Aleksa Mitić[3], Slobodan Andžić[4], Miloš Radosavljević[5]

BEZBEDNOST BEŽIČNIH LOKALNIH MREŽA

UDK: 005.934:004.732 Pregledni rad

Rezime

Bežična lokalna mreža ili WLAN može se definisati kao bežično povezivanje dva ili više uređaja u lokalnu mrežu, unutar ograničenog prostora putem radiotalasa. U radu smo se ograničili na sam Wi-Fi. Wi-Fi je zapravo WLAN koji počiva na standardu IEEE 802.11. Prednost ovih mreža u odnosu na žičane mreže, ogleda se u mobilnosti klijenta, lakoj mogućnosti proširivanja i brzom i jeftinom uspostavljanju privremene mreže. Cilj ovog rada je upoznavanje sa osnovnim IEEE standardima i ovladavanje u oblasti bezbednosti WLAN-a, odnosno upoznavanje sa bezbednosnim mehanizmima zaštite koje postoje u samoj bežičnoj lokalnoj mreži. Da bi uspeli u tome, ovaj rad je podeljen na nekoliko celina. Prvo će biti reči o samom pojmu WLAN-a i njegovom načinu rada, zatim ćemo se upoznati sa njegovim osnovnim standardima i najnovijem standardu Wi-Fi 6, a onda će biti reči o bezbednosnim protokolima. Na kraju samog rada, ostavlja se mesto za praktičan deo zaštite jednog WLAN-a, kao i za mitove i savete koji se tiču same bezbednosti.

Ključne reči: bežične mreže, bezbenost mreža, lokalne mreže.

[3] Univerzitet za poslovne studije Banja Luka, Bosna i Hercegovina, aleksamitic@hotmail.com ORCID 0009-0002-3694-0240

[4] Beogradska akademija poslovnih i umetničkih strukovnih studija, Beograd, Srbija, s.andzic@bbs.edu.rs 0009-0006-0304-6401

[5] Visoka škola strukovnih studija biznisa BIZNIS, Niš, Srbija, radosavljevicm93@gmail.com ORCID 0000-0001-6449-9531

Uvod

WLAN (bežična lokalna mreža) je računarska mreža koja nam omogućava da pristupimo mrežnim resursima bez potrebe da se fizički povežemo na mrežu. WLAN koristi kratkotalasne signale između transmitera i prima i šalje mrežne pakete na isti način kao u žičanim (Eternet) mrežama. (Link University, 2020)

Postoje dva načina rada bežičnih mreža: **ad-hoc** (IBSS- Independent Basic Service Set) i **infrastrukturni** (BSS- Basic Service Set). Mreža ad-hoc uspostavlja se direktno između dva ili više računara (P2P- Peer-to-Peer). Nedostatak ovog načina rada je što svi umreženi računari moraju biti u relativno malom prostoru zbog male snage njihovih antena, pa se ovakav tip mreža uglavnom i ne koristi.

U infrastrukturnom načinu rada klijenti komuniciraju preko (bežičnih) pristupnih tačaka (WAP[6]). Pristupne tačke su zapravo uređaji (bežični ruteri) preko kojih klijenti mogu dobiti pristup mreži. Prednost ovog načina je bolji kvalitet signala, veća fleksibilnost u radu i veći domet signala. Osnovno područje rada bežičnog rutera je *mikroćelija*, odnosno prostor kojim je pokriven signal. Ona se može proširiti dodavanjem još bežičnih rutera, ali to proširenje mora od 10 do 15% preklopiti, kako ne bi dolazilo do gubljenja signala. (Плескоњић, Мачек, Ђорђевић, & Царић, Сигурност рачунарских мрежа, 2006)

Standardi (protokoli) u WLAN-u

Protokol, sam po sebi, služi kako bi nešto bilo standardizovano i na identičan način korišćeno od strane kako korisnika, tako i od proizvođača mrežne opreme. 802.11 je grupa protokola donesena od strane IEEE, standardizovanog tela s ciljem implementacije i razvoja bežične mreže. (CERT.hr, 2019)

Predviđena su tri načina realizacije fizičkog sloja standarda IEEE 802.11. Prvi je koristio prenos signala u *infracrvenom* opsegu spektra, a druga dva omogućavaju radio-prenos podataka upotrebom *tehnika proširenog spektra*, u frenkvencijskom opsegu od 2,4 GHz do 2,4835 GHz. Podržan je prenos na brzinama od 1 Mb/s i 2 Mb/s. (Васиљевић, Интернет протоколи и технологије, 2013)

[6] Wireless Access Point

Standard 802.11a je teoretski podržavao brzine do 54 Mb/s, ali realne brzine koje je mogao dostići su bile maksimalno 24 Mb/s. Ovaj standard, za razliku od standarda 802.11b, koristi OFDM[7] tehnologiju na frenkvencijskom opsegu od 5GHz i svoju primenu nalazi u poslovnim okruženjima gde nije bilo potrebe za signalom van jedne prostorije, a gde veće brzine igraju važnu ulogu. (Цвејић, 2016)

Standard 802.11b funkcioniše na frenkvencijskom opsegu od 2.4 GHz i podržava maksimalne brzine od 11 Mb/s. Međutim, veliki broj prepreka je dovodio do smanjenja brzina od 11 Mb/s do 1 Mb/s. Najveći problem sa ovim standardom leži u činjenici da mnogi kućni uređaji rade na frenkvencijskom opsegu od 2,4 GHz, što može dovesti do interferencija signala. (Цвејић, 2016)

Standard 802.11g je poboljšana verzija 802.11b, koja nastaje 2003. godine. Koristi OFDM tehnologiju i radi na frenkvencijskom opsegu od 2,4 GHz. Teoretski može da dostigne brzine od 54 Mb/s. (Васиљевић, Интернет протоколи и технологије, 2013)

Standard 802.11n (Wi-Fi 4) je izdat 2009. godine. Predviđen je rad u oba frenkvencijska opsega, 2,4 GHz i manje korišćeni 5 GHz. Planirane su brzine od 600 Mb/s i korišćenje OFDM i MIMO[8] tehnologije. Tehnologija MIMO koristi više antena (prostorno raspoređenih) i multuputno prostiranje signala u četiri odvojena toka podataka. (Васиљевић, Интернет протоколи и технологије, 2013)

Standard 802.11ac (Wi-Fi 5) je nastao 2013. godine i donosi poboljšanja u MIMO tehnologiji, nazvanom MU-MIMO[9], koji koristi 8 antena, od kojih svaka može teoretski da prenese 433 Mb/s. Ovaj standard funkcioniše na frenkvencijskom opsegu od 5 GHz i svoje probleme rešava korišćenjem Beamforming tehnologije (pojačanje signala prema poziciji prijemnika). (Цвејић, 2016)

Budućnost standarda 802.11 (Wi-Fi 6)

Wi-Fi je poput vazduha ili vode. Postao je toliko sveprisutan da ga shvatamo zdravo za gotovo. Danas ljudi imaju besplatan pristup Internetu u svim većim gradovima, gde je brzina postala takmičenje između njih. Vlade se takmiče kako i na koji način će

[7] Orthogonal Frequencz Division Multiplexing
[8] Multiple Input – Multiple Output
[9] Multi-User Multiple Input – Multiple Output

ponuditi javan besplatan Internet i time privući preduzeća, ljude i time pružiti im isplativ pristup informacijama. Novi standard WiFi 6 je najnaprednija tehnologija koja je na raspolaganju za sve to. (GovInsider, 2019)

Wi-Fi 6 (Standard 802.11ah) je zvanično predstavljen 2018. godine i donosi brojne inovacije koje povećavaju efikasnost protoka, ali je ostavljena i mogućnost da se specifikacije koriste i na frenkvencijama koje bi se oslobodile u budućnosti. Regulatorna tela, poput američke Federalne komunikacione komisije i Evropske komisije, razmatraju „oslobađanje" frenkvencijskog ospega 5925-7125 MHz za nelicencirano korišćenje, pa je 2019. godine predloženo da se komunikacija između vozila koja se koristi u svrhe bezbednosti saobraćaja, izmesti na 5,9 GHz. Značaj uvođenja ospega na 6 GHz ima veliki značaj, s obzirom na to da će zbog širine od čak 1,2 GHz i naprednih tehnika biti znatno efikasniji. (Мировић, 2020)

Međutim, savremeni uređaji koji rade na frenkvencijskom opsegu od 6 GHz neće moći da se koriste za frenkvencijski opseg od 5 GHz, te iz tog razloga je Wi-Fi 6 ipak radi na manjim frenkvencijskim opsezima.

Pomenuti **Wi-Fi 6** je dizajniran isključivo za javna mesta gde ima puno ljudi, poput železničkih stanica, stadiona ili aerodroma. Dalje biće koristan kada je u pitanju IoT[10] ili recimo u kompanijama koje zahtevaju korišćenje aplikacija poput videokonferencija. Sam standard nudi *duže trajanje baterije, poboljšanje performansi* i *proširenje pokrivenosti*. Ono što je važno jeste da se standard slojevito nadovezuje na MU-MIMO sa LTE tehnologijom koja se naziva OFDMA[11] i da omogućava gotovo 40% povećanje čiste propusnosti zahvaljujući QAM[12] modulaciji. Na laičkom jeziku, prema Zeusu Kerevalu, raniji Wi-Fi je bio kao dugi red klijenata koji čekaju jednog blagajnika u banci, dok je MU-MIMO označavao četiri blagajnika koji mogu

[10] Internet of Things
[11] Orthogonal Frequency Division Multiple Access
[12] Quadrature Amplitude Modulation

uslužiti četiri reda klijenata, dok je OFDMA značio da svaki blagajnik može istovremeno poslužiti četiri klijenta. U odnosu na Wi-Fi 5 (802.11as) koji radi na frenkvencijskom opsegu od 5 GHz, Wi-Fi 6 radi na frenkvencijskim opsezima od 2,4 GHz i od 5 GHz i uvodi tehnologiju zvanu „target wake time“, koja se koristi za poboljšanje učinkovitosti buđenja i spavanja na pametnim telefonima. (Џаја, 2019)

Bezbednosni protokoli u WLAN-u

Pored toga što su bezbednosni protokoli definisani standardima, činjenica je da je WLAN najslabija bezbednosna karika neke organizacije. Sami standardi ne zadovoljavaju tri osnovna bezbednosna zahteva. To su *autorizacija korisnika, pouzdana autentifikacija korisnika* i *zaštita privatnosti*. Većina organizacija koje imaju WLAN oslanjaju se na zaštitu definisanu standardima ili, da nesreća bude veća, ne koriste nikakve bezbednosne protokole. (Плескоњић, Мачек, Ђорђевић, & Царић, Сигурност рачунарских мрежа - приручник за лабораторијске вежбе, 2006)

WEP (Wired Equivalent Privacy)

WEP je definisan u standardu 802.11 i za cilj ima integritet poruka, poverljivost podataka i kontrolu pristupa. Na sloju veze OSI[13] modela, WEP se koristi radi zaštite podataka. (Плескоњић, Мачек, Ђорђевић, & Царић, Сигурност рачунарских мрежа, 2006)

Postoje dve vrste autentifikacije: ***sistem otvorene autentifikacije*** i ***sistem autentifikacije deljenim ključem***. Prva autentifikacija dozvoljava bilo kojem bežičnom uređaju da pristupi WLAN-u, a druga zahteva da klijent i bežični ruter imaju identičan ključ za autentifikaciju. Prva opcija se najčešće koristi kod javnih bežičnih rutera – „hot-spots“, a druga opcija se praktično i ne koristi, jer napadač može lako provaliti ključ samim prisluškivanjem saobraćaja. (Васиљевић, Михајловић,

[13] Open Systems Interconnection Reference Model

Рокнић, & Гавриловић, 2012)

WEP proces šifrovanja se sastoji od sledećih koraka. Prvo klijent uspostavlja konekciju sa (bežičnim) ruterom, onda klijent kreira oznaku podataka koristeći CRC-32[14] algoritam i kači je na kraju okvira podatka, zatim paket se šifruje sa RC4 algoritmom i šalje se preko bežične lokalne mreže. Bežični ruter prima paket i dešifruje ga koristeći tajni ključ i na kraju on proverava CRC-32 i šalje paket u lokalnu mrežu. (Link University, 2020)

Sama bezbednost WEP-a zasnovana je na tajnosti ključa. Uvođenjem *inicijalizovanog vektora* (IV) je rešilo problem pravilne upotrebe RC4 algoritma koji zahteva da se ista vrednost ključa nikada ne koristi više puta. Međutim, javlja se problem u samoj arhitekturi WEP-a. Naime, veličina polja u kojem se nalazi IV je mala (svega 24 bita) i što se IV šalje bez šifrovanja, a to je sve zbog toga što prijemna strana mora da zna vrednost IV kako bi mogla da generiše isti ključ i da dešifruje podatke. (Васиљевић, Михајловић, Рокнић, & Гавриловић, 2012)

Postoje dve vrste *napada na WEP*: ***pasivni*** i ***aktivni***. Kod prve vrste napada vrši se pasivno prisluškivanje i analiza prikupljenog mrežnog saobraćaja, a kod druge napadač utiče na komunikaciju tako što menja podatke i ometa saobraćaj (ponavljanje vektora, obrtanje bitova, napad čovek u sredini, ponavljanje paketa) (Mihajlović, Todorov, 2024).

Primer napada ponavljanjem paketa na WEP, u teoriji, je kada su Flučer i saradnici iskoristili slabost u samom RC4 algoritmu (Vasilkov, 2025). Naime, utvrdili su da se neki bitovi mnogih ključeva po pravilu mogu izvesti iz neprekidnog ključa i da se ceo ključ može otkriti vrlo lako, ukoliko se takav napad uzastopno ponavlja i objavili rezultate. U praksi, nakon što su saznali za otkriće Flučera i saradnika, jedan student na letnjem kursu i dva istraživača su za samo sedam dana provalili prvi 128-bitni ključ jedne industrijske bežične lokalne mreže i time potvrdili teoriju, a svoje rezultate objavili. Nakon objave rezultata „provalnika“, CNN je objavio prilog pod naslovom „Novopečeni

[14] Cyclic Redundancy Check

hakeri razbijaju bežične šifre“ u kome su ljudi iz industrije pokušali da omalovaže njihove rezultate argumentacijom da je to što su uradili bilo sasvim jednostavno posle objavljivanja rezultata Flučera i saradnika. (Tanenbaum & Wetherall, 2011)

WPA/WPA2 (Wi-Fi Protected Access)

WPA je predstavljen 2003. godine, od strane Wi-Fi Alijanse, a **WPA2** 2004. godine i poznatiji je kao **standard 802.11i**. Razlika između WPA i WPA2 je u vrsti algoritma za šifrovanje. Naime, prvi koristi RC4 algoritam, koji je bolje implementiran nego u nesrećnom WEP-u i koji je kompatibilan sa uređajima koji ga koriste, a drugi koristi AES[15] algoritam. WPA i WPA2 mogu raditi u dva režima rada. Prvi je režim za *SOHO*[16] *mreže*, koji koristi *deljeni tajni ključ* (PSK[17]), a drugi režim za *korporacijske mreže*, koji koristi RADIUS[18] server.

WPA i WPA2, za razliku od WEP-a, koriste čitavu hijerarhiju ključeva i svi ključevi se izvode iz *glavnog ključa* (PMK[19]) koji je dužine 256 bitova. PMK se izračunava tako što se 4096 puta računa heš funkcija za PSK u kombinaciji sa SSID oznakom. Jednom kada proračuna PMK, klijent sa bežičnim ruterom kreira *privremeni ključ* (PTK[20]), koji se dobija od PMK-a, nasumičnog broja koji je generisala pristupna tačka (A-nonce) i klijent (S-nonce), MAC adresu rutera i klijenta. (Васиљевић, Михајловић, Рокнић, & Гавриловић, 2012)

WPS (Wi-Fi Protected Setup)

WPS je bezbednosni protokol koji je takođe predstavljen od strane Wi-Fi Alijanse 2006. godine. Cilj ovog protokola je bio olakšati i ubrzati korisnicima pristup bežičnim mrežama. Da bi WPS radio mora biti postavljena lozinka na bežičnom ruteru koja

[15] Advanced Encryption Standard
[16] Small Office/Home Office
[17] Pre-Shared Key
[18] Remote Authentication Dial-In User Service
[19] Pairwise Master Key
[20] Pairwise Transient Key

mora podržavati taj protokol. Međutim, preporuka danas je da se ova opcija ne uključuje ili ako je opcija uključena, da se isključi.

WPS omogućava 4 načina povezivanja. Prvi način povezivanja je jednostavnim pritiskom WPS dugmeta na bežičnom ruteru. Drugi način povezivanja je istovremenim pritiskom WPS dugmeta na bežičnom ruteru i na uređaju koji se spaja na mrežu (npr: bežični štampač). Treći način je povezivanje preko osmokarakternog PIN-a, koji je automatski generisan, a sam korisnik ga ne može menjati. Četvrti i poslednji način povezivanja takođe podrazumeva upotrebu PIN-a. Neki uređaji, koji se spajaju na WLAN, nemaju WPS dugme, ali imaju WPS podršku, koja generiše PIN klijenta. Nakon toga, taj PIN se unosi ručno na bežičnom ruteru i tim unosom se uređaj dodaje na mrežu. (Rusen, 2017)

Evaluacija bezbednosti WLAN-a

Deset saveta profesionalnih mrežnih administratora

Na pitanje ***kako da zaštimo svoju Wi-Fi mrežu***, profesionalni mrežni administratori daju sledećih 10 saveta:

1. Promenite ime (SSID[21]) vaše kućne bežične mreže, ali nikako ne koristite svoje ime i prezime kao SSID.
2. Izaberite jaku (da ima bar 20 karaktera i da uključuje brojeve, slova, kao i razne simbole) i jedinstvenu lozinku za vaš bežični internet.
3. Povećajte bezbednost tako što ćete aktivirati enkripciju mreže.
4. Deaktivirajte WLAN kada niste kod kuće.
5. Pronađite bezbednu poziciju za ruter, tako što ćete ga staviti što bliže sredini kuće, nikako pored prozora.
6. Izaberite jaku lozinku za administratora mreže, kao što je opisano u drugom savetu (Paspalj, Paspalj, Milojević, 2024).
7. Isključite pristup interfejsu rutera na daljinu, tako što ćete pristupiti admin panelu i potražiti „Remote access" ili "Remote Administration".

[21] Service Set Identifier

8. Ažurirajte softver rutera (firmware) na najnovije bezbednosne verzije.
9. Postarajte se da imate dobar „firewall“ u svom sistemu (ako ga ruter već ne poseduje), kako bi pazio na zlonamerne pokušaje pristupa mreži.
10. Zaštitite uređaje koji se najčešće povezuju na vaš WLAN, tako što ćete instalirati sigurnosni softver protiv virusa. (IT Academy, 2020)

Mitovi o bezbednosnim postavkama

WEP je dovoljan za zaštitu. Naravno da je bolja ikakva nego nikakva zaštita, ali ovaj protokol kao što smo videli ima dosta propusta.

Skrivanje SSID-a. Ako sakrijemo naziv bežične mreže, nećemo ga videti kada izlistamo dostupne mreže (Mihajlović et. all, 2024). Međutim, danas postoje razni alati kojima napadač može lako otkriti skrivenu mreža.

Filtriranje po MAC[22] adresama. Ruteri imaju ugrađenu funkciju da omoguće spajanje računara sa samo određenim MAC adresama (hardverska adresa računara). Međutim, danas postoje alati koji menjaju MAC adresu i napadaču je dovoljno da postavi MAC adresu da bude identična sa računarom koji ima pristup mreži.

Ograničavanje/isključivanje DHCP[23] usluge. Da bi računar mogao pristupiti Internetu, potrebno mu je dodeliti lokalnu IP adresu. Taj posao dodele adrese pretežno obavlja ruter preko DHCP usluge i ako isključimo tu funkciju teoretski možemo onemogućiti napadača. Međutim, napadaču je dovoljno da sazna IP adresu mreže i da statički konfiguriše IP adresu iz tog opsega.

Ograničavanje jačine signala. Čak i da smanjimo jačinu signala na jednu prostoriju, na tržištu postoje mrežne kartice koje hvataju signal i na udaljenosti preko 1 kilometar. (CERT.hr,

[22] Media Access Control Address
[23] Domain Host Control Protocol

2019)

Podešavanje bezbednosti WLAN-a na ruteru TP-LINK

Nakon što uđemo u naš omiljeni pretraživač i ukucamo adresu rutera 192.168.1.1 i ukucamo korisničko ime i lozinku administratora, tražimo karticu „***Wireless security***" u okviru zalistka „Wireless". Na ovoj kartici možemo odabrati mehanizam kontrole pristupa koji želimo da koristimo.

Prvi mehanizam kontrole pristupa je WEP protokol i kod njega možemo odabrati dužinu ključa koju želimo da koristimo (40/64 bit, 104/128 bit ili 128/154 bit). Možemo odabrati tip autentifikacije, da li će se koristiti deljeni ključ ili će ona biti otvorenog tipa. Takođe možemo odabrati kog će formata biti naša lozinka – heksadecimalni ili ASCII[24] kod.

Drugi čine WPA-PSK i WPA2-PSK protokoli koji koriste potvrdu integriteta ključeva i čitavu hijerarhiju ključeva za šifrovanje. Ovi mehanizmi zaštite su dosta napredniji i preporučuje se njihovo korišćenje. Da bismo konfigurisali WPA2 mehanizam zaštite za mreže potrebno je opciju „Version" postaviti na „WPA2-PSK", opciju „Encryption" postaviti na „AES", a u polju „PSK Password" treba uneti deljeni ključ.

Ako je tajnost podataka od najvećeg značaja, onda govorimo o trećem mehanizmu kontrole pristupa koji se naziva WPA/WPA2-PSK i može koristiti kod manjih firmi, ali najčešće se koristi u sistemima koji imaju veću mrežnu infrastrukturu (Stankov, Roganović, 2022). Ovaj mehanizam zahteva postojanje RADIUS servera za autentifikaciju, koji proverava da li je klijent koji želi da pristupi mreži postoji u bazi korisnika. Kod WPA/WPA2-PSK mehanizma klijent se prijavljuje kombinacijom korisničko ime/lozinka. (Васиљевић i dr. 2012)

Zaključak

Kao što smo rekli, WLAN je bežična lokalna mreža u kojoj se dva ili više uređaja povezuju putem radiotalasa. Saznali

[24] American Standard Code for Information Interchange

smo da za sad postoje 6 verzija standarda IEEE 802.11. Iako je izašla najnovija verzija, standard Wi-Fi 6, sa svojom izuzetnom OFDMA tehnologijom, ona se ipak ne koristi još uvek toliko, s obzirom na današnju cenu uređaja koji podržavaju ovaj standard. Danas je najviše najrasprostanjen standard 802.11n, koji radi u dva osega, 2,4 GHz i 5 GHz i koristi čuvenu MIMO tehnologiju.

Činjenica je da su bežične mreže najslabija karika bezbednosna karika i pored toga što su im bezbednosni protokoli definisani standardima. Međutim, sami standardi ne zadovoljavaju osnovne bezbednosne zahteve poput pouzdane autentifikacije korisnika, zaštite privatnosti i autorizacije korisnika.

Bezbednosni protokoli koji se koriste u WLAN-u su WEP, WPA-PSK ili WPA2-PSK, kombinacija WPA/WPA2-PSK i na kraju WPS kao dodatni protokol u sklopu prethodno navedenih. Poslednji (WPS) se ne preporučuje, kao ni prvi zbog svojih nedostataka koji su izloženi u ovom radu.

WPA/WPA2-PSK se koristi kod manjih firmi, ako je tajnost podataka od najvećeg značaja i ovaj protokol zahteva postojanje RADIUS servera za identifikaciju, odnosno klijent se prijavljuje kombinacijom korisničko ime i lozinka.

Najzad, protokoli koji se najviše preporučuju su WPA-PSK ili WPA2-PSK, koji koriste potvrdu integriteta ključeva i čitavu hijerarhije ključeva za šifrovanje.

Na kraju samog rada, dati su saveti mrežnih administratora, neki mitovi koji se susreću u praksi, kao i postupak podešavanja bezbednosti bežične lokalne mreže, odnosno WLAN-a.

Literatura

1) CERT.hr. (2019). *Sigurnost bežičnih mreža.* Preuzeto april 22, 2020 sa CERT.hr: https://www.cert.hr/NCBrSBM
2) GovInsider. (2019). *The Future of WiFi is here. It will transform cities forever*. https://govinsider.asia/connected-gov/the-future-of-wifi-is-here-it-will-transform-cities-forever/

3) IT Academy. (2020). *Kako da zaštitite svoju Wi-Fi mrežu? 10 saveta profesionalnih mrežnih administratora.* https://www.it-akademija.com/cms/mestoZaUploadFajlove/ITA_Administracija.pdf
4) Link University. (2020). *Bežična mreža (Wireless Network)*. http://www.link-university.com/lekcija/Be%C5%BEi%C4%8Dna-mre%C5%BEa-(Wireless-Network)/5366
5) Rusen, C. A. (2017). *What is WPS (Wi-Fi Protected Setup) and how does it work?* https://www.digitalcitizen.life/simple-questions-what-wps-wi-fi-protected-setup
6) Tanenbaum, A. S., & Wetherall, D. J. (2011). *Computer Networks.* Boston: Pearson Education.
7) Vasiljević, V. (2013). *Internet protokoli i tehnologije.* Beograd: Visoka škola elektrotehnike i računarstva strukovnih studija.
8) Vasiljević, V., Mihajlović, V., Roknić, M., & Gavrilović, P. (2012). *Bežični komunikacioni sistemi - Priručnik za laboratorisjke vežbe.* Beograd: Visoka škola elektrotehnike i računarstva strukovnih studija.
9) Mirović, J. (2020). *Wi-Fi 6: Wi-Fi za 2020. godinu*. https://pcpress.rs/wi-fi-6-wi%E2%80%91fi-za-2020-godinu/
10) Pleskonjić, D., Maček, N., Đorđević, B., & Carić, M. (2006). *Sigurnost računarskih mreža - priručnik za laboratorijske vežbe.* Beograd: Viša elektrotehnička škola.
11) Cvejić, N. Analiza bezbednosti IEEE 802.11 mreža u Nišu i njeni sigurnosni propusti. Fakultet informacionih tehnologija, Beograd.
12) Džaja, J. Bežični sustav WiFi. Fakultet informatike u Puli, Pula.
13) Vasilkov, Z. (2025). Veštačka inteligencija u službi sprovođenja zakona u Evropskoj uniji i Republici Srbiji. *Oditor*, *11*(1), 131-167. https://doi.org/10.59864/Oditor72501ZV

14) Paspalj, M., Paspalj, D. & Milojević, I. (2024). Održivost savremenih ekonomskih sistema. Održivi razvoj, 6 (1), 33-45. https://doi.org/10.5937/OdrRaz2401033P
15) Mihajlović, M., Marković, S., Vujanić, I., P. Marijanović, R., & Hemed Ramadhani, I. (2024). Knowledge and information management in the company as a strategic business resource. *Oditor*, *10*(3), 53-67. https://doi.org/10.59864/Oditor32403MM
16) Mihajlović, M. & Todorov, J. (2024). Analiza uticaja nedostataka resursa i satisfakcija stanovništva. Održivi razvoj, 6(1), 47-62. https://doi.org/10.5937/OdrRaz2401047M
17) Stankov, B. & Roganović, M. (2022). Pružanje podrške i podsticanje razvoja malih i srednjih preduzeća u Evropskoj uniji. Akcionarstvo, 28(1), 21-44.

WIRELESS LAN SECURITY

Abstract

A wireless local area network or WLAN can be defined as the wireless connection of two or more devices in a local area network, within a limited area, by means of radio waves. We limited our work to Wi-Fi itself. Wi-Fi is actually a WLAN based on the IEEE 802.11 standard. The advantage of these networks compared to wired networks is reflected in the mobility of the client, the easy possibility of expansion and the quick and cheap establishment of a temporary network.

The goal of this work is to get familiar with the basic IEEE standards and to master the area of WLAN security, that is, to get to know the security protection mechanisms that exist in the wireless local network itself. In order to succeed in this, this work is divided into several parts. First, we will talk about the very concept of WLAN and how it works, then we will get acquainted

with its basic standards and the latest Wi-Fi 6 standard, and then we will talk about security protocols. At the end of the paper, a place is left for the practical part of protecting a WLAN, as well as for myths and advice concerning security itself.
Key words: wireless networks, network security, local networks.

Datum prijema (Date received): 21.06.2025.
Datum prihvatanja (Dateaccepted):18.10.2025.