. Fizička arhitektura mreže

Prije prikazivanja fizičke arhitekture, potrebno je razumjeti koji su osnovni dijelovi računalnih mreža, pa tako i lokalnih računalnih mreža te Wi-Fi mreža, te kako oni međusobno funkcioniraju da bi stvorili mrežu i ostvarili prijenos podataka. U nastavku su opisani svi tipični

[1] Najkorišteniji opis logičke arhitekture mreže.

uređaji, odnosno dijelovi računalne mreže, s fokusom na bežične lokalne tj. Wi-Fi mreže. Prema [1], to su:

- Odašiljač, tj. pošiljatelj, odnosno izvor: uređaj u mreži od kojeg potječe slanje informacije.
- Prijamnik, odnosno destinacijski uređaj ili primatelj informacije: uređaj u mreži koji prima informaciju. U Wi-Fi mrežama obično su prijamnik i odašiljač objedinjeni u jednom uređaju, te je to krajnji uređaj u mreži, odnosno terminalni uređaj[2]. To su najčešće pametni telefoni, *tableti* ili računala.
- Mrežni krug: komunikacijski krug, odnosno put kojim putuju informacije u mreži. Uspostavlja se preko određenog komunikacijskog medija između dvije ili više točaka u mreži. Obično implicira logičku konekciju preko fizičkog voda.
- Link: segment između dvije točke u mrežnom krugu. Obično se mrežni krugovi sastoje od više linkova, ali u vrlo jednostavnoj mreži se mogu sastojati i od samo jednog linka, primjerice kad se povezuju računalo i printer putem kabela.
- Kanal: u standardnom korištenju, kanal je jednosmjerna veza između odašiljača i prijamnika. No u kontekstu lokalnih računalnih mreža, najčešće se koristi kao logička konekcija putem fizičkog mrežnog kruga, kako bi se održavala jedna podatkovna konverzacija. Fizički mrežni krug se može konfigurirati i tako da podržava višestruke takve konverzacije. U Wi-Fi mrežama, kanal označava odjeljivanje prijenosnog medija, kako bi što više podatkovnih konverzacija, odnosno veza stalo u jedan frekvencijski opseg, bez da smetaju jedne drugima.
- Preklopnik ili *switch*: uređaj koji uspostavlja, održava i preklapa logičke konekcije preko fizičkog mrežnog kruga. U paketnim mrežama, kao što su računalne mreže, pa tako i Wi-Fi mreže, preklopnici obavljaju istu zadaću, ali s tom razlikom da obavljaju radnje nad paketima, te ih šalju na zadanu destinaciju preko sljedećeg uređaja u mreži, te tako uspostavljaju odnosno preklapaju konekciju. Često su i mnogo inteligentniji od čistog preklapanja konekcija, pa tako mogu uzimati u obzir

[2] Terminalni uređaj: uređaj na kraju komunikacijske mreže u kojem se obavlja pretvorba različitih načina informacija u električne signale prilagođene za prijenos komunikacijskim kanalom i obratno.

prioritete, znati preko kojeg uređaja je najbolje poslati poruku koju su dobili i slično.

- Usmjerivač ili *router*: inteligentniji uređaj od preklopnika, koji je sposoban donositi odluke na temelju pogleda na mrežu u cjelini. To je glavna razlika usmjerivača u odnosu na preklopnik, koji vidi samo idući uređaj u mreži i ne zna što se događa u ostatku mreže, niti zapravo zna da postoji ostatak mreže. Usmjerivači su programibilni uređaji koji se mogu podesiti tako da obavljaju usmjeravanje paketa na najbolji način s obzirom na mrežu u koju su smješteni, uzimajući u obzir trenutno zagušenje i promet u mreži, uređaje koji su smješteni u mreži, te šaljući pakete najoptimalnijom mogućom rutom u mreži.
- Mreža: sama mreža je skup elemenata koji zajedno rade kako bi podržali, odnosno omogućili protok informacija. Sastoji se upravo od gore nabrojanih elemenata.
  Kod računalnih mreža, postoji podjela mreža s obzirom na područje koje pokrivaju: to su lokalna mreža (engl. *Local Area Network* – LAN), metropolitanska ili gradska mreža (engl. *Metropolitan Area Network* – MAN), te mreža širokog područja (engl. *Wide Area Network* – WAN).

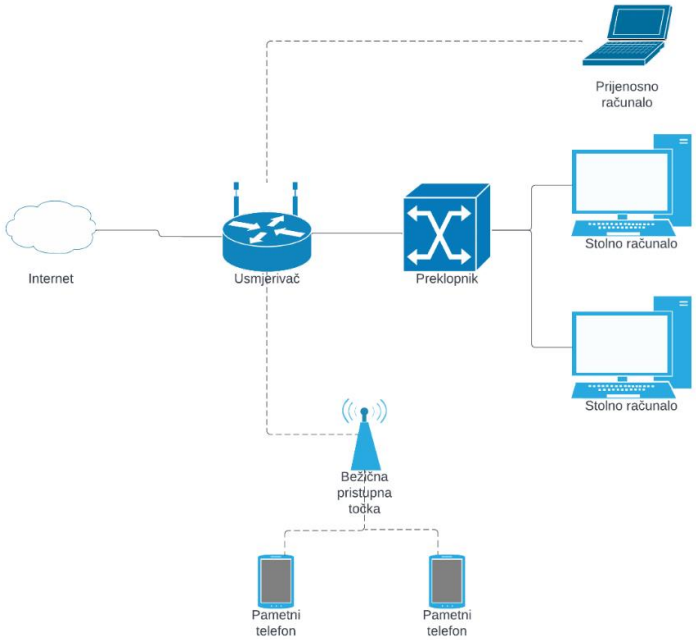
Kod Wi-Fi mreža dobro je definirati i uređaje koji su tipični za takve mreže, a koji se ne koriste kod primjerice žičnih lokalnih računalnih mreža. To su:

- Pristupne točke (engl. *Access Point* – AP): uređaj koji omogućuje bežičnim terminalnim uređajima da se spoje na mrežu. Spajaju se na ostatak mreže jednim kabelom, te podržavaju spajanje većeg broja bežičnih uređaja i omogućuju im pristup ostatku mreže. Postoji više izvedbi AP-a, pa tako oni mogu biti zasebni uređaji koji se spajaju na usmjerivač, ili pak mogu biti usmjerivači koji imaju integriran AP u sebi, odnosno mogu biti integrirani u usmjerivače.
- Repetitor ili *repeater*: uređaj koji jednostavno pojačava bežični signal koji dobiva od bežičnog usmjerivača ili pristupne točke, te na taj način proširuje doseg bežične mreže. To su vrlo jednostavni uređaji koji samo uzimaju primljeni signal te ga ponovo šalju dalje većom snagom.

- Bežične mrežne kartice: kod žičnih računalnih mreža koriste se klasične mrežne kartice, s jednim ili više konektora za spajanje na mrežu putem kabela. Kod bežičnih, pa tako i Wi-Fi mreža, koriste se bežične kartice, sa antenom koja služi za primanje i slanje signala u mreži.

Uz sve navedeno, pametni telefoni, prijenosna računala i slični uređaji koji se koriste u Wi-Fi mrežama obično u sebi imaju integrirane sve sustave koji su im potrebni za spajanje na mrežu. To su bežična mrežna kartica, antene i sl. Također zbog toga imaju i mogućnost sami postati svojevrsni usmjerivač i pristupna točka korištenjem opcije *hotspot*, koja omogućava uređaju da stvori svoju Wi-Fi mrežu putem ugrađenih antena, te se obično koristi da bi se podijelio pristup Internetu uređajima oko sebe. Tako se pametni telefoni mogu spojiti na mobilnu mrežu s pristupom Internetu, te putem lokalne Wi-Fi mreže omogućiti uređajima oko sebe pristup Internetu preko te mobilne mreže.

Na slici 1. prikazana je fizička arhitektura uobičajene kućne mreže koja koristi Wi-Fi s prikazanim najvažnijim elementima mreže. Isprekidana crta na slici 1. prikazuje bežičnu vezu, a puna crta prikazuje žičnu vezu. Vidljivo je da se neki uređaji mogu spajati na istu mrežu putem žice, a neki putem Wi-Fi bežične veze.



Slika 1. Uobičajena kućna mreža

Također, pristupne točke pomažu proširiti mrežu, tako da se uređaji poput pametnih telefona mogu spojiti na mrežu čak i kad su predaleko da bi ostvarili vezu s bežičnim usmjerivačem, primjerice kad je korisnik na dvorištu ili ispred kuće. Naposljetku, svi elementi mreže se spajaju na Internet putem infrastrukture mrežnog operatora.

2.1.2. Logička arhitektura mreže

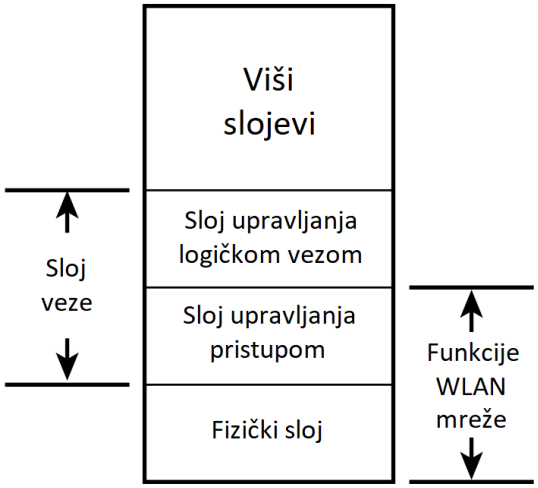
Logička arhitektura Wi-Fi mreže najbolje se može prikazati OSI modelom mreže. Prema [2], OSI model se sastoji od sedam slojeva, a to su:

1. Fizički sloj – prenosi sirove podatke preko fizičkog prijenosnog medija. Zadužen je za definiranje konektora, vrste električnog kabela ili bežične tehnologije kojom se će se prenijeti podaci odnosno signal.
2. Podatkovni sloj – uspostavlja i terminira konekciju između dva fizički povezana čvora u mreži. Raspodjeljuje pakete u okvire te ih šalje od izvora prema odredištu. Ovaj sloj koristi fizičke adrese uređaja, kod Wi-Fi mreža to su adrese upravljanja pristupom (engl. *Medium Access Control* – MAC).
3. Mrežni sloj – ima dvije glavne funkcije: pretvaranje segmenata u mrežne pakete kod izvora, te zatim sklapanje paketa natrag u segmente na odredištu, te usmjeravanje paketa putem najboljeg i najefikasnijeg puta u mreži. Ovaj sloj koristi mrežne adrese, u Wi-Fi-ju to su Internet protokol (engl. *Internet Protocol* – IP) adrese.
4. Transportni sloj – uzima podatke prenesene u sloju sesije i pretvara ih u segmente na izvorišnom kraju mreže. Zadužen je za kontrolu toka, slanje podataka brzinom koja odgovara odredišnom uređaju, te provjeru jesu li podaci poslani ispravno, te ako nisu, traženje ponovnog slanja.
5. Sesijski sloj – kreira komunikacijske kanale, koji se zovu sesije, između uređaja. Zadužen je za otvaranje sesija, osiguravanje da ostanu otvorene i funkcionalne dok traje prijenos podataka, te njihovo zatvaranje kad stane prijenos podataka.
6. Prezentacijski sloj – priprema podatke za aplikacijski sloj, dakle definira kako će uređaji kodirati, kriptirati i komprimirati podatke tako da se oni ispravno prime i

pročitaju na odredišnom kraju mreže. Također priprema podatke s aplikacijskog sloja za prijenos putem sesijskog sloja.

7. Aplikacijski sloj – koristi ga krajnji softver kojeg koristi korisnik, poput internetskog pretraživača ili E-mail klijenta. Koristi protokole koji omogućavaju softveru, odnosno programima da prime i šalju podatke te da ih smisleno prikazuju korisnicima.

Wi-Fi mreža spada u bežične lokalne računalne mreže (engl. *Wireless Local Area Network* – WLAN), pa samim time za nju vrijedi i logička arhitektura WLAN mreže. Na slici 2. prikazana je logička arhitektura WLAN-a, na kojoj se vidi kojim slojevima OSI modela pripadaju njene funkcionalnosti.



Slika 2. Logička arhitektura WLAN mreže
Izvor: *[3]*

Kao što je vidljivo na slici, kod WLAN, pa tako i Wi-Fi mreža, funkcije mreže spadaju u donji dio sloja veze, koji je podijeljen u sloj upravljanja logičkom vezom (engl. *Logical Link Control* – LLC) i sloj upravljanja pristupom tj. MAC sloj, te fizički sloj. Iznad toga su viši slojevi koje ne kontrolira sama Wi-Fi mreža.

Fizički sloj omogućava prijenos sirovih podataka preko komunikacijskog kanala tako što definira električna, mehanička, proceduralna i ostala fizikalna svojstva prijenosa podataka, kao

što su vrsta konektora, prijenosnog medija, pri čemu je to zrak u slučaju Wi-Fi mreže, frekvencija signala i tako dalje. Ovdje primjerice spada i kontrola tehnike proširenog spektra, koja omogućava da se signal efikasnije i sa što manje smetnji prenese putem radiovalova. U te tehnike proširenog spektra pripadaju dvije metode: frekvencijsko preskakanje proširenog spektra[3] (engl. *Frequency Hopping Spread Spectrum* – FHSS) te direktna sekvenca proširenog spektra[4] (engl. *Direct Sequence Spread Spectrum* – DSSS), [3].

Sloj upravljanja pristupom je zadužen za to da uređaji pravilno dijele prijenosni medij. Kako je kod Wi-Fi mreže prijenosni medij zrak, dakle koriste se radiovalovi za prijenos podataka, takav način prijenosa je vrlo osjetljiv na smetnje i zbog toga sloj upravljanja pristupom ima vrlo važnu zadaću. U WLAN mrežama, pa tako i u Wi-Fi mrežama, koristi se protokol višestrukog pristupa opažanjem nositelja (engl. *Carrier Sense Multiple Access* – CSMA). To je protokol koji osluškuje aktivnosti u mreži, te ako ih ima, čeka prvi slobodan trenutak da pošalje podatke, [3].

2.2. Karakteristike prijenosa podataka radiovalovima

Wi-Fi mreže koriste različite frekvencije za prijenos podataka, kao i različite kanale kojima su te frekvencije podijeljene u podskupine. Kako bi se bolje razumio prijenos podataka Wi-Fi mrežom, upravo iz razloga što Wi-Fi mreža kontrolira donja dva sloja u OSI modelu – fizički i podatkovni sloj, potrebno je opisati kako Wi-Fi kontrolira prijenos podataka te koja su pravila prijenosa podataka na fizičkoj razini. Wi-Fi mreža je najranjivija upravo zbog toga što koristi zrak kao prijenosni medij, pa je važno shvatiti kako radiovalovi putuju zrakom, na koji način su raspodijeljeni, te koji je princip rada mreže na fizičkoj razini.

2.2.1. Frekvencijski spektar Wi-Fi tehnologije

Wi-Fi mreža koristi takozvani industrijski, znanstveni i medicinski spektar frekvencija (engl. *Industrial, Scientific and Medical* – ISM). Taj spektar se zove i nelicenciranim spektrom, iz razloga što je on međunarodno dogovoren i za njegovo korištenje nije potrebno imati licencu. Taj frekvencijski spektar koristi vrlo široka paleta uređaja, ne samo Wi-Fi uređaji, već i mikrovalne

[3] FHSS metoda se koristi za izbjegavanje interferencije te sprječavanje prisluškivanja.
[4] DSSS metoda se primarno koristi za smanjenje interferencije.

pećnice, te vrlo veliki broj ostalih uređaja koji se bežično povezuju, npr. Putem Bluetooth tehnologije, te ostali uređaji u raznim industrijskim i medicinskim granama. Cijeli ISM spektar podijeljen je u dva glavna frekvencijska spektra, [4]:

- 2400-2500 MHz: zove se i 2.4 GHz spektar, a koristi se najviše za Wi-Fi mreže, no osim toga koriste ga i mikrovalne, Bluetooth itd.
- 5725-5875 MHz: zove se još i 5 GHz Wi-Fi spektar, iako je bliži području od 5.8 GHz. Donosi povećanu širinu pojasa i brzinu prijenosa, no s obzirom na to da je na višoj frekvenciji, oprema je malo skuplja, ali i interferencija može biti manja upravo zbog manje uređaja koji koriste tu frekvenciju, te činjenice da se koristi više za direkcionalno slanje podataka. Može sadržavati do 23 kanala koji se ne preklapaju, za razliku od 2.4 GHz spektra, koji ima 13 kanala koji se međusobno preklapaju.

Kod 802.11 standarda, koji je sinonim za Wi-Fi mreže, različite varijante standarda koriste i različita frekvencijska područja. U tablici 1. prikazani su svi 802.11 standardi te frekvencije koje koriste.

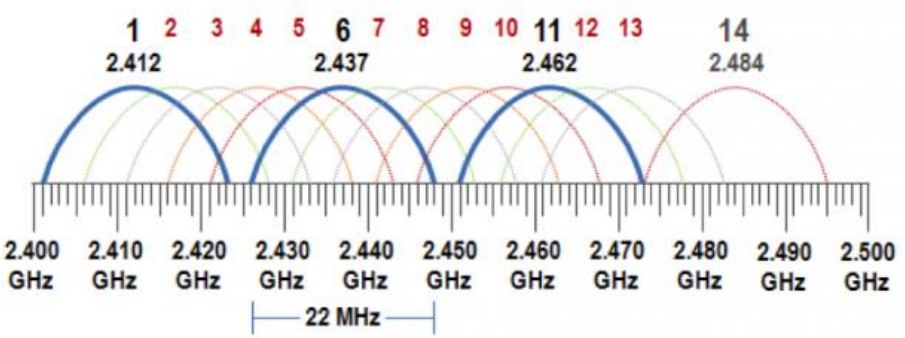
Tablica 1. Frekvencijska područja 802.11 standarda [4]

Verzija standarda	**Korišteni frekvencijski pojas**
802.11a	5 GHz
802.11b	2.4 GHz
802.11g	2.4 GHz
802.11n	2.4 i 5 GHz
802.11ac	Do 6 GHz
802.11ad	Do 60 GHz
802.11af	Ispod 1 GHz
802.11ah	700, 860, 902 MHz, ovisno o zemlji
802.11ax	2.4, 5 i 6 GHz

Kao što je vidljivo u tablici 1., neki standardi koriste i druga frekvencijska područja, čak i do 60 GHz, koja također pripadaju ISM frekvencijskom spektru, međutim te frekvencije nisu tako često korištene te ti standardi nisu toliko zastupljeni poput ostalih, primjerice 802.11b, g, n i ac.

2.2.2. Podjela 2.4 GHz i 5 GHz spektra na kanale

Kako bi se smanjila interferencija brojnih Wi-Fi uređaja na istom prostoru, koristi se podjela frekvencijskog spektra na kanale. Tako spektar frekvencije 2.4 GHz ima 14 kanala na koje je podijeljen, ali koji se ipak međusobno preklapaju. Na slici 3. prikazana je raspodjela kanala u tom spektru.

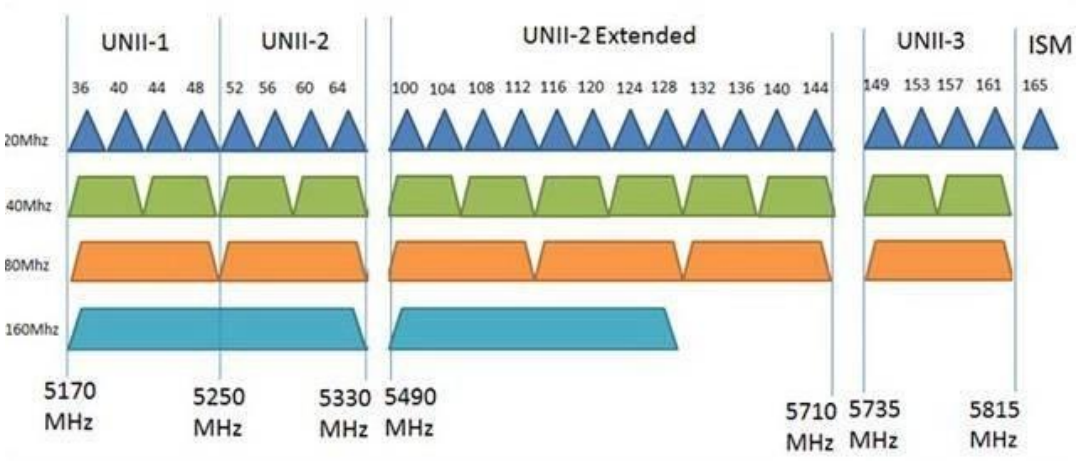


Slika 3. Raspodjela kanala u 2.4 GHz spektru, *[5]*

Kao što je vidljivo na slici 3., zapravo ima smisla koristiti samo 3 kanala od svih 14, jer su to 3 kanala koja se međusobno ne preklapaju te tada dolazi do najmanje interferencija između uređaja. Obično se tvornički uređaji podešavaju da rade na 1., 6. ili 11. kanalu, iako su moguće i druge kombinacije, primjerice 2., 7. i 12. kanal. U praksi je čest slučaj podešavanja mreže od nestručnih osoba, koje kućnu Wi-Fi mrežu postavljaju da radi na primjerice 4. kanalu, jer na nekoj od aplikacija za analizu Wi-Fi signala u okolini vide da na tom kanalu ne radi nijedna mreža oko njih. No to samo dovodi do problema s interferencijom, jer tada ta mreža koja radi na 4. kanalu uvodi smetnje u okolne mreže na 1. ili 6. kanalu, koje su obično tvornički, i to s razlogom, automatski podešene na rad na tim kanalima.

Osim navedenog, također je važno istaknuti da se 14. kanal ne koristi ni u Europi po europskim standardima, ni u Sjevernoj Americi po američkim standardima, već samo u Japanu za rad 802.11b mreža.

5 GHz spektar je podijeljen na 23 kanala koji se međusobno ne preklapaju te je samim time lakše podesiti mrežu u tom spektru bez problema s interferencijom. Tome pomaže i drukčiji način korištenja 5 GHz spektra, zbog činjenice da je više frekvencije uputno koristiti kod direkcionalnog[5] prijenosa signala. Na slici 4. prikazan je 5 GHz spektar frekvencija i njegova raspodjela na kanale. Kao što je prikazano na slici, nijedan kanal se ne preklapa s drugim, te se također kanali mogu i grupirati zajedno, kako bi se dobila veća širina pojasa. Kanali su širine 20 MHz kad se ne grupiraju, a grupiranjem se mogu dobiti širine pojedinačnog kanala od 40 MHz, 80 MHz, te čak i 160 MHz. Prema [4], mnogi Wi-Fi usmjerivači imaju opciju *dual band* rada, pri čemu mogu raditi istovremeno i na 2.4 GHz i 5 GHz spektru, pa tako nuditi uređajima oko sebe spajanje na jedan ili drugi način.



Slika 4. Raspodjela kanala u 5 GHz spektru, *[6]*

Iako je očito da 5 GHz spektar ima mnogo prednosti nad 2.4 GHz spektrom, ipak je 2.4 GHz spektar još uvijek mnogo više zastupljen u korištenju, a tako će vjerojatno i ostati, jer ta dva spektra nisu međusobno isključiva, već se koriste u različitim uvjetima rada. Tako ima i smisla da je 2.4 GHz spektar mnogo popularniji u kućnim mrežama, jer u takvim uvjetima rada Wi-Fi mreže poželjno je imati omnidirekcionalne antene[6] i širenje signala u svim smjerovima, a u takvim uvjetima je mnogo efikasniji rad uređaja u 2.4 GHz spektru zbog lakoće širenja signala i manjeg zagušenja, zbog niže frekvencije.

[5] Prijenos signala koji je vrlo usmjeren i ima uzak snop širenja.
[6] Antene koje odašilju signal u svim smjerovima oko sebe.

2.2.3. Jačina signala

Jačina odašiljanja signala je vrlo važna karakteristika svake Wi-Fi mreže. Svaki uređaj koji ima mogućnost spajanja na mrežu ili stvaranja Wi-Fi mreže, dakle koji ima odašiljač i prijemnik, mora imati i antenu koja je odgovarajuća za odašiljanje i prijem Wi-Fi signala. Ovisno o korištenom 802.11 standardu, antene mogu podržavati različite frekvencijske opsege, te prema tome biti i različitih dimenzija. No i dalje su kod kućnih usmjerivača najčešće antene duljine otprilike četvrtine valne duljine signala koji trebaju primiti ili odaslati. Antene bi trebale biti duge kao polovica valne duljine, ili duljine koja se dobije dijeljenjem valne duljine cijelim brojem, dakle polovicu valne duljine, četvrtinu valne duljine itd. Međutim kod premale dimenzije antene dolazi do negativnih učinaka kao što su efikasnost i impedancija antene, pa je potrebno pronaći kompromis između veličine antene i njenih karakteristika, koje se poboljšavaju povećavanjem dimenzija antene. Zato se u praksi obično uzimaju antene veličine polovice ili četvrtine valne duljine signala, [7].

Prema [8], antene također imaju pet važnih karakteristika po kojima se razlikuju, koje su navedene u nastavku:

- Rezonantna frekvencija: frekvencija na kojoj antena radi, odnosno na kojoj je električka duljina antene jednaka polovici valne duljine, jer fizička dimenzija antene koja ostvaruje najbolji učinak odgovara polovici valne duljine.
- Usmjerenost i dobitak: parametar koji pokazuje koliku količinu elektromagnetskog zračenja antena proizvodi u nekom smjeru u odnosu na zamišljenu antenu koja zrači kuglasti val, koja se zove izotropni radijator. Svaka stvarna antena ima neku usmjerenost koja je veća od 1 ili 0 dB, što znači da koncentrira zračenje u nekom smjeru.

  Dobitak je veličina koja pokazuje koliko neka antena zaista zrači, odnosno kolika je njena stvarna korisnost. U odnosu na usmjerenost, dobitak sadrži i informaciju o prilagodbi antene na izvor energije.

- Polarizacija: definira se kao smjer titranja vektora električnog polja kojeg antena zrači. Većina antena zrači linearno polarizirani val, a posebne vrste kružno polarizirani.
- Impedancija: kako je antena sredstvo kojim prilagođavamo impedanciju signalnog vodiča koji izlazi iz odašiljača, recimo 50 Ω, na impedanciju slobodnog prostora, 377 Ω, ulazna impedancija antene je impedancija koju vidi generator signala. Ona bi trebala biti jednaka impedanciji signalnog vodiča ili generatora signala.
- Dijagram zračenja: geometrijski prikaz raspodjele gustoće snage ili jakosti električnog polja u prostoru oko antene. Obično se daje u horizontalnoj ili vertikalnoj ravnini. Prema dijagramu zračenja, antene se dijele na usmjerene i neusmjerene.

Jačina odašiljanja signala kod Wi-Fi mreža, a također i ostalih bežičnih mreža, mjeri se jedinicom dBm, koja označava razinu snage u decibelima u odnosu na referentnu snagu od 1 mW. Bilo bi vrlo nezgodno prikazati jačinu, tj. snagu izračenog signala u Watima ili nekoj drugoj mjernoj jedinici, pa se zato snaga prikazuje u odnosu na tu referentnu snagu.

Prema [9], najveća zakonski dozvoljena snaga poslana prema anteni u ISM frekvencijskom području je 30 dBm ili 1 W. U praksi će to, naravno, biti nešto, iako gotovo zanemarivo manje, zbog gubitaka u samoj anteni. Maksimalna dozvoljena efektivna izotropna izračena snaga (engl. *Effective Isotropic Radiated Power* – EIRP) je 36 dBm ili 4 W. Prema tome, obavezno je paziti na to da bilo koja oprema, pa tako i oprema u Wi-Fi mreži, ne prelazi dozvoljene granice jačine signala.

S druge strane, u većini slučajeva u gradskom okruženju, s obzirom na to da sva Wi-Fi oprema koja se može legalno kupiti već podliježe navedenim ograničenjima, korisnici i vlasnici Wi-Fi mreže imaju problema oko preslabe jačine signala. Zbog vrlo često nepogodnog prostora u gradu za širenje Wi-Fi signala, potrebno je smjestiti usmjerivač ili pristupnu točku na takvo mjesto gdje signal doseže potrebnu udaljenost[7].

[7] Obično najbolje na mjestu gdje nema puno prepreka i signal ne mora prolaziti kroz zidove.

Istovremeno je potrebno paziti da signal ne doseže preveliku udaljenost, što na jedan način umanjuje sigurnost Wi-Fi mreže, jer tako udaljeniji uređaji dobivaju priliku za spajanje na mrežu, a također i često smeta drugim Wi-Fi mrežama u okolini, pogotovo ako rade na istom kanalu.

Jačina signala u gradskom okruženju se obično nalazi u rasponu od -30 dBm, što predstavlja najveću moguću jačinu, do -90 dBm, koja je donja granica za funkcioniranje mreže. U tablici 2. je opisano kakva se kvaliteta signala može očekivati za određenu jačinu u dBm skali. U aplikacijama i programima za skeniranje Wi-Fi mreža ta vrijednost se označava kao indikator jačine primljenog signala (engl. *Received Signal Strength Indicator* – RSSI).

Tablica 2. Očekivana kvaliteta primljenog signala s obzirom na jačinu signala [10]

Jačina signala	**Očekivana kvaliteta**
-30 dBm	Maksimalna jačina signala, u neposrednoj blizini usmjerivača ili pristupne točke
-50 dBm	Sve do ove razine se smatra odličnom kvalitetom signala
-60 dBm	Još uvijek dobra i pouzdana jačina signala
-67 dBm	Minimalna jačina signala za usluge koje trebaju pouzdanu i brzu vezu, poput VoIP usluga, video *streaminga* i sl.
-70 dBm	Kvaliteta signala dovoljna za jednostavno surfanje i slanje e-mail poruka
-80 dBm	Najniža jačina signala potrebna da bi se ostvarila veza
-90 dBm	Vjerojatno nije moguće uopće se povezati na mrežu i koristiti bilo kakvu uslugu

Kako je vidljivo u tablici, poželjno je da razina signala ne bude manja od -67 dBm ili eventualno -70 dBm ako se obavljaju jednostavnije zadaće na Internetu. Za današnje pojmove korištenja Interneta, što uključuje pregled video sadržaja, *streamanje* video i audio sadržaja i slično, svaka razina signala slabija od -67 dBm je neprihvatljiva.

2.3. Razvoj IEEE 802.11 standarda kroz povijest

IEEE 802.11 standard za Wi-Fi mreže prošao je velik broj modifikacija i verzija kroz godine. Prema [1], originalna verzija standarda ratificirana je 1997. godine, te je podržana bila maksimalna brzina prijenosa podataka od 2 Mbps te je korištena frekvencija od 2.4 GHz, ali zbog teško izvedive kompatibilnosti rada uređaja na mreži taj standard nije značajnije korišten na tržištu. Nakon njega, verzije IEEE 802.11 standarda označavane su slovima, te je do danas formirano nekoliko značajnijih standarda, od kojih se i velik broj starijih još uvijek koristi te su podržani od većine uređaja na tržištu[8].

2.3.1. IEEE 802.11b

802.11b standard je koristio iste frekvencije koje će koristiti i većina budućih verzija, otprilike 2.4 GHz. Najveća maksimalna brzina je bila 11 Mbps, iako je u praksi očekivana brzina bila oko 2 ili 3 Mbps, a domet otprilike 45 metara. 802.11b uređaji su bili jeftini, ali standard je imao najnižu brzinu od svih. Koristio je neregulirane frekvencije od 2.4 GHz, te je dolazilo do čestih interferencija zbog mikrovalnih pećnica, bežičnih telefona i ostalih kućanskih uređaja koji su već koristili tu frekvenciju, [11].

2.3.2. IEEE 802.11a

Dok je 802.11b bio u razvoju. IEEE odbor za standardizaciju već je kreirao i novo proširenje originalnom 802.11 standardu, 802.11a. Iako se prema nazivlju može pretpostaviti da je 802.11a stvoren prije 802.11b standarda, zapravo su stvoreni otprilike u isto vrijeme. Ovaj standard koristio je frekvencije od 5 GHz, te je maksimalna teoretska brzina prijenosa podataka iznosila 54 Mbps. Imao je manji domet zbog više frekvencije, ali i manje problema s interferencijom. Uz to, 802.11a i 802.11b su bili međusobno nekompatibilni zbog različitih frekvencija koje su koristili, [11]. Prema [12], 802.11b standard je na kraju ispao popularniji kod kućnih korisnika, a 802.11a se vrlo rijetko može vidjeti u domovima i nije se puno koristio van poslovnog dijela tržišta, većinom iz razloga što su oprema i uređaji za 802.11b standard bili jeftiniji.

[8] Koriste se stariji standardi poput 802.11a i 802.11b.

2.3.3. IEEE 802.11g

Ovaj standard pokušao je iskoristiti najbolje od postojećih karakteristika 802.11a i 802.11b standarda. Podržavao je maksimalnu teoretsku brzinu prijenosa od 54 Mbps, te koristi frekvenciju od 2.4 GHz. Koristio je istu tehnologiju ortogonalnog multipleksiranja podjelom frekvencije (engl. *Orthogonal Frequency Division Multiplexing* – OFDM) kao i 802.11a, ali s obzirom na to da koristi frekvenciju od 2.4 GHz, ima veći domet. Uređaji koji podržavaju 802.11g kompatibilni su s 802.11b uređajima, [12].

2.3.4. IEEE 802.11n

802.11n standard, poznat i kao Wi-Fi 4, učinio je Wi-Fi tehnologiju još bržom i pouzdanijom. Podržava maksimalnu teoretsku brzinu prijenosa od 300 Mbps odnosno 450 Mbps ako se koriste tri antene. Ovaj standard koristi tehnologiju višestrukih ulaza i višestrukih izlaza (engl. *Multiple Input Multiple Output* – MIMO), kod koje se koristi više prijemnika i odašiljača istovremeno u jednom uređaju, što omogućava vrlo velike brzine prijenosa bez povećavanja širine pojasa ili snage odašiljanja signala, [12].

2.3.5. IEEE 802.11ac

Ovaj standard, uveden i pod imenom Wi-Fi 5, učinio je iznimno velik skok kod brzina prijenosa. Teoretski su podržane brzine od 433 Mbps do čak nekoliko gigabita po sekundi. Kako bi se to ostvarilo, 802.11ac radi isključivo na frekvencijama od 5 GHz, podržava do 8 istovremenih prijenosa podataka po uređaju, za razliku od 4 prijenosa kod 802.11n, povećala se širina kanala na 80 MHz, te koristi tehnologiju zvanu *beamforming.* S *beamforming* tehnologijom antene prenose signal specifičnom uređaju, a ne kroz cijeli prostor oko sebe. Osim toga, 802.11ac koristi i višekorisničku MIMO tehnologiju (engl. *Multi-User Multiple Input Multiple Output* – MU-MIMO), koja može usmjeriti tokove odašiljanja signala i prema nekoliko uređaja istovremeno.

2.3.6. IEEE 802.11ax

IEEE 802.11ax, poznat i kao Wi-Fi 6, unio je nova poboljšanja, te povećao brzinu prijenosa do čak 9.6 Gbps. Najznačajnija poboljšanja su: umanjivanje zagušenja u mreži u javnom prostoru, bolja podrška korištenja spektra frekvencija od 2.4 GHz i 5 GHz, povećanje broja uređaja i tokova

signala kod MU-MIMO tehnologije, sa 4 uređaja i 4 toka na 8 uređaja i 8 tokova, te općenito bolje performanse mreže.

Danas je u razvoju i idući standard, 802.11be, koji će se nazivati i Wi-Fi 7, koji obećava još veće brzine prijenosa podataka, veći domet, još manje zagušenje u većim mrežama, podržavanje rada na više frekvencija odjednom, te još veću količinu podataka koji se mogu prenijeti signalom koristeći kvadraturnu amplitudnu modulaciju[9] (engl. *Quadrature Amplitude Modulation* – QAM) koristeći 4096-QAM[10] tehnologiju.

[9] Kod QAM modulacije se kombiniraju dva amplitudno modulirana signala u jedan kanal da bi se dobio jedinstven signal.

[10] Oblik QAM modulacije kod kojeg prijenosni signal može imati 4096 oblika.

3. Elementi sigurnosti Wi-Fi mreža

Wi-Fi mreže su s vremenom postale iznimno sigurne, s obzirom na to da su promijenile nekoliko sigurnosnih standarda koji se odnose na zaštitu i enkripciju mreže zaporkom. No bez obzira na to, i dalje postoje brojne prijetnje Wi-Fi mrežama, i to iz razloga što su bežične mreže upravo najranjivije jer je medij kojim podaci putuju zrak. Zbog toga je potrebno imati i ostale različite sigurnosne mehanizme koji osiguravaju bezbrižno i sigurno korištenje Wi-Fi mreža uz što manje rizika.

S obzirom na to da je kod Wi-Fi mreža prijenosni medij zrak, potrebno je imati sigurnosne mehanizme koji će osim zabrane pristupa uređajima koji nemaju ispravnu zaporku za pristup mreži, također regulirati promet mrežom i mogućnost spajanja uređaja. Neki od tih mehanizama su primjerice: filtriranje spojenih uređaja po fizičkoj adresi uređaja, odnosno adresi kontrole pristupa mediju (engl. *Media Access Control Address* – MAC adresa), statičko adresiranje po adresi Internet protokola, odnosno logičkoj adresi (engl. *Internet Protocol Address* – IP adresa), te sakrivanje identifikatora mreže, odnosno imena mreže (engl. *Service Set Identifier* – SSID).

Na Wi-Fi mrežu se, kao i na svaki informacijsko komunikacijski sustav, mogu primijeniti čimbenici informacijske sigurnosti. Prema [13], svaki od elemenata informacijsko-komunikacijskog sustava posjeduje određene ranjivosti koje mogu biti iskorištene u svrhu narušavanja njegove sigurnosti čime se paralelno narušava i sigurnost informacija koje se unutar sustava pohranjuju, obrađuju ili prenose. Upravo iz tog razloga potrebno je obratiti pozornost na čimbenike, odnosno elemente informacijske sigurnosti koje je nužno promatrati, analizirati i njima upravljati kako bi se optimizirala razina sigurnosti sustava i informacija.

Osim navedenog, svaka mreža, pa tako i Wi-Fi mreža, ima određene zahtjeve odnosno načela ili etiku što se tiče sigurnosti mreže. Ti zahtjevi su također i načela informacijske sigurnosti i svakog informacijsko komunikacijskog sustava.

Prema [13], ta su načela obuhvaćena terminom CIA model (engl. *Confidentiality, Integrity, Availability* – CIA), u koji spadaju povjerljivost, cjelovitost i dostupnost:

- Povjerljivost: osobina sustava koja osigurava otkrivanje informacija i podataka isključivo autoriziranim osobama, entitetima i procesima, u definirano vrijeme i definiranom procedurom.
- Cjelovitost: podrazumijeva zaštitu informacija od namjerne ili slučajne neovlaštene modifikacije uzrokovane ljudskim utjecajem ili pogreške u radu sustava.
- Dostupnost: odnosi se na raspoloživost tražene informacije ovlaštenim korisnicima u danom trenutku i prema zadanim uvjetima, što uključuje uvjete povjerljivosti i integriteta. Ukoliko ti uvjeti nisu ispunjeni tada primarna funkcija sustava gubi značaj, odnosno nije u mogućnosti ispuniti zahtjeve postavljene od krajnjih korisnika.

Uz navedeno, često se primjenjuje i termin AAA (engl. *Authentication, Authorization, Audit* – AAA), koji označava autentikaciju, autorizaciju i reviziju tj. nadzor:

- Autentikacija: sigurnosni mehanizam koji osigurava legitimitet osobe. Jedan od primjera autentikacije je zaporka koju samo legitimni korisnik poznaje.
- Autorizacija: nakon što korisnik pruži informacije nužne za autentikaciju dodjeljuje mu se autorizacija, odnosno prava pristupa.
- Revizija: proces evaluacije učinkovitosti provedenih sigurnosnih mehanizama. Često se u tu svrhu koristi, kao jedna od metoda, penetracijsko testiranje. Proces penetracijskog testiranja obuhvaća aktivnu i detaljnu analizu informacijsko komunikacijskih sustava s ciljem otkrivanja sigurnosti propusta i ranjivosti u dizajnu, implementaciji ili održavanju. Otkriveni propusti se dokumentiraju i navode u izvještaju uz vjerojatnost iskorištavanja otkrivenih nedostataka i moguće posljedice te podrazumijevaju pružanje smjernica za smanjenje utvrđenog rizika.

3.1. Sigurnosne prijetnje Wi-Fi mrežama

Korisnici Wi-Fi mreža su pod sigurnosnim rizikom već samim time što koriste Wi-Fi mreže koje su često nesigurne i nezaštićene, a osim toga se taj sigurnosni rizik još više povećava zbog toga što također koriste mobilnu tehnologiju za pristup *online* bankovnim transakcijama, ali i drugim osjetljivim aktivnostima. Nedavna globalna zdravstvena kriza[11] je pomogla istaknuti važnost sigurnosti Wi-Fi mreža, jer su mnoge tvrtke morale omogućiti svojim zaposlenicima rad od kuće. Međutim kućne Wi-Fi mreže koje su neadekvatno zaštićene mogu biti prijetnja sigurnosti poslovne mreže te tvrtke, [14].

Također, masovno širenje javnih Wi-Fi mreža uzrokuje daljnje širenje sigurnosnih problema individualnim korisnicima, ali i tvrtkama. Takve mreže su po definiciji otvorene, i prema tome nezaštićene. Pristupanjem otvorenim javnim Wi-Fi mrežama korisnici su izloženi *malwareu, spywareu* i ostalim nepoželjnim aktivnostima. Osim navedenog, neki od čestih vrsta napada su lažiranje IP adrese, poznato i kao IP *spoofing*, kojim se izvode druge vrste napada poput napada uskraćivanjem resursa[12] (engl. *Denial of Service* – DoS) te *man in the middle* napadi, zatim lažiranje fizičkih adresa, odnosno MAC adresa uređaja, te takozvani *piggybacking*[13] i *wardriving*[14] napadi, [14].

Lažne pristupne točke su pristupne točke koje su dodane u nečiju mrežu bez znanja vlasnika mreže. Preko takve pristupne točke može se omogućiti upad u mrežu bilo kome tko je u fizičkoj blizini te pristupne točke, koju kontrolira zlonamjerna osoba. Na taj način mogu se izvoditi MITM napadi, poplaviti mrežu beskorisnim informacijama, uzrokujući DoS napade, ili primjerice odašiljati lažan SSID mreže te predstavljati atraktivne mogućnosti poput besplatne veze s Internetom. Jednom kad se korisnik poveže na lažni AP, on i sam nastavlja dalje odašiljati lažni SSID mreže, inficirajući i druge klijente koji se spajaju na mrežu, [15].

[11] Kriza potaknuta COVID-19 virusom 2019. godine.
[12] Napad kod kojeg se preopterećuje server do granice gdje više ne može pružati uslugu te se usluga ugasi.
[13] Napad u kojem haker dobiva pristup mreži u intervalima neaktivnosti konekcije legitimnog korisnika mreže.
[14] Kod *wardriving* napada haker pronalazi ranjive mreže krećući se područjem u nekom vozilu.

Također postoje i takozvani *man in the middle* napadi. Ova vrsta napada se bazira na prisluškivanju i modificiranju informacija između dvije strane bez njihovog znanja. Napadač postaje čovjek u sredini, te se pretvara istovremeno da je i korisnik i aplikacija s kojom korisnik komunicira, u namjeri da ukrade povjerljive podatke. Tijekom tog vremena korisnik misli da komunicira s aplikacijom, ne znajući što se zapravo događa, [16].

Napadi uskraćivanjem resursa, poznati i kao DoS napadi, događaju se kad napadač preplavi Wi-Fi mrežu podacima, odnosno prometom, tako da mreža više ne može posluživati korisnike. Napadač šalje velik broj zahtjeva centralnom serveru odnosno usmjerivaču, te ga tako preopteretі prometom. Ti zahtjevi za uslugom nisu legitimni i imaju lažne povratne adrese, tako da se usmjerivač, odnosno poslužitelj usluge zavara i ne može autenticirati pošiljatelja zahtjeva. Kako se ti lažni zahtjevi konstantno obrađuju, mreža postaje zagušena i više ne može posluživati legitimne korisnike mreže.

Osim ovih, također se koriste i distribuirani DOS napadi (engl. *Distributed Denial of Service* – DDoS), koji koriste veći broj uređaja s kojih se napada mreža. DDoS napadači obično koriste takozvani *botnet* – grupu uređaja povezanih na Internet, koji su na neki način oteti, te njihovi vlasnici ni ne znaju da se njihov uređaj koristi za slanje lažnih zahtjeva u pozadini, kako bi doprinijeli DDoS napadu. DDoS, u usporedbi s običnim DoS napadima, omogućuju slanje eksponencijalno većeg broja poslanih zahtjeva u mrežu koja se napada, te se time povećava snaga napada, kojim se tada mogu napadati i mnogo veće mreže. Pogotovo je rizično današnje vrijeme, kada postoji iznimno velik broj uređaja interneta stvari (engl. *Internet of Things* – IoT) koji se mogu oteti i iskoristiti za *botnet* mreže[15] i DDoS napade, [17].

Vrsta napada poznata kao *piggybanking* je relativno bezopasna za mrežu u usporedbi s ostalim napadima, ali i dalje se njime mreža pojačano izlaže sigurnosnim rizicima. To je napad kod kojeg se korisnik spaja na Wi-Fi mrežu s ciljem da ostvari vezu s Internetom, bez znanja ili pristanka vlasnika mreže. To se obično radi kako bi korisnik uštedio, ne plaćajući pristup Internetu, već

[15] Mreža računala nad kojima napadač ima djelomičnu kontrolu tako što na njih instalira aplikaciju koja obavlja zadatak koji mu je potreban

iskorištavajući tuđu mrežu za spajanje. Većinom ovakve napade ne izvode hakeri, već obične osobe koje jednostavno žele iskoristiti Wi-Fi u blizini za besplatan pristup Internetu.

Wardriving napad je aktivnost kojom se traže javno dostupne Wi-Fi mreže, obično iz nekog vozila, koristeći se prijenosnim računalom ili pametnim telefonom. Softver koji se koristi za *wardriving* je besplatno dostupan na Internetu. Na najbazičnijoj razini, *wardriving* je ono što svaki pametni telefon radi kad se uključi Wi-Fi povezivost: prikazuje sve dostupne Wi-Fi mreže u blizini te ih konstantno skenira u potrazi za novima. Ova vrsta napada također nije sama po sebi štetna za mreže niti se samim *wardriving* postupkom može napasti mreža, ali je alat koji koriste hakeri kako bi izveli druge oblike napada, te se zbog toga smatra relativno nepoželjnim postupkom, te spada u sivu zonu, [18].

Napad lažiranjem MAC adrese, poznat i kao MAC *spoofing*, najčešće se koristi kako bi se izbjegla zaštita nekih mreža koja filtrira uređaje prema MAC adresi, te prema tome zabranjuje određenim MAC adresama da se spajaju na mrežu. Tada napadač koristi ovu tehniku kako bi lažno predstavio MAC adresu svog uređaja, zavarao mrežu da se na nju spaja neki drugi uređaj koji nije zabranjen, te nakon upada u mrežu nastavio s napadom.

3.2. Zaštita i enkripcija mreža

Najviše fokusa kod sigurnosti Wi-Fi mreža se dalo sigurnosnom mehanizmu zaštite mreže putem zaporke koja se mora unijeti u uređaj prilikom spajanja na mrežu. Taj način zaštite je s vremenom najviše evoluirao, te je trenutno aktualna četvrta po redu verzija tog zaštitnog protokola. Protokole za zaštitu je razvijala *Wi-Fi Alliance* organizacija, čiji glavni zadatak je promovirati bežične tehnologije i interoperabilnost. Organizacija je predstavila prvi protokol kasnih devedesetih godina, a otad su protokoli poboljšavani sve snažnijom enkripcijom.

3.2.1. WEP

Prvi protokol, zvan WEP (engl. *Wired Equivalent Privacy*), je bio standardna metoda zaštite mreže od kasnih devedesetih do 2004. godine. S obzirom na to da se kod Wi-Fi mreža podaci prenose radiovalovima, relativno je lako presresti komunikaciju ako se ne koristi nikakva zaštita. 1997. je zato stvoren WEP protokol, čiji je cilj bio kriptirati podatke koji se prenose, tako da oni

koji presretnu podatke između dva uređaja ne mogu pročitati ništa, dok svi uređaji koji su autorizirani u mreži mogu prepoznati i dekriptirati podatke. Svi uređaji na mreži su koristili isti enkripcijski algoritam.

WEP koristi 64 ili 128 bitnu enkripciju, te su svi podaci, bez obzira na uređaj, koristili isti enkripcijski ključ.

Jedan od glavnih ciljeva WEP protokola bio je spriječiti MITM napade, što je i činio neko vrijeme. No unatoč izmjenama protokola i povećanoj duljini ključa, s vremenom su otkrivene mnoge mane, a zahvaljujući povećanju računalne snage, postalo je još lakše iskoristiti te mane. Danas se WEP se više ne smatra sigurnim protokolom te se smatra kako bi obavezno trebao biti zamijenjen novijim verzijama. No bez obzira na to, još uvijek se ponegdje koristi, većinom zato što mrežni administratori odnosno vlasnici mreža ne promijene tvorničke postavke sigurnosti usmjerivača ili u slučajevima kad su uređaji previše stari da bi podržavali novije sigurnosne protokole, [19].

3.2.2. WPA

WPA (engl. *Wi-Fi Protected Access*) uveden je 2003. godine. Dijeli neke sličnosti sa WEP protokolom, ali uvedena su poboljšanja fokusirana na rukovanje sigurnosnim ključevima i načinom na koji se korisnici autoriziraju u mreži. Dok je WEP davao svakom autoriziranom uređaju isti ključ za enkripciju, WPA koristi protokol TKIP (engl. *Temporal Key Integrity Protocol*), koji dinamički mijenja ključ koji uređaji koriste. To sprječava napadače da stvore vlastiti sigurnosni ključ koji odgovara onome kojeg koristi i mreža. TKIP standard je kasnije zamijenjen AES (engl. *Advanced Encryption Standard*) standardom.

Osim toga, WPA uključuje i provjere integriteta poruka kako bi otkrio je li napadač uhvatio ili izmijenio pakete koji se prenose. Enkripcijski ključevi su 256 bitni, što je znatno povećanje u odnosu na 64 i 128 bitne kod WEP-a. No opet su otkrivene mane i ovog sigurnosnog standarda, unatoč svim poboljšanjima, te je razvijen idući standard – WPA2, [19].

3.2.3. WPA2

WPA2, druga verzija WPA protokola, je razvijen 2004. Baziran je na RSN (engl. *Robust Security Network*) mehanizmu, te ima dva načina rada:

- Privatni način odnosno unaprijed dijeljeni ključ (engl. *WPA2 Pre-shared Key* – WPA2-PSK): oslanja se na dijeljeni ključ za pristup, te se obično koristi u kućnom okruženju.
- Poslovni način, takozvani *enterprise mode* (engl. *WPA2 Enterprise Mode* – WPA2-EAP): kao što mu i ime govori, prikladniji je za poslovne mreže.

Oba načina koriste CCMP protokol (engl. *Counter Mode Cipher Block Chaining Message Authentication Code Protocol* – CCMP). Taj protokol se bazira na AES algoritmu, koji omogućuje verifikaciju autentičnosti i integriteta poruka.

No unatoč svemu, i WPA2 ima određene mane. Na primjer, osjetljiv je na napade reinstalacije ključa (engl. *Key Reinstallation Attacks* – KRACK). KRACK napadi iskorištavaju slabost WPA2 koja dopušta napadaču da se pretvore u klon mreže koju napadaju, te prisile žrtvin uređaj da se spoji na tu kloniranu, zlonamjernu mrežu koju su stvorili. To omogućava napadaču da dekriptira mali komadić podataka koji se može iskoristiti da se probije enkripcijski ključ. No ipak se uređaji mogu ažurirati zakrpom koja onemogućava iskorištavanje te slabosti, te se WPA2 i dalje smatra mnogo sigurnijim od WEP ili WPA protokola, [19].

3.2.4. WPA3

WPA3, trenutna verzija WPA protokola, dizajniran je s namjerom da uvede još jednostavniju konfiguraciju i još jaču enkripciju od svih prethodnika. Stvoren je 2018. godine, te uvodi nove mogućnosti i za privatne i za poslovne korisnike. Prema [19], to su:

- Individualizirana enkripcija podataka: kad se korisnik prijavi na mrežu, WPA3 prijavi uređaj kroz proces drukčiji od ranijeg dijeljenja lozinke, odnosno ključa. Koristi se Wi-Fi protokol opskrbe uređaja (engl. *Device Provisioning Protocol* – DPP), koji omogućava korisnicima da koriste NFC tehnologiju (engl. *Near Field Communication*) ili QR (engl. *Quick Response*) kodove kako bi se prijavili na mrežu.

- Protokol simultane autentikacije: koristi se za kreiranje sigurnog rukovanja, takozvanog *handshakea* uređaja, kod kojeg se terminalni uređaj spaja na bežičnu pristupnu točku te zatim oba uređaja komuniciraju kako bi verificirali autentikaciju i konekciju. Čak i ako je korisnička zaporka slaba, WPA3 ima sigurniji *handshake* zbog Wi-Fi DPP protokola.
- Snažnija zaštita protiv *brute-force* napada: WPA3 štiti protiv *offline* pogađanja lozinke omogućavajući korisniku samo jedan pokušaj upisivanja lozinke, čime se prisiljava korisnika da komunicira direktno s Wi-Fi uređajem, što znači da mora biti fizički prisutan svaki put kad upisuje lozinku. Za razliku od WPA3, WPA2 nema ugrađene metode za enkripciju i privatnost kod javnih otvorenih mreža, što znači da su kod takvih mreža *brute-force* napadi značajna prijetnja.

WPA3 je postao široko rasprostranjen 2019. te je kompatibilan s uređajima koji koriste WPA2 protokol, [19].

3.3. Rješenja za zaštitu od sigurnosnih prijetnji

Sve navedene sigurnosne prijetnje mogu se uvelike umanjiti već i sigurnim ponašanjem prilikom korištenja Wi-Fi mreža. Uz to, postoje i brojna druga rješenja i postupci koji se mogu poduzeti kako bi se uvelike povećala zaštita i sigurnost korištenja Wi-Fi mreža, te umanjila mogućnost napada na mrežu. Prema [20], ta rješenja su sljedeća:

- Enkripcija
- Zaštita bežične pristupne točke
- Minimiziranje rizika za DoS napad
- Tehnike skrivanja signala
- Sigurno korištenje Wi-Fi mreža i
- Tehnike mekog računalstva.

Osim navedenog, prema [14], kućni korisnici mogu također unaprijediti sigurnost svojih Wi-Fi mreža sljedećim rješenjima:

- Filtriranje prema MAC adresama
- Virtualne privatne mreže (engl. *Virtual Private Networks* – VPN) i
- Sigurnosni softver.

3.3.1. Enkripcija

Moguće je koristiti različite metode enkripcije Wi-Fi komunikacije, te je to jedan od najsigurnijih načina za zaštitu podataka koji se prenose mrežom. Osim toga, važno je koristiti i simetrične, ali i asimetrične metode enkripcije.

3.3.2. Zaštita bežične pristupne točke

Veliku ulogu kod upada u bežičnu mrežu igraju nezaštićene pristupne točke. Kako bi se oduprlo napadima, važno je ukloniti lažne pristupne točke, te tvorničku konfiguraciju usmjerivača ili pristupne točke ažurirati kako bi spajanje na mrežu bilo sigurno.

3.3.3. Minimiziranje rizika za DoS napad

Problematična područja mreže se mogu otkriti kroz rutinske preglede bežične mreže. Uklanjanje problematičnih uređaja u većim mrežama može umanjiti rizik od događanja DoS napada.

3.3.4. Tehnike skrivanja signala

S obzirom na to da napadači moraju prvo otkriti, locirati i identificirati Wi-Fi mrežu da bi ju napali, dobar dio napada se može jednostavno izbjeći na način da se ne odašilje SSID mreže. Pristupna točka konstantno šalje SSID *broadcast* signalom svim uređajima u blizini. Ako se to odašiljanje SSID-a isključi ako nije potrebno odnosno ako se mreža ne koristi, to će također povećati sigurnost mreže.

3.3.5. Sigurno korištenje Wi-Fi mreža

Dobar dio napada na mrežu se također može izbjeći tako da se korisnici jednostavno ne ponašaju rizično. To uključuje korištenje tehnologije vatrozida, tehnike enkripcije podataka, te izbjegavanje pristupanja javnim Wi-Fi mrežama, koje su često nesigurne.

3.3.6. Tehnike mekog računalstva

Meko računalstvo je relativno nova grana računalstva, kod koje se koristi takozvana *fuzzy* logika, strojno učenje, neuronske mreže i slične tehnike. Takvi načini korištenja računala donose sasvim nova rješenja koja se ne mogu postići korištenjem tradicionalnih programskih rješenja, koja uvijek daju egzaktne i jedinstvene rezultate. Prema [20], to su:

- Neuronske mreže: programski sustavi inspirirani pravim mrežama neurona u mozgu, koji mogu biti mnogo efikasniji u nekim zadaćama, pa čak i riješiti neke probleme odnosno zadaće koje tradicionalni računalni sustavi i programi ne mogu riješiti. Kod Wi-Fi mreža oni također mogu pomoći kod unaprjeđenja zaštite mreže.
- *Fuzzy* logika: sustav baziran na pravilima i odlukama drukčijima nego kod standardne logike kako bi se efikasno riješili neki problemi koji se ne mogu riješiti tradicionalnom računalnom logikom, koja je jednoznačna i samim time ograničena u nekim specifičnim situacijama.
- Genetski algoritmi: posebna vrsta računalnog algoritma koja ima određena biološka obilježja učenja. Drugim riječima, takvi algoritmi su inspirirani samom evolucijom i genima, pa tako dolaze do rješenja određenom vrstom prirodne selekcije te pomoću takve selekcije odlučuju i dolaze do rješenja.

3.3.7. Filtriranje prema MAC adresama

Filtriranje uređaja koji se mogu spojiti na mrežu prema MAC adresama je relativno efikasna zaštita protiv neželjenih i zlonamjernih spajanja na mrežu. Iako se može zaobići tehnikama MAC *spoofinga*, i dalje donosi određenu dozu zaštite u mrežu.

3.3.8. VPN mreže

Virtualne privatne mreže omogućavaju korisnicima stvoriti sigurne tunele između nezaštićene Wi-Fi mreže i Interneta, te također mogu kriptirati komunikaciju, sakriti IP adresu korisnika, te zaštititi identitet korisnika.

3.3.9. Sigurnosni softver

Korištenje različitog sigurnosnog softvera omogućava daljnju zaštitu Wi-Fi mreže. Korištenjem vatrozida, antivirusnih programa, različitih filtera na ulazu u mrežu i sličnih metoda, uvelike se poboljšava sigurnost mreže jer se velik dio rizičnih i sumnjivih upada i podataka uklanja na ulazu u mrežu.

4. Primjena i razvoj javnih i privatnih Wi-Fi mreža

Wi-Fi je u potpunosti promijenio svijet i to na nekoliko različitih načina. Dolaskom Interneta, čovječanstvo je postalo mnogo povezanije, tok informacija se eksponencijalno povećao, kao i količina informacija dostupnih prosječnom čovjeku. No dolaskom Wi-Fi tehnologije, sve se još jednom promijenilo i promjene su se ubrzale, upravo zbog mogućnosti bežičnog spajanja na Internet.

4.1. Povijesni razvoj Wi-Fi mreža

Pojavom IEEE 802.11 standarda krajem devedesetih godina prošloga stoljeća, način spajanja na kućnu mrežu koja omogućuje pristup Internetu uvelike se olakšao. Osim olakšanog spajanja na kućnu mrežu a time i na Internet, kućni korisnici su postali i mobilniji unutar vlastitog doma pojavom prijenosnih računala s mogućnošću spajanja na Wi-Fi mrežu, pa tako mjesto za spajanje na Internet nije bila samo radna soba ili radni stol sa računalom, već i dnevna soba, kuhinja te sva ostala mjesta u domu.

Već vrlo brzo nakon pojave same Wi-Fi tehnologije, operatori diljem svijeta počeli su nuditi i Wi-Fi povezivost uz klasični kabelski Internet, [21]. S obzirom na pojavu novih uređaja, dlanovnika, drugim nazivom digitalnih osobnih pomagača[16] (engl. *Personal Digital Assistant* – PDA) otprilike u isto vrijeme, postalo je jasno da se sprema nova revolucija, koja će ubrzano proširiti i olakšati širenje Interneta diljem svijeta. Prema [22], već 1999. godine Wi-Fi je postao dostupan kućnim korisnicima zbog tvrtke Apple, koja je omogućila Wi-Fi povezivost na svojim iBook[17] uređajima. Ostali proizvođači su, naravno, slijedili njihov primjer. Do 2000. godine već se više korisnika zapadnog svijeta povezivalo na Internet putem bežičnih tehnologija, odnosno Wi-Fi-ja, nego putem analognih tehnologija. Daljnjim ubrzanim razvojem došlo se do toga da je 2010. godine u svijetu postojalo već preko milijun Wi-Fi mreža.

[16] Preteča pametnog telefona, uređaj zamišljen kao svojevrsni organizator.
[17] Linija prijenosnih računala tvrtke Apple.

Ubrzo nakon pojave same Wi-Fi tehnologije, došlo je i do pojave javnih Wi-Fi mreža. Oduvijek su javne ustanove poput knjižnica i škola bile mjesto na kojem se prvo u gradu moglo doći do novih tehnologija, još od pojave telefona, televizije, pa tako i Interneta. Prateći taj razvitak, ubrzo je Internet zavladao knjižnicama, a preko njih se prelio i u novu vrstu kafića – takozvani Internet cafe. Na ovakvim mjestima ljudi su mogli popiti kavu ili bilo koje drugo piće, ali uz to dobiti i besplatni pristup Internetu. U početku je to bila žičana veza, ali nakon toga, dolaskom Wi-Fi mreža, Internet cafe je postao sinonim za mjesto sa besplatnom Wi-Fi vezom, gdje se moglo doći sa vlastitim računalom i spojiti na Internet. Prema [23], jedno od prvih takvih mjesta u svijetu nastalo je u Mađarskoj devedesetih godina prošloga stoljeća, gdje je privatna grupa ljudi osnovala takve pionirske ustanove pod nazivom *Telehaus,* ili tele-kuće u nekoliko gradova. Ta ideja je postala tako popularna da su je odmah prigrlile susjedne države i ostatak svijeta. Nakon toga, 2000ih godina, slični programi su uvedeni u mnoge zemlje u razvoju kako bi se pristup Internetu lakše uveo u stanovništvo. Kroz takve ustanove su stanovnici tih zemalja mogli imati pristup Internetu u ogromnom broju javnih ustanova, kao što su poštanski uredi, knjižnice, državni uredi i škole.

U današnje vrijeme, život bez javnih Wi-Fi mreža postao je gotovo nezamisliv. Prema [24], u SAD-u je 1998. pušten u rad MobileStarov sustav prvih Wi-Fi pristupnih točaka u zračnim lukama i hotelima, 2017. je ukupan broj javnih Wi-Fi mreža u SAD-u dostigao 25.7 milijuna, a ove godine, 2022., ukupan broj Wi-Fi pristupnih točaka će doseći čak 77 milijuna. Diljem svijeta gotovo svi kafići i restorani nude besplatne Wi-Fi mreže na koje se gosti mogu povezati, busovi i vlakovi također nude besplatni pristup Wi-Fi mreži te Internetu, pa čak i cijeli gradovi imaju sustav besplatno dostupne Wi-Fi povezivosti s Internetom u centru grada, na svim javnim površinama. Jasno je da je Wi-Fi postao jednako važna tehnologija kao i sam Internet.

4.2. Primjena Wi-Fi mreža u javnoj i privatnoj sferi

Wi-Fi mreže su prvenstveno nastale kao bežični oblik lokalnih računalnih mreža, te su time postale novi oblik pristupa Internetu. Zbog toga u prvo vrijeme nije bilo druge primjene Wi-Fi tehnologije osim čistog povezivanja računala te povezivanja računala i lokalnih mreža na Internet. Međutim, već u samoj srži primjene Wi-Fi tehnologije se krije moć bežičnog povezivanja, pa se

tako Wi-Fi u privatnoj sferi, dakle u kućnom korištenju, koristi na nebrojeno mnogo načina, te osim pukog spajanja uređaja na Internet i međusobno, koristi se za svrhe poput bežičnog udaljenog ispisa, *streaming* video i audio datoteka kroz kućnu mrežu, primjerice sa računala na televizor, pa i sinkroniziranja notifikacija između pametnog telefona i računala, tako da je moguće istovremeno primiti notifikacije sa *smartphonea* na računalu. Osim navedenog, dolaskom IoT koncepta, došao je na svijet velik broj kućanskih uređaja s mogućnošću povezivanja na Wi-Fi, pa se tako perilice rublja, klima uređaji, mikrovalne pećnice i ostali uređaji mogu kontrolirati na daljinu, preko Interneta.

Već i ove kućne primjene Wi-Fi tehnologije daju za pretpostaviti da će u javnoj sferi te primjene biti još raznolikije, a pogotovo u poslovnom svijetu i industrijske svrhe, gdje je moguće uvelike olakšati posao i smanjiti određene troškove upravo korištenjem Wi-Fi mreža. Osim skladišta, gdje se mnogi uređaji, od senzora do viličara, mogu povezati međusobno putem Wi-Fi mreže, i na cesti odnosno u prometu je moguće uvelike iskoristiti dobrobiti te tehnologije i povezivanjem automobila međusobno uvećati sigurnost cestovnog prometa.

Također, postoje i razna istraživanja koja eksperimentiraju s nekonvencionalnim primjenama Wi-Fi tehnologije. Primjerice, u istraživanju od Wei Wanga, Alex X. Liua, te Muhammada Shahzada [25], Wi-Fi tehnologija i njeni signali koji su ionako već svuda oko nas koriste se za prepoznavanje čovjekovog hoda. U istraživanju se koriste komercijalni Wi-Fi uređaji da bi se pomoću njih prepoznali određeni uzorci u hodu koji se mogu iskoristiti za prepoznavanje određene osobe. Temelji se na tome da se zbog razlika u hodu ljudi Wi-Fi signal reflektira od čovjeka na različite načine, što se može prepoznati na Wi-Fi prijemniku. Kako bi se profilirao način hoda ljudi, koristilo se procesiranje signala da bi se generirali spektrogrami koji su slični onima koji su generirani od strane specifično dizajniranih Doppler radara. Nadalje, da bi se ekstrahirale značajke iz spektrograma koje najbolje prikazuju uzorke hodanja, koristila se auto korelacija refleksije signala s torza da bi se eliminirale nesavršenosti iz spektrograma.

Iz svega navedenog može se zaključiti da Wi-Fi ima iznimno mnogo primjena, kako u privatne i kućne, tako i u javne i poslovne svrhe, te da se stalno otkrivaju i nove svrhe u koje se Wi-Fi tehnologija može iskoristiti, poput gore navedenog istraživanja.

5. Pregled postojećih istraživanja iz područja sigurnosti Wi-Fi mreža u javnom okruženju

Postoje mnoga istraživanja koja se bave sa sigurnošću i sigurnosnim rizicima Wi-Fi mreža. Između ostalih, tu su i ona koja se specifično bave skeniranjem Wi-Fi mreža i tehnikom *wardrivinga* kako bi se saznalo koliko su Wi-Fi mreže na nekom području sigurne, te također i neka koja pomoću ankete ispituju svjesnost korisnika o sigurnosnim rizicima Wi-Fi mreža. Zadnjih godina naglo je porastao broj takvih istraživanja, prvenstveno iz razloga što su Wi-Fi mreže postale iznimno rasprostranjene, te su praktički neizostavni dio današnjeg svijeta. Neka od njih su navedena u nastavku.

U istraživanju [26] koristi se *wardriving* tehnika kako bi se istražila sigurnost Wi-Fi mreža u gradu Varna u Bugarskoj. Za skeniranje Wi-Fi mreža u gradu korišten je uređaj kućne izrade baziran na računalu Raspberry Pi 3 Model B, uz to GPS uređaj Holux M-1200E kako bi se putem bilježila točna pozicija, te Wi-Fi modul CanaKit. Wi-Fi mreže su skenirane pomoću Kismet programskog alata te su dobiveni podaci procesirani i analizirani u Microsoft Excelu. Na uzorku od 19136 mreža, analizirani su podaci poput korištene Wi-Fi enkripcije u mreži, najčešće korištenih SSID imena mreže i slično. Dobiveni podaci su uspoređeni i s podacima ranijeg istraživanja na istom području. Zaključeno je da se u deset godina broj Wi-Fi mreža povećao 16 puta, sigurnost mreža se povećala jer se puno više počela koristiti enkripcija i to u korist WPA2, a nauštrb WPA i WEP enkripcije. U tih deset godina sigurnost Wi-Fi mreža u gradu se uvelike povećala, ali zabrinjavajuće je to što je puno veći broj mreža počeo koristiti WPS funkciju usmjerivača, što znači da im to uvelike narušava sigurnost dobivenu zbog WPA2 enkripcije. Također, nije dobro što 13.3 % mreža koristi tvornički SSID, što znači da one koriste i tvornički postavljenu lozinku koja ima tek minimum dužine potrebne za izbjegavanje napada koji koriste rječnike lozinki. Dane su sljedeće preporuke, [26]:

1. Povećati svjesnost korisnika o sigurnosnim problemima i efektima koje imaju.
2. Koristiti isključivo WPA2 enkripciju.
3. Isključiti WPS funkciju na svim uređajima.

4. Koristiti lozinku od barem 12 znakova sa velikim i malim slovima te brojevima.
5. Ažurirati *firmware* usmjerivača na posljednju verziju ili koristiti alternativni *firmware* poput OpenWRT/DD-WRT.

U studiji *Practicing safe public Wi-Fi - Assessing and managing data-security risks*, autora Mark A. Gregory, Ian McShane i Chris Wilson, izrađeno je istraživanje pomoću online ankete, u kojem su ispitani korištenje javnih Wi-Fi mreža te percepcija korisnika o sigurnosti javnih Wi-Fi mreža. Kroz anketu je otkriveno da je preko pola australske populacije koristilo javnu Wi-Fi mrežu u razdoblju od tri mjeseca prije ankete. Uz to, pažnja je dana na dva specifična rizika, [27]:

1. Gotovo svaki peti korisnik javne Wi-Fi mreže je bio izložen značajnom riziku prilikom obavljanja novčane transakcije bez poduzimanja ikakve mjere opreza.
2. Svaki sedmi korisnik javne Wi-Fi mreže obavlja aktivnosti vezane za posao na nesigurnim Wi-Fi mrežama, što izlaže organizacije i tvrtke značajnom riziku.

Usprkos takvim rezultatima, tvrdi se da su prema drugim istraživanjima korisnici voljni promijeniti navike ako u potpunosti razumiju sigurnosne rizike kojima se izlažu. Prema tome, dane su tri preporuke na razini cijelog sustava države za poboljšanje sigurnosti korištenja javnih Wi-Fi mreža, [27]:

1. Australske vladine organizacije za komunikacije bi trebale pojasniti zahtjeve za licenciranje i odgovornosti koje se odnose na pružatelje javnih Wi-Fi mreža. Neizvjesnost u ovom području postaje sve problematičnija kako se povećava broj Wi-Fi mreža i kako se one nastavljaju integrirati s reguliranim mobilnim mrežnim uslugama kroz *handover* mehanizme.
2. Davatelji javnih Wi-Fi usluga bi trebali zauzeti stav „prvo educiraj“ u svojim uvjetima korištenja. Neki uvjeti korištenja koji reguliraju javni Wi-Fi trebaju reviziju u oblik koji je bliži i intuitivniji korisnicima. Trenutačni obrambeni pristup fokusiran na sigurnost velikih korporacija ima vrlo malo edukativne vrijednosti te u konačnici dovodi u pitanje opravdanost pružanja javne Wi-Fi mreže.

3. Vladina, industrijska i potrošačka tijela u tom području trebaju razmisliti o uvođenju kampanje za povećanje sigurnosti javnih Wi-Fi mreža. Ostala literatura također ukazuje na učinkovitost dobro ciljanih kampanja podizanja svijesti, posebno pri postizanju široke svijesti o problemu i utjecanju na rizično ponašanje.

Autori Aini Zuriyati Abdul Kadir, Muriati Muda i Akhyari bin Nasir u svom istraživanju *A study of security awareness in using wireless networks* [28] otkrili su da je promet koji su stvarali studenti na javnoj Wi-Fi mreži fakulteta u Kemamanu u Maleziji činio većinu Internet prometa za web surfanje. Uz to, studenti su većinom koristili laptope s bežičnom Wi-Fi vezom kao primarno računalo. Iako su web protokoli činili većinu prometa na mreži, promet koji je vezan za sigurnosne kopije i dijeljenje datoteka je činio neobično velik dio ukupnog prometa na mreži. Zato je provedeno istraživanje na 200 studenata kako bi se saznalo kakve radnje studenti obavljaju na Internetu na koji se spajaju putem Wi-Fi mreže.

Na temelju dobivenih podataka, saznalo se da se 82.8 % korisnika spaja na Internet putem javne Wi-Fi mreže. No korisnici nisu svjesni koliko je za njih važno da znaju sigurnosne rizike koji prijete na javnim Wi-Fi mrežama. Prema istraživanju, veći dio korisnika se osjeća neutralno što se tiče zabrinutosti o računalnoj sigurnosti, a isto tako su neutralni u vezi zabrinutosti o sigurnosti Wi-Fi mreža. Navedeni rezultati u vezi svjesnosti o računalnoj sigurnosti i sigurnosti Wi-Fi mreža su vidljivi u tablici 3.

Tablica 3. Svjesnost korisnika o sigurnosti pri korištenju računala i Wi-Fi mreža [28]

Pitanje	Jako	Ponekad	Neutralno	Donekle	Malo
Sveukupna zabrinutost zbog računalne sigurnosti	17.3%	35.2%	42.9%	2.6%	2.0%
Sveukupno znanje o sigurnosti korištenja Wi-Fi mreža	17.9%	33.3%	41.5%	5.1%	2.1%

Nakon provedenog istraživanja, zaključeno je da bi se korisnici trebali educirati kroz edukativni program kako bi se povećala njihova svjesnost o rizicima koji prijete pri korištenju

javnih Wi-Fi mreža. Njihov trenutačni pristup kod kojeg nema zabrinutosti oko sigurnosti na Wi-Fi mrežama može biti problematičan u budućnosti, te je prema tome nužno pojačati edukaciju korisnika.

Nadalje, u istraživanju autora R. Sridaran, *Wireless Local Area Networks: Threats and Their Discovery Using WLANs Scanning Tools* [xy], nabrojani su neki od programskih alata za Wi-Fi mreže koji se mogu koristiti za skeniranje mreža, ali i za hakiranje i dohvaćanje raznih podataka od WLAN mreže. To su alati poput NetStumblera, inSSIDera, NetMona, AirPcapa, KisMeta i drugih. Alati su podijeljeni na aktivne, koji šalju ciljane pakete sa zahtjevom za uslugom ili *broadcast* pakete, te pasivne, koji analiziraju pakete koji su već poslani u mreži kako bi se moglo zaključiti koji klijenti komuniciraju sa kojim AP-om. Koristeći te alate, analizirale su se njihove mogućnosti hakiranja te iskorištavanja propusta u mrežama, kao i na koje se sve načine općenito mogu koristiti pri analiziranju WLAN mreža.

Zaključeno je da su WLAN mreže najrasprostranjenija tehnologija u svijetu koja je sklona brojnim vrstama napada, te je vrlo osjetljiva na hakerske prijetnje. Razni aktivni i pasivni alati za Wi-Fi mreže mogu se iskoristiti za napade i dobivanje informacija o Wi-Fi mreži. Alati korišteni u istraživanju poput raznih *stumblera*, Kismeta i KisMaCa omogućili su razbijanje WEP i WPA zaštite u Wi-Fi mrežama, te je zaključeno da bi se WEP i WPA trebali napustiti kao način zaštite Wi-Fi mreža.

Autori Arjun K. Pillay, Mohammed Farik i Edwin Liava'a su u svom istraživanju iz 2017. godine, *Campus Area Network Wi-Fi Security* [xy], analizirali sigurnost Wi-Fi mreža i stvorili preporuke na temelju Wi-Fi mreža na kampusu sveučilišta u Fijiu. Korišten je *Acrylic Wi-Fi Home Go Pro* praogramski alat za analiziranje Wi-Fi mreža kako bi se identificirali AP-ovi, kanali na kojima mreže rade, proizvođači usmjerivača te sigurnosni protokol kojeg mreže koriste. Prikupljeni podaci su se nadalje analizirali u programu *Weka* te su dane preporuke i zaključci.

U istraživanju je potvrđeno da bi WPA2-PSK trebao biti prioritet kada se govori o sigurnosti Wi-Fi mreža. Dane su preporuke da se imena mreža odnosno SSID mreža promijeni u identifikacijske brojeve studenata i osoblja fakulteta i da se dopušta povezivanje isključivo njima. Korisnici trebaju upisivati što snažnije lozinke pri postavljanju svoje Wi-Fi mreže. Također, ako

terminalni uređaj želi uspostaviti vezu koristeći WEP sigurnosni protokol, pristup tom uređaju treba biti odbijen iz sigurnosnih razloga.

Zaključeno je da Wi-Fi mreže na području kampusa nisu dovoljno sigurne te da postoji mogućnost da će biti napadnute od strane hakera zbog nedovoljno snažne zaštite mreža. No pozitivna stvar u cijeloj situaciji je da se ipak većina korisnika povezuje na Wi-Fi mreže koristeći WPA2-PSK sigurnosni protokol i to putem najnovijih Samsung uređaja temeljenih na Android operativnom sustavu. To daje nove mogućnosti i prilike za daljnja istraživanja tog trenda.

6. Studija slučaja: ispitivanje sigurnosti Wi-Fi mreža u javnom okruženju grada Trogira

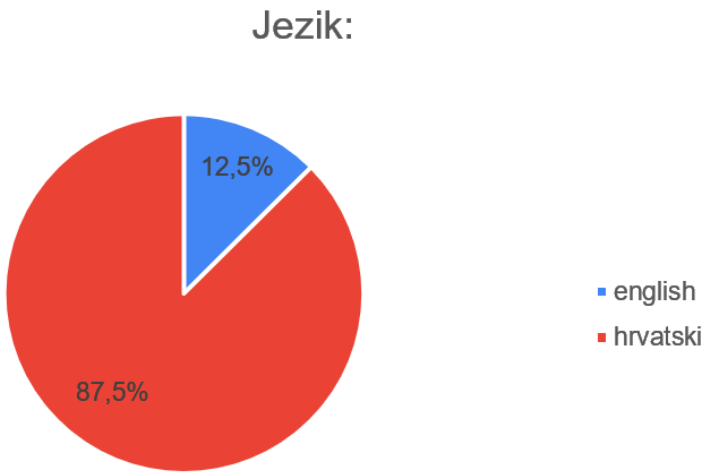
Kako bi se došlo do predodžbe koliko su sigurne Wi-Fi mreže u javnom okruženju grada Trogira, kao i koliko je rizično ponašanje samih korisnika u svijetu Wi-Fi mreža, istraživanje je obavljeno na dva načina: anketiranjem korisnika te skeniranjem mreža na području grada Trogira. Na taj način dobiva se uvid u stanje informiranosti korisnika te se samim time dobiva i uvid u to koliko su njihove Wi-Fi mreže sigurne, a s druge strane skeniranjem mreža na području grada može se steći uvid u konkretno stanje na terenu, to jest kako zaista djeluju postojeće Wi-Fi mreže što se tiče sigurnosti i sigurnosnih rizika.

6.1. Ispitivanje svjesnosti korisnika o sigurnosti putem anketnog upitnika

Anketni upitnik se sastojao od trinaest pitanja s unaprijed ponuđenim odgovorima, te je za obavljanje ankete korišten web alat *Google Forms*. Upitnik je proveden korištenjem društvenih mreža i e-pošte za anketiranje lokalnog stanovništva, te također anketiranjem stanovništva i stranih turista na terenu, na području grada Trogira. Ispitivanje je obavljeno u razdoblju od 13. srpnja do 20. kolovoza 2022. te je anketnom upitniku pristupio 271 ispitanik.

Potreban broj ispunjenih upitnika za relevantnost dobivenih podataka (uzorka) dobiven je korištenjem *Raosoft online* kalkulatora [xy], te je uz broj populacije od 338 897 ljudi, razinom pogreške od 5 % i razinom točnosti od 90 %, dobivena brojka od 271 osobe. Broj populacije je dobiven kombinacijom popisa stanovništva Republike Hrvatske 2021. godine [29] te podacima iz *e-Visitora* za ostvaren broj noćenja u gradu Trogiru u srpnju [30] i kolovozu [31] 2021. godine.

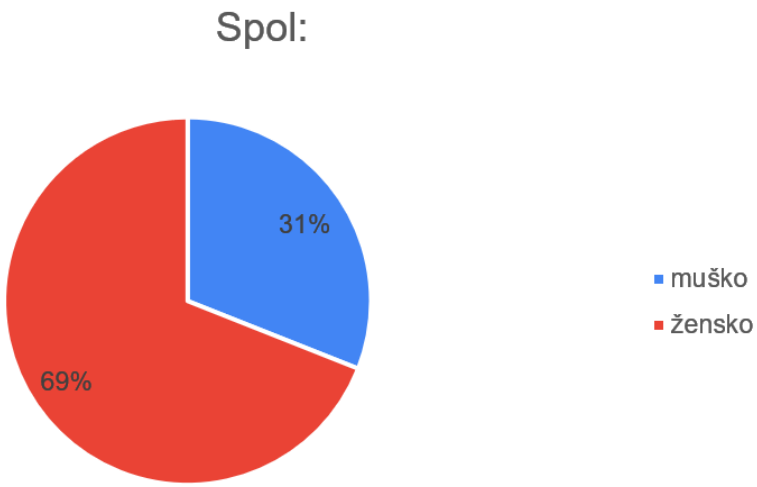
Anketa se na početku dijelila na hrvatski i engleski jezik, iz razloga da strani turisti lakše ispunjavaju anketu. Time je ujedno dobivena informacija koliko je stranih turista u odnosu na lokalno stanovništvo pristupilo anketi. Rezultati pitanja se vide u grafikonu 1.



Grafikon 1. Jezik odgovora na anketu

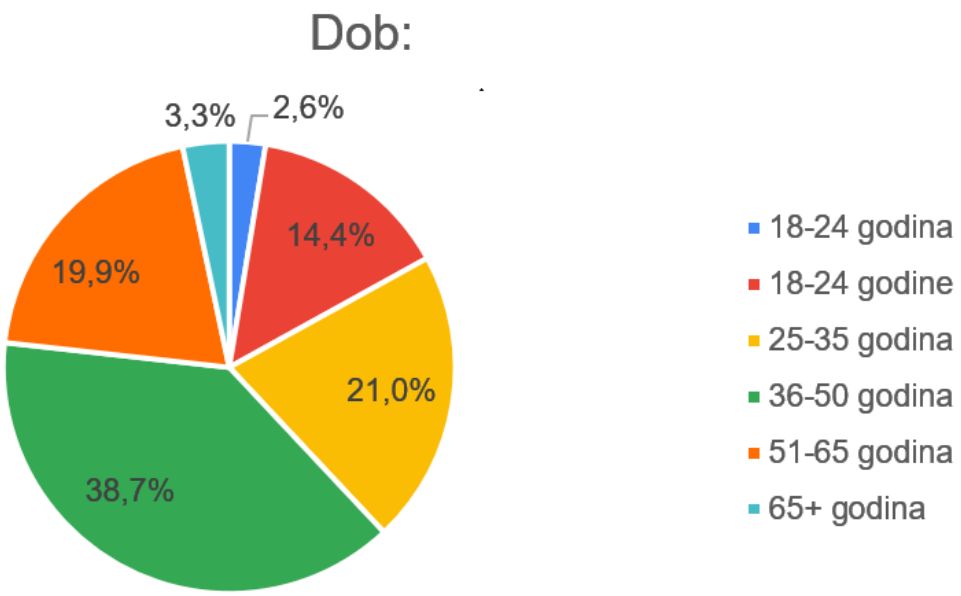
Kao što je vidljivo iz grafikona, većina ispitanika bilo je lokalno stanovništvo, pri čemu je većina tih ispitanika bila vlasnik ili suvlasnik apartmana u gradu. Samim time može se zaključiti da su odgovori tih ispitanika direktno vezani za sigurnost Wi-Fi mreža u gradu, jer većina apartmana nudi pristup Internetu putem svoje kućne Wi-Fi mreže.

U grafikonu 2. prikazan je spol ispitanika. Veći dio ispitanika bio je ženskog spola, 69 % u odnosu na 31 % muškaraca koji su pristupili anketi.



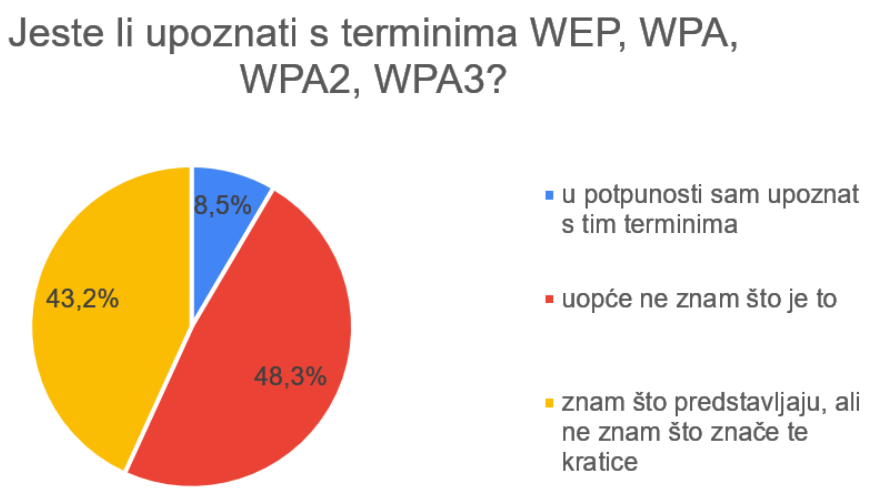
Grafikon 2. Spol ispitanika

Osim navedenog, ispitanici su odgovorili i na pitanje kojoj dobnoj skupini pripadaju. Većina ispitanika je bila u dobi između 36 i 50 godina. To je i očekivani rezultat, s obzirom na to da su vlasnici apartmana većinom pripadnici upravo te dobne skupine. Kao što je vidljivo u grafikonu 3, 38,7 % ispitanika pripada dobnoj skupini 36-50 godina, odmah nakon toga slijedi dobna skupina 25-35 godina sa 21 %, te nakon toga i skupina 51-65 godina sa 19,9 % ispitanika.



Grafikon 3. Dobne skupine ispitanika

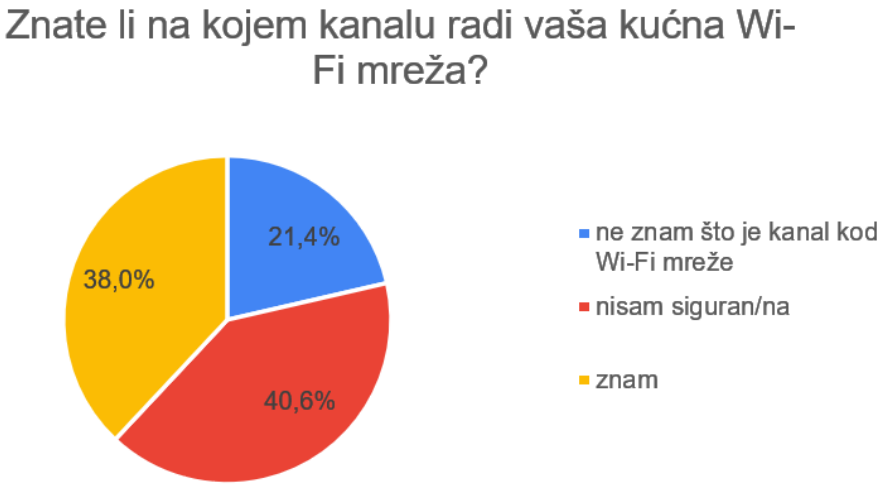
Iduće pitanje koje je postavljeno ispitanicima bilo je jesu li upoznati s terminima WEP, WPA, WPA2 i WPA3. Rezultati su vidljivi u grafikonu 4. Većina ljudi, 47,3 % ispitanika, uopće ne zna što predstavljaju ti termini. Iako je takav rezultat vrlo očekivan, ipak je poželjno da korisnici i vlasnici Wi-Fi mreža znaju kakvu zaštitu je poželjno da njihov usmjerivač ili pristupna točka posjeduje. U grafikonu 4. je vidljivo da je tek 8,5 % anketiranih upoznato s tim terminima, a što su mahom bili mlađi ispitanici.



Grafikon 4. Upućenost korisnika u sigurnosne standarde Wi-Fi mreža

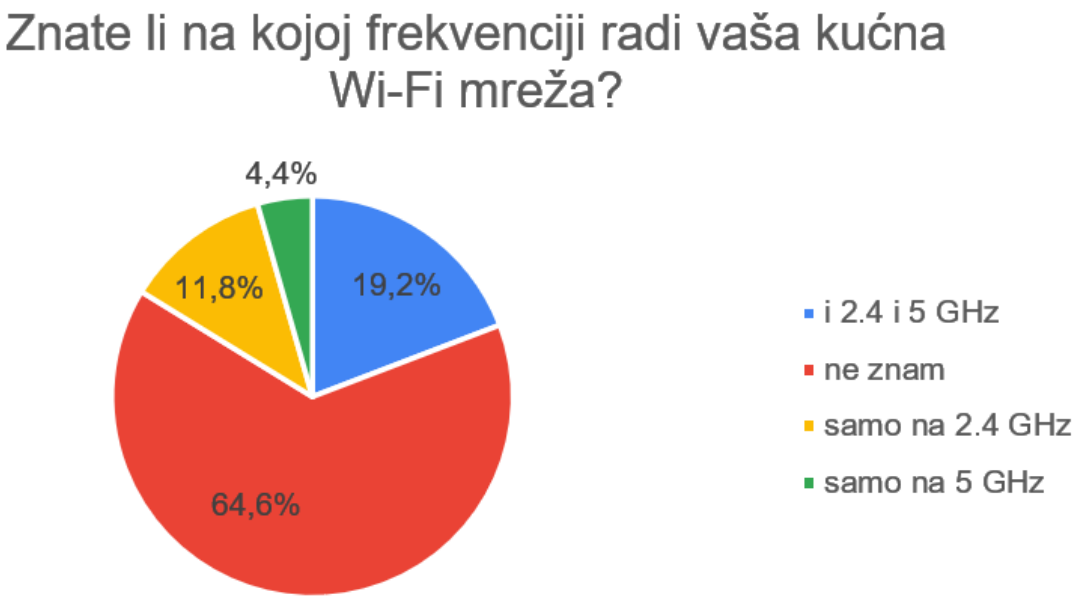
Iduće pitanje koje je postavljeno ispitanicima je znaju li na kojem kanalu radi njihova kućna Wi-Fi mreža. Zanimljivo je da tek 21,9 % ispitanika nije uopće znalo što je kanal kod Wi-Fi mreže, te je popriličan broj ispitanika, 36,7 %, odgovorio da zna na kojem kanalu radi njihova mreža. S druge strane, to ne mora značiti da su njihove mreže podešene za rad na optimalnom kanalu.

Također, i dalje velika većina ljudi nije upoznata s tom informacijom, kako je vidljivo na grafikonu 5.



Grafikon 5. Upućenost korisnika u informaciju na kojem kanalu radi njihova mreža

Kako bi se saznalo jesu li korisnici upoznati s frekvencijama koje se koriste kod Wi-Fi mreža, postavljeno je i pitanje znaju li na kojoj frekvenciji radi njihova mreža. Rezultati su relativno slični kao kod prethodnog pitanja, ukupno 35,4 % ispitanika zna na kojoj frekvenciji radi njihova mreža, dok 64,6 % njih ne zna odgovor na to pitanje. Također, raspodjela frekvencija na kojima rade kućne Wi-Fi mreže u gradu je donekle neočekivana, iako je vrlo malen broj mreža koje rade isključivo na 5 GHz, zanimljivo je da ih ima 4,4 % ,a ne i manje od toga. Rezultati su vidljivi u grafikonu 6.



Grafikon 6. Raspodjela frekvencija na kojima rade mreže ispitanih korisnika

Možda i najvažnije pitanje u anketi bilo je jesu li korisnici mijenjali lozinku na svojim usmjerivačima odnosno pristupnim točkama kad su instalirali Wi-Fi mrežu u kući. Ovdje su odgovori ispitanika iznenađujuće pozitivni, kao što je vidljivo na grafikonu 7. Većina ispitanika je promijenila lozinke svojih Wi-Fi mreža, a iznimno mali broj ispitanika nije razumio o čemu se radi u pitanju, dakle svjesni su postojanja lozinke te znaju da se ona može promijeniti. No iako je većina ispitanika mijenjala lozinku, i dalje postoji mogućnost da su te korisničke lozinke manje sigurne

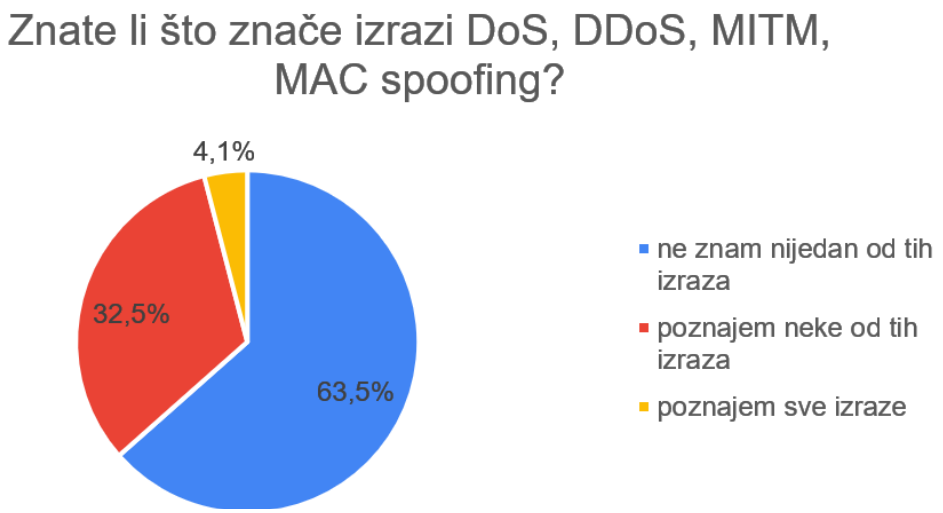
od onih tvornički postavljenih. To se nažalost ne može saznati osim metodama hakiranja kako bi se saznala lozinka svake od mreža.

Grafikon 7. Raspodjela ispitanika s obzirom na to jesu li mijenjali tvorničku lozinku mreže

Rezultati idućeg pitanja su poprilično neočekivani, kao što je vidljivo u grafikonu 8. Iako velika većina korisnika nije upoznata s izrazima kao što su DoS, MiTM te MAC *spoofing*, relativno je velik broj ispitanika upoznat barem s nekima od tih izraza, čak 32,5 % njih. Razlog tome su vjerojatno poneke edukativne emisije te članci na Internetu gdje su korisnici čuli neke od tih izraza, te su svjesni da postoje određene opasnosti na Internetu.

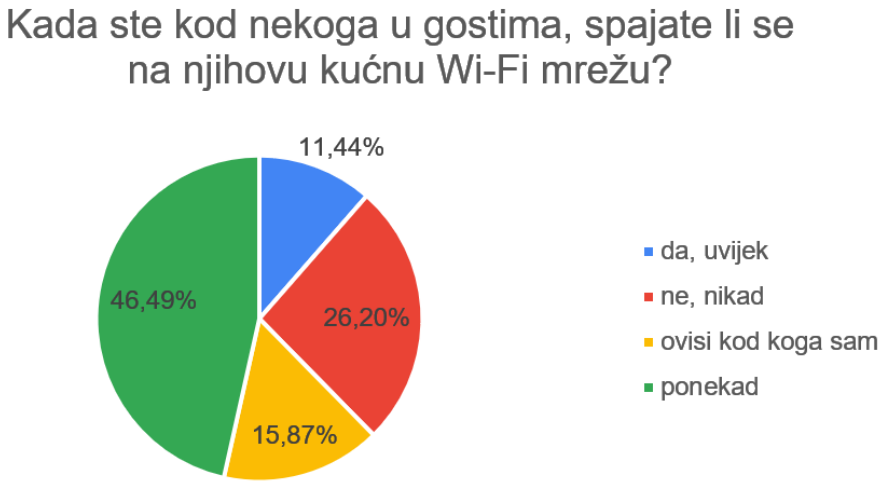
Sljedeća tri pitanja vezana su za iskustva i navike korisnika Wi-Fi mreža, te se ispitanike pitalo spajaju li se na tuđe Wi-Fi mreže kad su kod nekoga u gostima, spajaju li se na javne i/ili gradske Wi-Fi mreže, te je li im se ikad dogodio neovlašteni upad odnosno napad u njihovoj mreži. Između ostalog, velik broj ispitanika se nikad ne spaja na javne ili tuđe privatne Wi-Fi mreže, što se može objasniti iznimnom rasprostranjenošću mobilnih mreža i mobilnog Interneta, te zbog

toga većina korisnika jednostavno nema potrebu spajati se na druge Wi-Fi mreže iz razloga što u vlastitoj tarifi imaju dovoljno mjesečnog prometa dostupnog za svoje potrebe na Internetu.



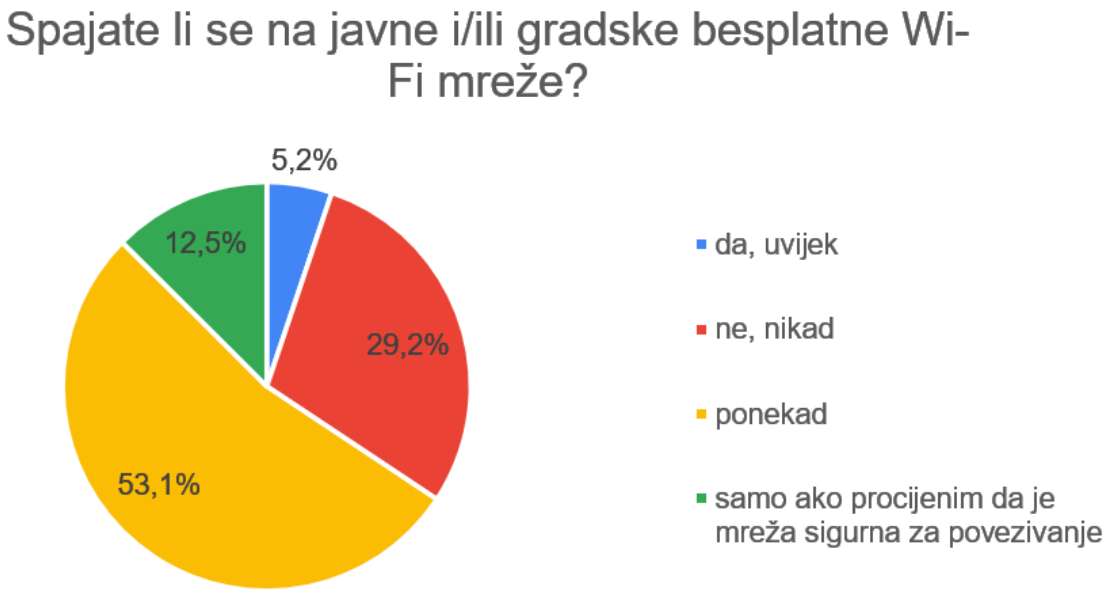
Grafikon 8. Upućenost ispitanika u nazive napada koji im prijete na Wi-Fi mrežama

U grafikonu 9. vidljivo je da se većina korisnika ponekad spoji na tuđu Wi-Fi mrežu kad su kod nekoga, ali poprilično malen broj njih razmišlja o tome na čiju će se mrežu spajati – tek 15,87 % korisnika se spaja na nečiju mrežu ovisno o tome kod koga su.



Grafikon 9. Navike ispitanika s obzirom na spajanje na tuđe privatne Wi-Fi mreže

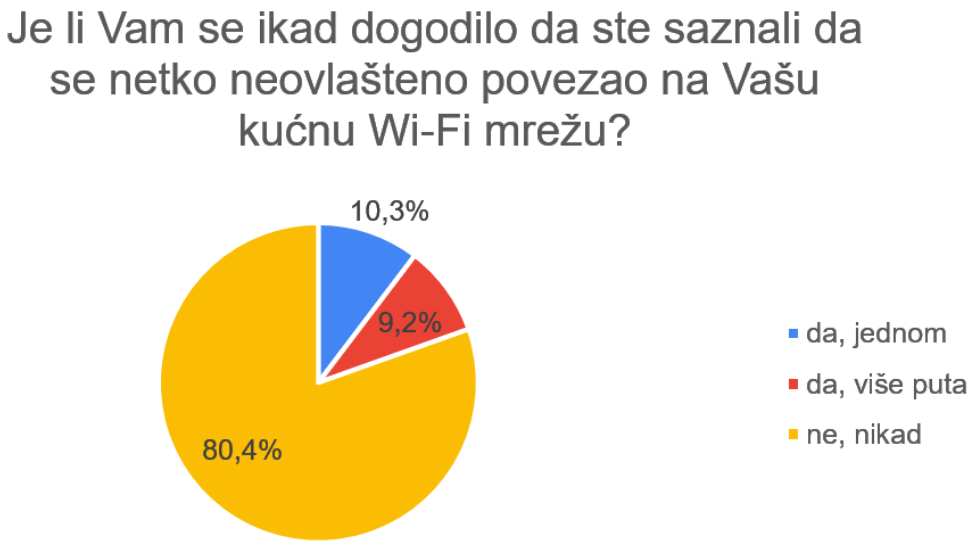
Kako je vidljivo u grafikonu 10., također vrlo mali broj korisnika razmišlja o tome je li neka javna besplatna Wi-Fi mreža sigurna za povezivanje. Većina korisnika bez razmišljanja se spaja na takve mreže, a tek 12,5 % njih se spaja na takve mreže samo ako procijene da je mreža sigurna za povezivanje.



Grafikon 10. Korisničke navike spajanja na javne besplatne Wi-Fi mreže

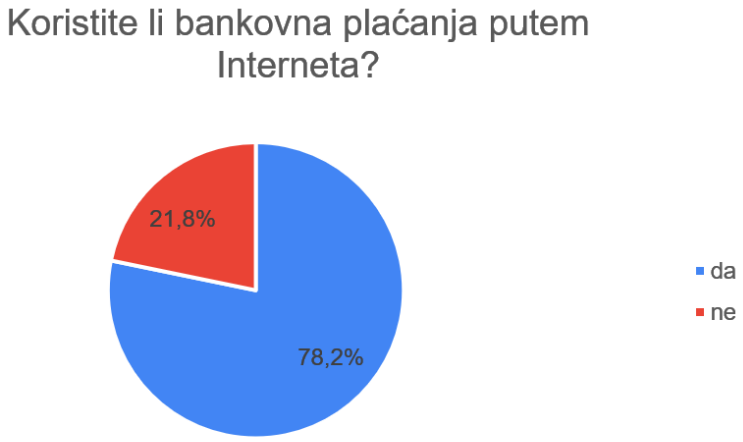
Velika većina ispitanika nije imala nikakav događaj vezan za neovlašteni upad u njihovu vlastitu mrežu, kao što je vidljivo u grafikonu 11. No s obzirom na to da je čak 10,3 % ispitanika imalo jedno takvo iskustvo, a 9,2 % njih više takvih iskustava, može se zaključiti da jedan dio onih koji tvrde da nisu imali takav događaj jednostavno nisu bili ni svjesni tog upada u mrežu, te da su ipak takve aktivnosti češće nego što bi se moglo pretpostaviti.

Ovdje su u najvećoj šteti turisti, koji naravno nisu svjesni da se možda već nekoliko puta dogodio neovlašteni upad u nečiju kućnu mrežu, a na koju se oni spajaju kad su kod nekoga u tom apartmanu.



Grafikon 11. Iskustva ispitanika s neovlaštenim upadima u njihovu Wi-Fi mrežu

Kako bi se saznalo kakve su navike ispitanika što se tiče bankovnih plaćanja preko Interneta, odnosno koliko je rizično spajanje na Wi-Fi mreže za korisnike s obzirom na to da možda obavljaju plaćanja putem Interneta, postavljeno im je pitanje koriste li bankovna plaćanja *online* putem. Rezultati su vidljivi u grafikonu 12.



Grafikon 12. Navike ispitanika u vezi bankovnih plaćanja putem Interneta.

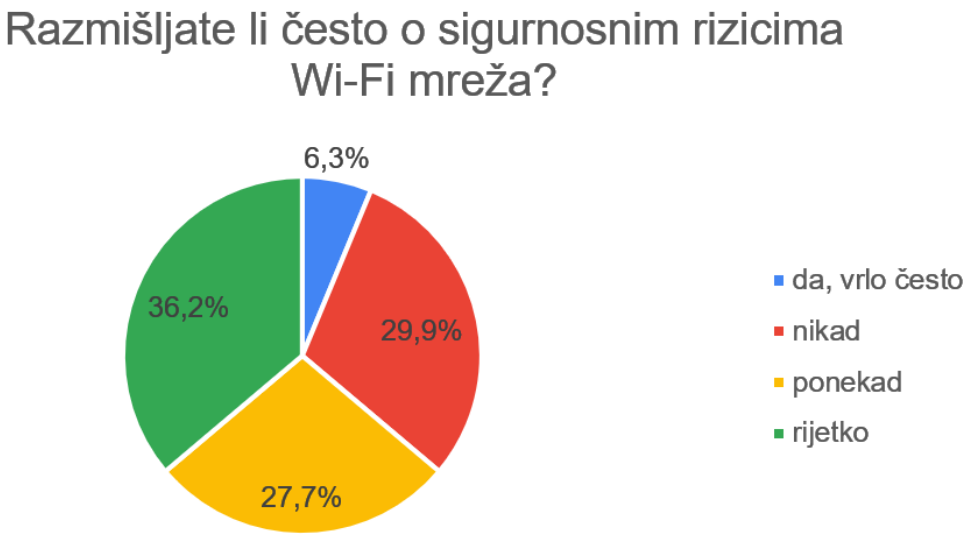
Rezultati su prilično očekivani i kod ovog pitanja, s obzirom na to da većina korisnika uistinu koristi plaćanja putem Interneta. To znači da im je sigurnost dodatno ugrožena zbog

obavljanja visokorizičnih radnji putem Interneta, a dok se spajaju na možda nesigurne Wi-Fi mreže.

Iduća dva pitanja vezana su za osobna promišljanja i doživljaje ispitanika što se tiče sigurnosti i sigurnosnih rizika Wi-Fi mreža. Kod pitanja osjećaju li se sigurno kad se spajaju na tuđu Wi-Fi mrežu, većina korisnika se osjeća sigurno ili uopće ni ne razmišlja o sigurnosti prilikom spajanja na neku Wi-Fi mrežu, ukupno njih 66,8 %. U velikoj manjini su ispitanici koje je strah spajati se na druge Wi-Fi mreže, tek 5,9 % ispitanika, kao što je vidljivo u grafikonu 13.

Grafikon 13. Osjećaj sigurnosti kod ispitanika kada se spajaju na tuđu Wi-Fi mrežu

Na kraju ankete, ispitanici su pitani razmišljaju li često o sigurnosnim rizicima Wi-Fi mreža. Kako je prikazano na grafikonu 14., rezultati su vrlo slični kao kod prethodnog pitanja. U velikoj manjini su korisnici koji vrlo često razmišljaju o tome, njih 6,3 %. 27,7 % ispitanika ponekad razmišlja o tome, a ukupno 66,1 % njih o tome ne razmišlja nikad ili rijetko. Prema tome, može se zaključiti da korisnici nisu ili su vrlo malo svjesni rizika koji im prijete na Wi-Fi mrežama te su vrlo malo zabrinuti za svoju sigurnost na Wi-Fi mrežama.



Grafikon 14. Razmišljanja ispitanika o sigurnosnim rizicima Wi-Fi mreža

To može nepovoljno utjecati na sigurnost tih korisnika na Wi-Fi mrežama, pa i Internetu, jer ako ne razmišljaju o sigurnosnim rizicima, malo je vjerojatno da će i prilikom posjećivanja sumnjivih mjesta na Internetu biti nepovjerljivi, te postoji realna mogućnost da će otvarati sumnjive poruke e-pošte i raditi slične rizične aktivnosti.

6.2. Zaključak analize anketnog upitnika

Nakon prikazanih i analiziranih informacija koje su dobivene od ispitanika, može se reći da korisnici nisu dovoljno svjesni sigurnosnih rizika koji prijete na Wi-Fi mrežama. Iako se u ponekim pitanjima može steći dojam da je relativno velik broj korisnika upoznat s tehničkim aspektima Wi-Fi mreža, nakon što se analiziraju svi odgovori i pitanja, zaključak je da nisu dovoljno upoznati sa sigurnosnim aspektima Wi-Fi mreža. Navedeno se može poboljšati kampanjama za edukaciju korisnika o sigurnosnim aspektima Wi-Fi mreža, koje postaju sve potrebnije kako Wi-Fi mreže sve više ulaze u ljudske živote, a pogotovo kad se gleda turistička sfera te potrebe koje turisti imaju prilikom unajmljivanja smještaja u gradu. Velika većina gostiju želi imati besplatan Wi-Fi u svom apartmanu, a s obzirom na to da domaće stanovništvo nije dovoljno upoznato sa sigurnosnim rizicima Wi-Fi mreža, postoji realna mogućnost da se turisti često spajaju na nesigurne Wi-Fi

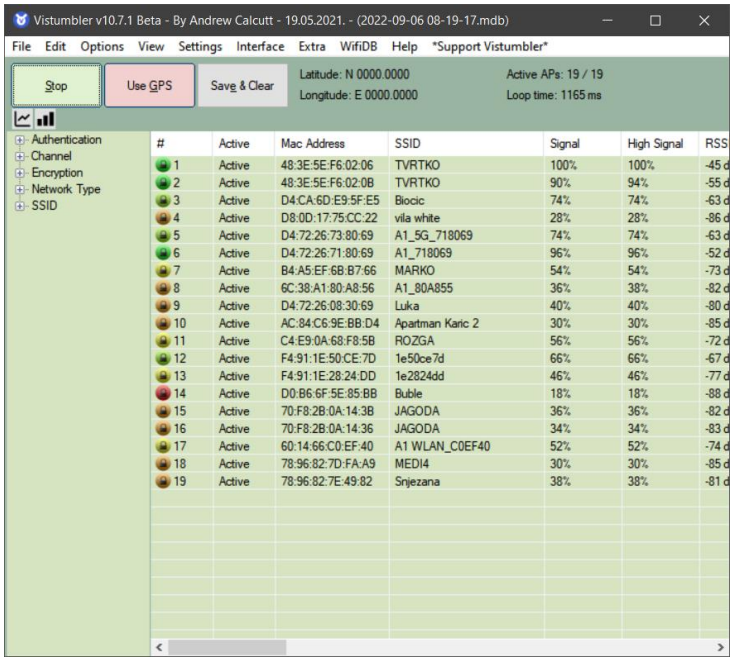
mreže. Također je to slučaj i sa lokalnim stanovništvom, koje također ima rizično ponašanje na Wi-Fi mrežama, iako se to donekle kompenzira malim brojem spajanja na javne i gradske Wi-Fi mreže iz razloga što je mobilni Internet postao iznimno rasprostranjen i dostupan.

6.3. Ispitivanje sigurnosti Wi-Fi mreža u gradu metodom skeniranja Wi-Fi mreža

Osim istraživanja putem anketnog upitnika, obavljeno je i skeniranje Wi-Fi mreža u gradu Trogiru putem aplikacije *Vistumbler* kako bi se došlo do podataka o tome kako je stvarno stanje na terenu što se tiče Wi-Fi mreža. Tako je moguće saznati koji su SSID-ovi mreža, kakav sigurnosni protokol koriste, jesu li javno otvorene ili privatne i dr.

6.3.1. Opis i metodologija provedenog istraživanja

Kao programski alat za skeniranje Wi-Fi mreža i prikupljanje informacija o njima korišten je programski alat *Vistumbler*. To je skener bežičnih mreža napisan u programskom jeziku *AutoIT*, namijenjen operativnim sustavima Windows. Glavna svrha programskog alata je mapiranje i vizualiziranje te prikupljanje podataka o svim Wi-Fi mrežama u blizini uređaja koji obavlja skeniranje, [32].



Slika 5. Sučelje alata Vistumbler

Na slici 5. prikazano je kako izgleda sučelje programskog alata Vistumbler. Kao što je vidljivo na slici, program ima poprilično jednostavno sučelje, te je nakon skeniranja Wi-Fi mreža moguće filtrirati ih po bilo kojem kriteriju odnosno informaciji koja je prikupljena, te je zatim moguće i izvesti datoteku koja sadrži informacije o mrežama u željenom obliku, poput recimo CSV, KML ili GPX formata. Za ovo istraživanje, nakon skeniranja mreža podaci su spremljeni u formatu VS1, koji je nativni Vistumblerov format datoteke, kako bi se kasnije datoteka mogla opet otvoriti u alatu te zatim izvesti u CSV oblik.

Samo skeniranje je obavljeno 5. rujna 2022. godine u večernjim satima, koristeći prijenosno računalo Lenovo Ideapad 3 15ARE05, s integriranom mrežnom karticom Qualcomm Atheros QCA61x4A. Skeniranje je obavljeno pješke, jer zbog veličine ulica nije bilo moguće odraditi skeniranje bilo kojim prijevoznim sredstvom. Put kojim se hodalo praćen je pomoću aplikacije *OsmAnd* na pametnom telefonu *Xiaomi Poco X3*. Zapisani put je izvezen u obliku GPX datoteke na računalo te prebačen u oblik slike. Kroz otprilike 35 minuta hodanja, pokriven je prostor naseljenog centra grada te su prikupljene informacije o svim uhvaćenim Wi-Fi mrežama. Iako je područje relativno maleno, dobiven je iznimno velik broj skeniranih Wi-Fi mreža za takav teritorij. Pokriveno je područje stare jezgre grada Trogira, odnosno uži centar grada.

Slika 6. Mapa skeniranog područja

To područje je izabrano iz razloga što u tom dijelu grada postoji najviše apartmana, restorana te ostalih ugostiteljskih i poslovnih objekata, uz također određeni broj privatnih

stanova. Na slici 6. prikazano je na mapi koji dio grada je pokriven, te kojim ulicama se prolazilo prilikom skeniranja.

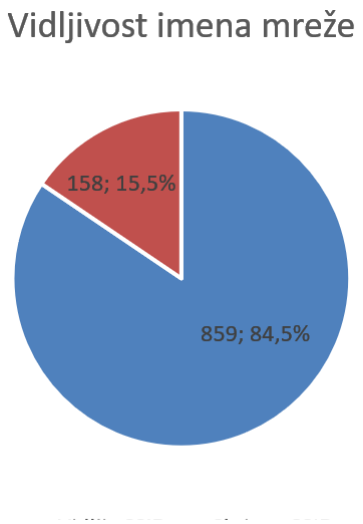
Nakon obavljenog skeniranja, podaci su spremljeni u formatu datoteke VS1, te zatim izvezeni u obliku CSV i konvertirani u XSLX format, kako bi se mogli obraditi u Microsoft Excelu. Nad dobivenim podacima izvršena je analiza tako da se mogu izdvojiti informacije koje su od određenog interesa i značaja što se tiče sigurnosti Wi-Fi mreža u gradu.

6.3.2. Rezultati skeniranja i analiza dobivenih informacija

Nad dobivenim rezultatima skeniranja obavljena je analiza, te su u nastavku prikazane informacije koje su značajne za sliku sigurnosti Wi-Fi mreža u gradu. Kroz te informacije može se zaključiti kakvo je stvarno stanje na terenu i koliko su gradske Wi-Fi mreže zapravo sigurne, odnosno koliko su se vlasnici mreža i poslovnih objekata, kao i privatnih stanova, osigurali od rizika koji postoje na Wi-Fi mrežama.

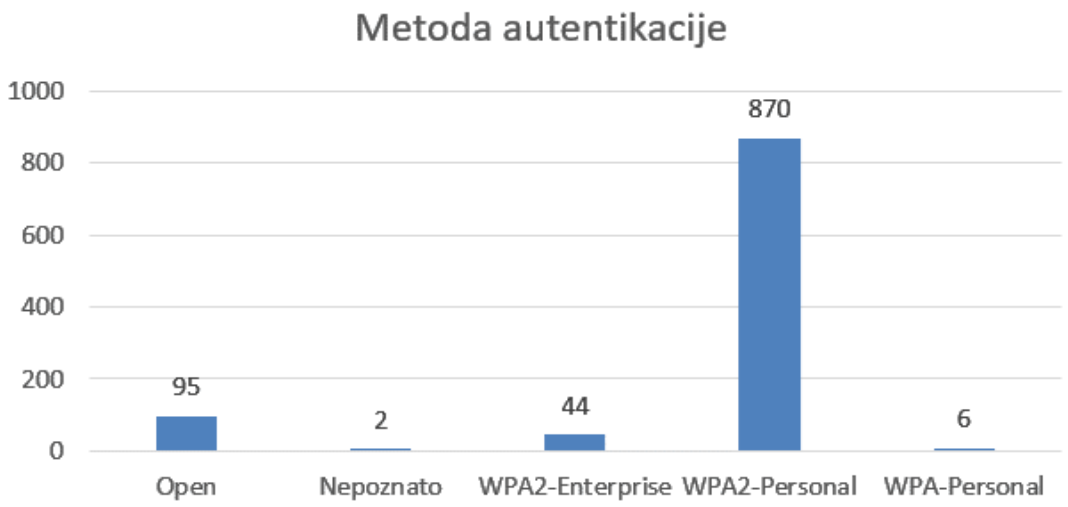
Iako je dobivena brojka od ukupno 1017 Wi-Fi mreža, stvaran broj lokalnih bežičnih mreža je nešto manji, iz razloga što je uhvaćen svaki AP i usmjerivač, odnosno uređaj putem kojeg se može spojiti na Wi-Fi mrežu, sa jedinstvenom MAC adresom. Dakle, uhvaćeno je ukupno 1017 uređaja koji su *access pointovi*, usmjerivači, repetitori ili drugi uređaji preko kojih se korisnici spajaju na mrežu. Izbacivanjem dupliciranih imena mreža, odnosno SSID-ova, dolazi se do brojke od 573 jedinstvenih imena, dakle 573 različite Wi-Fi mreže u gradu, što je i dalje pozamašan broj mreža za relativno malen prostor.

Već na početku analize može se zamijetiti zanimljiva činjenica: postoji značajan broj mreža, odnosno uređaja kojima je skriven SSID mreže. To odmah daje za naslutiti da je sigurnosno stanje mreža u gradu na relativno dobroj razini, jer skrivanje imena mreže u startu otežava neovlašteno spajanje na mrežu. U grafikonu 15. vidljiv je odnos između mreža s vidljivim odnosno nevidljivim imenom mreže. 15,5 % uređaja skriva SSID, te iako su u manjini, to je svakako pozitivna stvar što se tiče sigurnosti.



Grafikon 15. Odnos mreža s vidljivim ili nevidljivim imenom mreže

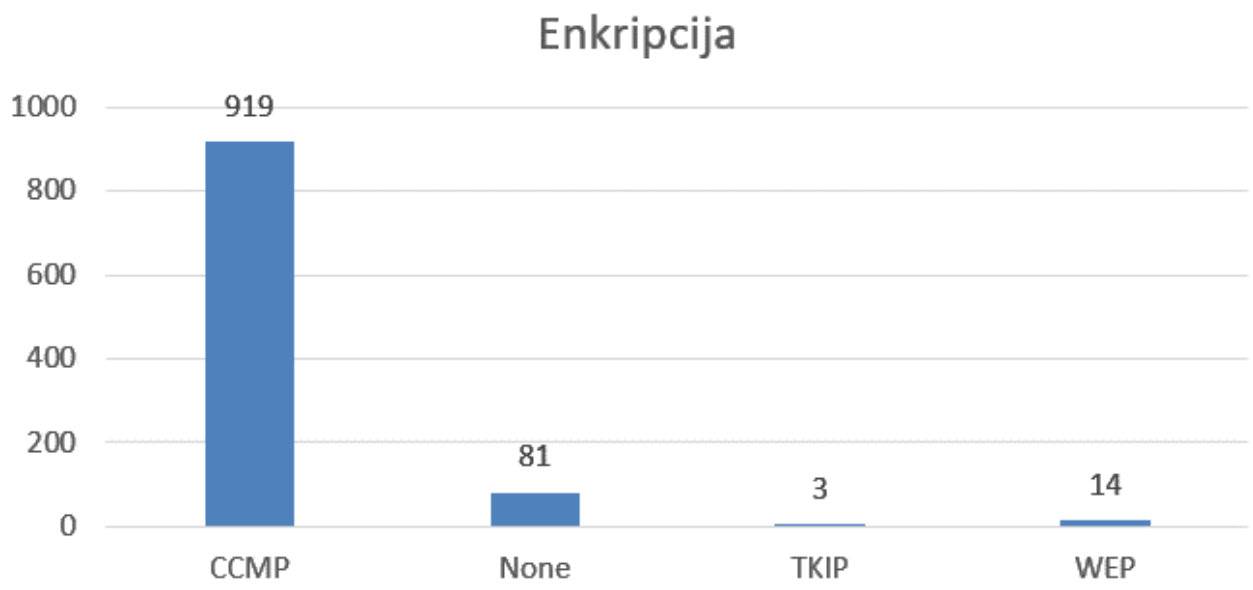
Sljedeći kriterij po kojem se mreže mogu razvrstati je osnovna karakteristika koju se uzima u obzir kod sigurnosti Wi-Fi mreža – Metoda autentikacije, odnosno sigurnosni protokol koji se koristi za autentikaciju prilikom spajanja na mrežu. Ovdje su rezultati također poprilično pozitivni, no kako je vidljivo u grafikonu 16., ipak postoji određen, iako malen, broj mreža sa slabom do nikakvom zaštitom. 95 mreža je potpuno otvoreno, dakle bez ikakve zaštite, što donekle ima smisla, s obzirom na to da grad Trogir ima javnu gradsku mrežu, koja prema rezultatima skeniranja broji 20 pristupnih točaka, a javne mreže obično ne nude nikakvu zaštitu zbog jednostavnosti spajanja. Određen broj tih otvorenih mreža pripada bankama i sličnim objektima, a ostatak ugostiteljskim objektima, koji bi ipak trebali zaštititi svoje mreže nekom metodom autentikacije.



Grafikon 16. Metode autentikacije koje koriste Wi-Fi mreže

Osim toga, određen broj mreža, njih šest, koristi zaštitu WPA, što je znak da koriste zastarjelu opremu i da njihove mreže nisu sigurne. No isto tako je pozitivan podatak da 44 mreže koriste WPA2-Enterprise zaštitu, koja koristi RADIUS server i sigurnija je od WPA2-Personal zaštite koja je namijenjena za kućne mreže. Naravno, poželjno bi bilo da se veći broj objekata prebaci na takvu zaštitu.

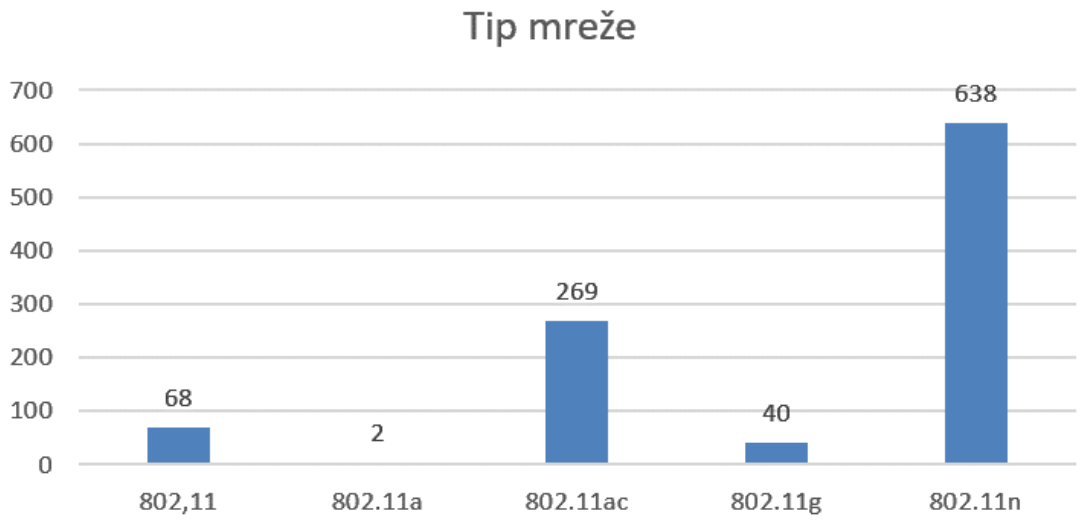
Osim metode autentikacije, programskim alatom *Vistumbler* može se saznati i koji enkripcijski protokol koriste mreže. Kao što je vidljivo u grafikonu 17., podaci u velikoj mjeri koreliraju s metodom autentikacije, što je očekivano. Ono što je i kod ovog grafikona zanimljivo je to što određen broj otvorenih mreža bez autentikacije ipak ima uključenu enkripciju. To je svakako pozitivan izbor, međutim s obzirom na to da se enkripcijski ključ prilikom spajanja na mrežu u početku šalje nezaštićen može se presresti od strane napadača. Pitanje je koliko je to vjerojatno, i ima li smisla zbog toga imati enkripciju na javno dostupnoj otvorenoj mreži, ali i dalje enkripcija na takvoj mreži predstavlja određen sloj zaštite.



Grafikon 17. Metoda enkripcije koju koriste mreže

Nakon enkripcije, slijedi i podatak po kojem se može znati koliko je mrežna oprema u skladu s vremenom, odnosno koliko je zastarjela ili nije. To je informacija o tipu mreže, dakle radi li mreža na 802.11a standardu, 802.11 b, n, g ili pak novijem.

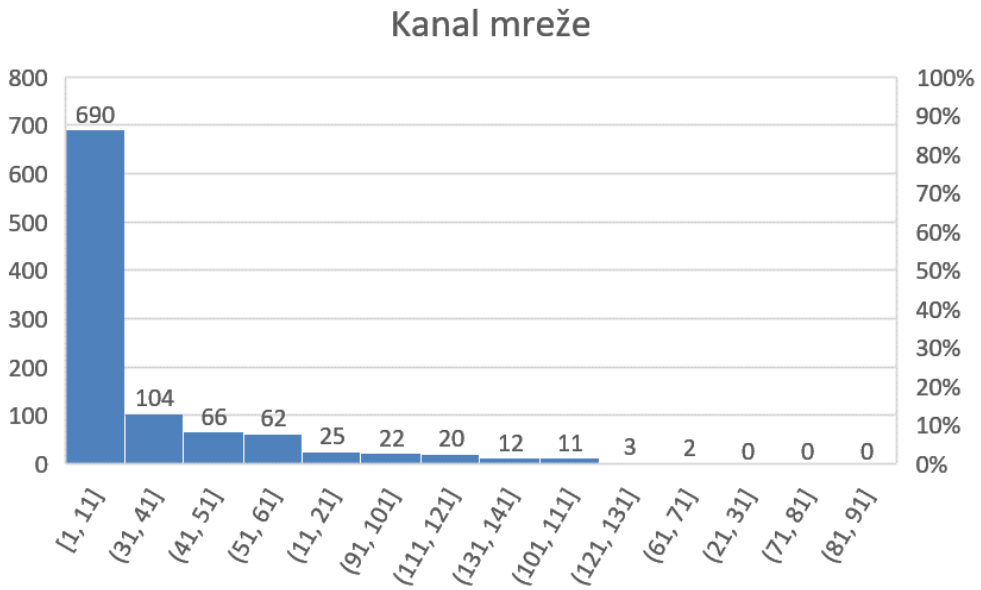
Ovdje su podaci također relativno pozitivni, no opet postoji mjesto za napredak. Kao što je prikazano na grafikonu 18, većina mreža radi na 802.11n standardu, koji je danas iako donekle star, i dalje relevantan standard kod kućnih Wi-Fi mreža. Nudi WPA2 sigurnosni protokol, što je najvažnija sigurnosna stavka kod Wi-Fi mreže. Pozitivna je činjenica što velik broj mreža, njih 269, radi na novijem 802.11ac standardu, što govori da je velika količina mrežne opreme gradskih



Grafikon 18. Standard na kojem rade Wi-Fi mreže

mreža novijeg datuma. 68 mreža ne daje informaciju o tome koji točno standard koriste, a 2 mreže rade na 802.11a standardu, što je znak da vjerojatno koriste i stariju mrežnu opremu.

Posljednja informacija koja je relevantna je kanal na kojem rade mreže, prema čemu se može zaključiti jesu li korisnici koji su mijenjali kanal na kojem radi njihova mreža, učinili grešku te postavili mrežu na rad na nekom od kanala koji se ne koriste, ako je u pitanju 2.4 GHz mreža, što znači da će dolaziti do kolizije, a također govori i o edukaciji korisnika.



Grafikon 19. Kanal na kojem rade Wi-Fi mreže

Prema grafikonu 19., vidljivo je da velika većina mreža radi na kanalima od 1 do 11, što govori da su to mreže koje funkcioniraju na frekvenciji od 2.4 GHz, dok ostatak mreža radi na frekvenciji od 5 GHz. To korelira sa anketnim pitanjem u kojem se ispitanike tražilo da odgovore na kojoj frekvenciji radi njihova mreža, gdje su odgovori bili vrlo slični rezultatima dobivenima u ovom grafikonu.

Što se tiče mreža koje rade isključivo na 2.4 GHz, na grafikonu 20 prikazano je koje sve kanale koriste te mreže. Većina njih koristi kanale 1, 6 ili 11, što je logično, te mrežna oprema po tvorničkim postavkama skače između ta tri kanala jer između njih nema interferencije, kao što je prikazano na slici 3 u prvom dijelu rada.

Grafikon 20. Kanali mreža koje rade na frekvenciji od 2.4 GHz

Međutim, postoji i relativno velik broj mreža koje rade na svim ostalim kanalima, pto znači da si vjerojatno međusobno smetaju, a taj podatak nam govori i to da su vlasnici tih mreža vrlo vjerojatno sami postavljali kanale na kojima će mreža raditi jer je mala mogućnost da bi usmjerivači i pristupne točke automatski odabrali neke od tih kanala za rad. Prema tome, može

se zaključiti i da su te mreže manje sigurne od ostalih jer su možda vlasnici postavljali i slabije zaporke od predviđenih.

6.3.3. Zaključak provedene analize

Prema svemu navedenom i prema informacijama koje su dobivene skeniranjem i analizom, zaključci su slični kao i kod analize rezultata anketnog upitnika. Korisnici su relativno neupoznati sa sigurnosnim aspektima Wi-Fi mreža, no pozitivno je u svemu tome što uređaji već tvornički dolaze s WPA2 zaštitom u velikoj većini slučajeva, te s relativno jakim lozinkama, a uz to ipak postoji određen broj vlasnika Wi-Fi mreža koji su, barem što se tiče sigurnosnih postavki mrežne opreme, relativno dobro educirani.

S obzirom na situaciju, može se reći da iako većina korisnika nije educirana o sigurnosnim rizicima i aspektima Wi-Fi mreža, stanje u gradu što se tiče sigurnosti mreža je zadovoljavajuće. No unatoč tome, uvijek postoji mjesto za napredak, te bi svakako pozitivan učinak imala određena edukativna kampanja koja bi educirala korisnike o sigurnom korištenju Wi-Fi mreža, u kombinaciji sa zamjenom zastarjele mrežne opreme u poslovnim, ali i stambenim objektima.

7. Zaključak

Wi-Fi tehnologija postala je uvjerljivo najrasprostranjeniji način pristupa Internetu u današnje vrijeme. Rastom popularnosti pametnih telefona, tableta i sličnih terminalnih uređaja postalo je jasno da je Wi-Fi tehnologija nezamjenjiva pri korištenju Interneta u današnjem svijetu. Posljednjih godina postalo je iznimno često i raditi od kuće, te se time prenosi još više povjerljivih informacija putem Wi-Fi mreža. Korištenjem internetskog bankarstva te *online* plaćanja, još je više jasno da postoje značajni rizici krađe povjerljivih podataka ako dođe do narušavanja sigurnosti Wi-Fi mreže kojom se prenose ti podaci.

Kako bi se dao uvid u stvarno stanje sigurnosti Wi-Fi mreža, u svijetu su dostupna brojna istraživanja u tom području, pa tako i u području ispitivanja samih korisnika o njihovoj educiranosti o toj temi. Iznimno je važno da korisnici koriste Wi-Fi mreže na siguran način, a posebice ako koriste tu tehnologiju za obavljanje ranije opisanih zadaća. S obzirom na to da je ta tehnologija postala svakodnevica, iznimno velika količina podataka se svakim danom prenese putem Wi-Fi mreža.

Osim ispitivanja korisnika o njihovom znanju te korištenju Wi-Fi mreža, programskim alatima za skeniranje mreža u blizini moguće je steći dojam o tome kakve su mreže na određenom području, a pogotovo što se tiče njihovih sigurnosnih karakteristika. Tim alatima, među kojima je i *Vistumbler*, moguće je doći do iznimno mnogo podataka o obližnjim mrežama iz kojih se može mnogo toga saznati. Zato je u ovom radu osim anketnog ispitivanja, odrađeno i skeniranje obližnjih mreža programskim alatom *Vistumbler*.

Ispitivanjem korisnika o njihovoj svjesnosti o rizicima Wi-Fi tehnologije stekao se uvid u to kako korisnici razmišljaju te koja je njihova razina znanja u tom području. Analizom rezultata ankete vidljivo je da iako korisnici koriste Wi-Fi mreže svakodnevno, nisu zadovoljavajuće educirani o njihovim sigurnosnim rizicima. Tome pomaže činjenica da su mrežni uređaji i oprema tvornički podešeni za rad na najsigurniji mogući način, počevši od što kompliciranije zaporke za pristup mreži, do automatskog odabira kanala na kojem uređaj radi. No nije tako kod svakog

proizvođača mrežne opreme, te je i dalje imperativ što je moguće više educirati korisnike kako bi njihovo korištenje Wi-Fi tehnologije bilo što sigurnije.

Skeniranjem Wi-Fi mreža u gradu Trogiru pomoću programskog alata *Vistumbler*, prikupljeno je dovoljno podataka da bi se moglo zaključiti da je stanje sigurnosti mreža u gradu zadovoljavajuće, no i dalje ima mnogo mjesta za napredak. I dalje postoji nezanemariv broj mreža bez ikakve zaštite, pa tako i enkripcije veze, a određen broj mreža koristi i zastarjele sigurnosne protokole. Iako je broj takvih mreža malen, potrebno je poboljšati situaciju što se tiče njihove sigurnosti.

Zbog svega navedenog, može se zaključiti da uvijek ima mjesta za napredak na prostorima poput grada Trogira, pogotovo zbog spomenutih mreža koje imaju zastarjele sigurnosne protokole, a još više zato što u takvom turističkom gradu postoji veća mogućnost da se dogodi neželjeni napad odnosno ostvarenje sigurnosne prijetnje putem Wi-Fi mreže. Velik broj turista, ali i domaćeg stanovništva se svakodnevno spaja na Internet putem tuđih Wi-Fi mreža i potrebno je što je moguće više umanjiti rizike korištenja Wi-Fi tehnologije.

Popis literature

[1] Horak R. Telecommunications and Data Communications Handbook Hoboken, New Jersey: John Wiley & Sons, Inc.; 2007.

[2] OSI Model. Preuzeto sa: https://www.imperva.com/learn/application-security/osi-model/ (Pristupljeno 16.6.2022.)

[3] Geier J. Wireless LANs, Second Edition Indianapolis, Indiana: Sams Publishing; 2002.

[4] Wi-Fi Channels, Frequencies, Bands & Bandwidths. Preuzeto sa: https://www.electronics-notes.com/articles/connectivity/wifi-ieee-802-11/channels-frequencies-bands-bandwidth.php (Pristupljeno 16.6.2022.)

[5] 2.4 GHz Channel Planning. Preuzeto sa: https://www.extremenetworks.com/extreme-networks-blog/2-4-ghz-channel-planning/ (Pristupljeno 16.6.2022.)

[6] Best 5GHz Channel for your WiFi Router. Preuzeto sa: https://www.getwox.com/best-5ghz-channel/ (Pristupljeno 16.6.2022.)

[7] Understanding Antenna Specifications and Operation, Part 1. Preuzeto sa: https://www.digikey.com/en/articles/understanding-antenna-specifications-and-operation (Pristupljeno 16.6.2022.)

[8] Muštra M. Mobilni komunikacijski sustavi, predavanja iz kolegija Mobilni komunikacijski sustavi, Fakultet prometnih znanosti, Zagreb. 2019..

[9] FCC Rules for Unlicensed Wireless Equipment operating in the ISM bands. Preuzeto sa: https://afar.net/tutorials/fcc-rules/ (Pristupljeno 17.6.2022.)

[10] Wi-Fi Signal Strength: What Is a Good Signal And How Do You Measure It. Preuzeto sa: https://eyenetworks.no/en/wifi-signal-strength/ (Pristupljeno 17.6.2022.)

[11] 802.11 Standards Explained: 802.11ax, 802.11ac, 802.11b/g/n, 802.11a. Preuzeto sa: https://www.lifewire.com/wireless-standards-802-11a-802-11b-g-n-and-802-11ac-816553 (Pristupljeno 19.6.2022.)

[12] The evolution of Wi-Fi standards: a look at 802.11a/b/g/n/ac/ax. Preuzeto sa: https://www.actiontec.com/wifihelp/evolution-wi-fi-standards-look-802-11abgnac/ (Pristupljeno 19.6.2022.)

[13] I. C. Sigurnost i zaštita informacijsko komunikacijskog sustava, nastavni materijali za kolegij Sigurnost i zaštita informacijsko komunikacijskog sustava, Fakultet prometnih znanosti, Zagreb. 2020..

[14] What Is Wi-Fi Security? Preuzeto sa: https://www.cisco.com/c/en/us/products/wireless/what-is-wi-fi-security.html#~devices (Pristupljeno 21.6.2022.)

[15] Understanding Rogue Access Points. Preuzeto sa: https://www.juniper.net/documentation/en_US/junos-space-apps/network-director4.0/topics/concept/wireless-rogue-ap.html (Pristupljeno 22.6.2022.)

[16] Most Popular Types of WiFi Cyberattacks. Preuzeto sa: https://socialwifi.com/knowledge-base/network-security/most-popular-types-wifi-cyberattacks/ (Pristupljeno 22.6.2022.)

[17] Understanding Denial-of-Service Attacks. Preuzeto sa: https://www.cisa.gov/uscert/ncas/tips/ST04-015 (Pristupljeno 22.6.2022)

[18] What is wardriving? Definition and explanation. Preuzeto sa: https://www.kaspersky.com/resource-center/definitions/what-is-wardriving (Pristupljeno 22.6.2022.)

[19] WEP, WPA, WPA2 and WPA3: Differences and explanation. Preuzeto sa: https://www.kaspersky.com/resource-center/definitions/wep-vs-wpa (Pristupljeno 26.6.2022.)

[20] Survey on Wireless Network Security. Preuzeto sa: https://www.researchgate.net/publication/353226520_Survey_on_Wireless_Network_Security (Pristupljeno 19.6.2022)

[21] 15 years of Wi-Fi. Preuzeto sa: https://fon.com/fon-wifi-infographic/ (Pristupljeno 13.7.2022.)

[22] The History of Public Wi-Fi and Why it has Become a Problem. Preuzeto sa: https://goosevpn.com/blog/the-history-of-public-wi-fi-and-why-it-has-become-a-problem (Pristupljeno 13.7.2022.)

[23] Public Access: Past and Present. Preuzeto sa: https://a4ai.org/news/public-access-past-and-present/ (Pristupljeno 13.7.2022.)

[24] Next-Gen Connectivity & 5G. Preuzeto sa: http://wififorward.org/issues/next-gen-connectivity-5g/ (Pristupljeno 13.7.2022.)

[25] Gait recognition using wifi signals. Preuzeto sa: https://dl.acm.org/doi/abs/10.1145/2971648.2971670 (Pristupljeno 13.7.2022.)

[26] A Study of Wi-Fi Security in City Environment. Preuzeto sa: https://www.researchgate.net/publication/336880475_A_Study_of_Wi-Fi_Security_in_City_Environment (Pristupljeno 10.8.2022.)

[27] Practicing safe public wi-fi - Assessing and managing data-security risks. Preuzeto sa: https://www.researchgate.net/publication/312043761_Practicing_safe_public_wi-fi_-_Assessing_and_managing_data-security_risks (Pristupljeno 10.8.2022.)

[28] A study of security awareness in using wireless networks. Preuzeto sa: https://www.researchgate.net/publication/303130122_A_study_of_security_awareness_in_using_wireless_networks (Pristupljeno 10.8.2022.)

[29] Prvi rezultati popisa stanovništva 2021. Dostupno na: https://bit.ly/3npJZVK (Pristupljeno 15.7.2022.)

[30] Broj noćenja TZ Splitsko dalmatinske županije u 7. mjesecu 2021. Preuzeto sa: https://www.dalmatia.hr/wp-content/uploads/2021/12/7srpanj2021eVisitor04082021-u-1005.pdf (Pristupljeno 15.7.2022.)

[31] Broj noćenja TZ Splitsko dalmatinske županije u 8. mjesecu 2021. Preuzeto sa: https://www.dalmatia.hr/wp-content/uploads/2021/12/8kolovoz2021eVisitor0609u0740.pdf (Pristupljeno 15.7.2022.)

[32] Vistumbler. Preuzeto sa: https://www.vistumbler.net (Pristupljeno 6.9.2022.)

Popis kratica i akronima

AAA	engl. Authentication, Authorization, Audit
AES	engl. Advanced Encryption Standard
AP	engl. Access Point
CCMP	engl. Counter Mode Cipher Block Chaining Message Authentication
CIA	engl. Confidentiality, Integrity, Availability
CSMA	engl. Carrier Sense Multiple Access
DDoS	engl. Distributed Denial of Service
DoS	engl. Denial of Service
DPP	engl. Device Provisioning Protocol
DSSS	engl. Direct Sequence Spread Spectrum
EIRP	engl. Effective Isotropic Radiated Power
FHSS	engl. Frequency Hopping Spread Spectrum
IEEE	engl. Institute of Electrical and Electronics Engineers
IoT	engl. Internet of Things
IP	engl. Internet Protocol
ISM	engl. Industrial, Scientific and Medical
KRACK	engl. Key Reinstallation Attacks
LAN	engl. Local Area Network
LLC	engl. Logical Link Control
MAC	engl. Medium Access Control

MAN	engl. Metropolitan Area Network
MIMO	engl. Multiple Input Multiple Output
MITM	engl. Man in the Middle
MU-MIMO	engl. Multi-User Multiple Input Multiple Output
NFC	engl. Near Field Communication
OFDM	engl. Orthogonal Frequency Division Multiplexing
OSI	engl. Open Systems Interconnection
PDA	engl. Personal Digital Assistant
QAM	engl. Quadrature Amplitude Modulation
QR	engl. Quick Response
RSN	engl. Robust Security Network
RSSI	engl. Received Signal Strength
SSID	engl. Service Set Identifier
TKIP	engl. Temporal Key Integrity Protocol
VPN	engl. Virtual Private Network
WAN	engl. Wide Area Network
WEP	engl. Wired Equivalent Privacy
WLAN	engl. Wireless Local Area Network
WPA	engl. Wi-Fi Protected Access
WPA2-EAP	engl. WPA2 Enterprise Mode
WPA2-PSK	engl. WPA2 Pre-shared Key

Popis slika

Popis tablica

Popis grafikona

PRILOG

Anketni upitnik pod nazivom **Svjesnost korisnika o sigurnosnim rizicima korištenja Wi-Fi mreža**:

Jezik/language:

- hrvatski
- english

Svjesnost korisnika o rizicima korištenja Wi-Fi mreža

1. Spol:

- muško
- žensko

2. Dob:

- 18-24 godine
- 25-35 godina
- 36-50 godina
- 51-65 godina
- 65+ godina

3. Jeste li upoznati s terminima WEP, WPA, WPA2, WPA3?

- u potpunosti sam upoznat s tim terminima
- znam što predstavljaju, ali ne znam što znače te kratice
- uopće ne znam što je to

4. Znate li na kojem kanalu radi vaša kućna Wi-Fi mreža?

- znam
- nisam siguran/na
- ne znam što je kanal kod Wi-Fi mreže

5. Znate li na kojoj frekvenciji radi vaša kućna Wi-Fi mreža?

- samo na 2.4 GHz

- samo na 5 GHz
- i 2.4 i 5 GHz
- ne znam

6. Jeste li mijenjali lozinku na svojoj kućnoj Wi-Fi mreži kad ste ju uveli?

- jesam
- nisam, ne zamaram se time
- ne razumijem pitanje

7. Znate li što znače izrazi DoS, DDoS, MITM, MAC spoofing?

- poznajem sve izraze
- poznajem neke od tih izraza
- ne znam nijedan od tih izraza

8. Kada ste kod nekoga u gostima, spajate li se na njihovu kućnu Wi-Fi mrežu?

- da, uvijek
- ponekad
- ne, nikad
- ovisi kod koga sam

9. Spajate li se na javne i/ili gradske besplatne Wi-Fi mreže?

- da, uvijek
- ponekad
- samo ako procijenim da je mreža
- sigurna za povezivanje
- ne, nikad

10. Je li Vam se ikad dogodilo da ste saznali da se netko neovlašteno povezao na Vašu kućnu Wi-Fi mrežu?

- da, više puta
- da, jednom

- ne, nikad

11. Koristite li bankovna plaćanja putem Interneta?

- da
- ne

12. Osjećate li se sigurno kad se spajate na tuđu Wi-Fi mrežu?

- da, osjećam se sigurno
- ponekad razmišljam može li se nešto loše dogoditi prilikom spajanja na tuđu mrežu
- ne, strah me spajati se na tuđe Wi-Fi mreže
- uopće ne razmišljam o tome

13. Razmišljate li često o sigurnosnim rizicima Wi-Fi mreža?

- da, vrlo često
- ponekad
- rijetko
- nikad

User awareness about Wi-Fi networks security risks

1. Gender:

- male
- female

2. Age:

- 18-24 years
- 25-35 years
- 36-50 years
- 51-65 years
- 65+ years

3. Are you familiar with terms WEP, WPA, WPA2, WPA3?

- I am fully familiar with these terms

- I know what they represent, but I don't
- know what those abbreviations mean
- I don't know what it is

4. Do you know which channel your home Wi-Fi network is on?

- yes, I know
- I'm not sure
- I don't know what a Wi-Fi network
- channel is

5. Do you know what frequency your home Wi-Fi network works on?

- 2.4 GHz only
- 5 GHz only
- GHz and 5 GHz
- I don't know

6. Did you change the password on your home Wi-Fi network when you got it installed?

- yes, I did
- I didn't, I don't bother with that
- I don't understand the question

7. Do you know what the terms DoS, DDoS, MITM, MAC spoofing mean?

- I know all the terms
- I know some of those terms
- I don't know any of those terms

8. When you are at someone's house, do you connect to their home Wi-Fi network?

- yes, always
- sometimes
- no, never
- it depends who I'm at

9. Do you connect to public and/or city free Wi-Fi networks?

- yes, always
- sometimes
- only if I judge that the network is safe to
- connect to
- no, never

10. Have you ever found out that someone has unauthorized access to your home Wi-Fi network?

- yes, more than once
- yes, once
- no, never

11. Do you use bank payments via the Internet?

- yes
- no

12. Do you feel safe when you connect to someone else's Wi-Fi network?

- yes, i feel safe
- sometimes I wonder if something bad
- can happen when connecting to
- someone else's network
- no, I'm afraid to connect to other
- people's Wi-Fi networks
- I don't think about it at all

13. Do you often think about the security risks of Wi-Fi networks?

- yes, very often
- sometimes
- rarely
- never

Sveučilište u Zagrebu

Fakultet prometnih znanosti

Vukelićeva 4, 10000 Zagreb

IZJAVA O AKADEMSKOJ ČESTITOSTI I SUGLASNOSTI

Izjavljujem i svojim potpisom potvrđujem da je _____diplomski rad_____

(*vrsta rada*)

isključivo rezultat mojega vlastitog rada koji se temelji na mojim istraživanjima i oslanja se na objavljenu literaturu, a što pokazuju upotrijebljene bilješke i bibliografija. Izjavljujem da nijedan dio rada nije napisan na nedopušten način, odnosno da je prepisan iz necitiranog rada te da nijedan dio rada ne krši bilo čija autorska prava. Izjavljujem, također, da nijedan dio rada nije iskorišten za bilo koji drugi rad u bilo kojoj drugoj visokoškolskoj, znanstvenoj ili obrazovnoj ustanovi.

Svojim potpisom potvrđujem i dajem suglasnost za javnu objavu diplomskog rada pod naslovom _____Ispitivanje sigurnosti Wi-Fi mreža u javnom okruženju_____ , u Nacionalni repozitorij završnih i diplomskih radova ZIR.

Student/ica:

U Zagrebu, __6.9.2022.___ _____

(ime i prezime, *potpis*)