INTERNACIONALNI UNIVERZITET TRAVNIK INTERNATIONAL UNIVERSITY OF TRAVNIK

INTERNACIONALNI UNIVERZITET TRAVNIK U TRAVNIKU
FAKULTET INFORMACIONIH TEHNOLOGIJA TRAVNIK U TRAVNIKU

DIPLOMSKI RAD

BEŽIČNE MREŽE, UMREŽAVANJE I BEŽIČNI PRIJENOS

Mentor:
Prof. dr. Mladen Radivojević

Student:
Amna Kulović

Travnik, septembar 2019.

SADRŽAJ

UVOD

U danjašnje vrijeme svaki čovjek se barem jednom susreo sa uređajima koji koriste bežićnu mrežu. Svi se služimo pametnim telefonima s kojima se putem Wi-Fi-ja spajamo na Internet. Spajamo se ili na kućnu mrežu ili na besplatne mreže. Putem Interneta nam je dostupno mnogo toga, možemo da pristipamo društvenim mrežama, da slušamo muziku, gledamo filmove, učimo, itd...

Bežična tehnologija nam omogućava mobilnost i jednostavnost korištenja, ali većina korisnika ne razmišlja o sigurnosti. Korisnici su nedovoljno informisani o opasnostima koje donosi Internet. Mnogo njih ne obraća pažnju na to, a pristupaju važnim podacima kao što su: bankovni računi, e-mail i mnogo drugih sadržaja koji moraju da budu sačuvani i skriveni. Danas je sve više zlonamjernih radnji, gdje hakeri raznim metodama i tehnologijama napdaju račune korisnika zaobilazeći sve zaštite.

Danas je pitanje sigurnosti jedan od prioriteta za svakog korisnika Interneta. Bežična komunikacija je zbog svojih karakteristika izložena napadima zbog načina na koji se oni šalju i pri tome postoji mogućnost presretanja informacija. U standardima koji definišu računarske mreže, postoje određeni standardi sigurnosti, koje ću objasniti kasnije u ovom radu.

U ovom radu će biti opisane bežične mreže, elementi, prednosti, nedostaci i mogućnosti poboljšanja radi veće sigurnosti korisnika. Rad će biti podijeljen na četiri dijela. Prvi dio je uvodni dio, u kojem se opisuje tema rada i problemi koje istražujemo. U drugom dijelu se upoznajemo sa pojmom bežičnih mreža, njihovim karakteristikama, vrstama bežičnih tehnologija i standardima. U trećem dijelu se opisuju bežični uređaji koji se koriste za bežičnu tehnologiju. U četvrtom dijelu opisat ćemo sigurnost bežičnih mreža, sigurnosne mehanizme standarda 802.11, njegove mogućnosti i nadogradnje. Također ću opisati još neke standarde za sigurnost bežičnih mreža.

1. BEŽIČNE MREŽE, UMREŽAVANJE I BEŽIČNI PRIJENOS

Bežične mreže su računarske mreže koje povezuju dva ili više računara koji su povezani adekvatnim medijumom i koji međusobno mogu da komuniciraju i dijele resurse. Korisri se za prijenos kako digitalnih tako i analognih podataka, koji moraju biti prilagođeni odgovarajućim sistemima za prijenos. Mrežom se prenose računarski podaci, govor, slika, video, a aplikacije na stranama korisnika mogu biti takve da se zathjeva prijenos podataka u realnom vremenu(govor, video i sl.) ili to ne mora biti uslov(elektronska pošta, prijenos datoteka i sl.). [1]

Bežični prijenos podataka se počeo koristiti i prije razvoja računarskih komunikacijskih sistema i to za prijenos televizijskih i radijskih programa. Bitna razlika između televizijskih i radijskih programa , i prijenosa podataka je u tome što se u prethodnom slučaju obično želi prenijeti sadržaje većem broju primatelja, i pritom onemogućiti da ti sadržaji budu dosptupni drugima. Kod prijenosa podataka elektromagnetskim signalima u prostoru, ometanje prijenosa (sa strane) je mnogo lakše izvedivo nego što je to slučaj kod prijenosa sadržaja čvrstim vezama (kablovima). Zato je za uspostavu bežičnih komunikaeijskih sustava potrebno riješiti ta dva osnovna problema. Prvo, treba definirati način rada prijenosnog sistema, tako da sadržaje koji su namijenjeni određenom primatelju prima taj primatelj, a pritom budu nedostupni(nerazumljivi,), za sve druge do kojih ti sadržaji(signali) mogu doći. Drugo, prijenosni sistem treba biti otporan na (zlo) namjerna ometanja prijenosa podataka.[2]

Da bi se nemogućilo prisluškivanje ili kopiranje sadržaja prijenosa ili ometanje koriste se različite metode zapisivanja i prijenosa signala. Najpoznatije metode zovu se metode raširenog spektra frekvencija(eng. Spreed Spectrum Techniques), kojima je osnovno načelo da se za zapis i prijenos tih sadržaja koristi širi frekventni pojas od potrebnog. Takav način kodiranja i prijenosa sadržaja omogućava zaštitu i sigurnost sadržaja i smanjenje osjetljivosti prijenosa na vanjske smetnje.

U bežičnim komunikacijskim sistemima postoji puno metoda (ili tehnologija, kako se često nazivaju) zapisivanja i prijenosa sadržaja. U nastavku iznosimo kratke opise tri takve metode: FDMA, TDMA i CDMA. Te metode nazivaju se metodama fizičkog prijenosa podataka u bežičnim sistemima, ali mogu se koristiti i u žičanim sistemima.

FDMA (Frequency Division Multiple Access) znači višestruki pristup s podjelom frekvencija. FDMA je metoda prijenosa podataka kod koje se frekvencije iz nekog šireg pojasa frekvencija dijele na više užih pojaseva frekvencija, koji se nazivaju kanalima.

---

[1] Veinović, M., Jevremović, A.: Uvod u računarske mreže, Beograd, 2007.godine, str.12.
[2] Radovan, M.:Računalne mreže (1), Rijeka, 2010.godina, str.256-257
file:///C:/Users/korisnik/Downloads/vdocuments.mx_racunalne-mreze-1-mario-radovan.pdf

Pritom se svakoj komunikaciji (prijenosu podataka) dodjeljuje jedan kanal iz danog šireg frekventnog pojasa, tako da se u svakom od tih kanala izvodi jedan prijenos. Dakle, u jednom širem frekventnom pojasu odvija se više komunikacija istodobno, svaka u jednom dijelu toga frekventnog pojasa, odnosno u jednom kanalu. To ovdje znači da više komunikacija (ili komunikatora) ima istodobno pristup istom frekventnom pojasu, pri čemu valovi iz toga pojasa imaju ulogu nosioca podataka. Pritom svaka od tih komunikacija koristi jedan dio tog frekventnog pojasa. Od tuda dolazi naziv "višestruki pristup" (jednom frekventnom pojasu). Metoda FDMA je posebno pogodna za prijenos kod analognih komunikacijskih sustava; takvi su bili sustavi prve generacije mobilne telefonije (1G), tako da je FDMA bila glavna metoda zapisivanja i prijenosa sadržaja u mobilnoj telefoniji prve generacije. Ali FDMA se koristi i za prijenos digitalnih signala.

TDMA (Time Division Multiple Access) znači višestruki pristup s podjelom vremena. TDMA je metoda prijenosa podataka kod koje se jedan frekventni pojas (kanal) dijeli na vremenske intervale koji se obično nazivaju otvorima (slots). U svakom od tih intervala (otvora) prenosi se sadržaj jedne komunikacije; svakoj od komunikacija koje dijele jedan kanal dodjeljuje se svaki *n-ti* vremenski interval, i tako u krug; na taj način ostvaruje se "višestruki pristup" tom kanalu kao nosiocu podataka. Dakle, "višestruki pristup" (kanalu) ovdje znači da ta metoda rada omogućava da se na istom kanalu odvija više komunikacija istodobno (ili paralelno), odnosno da više komunikatora ima istodobno "pristup" tom kanalu. Sadržaji svake od tih komunikacija prenose se jedan kratak vremenski interval, i tako ciklički (u krug) za sve komunikacije koje trenutno koriste taj kanal. Ti vremenski intervali su kratki (mjere se u mikrosekundama), tako da se sve komunikacije u jednom kanalu (naprimjer, telefonski razgovori) odvijaju kao da dani kanal kontinuirano prenosi njihove sadržaje. Dakle, kod TDMA, na jednom kanalu (frekventnom pojasu nosivog signala) odvija se prijenos sadržaja većeg broja komunikacija koje međusobno dijele kapacitet tog kanala. Osnovna metoda rada TDMA može se mijenjati i upotpunjavati. Varijanta te metode, koja se naziva dinamička TDMA, dodjeljuje različitim komunikacijama različit broj vremenskih intervala (otvora), u zavisnosti od njihovih prioriteta i zahtjeva. Metoda TDMA pogodna je za prijenos digitalnih sadržaja (okvira), tako da je TDMA bila dominantna metoda zapisivanja i prijenosa sadržaja u mobilnoj telefoniji druge generacije (2G).[3]

CDMA (Code Division Multiple Access) znači višestruki pristup sa podjelom koda (ili kodova). Metoda CDMA spada u klasu metoda koje koriste raširenu spektar frekvencija, čije smo dvije osnovne metode rada (skakutanje frekvencija i izravna sekvencija) opisali iznad. Metoda CDMA je jedan oblik metode izravne sekvencije. Kod metode izravne sekvencije, svaki bit sadržaja (podataka) zapisuje (kodira) se sa *n* bitova; pritom se to kodiranje izvodi prema jednom slučajnom nizu bitova, kojeg se ovdje naziva kodom. Kod metode CDMA, ostvaruje se prijenos sadržaja od većeg broja komunikacija na jednom kanalu: zato govorimo o "višestrukom pristupu" kanalu kao nosiocu podataka. Prijenos sadržaja većeg broja komunikacija ostvaruje se na taj način da svaka

[3] Radovan, M.:Računalne mreže (1), Rijeka, 2010.godina, str.260-262
file:///C:/Users/korisnik/Downloads/vdocuments.mx_racunalne-mreze-1-mario-radovan.pdf

komunikacija koristi poseban (različit) slučajni niz bitova (kodu) pomoću kojeg kodira svoje sadržaje. Sadržaji svih komunikacija zapisuju se na isti kanal (to jest, na nosivi val iste frekvencije), jedan iza drugog, ali bez da se pojedinim komunikacijama dodjeljuju unaprijed zadani vremenski intervali (slotovi). Kodirani zapisi različitih komunikacija međusobno se razlikuju po tome što su kodirani pomoću različitih nizova bitova (koda). Na temelju toga, primatelj - koji poznaje kodove onih komunikacija čije sadržaje prima - razlikuje i razdvaja sadržaje tih komunikacija, koji se prenose pomoću nosivih signala iz istog kanala.

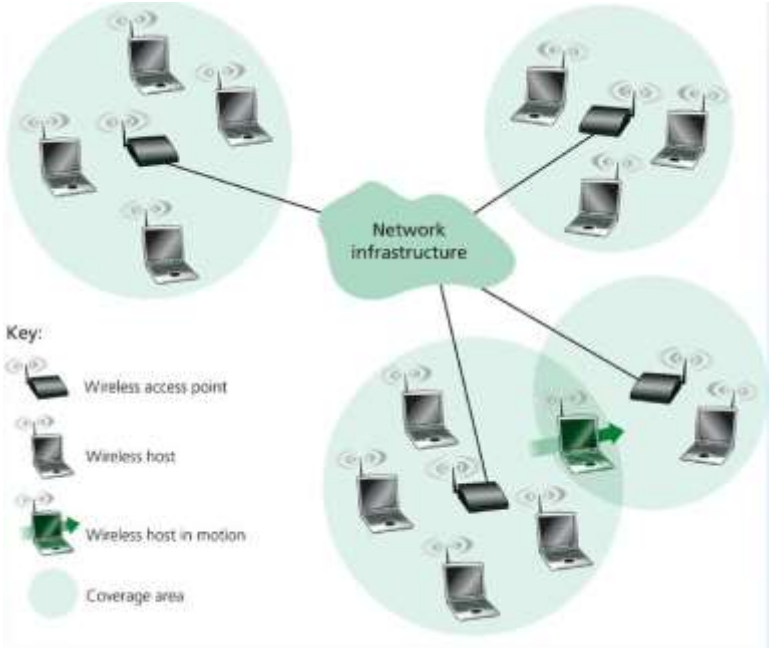
Dakle, CDMA koristi jedan frekventni pojas koji je višestruko širi od onog koji bi bio dovoljan za prijenos podatkovnih sadržaja danom brzinom (propusnošću). Kod te metode, svaki bit sadržaja kodira se (za prijenos) sa više bitova. U svakoj komunikaciji (prijenosu), izvor kodira svoje sadržaje sa posebnom kodom (nizom bitova); na temelju toga primatelj (koji poznaje tu kodu) prepoznaje kodirane sadržaje određene komunikacije i dekodira ("izvlači") te sadržaje iz kodiranih zapisa koje prima. Prijemni sustav primatelja prima "šum" koji nastaje zbrajanjem svih signala koji stižu na taj prijemni sustav. Razdvajanje (filtriranje) signala pojedinačnih komunikacija je zahtjevan proces koji uključuje postupke i metode kojima se ovdje ne trebamo baviti. U svakom slučaju, sadržaji različitih komunikacija kodirani su različitim kodama, što daje osnovu za razdvajanje tih sadržaja, kao i za njihovo dekodiranje. Dakle, na istom kanalu (frekventnom pojasu) odvija se više komunikacija; sadržaji tih komunikacija kodiraju se metodom izravne sekvencije, pri čemu svaka komunikacija koristi različitu kodu za kodiranje svojih sadržaja. Sustavi treće generacije mobilne telefonije (3G) većinom koriste CDMA metodu zapisivanja i prijenosa sadržaja na fizičkoj razini (uz neke dopune); pritom se u 3G govori o širokopojasnoj (wideband) CDMA, koja se označava sa W-CDMA. Širokopojasna CDMA doseže propusnost veza od oko 2 Mbps kod mobitela koji miruju ili se kreću brzinom koraka; kod mobitela u vožnji (autom) predviđena je propusnost od 384 Kbps (ili više). To je ogromno povećanje u odnosu na tehnologiju 2G, kod koje se propusnost obično kreće do 9,6 Kbps. Postoje poboljšanja sustava 2G, koja mogu doseći veće propusnosti, kao što su 28 Kbps, ili preko 100 Kbps; za takve tehnologije kaže se da su 2,5G ili više, ali su ipak manje od 3G.

1.1. Elementi bežične mreže

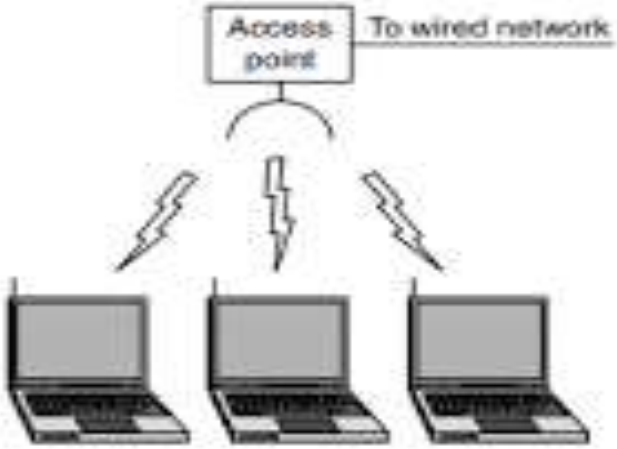
Osnovni elementi bežične mreže prikazani su:

- **čvor bežične mreže (eng. host)** – kao i kod ožičenih mreža, ovo su krajnji uređaji na kojima se izvršavaju aplikacije, a mogu biti stolna, prijenosna i džepna računala.
- **bežične veze** – računara se s baznom stanicom ili drugim računarima unutar mreže povezuju preko bežične komunikacijske veze. Različite tehnologije bežičnih veza karakteriziraju različite brzine prijenosa kao i različiti dometi.
- **bazna stanica** - ključni je gradivni element bežične mrežne infrastrukture zadužen za predaju i prijem podatkovnih paketa ka ili od pojedinih računara unutar mreže, kao i za koordiniranu predaju podataka većem broju računara pridruženih toj baznoj stanici. Pristupne točke (eng. Access Points - AP) kod 802.11 bežičnih mreža tipični su primjeri baznih stanica. Pristupne

tačke ne kontroliraju samo pristup mediju nego djeluju i kao mostovi ka drugim bežičnim i ožičenim mrežama.[4]



Slika 1. Elementi bežične mreže
https://slideplayer.com/slide/14101944/86/images/2/Elementi+be%C5%BEi%C4%8Dne+mre%C5%BEe.jpg



Slika 2. Access point
https://encrypted-tbn0.gstatic.com/images?q=tbn:ANd9GcQTlm3hB7Fgglu8WnhsKagydjZfK2jkyjYWLQEJsTMraX1l9W54hg

[4] https://www.cis.hr/www.edicija/LinkedDocuments/CCERT-PUBDOC-2008-04-225.pdf

1.2. Vrste bežićnih mreža

Osnovna karakteristika bežičnih mreža jeste rad bez korištenja komunikacionih kanala u vidu kablova. Bežične mreže za prenos podataka koriste radio talase ili svjetlosne signale s tim da su radio talasi daleko češće u upotrebi jer za njihovo korištenje nije potrebna optička vidljivost. Jedan od glavnih kriterijuma za kategorizaciju bežičnih mreža jeste udaljenost na kojoj je razmjena podataka putem njih nemoguća. Svaka bežična mreža ima specifičnosti i one se dijele na:

- Wi-Fi
- Bluetooth
- WiMax
- ZigBee
- IrDa
- RFID

1.2.1. Wi-Fi

Bežično (Wi-Fi) umrežavanje je vjerovatno najjednostavniji način umrežavanja, koje nudi srednju brzinu i ne zahtijeva dodatne kablove. Također, obuhvata Wi-Fi kartice (interne ili eksterna), uz koje se obično isporučuju i dogovarajuće antene. Za priključivanje neke mreže potreban je Hotspot, odnosno čvorište na koji se spajaju svi korisnici. Ako je mreža osigurana ona će tražiti WER ili noviji WPA (2) ključ. Ako je slobodna onda nema nikakvih ograničenja za spajanje.

Svako može biti hotspot, jedino umjesto obične kartice je potrebno kupiti Wireless Access Point koji nudi pokrivenost oko 30 metara, ali je uz razne pojačivače moguće proširiti pokrivenost. Najskuplja varijanta je kupiti Wireless Access Point Router koji sadrži priključak za DSL mode, Router, Ethernet Hub, Firewall i Access Point.

Standardi Wi-Fi:

- 802.11a – standard koji ima brzinu od 54 megabita u sekundi, ali najčešće ona iznosi oko 30 Mbps. Ovaj standard je skuplji, jer Wi-Fi kartice koje su zasnovane na ovom standardu rade na većim frekvencijama (5GHz).
- 802.11b – standard koji je predstavljen 1999. godine, u isto vrijeme kada i 802.11. Ova je najjeftinija varijanta Wi-Fi mreže. Brzina protoka u ovakvim mrežama je do 11 Mbps, ali kada ima nekih prepreka brzina spadne i do 2 Mbps.
- 802.11g – standard je predstavljen 2003. godine i ujedinio je prethodna dva standardna. Radi na 2.4 GHz, i ima skoro istu brzinu kao i standard 802.11a.
- 802.11n – je standard koji je predstavljen 2007.godine. Ovaj standard može raditi i na brzini od 2.4 GHz i na 5.4 GHz.[5]

[5] Veinović, M., Jevremović, A.: Uvod u računarske mreže, Beograd, 2007.godine, str.75-76
file:///C:/Users/korisnik/Downloads/US%20-%20Uvod%20u%20ra%C4%8Dunarske%20mre%C5%BEe.pdf

Slika 3. Wi-FI
https://previews.123rf.com/images/mitay20/mitay201305/mitay20130500055/19393710-home-wifi-network-internet-via-router-on-pc-phone-laptop-and-tablet-pc.jpg

1.2.2. Bluetooth

Bluetooth je tehnologija pomoću koje se vrši bežični prenos podataka između uređaja koji posjeduju istu tehnologiju. Bluetooth je tehnologija koja omogućava komunikaciju PDA (personal digital assistent) uređaja, mobilnih telefona, lap.top računara, PC računara, digitalnih foto-aparata i kamera. Bluetooth emituje ultra-ljubičaste zrake do drugog Bluetooth uređaja i tako je odvija komunikacija. Bluetooth je bežični standard koji je namijenjen niskopotrošnim uređajima sa kratkim dometom (od 10cm do 100m) i koji u sebi sadrži primopredajnik.[6]

Slika 4. Bluetooth
http://manuals.denon.com/DSB100/ALL/EN/fig/Bluetooth_Multi_Point_DSB100_BONDILoaiekyeh.png

[6] https://www.seminarski-diplomski.co.rs/INFORMATIKA/Bluetooth.html

Bluetooth specifikaciju razvili su 1994. godine Jaap Haarsten i Sven Mattisson, zaposlenici firme „Ericsson Mobile Platforms“ u Švedskoj. Udruga Bluetooth SIG, koju su osnovale tvrtke Ericsson, IBM, Intel, Toshiba i Nokia, obradila je te javno objavila specifikaciju 20. marta 1998. godine. Prva verzija protokola bila je Bluetooth 1.0, koja je ubrzo proširena određenim nadopunama na verziju Bluetooth 1.0B. Zbog brojnih problema u tim specifikacijama, proizvođači su imali problema s omogućivanjem međusobne komunikacije njihovih uređaja. Također, specifikacije su uključivale prenos BD_ADDR (eng. Bluetooth hardware device address) adresa pa nije bilo moguće osigurati anonimnost. Mnoge pogreške pronađene u Bluetooth specifikaciji ispravljene su u novoj verziji pod nazivom Bluetooth 1.1., koja je dobila oznaku IEEE (eng. Institute of Electrical and Electronics Engineers) standarda 802.15.1-2002. Između ostalog, dodana je podrška za nekriptirane kanale te uvedeno mjerenje RSSI (eng. Received Signal Strength Indicator) vrijednosti, tj. snage u prijamnom radio kanalu. Sljedeća verzija bila je Bluetooth 1.2, koja je u potpunosti sukladna s prethodnom verzijom uz sljedeća poboljšanja:

- brže povezivanje i otkrivanje uređaja,
- veća brzina prijenosa podataka,
- bolja kvaliteta govora preko audio kanala,
- uvedena provjera toka podataka.

Opisana verzija poznata je kao IEEE standard 802.15.1-2005. Verzija Bluetooth 2.0 objavljena je 10. novembra 2004. godine, a osnovna razlika u odnosu na prethodnu verziju je uvođenje bržeg prijenosa podataka. To je postignuto korištenjem tehnologije EDR (eng. Enhanced Data Rate), čija je nominalna brzina oko 3 Mbps. Prednosti koje donosi spomenuta tehnologija su:[7]

- tri puta veća brzina prijenosa podataka,
- smanjena složenost korištenja više simultanih veza i
- smanjena uporaba energije.

Sljedeća verzija koju je organizacija Bluetooth SIG objavila bila je Bluetooth 2.1, objavljena 26. jula 2007. i imala je sljedeća obilježja:

- EIR (eng. Extended Inquiry Response)
- EPR (eng. Encryption Pause/Resume)
- SSP (eng. Secure Simple Pairing)
- NFC (eng. Near Field Communication)
- NAF-PBF (eng. Non-Automatically-Flushable Packet Boundary Flag)

Dodatne specifikacije donosi verzija Bluetooth 3.0, objavljena 21. aprila 2009. Novosti koje uvodi ova verzija su:

[7] Ranjivosti Bluetooth tehnologije, str.6
https://www.cert.hr/wp-content/uploads/2019/04/NCERT-PUBDOC-2009-11-281.pdf

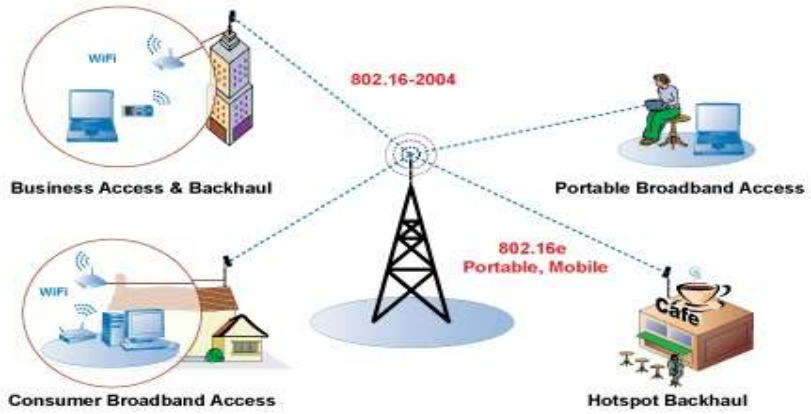
- AMP (eng. Alternate MAC/PHY)
- UCD (eng. Unicast Connectionless Data)
- otkrivanje veličine ključa za kriptiranje
- uveden dodatni nadzor energije

Posljednja verzija koja je objavljena je Bluetooth low energy, koja je objavljena 20. aprila 2009. Svojstva ove verzije su:

- Kanali za višeodredišno razašiljanje (eng.broadcast)
- Upravljanje topologijom
- Poboljšanje QoS (eng. Quality of Service)[8]

1.2.3. WiMax

WiMax je bežična tehnologija koja nam omogućava širokopojasni bežični pristup internetu uz upotrebu radio frekvencijskog spektra od 1 do 11 GHz. WiMax tehnologija je zasnovana na Ethernetu, porodici normi IEEE802. Postoje dva različita podstandarda koji nisu međusobno kompaktibilni, a razlika je prije svega u fizičkom sloju. Prvi od njih je IEEE 802.16-2004 (fiksni WIMAX) koji je objavljen 2004. godine. On se trenutaþno koristi, dok je drugi IEEE 802.16e standard (mobilni WIMAX) službeno objavljen u veljaþi 2006. Standard 802.16d je namijenjen fiksnoj mreži kao cjenovna alternativa kabelskom ili DSL uslugama. Standard IEEE 802.16e uveden je s namjerom da omogući korištenje u mobilnim aplikacijama. Nazvan je Mobile WiMAX, iako ga je moguüe koristiti i za fiksne aplikacije te se i u tom segmentu uporabe postižu značajne prednosti.[9]



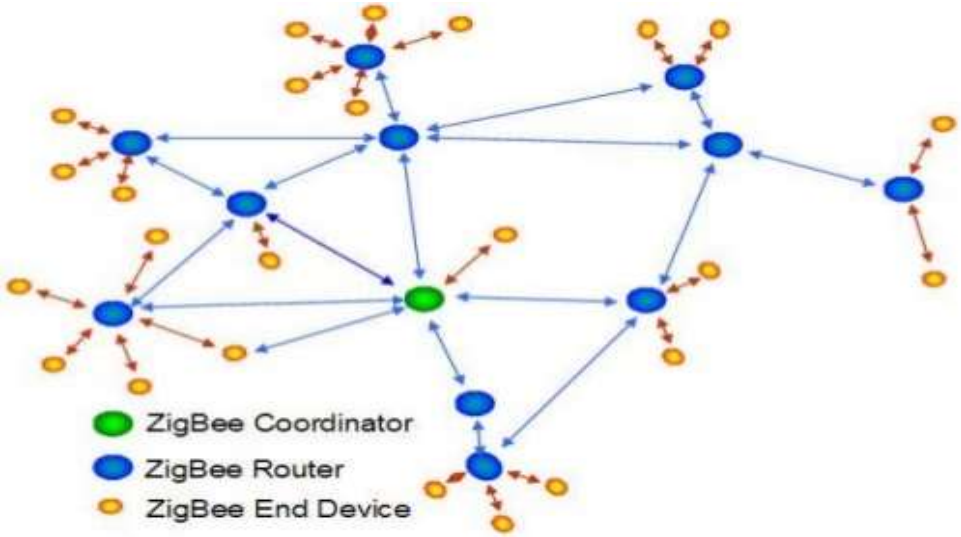
Slika 5. WiMax
https://www.lopol.org/sites/default/files/public/technology/uploaded-images/image-wimax-network.jpg

[8] Ranjivosti Bluetooth tehnologije, str.7
https://www.cert.hr/wp-content/uploads/2019/04/NCERT-PUBDOC-2009-11-281.pdf
[9] Padarić D.,Kukec M.,Veleučilište u Varaždinu, Varaždin, Hrvatska: WiMax 802.16 standard, str.54
file:///C:/Users/korisnik/Downloads/TG_1_2_2009_Padaric_Kukec_WIMAX_802_16_standard.pdf

1.2.4. ZigBee

ZigBee je mrežni protokol namijenjen za bežične privatne mreže sa malom potrošnjom energije kao što su senzorske mreže, te mreže za kotrolu, nadzor ili upravljanje. Temelje ZigBeea je IEEE specifikacija 802.15.4 za bežične privatne mreže (WPAN – wireless personal area networks) sa malom propusnošću. Ta specifikacija ne odreuđje samo malu propusnost mreže, već i malu potrošnju energije, te malu složenost. Propusnost je ograničena na 250 kbps na 2,4 GHz području, 20 kbps na 868 MHz (Europa) i 40 kbps na 915 MHz (Sjeverna Amerika i Australija) tzv. ISM (industrial, scientific and medical) frekvencijskom području. ZigBee je, kao nadogradnja na IEEE specifikaciju, izdala udruga ZigBee Alliance u kojoj su vodeći svjetski proizvođači.

ZigBee protokolarni niz je veoma jednostvan, te se djelomično temelji na OSI (open system interconnect) modelu. Na fizičkom sloju su definisana dva tipa uređaja: FFD (full functional device) i RFD (reduced functional device). Mrežni sloj i aplikacijski interfejs je razvila firma ZigBee Alliance, koji uključuju i sigurnosne mehanizme, te ZigBee ureađj (ZDO – ZigBee Device Object). Ova dva tipa specificiraju postavljanje mreže, odnos između pojednih ureađja u mreži. Aplikacijski sloj je ostavljen na korištenje korisniku, te može sadržavati do 240 raznih aplikacija.



Slika 6. ZigBee mreža
https://image.slidesharecdn.com/zigbeeforhomeautomation-13065323081836-phpapp01-110527165623-phpapp01/95/zigbee-for-home-automation-5-728.jpg?cb=1306515597

ZigBee koristi digitalne odašiljače i prijemnike za komuniciranje između uređaja. Tipična mreža se sastoji od tri vrste uređaja. Mrežni koordinator je uređaj koji konfiguriše mrežu, te upravlja protokom podataka unutar nje. Svaka ZigBee mreža mora imati jednog koordinatora. Ostali uređaji mogu biti routeri, koji kao i koordinator moraju biti FFD, te krajnji uređaji, koji su tipično RFD. Topologije koje su podržane su mreža (mesh),[10]

[10] Sveučilište u Zagrebu, Fakultet elektrotehnike i računarstva, Zavod za elektroničke sustave i obradu informacija, Seminarski rad iz kolegija: Sustavi za praćenje i vođenje procesa, ZigBee, Zagreb, 2006., str. 3-5 http://spvp.zesoi.fer.hr/seminari/2006/AndroBacan_ZigBee.pdf

zvijezda (star) te kombinirana (cluster tree). Zvijezda topologija je korisna ukoliko se radi o malom broju uređaja na nekom prostoru, te mogu komunicirati isključivo sa jednim routerom. Toplogija mreža omogućava više mogućih puteva, te čak i u slučaju isključenja routera može naći alternativni put.

1.2.5. IrDA

IrDa (eng. Infrared data Association) je način prijenosa podataka koji podrazumijeva infracrvene svjetlosne zrake kao osnovne nosioce komunikacije. IrDA adapteri omogućavaju korištenje ovih signala za prijensa podataka između računara. Glvni nedostatak infrared načina prijenosa podataka jeste potreba za optičkom vidljivošću i preciznim usmijerenjem svjetlosti kao i mala brzina prijenosa podataka. Iz tog razloga se IrDA interfejsi koriste za pokrivanje malih udaljenosti, a ovim adapterima su uglavnom opremljeni mobilni telefoni, lap-top računari, PDA uređaji. IrDa interfej sve više izlazi iz upotrebe od kako se pojavila Bluetooth tehnologija koja omogućava brži prijenos podataka, putem radio talasa.[11]

1.2.6. RFID

RDIF (eng. Radio frequency identification) je sistem daljinskog slanja i prijema podataka pomoću RFID kartica/odašiljača. RFID kartica je dosta mali objekat koji se može zalijepiti ili ugraditi u željeni proizvod i uređaj. RFID kartice sadrže u sebi antenu koja im omogućava prijem i slanje radio-talasa od RFID primopredajnika. Može se reći da je preteča RFID tehnologije jedna vrsta bubice (nastala 1945.god) koja je preko radio talasa slala signale. Izumitelj je ruski naučnik Leon Termin. Neku veću primjenu, kao i primjenu u aplikacijama za praćenje, RFID se pojavio osamdesetih godina i brzo zadobio veliku pažnju zbog svoje sposobnosti da prati pokretne objekte. Kao prefinjena tehnologija, sa neslućenim mogućnostima primjene, on se stalno razvija i spektar mogućih upotreba ove tehnologije se stalno širi. Pretpostavlja se da je prvi istraživački rad koji je objavljen delo Hari Stokmana koji je taj rad objavio 1948. godine pod naslovom ”Komunikacija kao odraz moći” i bilo je potrebno skoro 40 godina da bi RFID kartice zaživjele u praksi.
Problem koji se danas nastoji riješiti uvođenjem nove tehnologije je – kako pratiti jedinstveni proizvod od njegovog nastanka do krajnjeg potrošača. Standardni bar-kod identifikuje samo proizvođača i proizvod, ali ne i jedinstveni artikal. Bar-kod na omotu čokolade je isti na svakom omotu iste vrste čokolade, pa je nemoguće putem samog bar-koda izdvojiti tačno određeni proizvod. RFID transponder, naprotiv, nosi identifikator – serijski broj jedinstven samo za taj specifični proizvod.[12]

---

[11] Veionović, M., Jevremović, A.: Uvod u računarske mreže, Beograd, 2007.godine, str.70
file:///C:/Users/korisnik/Downloads/US%20-%20Uvod%20u%20ra%C4%8Dunarske%20mre%C5%BEe.pdf
[12] Uvod u RFID tehnologiju
https://www.automatika.rs/baza-znanja/obrada-signala/uvod-u-rfid-tehnologiju.html

RFID sistemi se klasifikuju u tri frekvenciona područja. Svako ima svoje karakteristike i tipično područje primene:

- Low Frequency – 100-500 kHz,a najčešće 125 kHz, najkraćeg dometa signala i najmanje brzine očitavanja i prenosa;
- High Frequency – 10-15 MHz, a najčešće 13,56 MHz, kratkog do srednjeg dometa signala, srednje brzine očitavanja i prenosa; Postoji i sistem standardizacije: ISO 15693 predstavlja standard za čipove i čitače koji rade na frekvenciji od 13,56 MHz.
- Ultra High Frequency (UHF) – rade u rasponu od 433 – 915 MHz, i 2,45 GHz, najvećeg dometa signala (pod FCC regulativom), veće brzine prenosa. Kod ovih transpondera ne sme biti prepreke između čitača i transpondera – UHF radio-talas ne prodire tako dobro kroz materijale i zahteva više energije za transmisiju u datom opsegu nego talas niže frekvencije. Tri su najčešće frekvencije (kao predstavnici ovih grupa) 125 kHz, 13,56 MHz i 2,45 GHz. Većina zemalja koristi 125 kHz ili 134 kHz područje za sisteme niske frekvencije, i 13,56 MHz za sisteme visoke frekvencije.[13]

[13] Uvod u RFID tehnologiju
https://www.automatika.rs/baza-znanja/obrada-signala/uvod-u-rfid-tehnologiju.html

1.3. Karakteristike bežičnih mreža

Korisnici Interneta danas imaju sve veću potrebu za mobilnošću. Stoga su bežične lokalne računalne mreže (WLAN) sve raširenji standard u radnim okruženjima, uredima, obrazovnim ustanovama, a naravno i domovima, raznim ugostiteljskim objektima i mnogim drugim mjestima. Sama jednostavnost spajanja i korištenja bežične lokalne mreže koje omogućava slobodno kretanje po manjem prostor bez prekida konekcije dovelo je do popularnosti i razvoja WLAN-a. [14] Uz uobičajena izobličenja signala koja su prisutna u svim vrstama prijenosa (žični, optički, bežični), kod WLAN-a se pojavljuju i smetnje kojih nema u drugim vrstama prijenosa:

- Gubitak snage EM zračenja uslijed prostiranja (engl. path loss) Snaga EM zračenja opada približno prema eksponencijalnom zakonu kako se povećava udaljenost odašiljača. To prigušenje signala ovisi o udaljenosti i snazi odašiljača, fizičkim preprekama (razni objekti) od kojih se zračenje reflektira, kao i o količini međudjelovanja (interferencije) s ostalim čvorovima koji odašilju signale. Npr. u području frekvencija oko 2.4 GHz prigušenje signala na udaljenosti do 100 metara iznosi čak 100 dB. ⍰
- Višestazno prostiranje (engl. multipath propagation) Ono nastaje kada se EM zrake iz jednog izvora na svom putu do odredišta reflektiraju od objekata. Tako na odredište stiže originalni signal i njegove zakašnjele verzije (više ili manje prigušene). Višestazno prostiranje uzrokuje povećanje kašnjenja i na kraju intersimbolnu interferenciju (ISI) koja se manifestira neželjenim proširenjem simbola u prijemu čime simboli ometaju jedni druge.
- Iščezavanje signala uslijed zasjenjenja (engl. shadow fading) uzrokovan je fizičkim preprekama na putu prostiranja EM zraka. Prigušenje signala ovdje ovisi o dielektričnim svojstvima materijala (prepreke).
- Kašnjenje signala uslijed prostiranja prijenosnim medijem[15]

[14] Sveučilište u Zagrebu, Fakultet prometnih znanosti, Završni rad: Pregled mrežnih simulatora u funkciji analize bežičnih mreža, Zagreb 2018, str. 3
https://repozitorij.fpz.unizg.hr/islandora/object/fpz%3A1321/datastream/PDF/view

[15] Jeren, B., Pale, P.:Sustavi za vođenje i praćenje procesa
http://spvp.zesoi.fer.hr/predavanja%202008/WE_skripta.pdf

1.3.1. Standardi

Paralelno sa rastom broja bežičnih tehnologija, broja proizvođača i uređaja pravila i standardi postali su od velike važnosti kako bi omogućili međusobnu komunikaciju svih tih uređaja. Uloga standarda je da omogući proizvodima različitih proizvođača međusobno komuniciranje. U nastavku je dat pregled najznačajnijih organizacija i standarda bežičnih mreža.

1.3.2. IEEE 802.11

IEEE (*eng. Institute of Electrical and Electronics Engineers*) razvio je najznačajnije standarde za bežične mreže. Međutim, najšire prihvaćen standard je IEEE 802.11 poznati i kao Wi-Fi. Postoji puno njegovih verzija, a tri najvažnije su 802.11a, 802.11b, 802.11g, koje sam već objasnila na prethodnim stranicama.

1.3.3. Wi-Fi Alliance

WI-FI Alliance je globalno neprofitni industrijski savez, a njegovi članovi su svjetske mreže raznih kompanija koje donose Wi-Fi. Njihov moto je „spajanje svih i svakog svugdje“. Wi-Fi Alliance promiče i testira na interoperabilnost bežične WLAN uređaje koji zadovoljavaju standarde 802.11b/g i 802.11a. Njihova misija je da certificiraju interoperabilnost Wi-Fi proizvoda i promiču Wi-Fi kao globalni standard za bežične mreže. Ovaj savez je do sada certificirao preko 25.000 proizvoda donoseći korisnicma najbolje iskustvo i podržavajući proširenu upotrebu Wi-Fi proizvoda i usluga na novim tržištima. Glavi cilj je da proizvod ispuni zahtjeve postavljenje od strane Wi-Fi Alliance testne matrice nakon čega proizvod dobije certifikat interoperabilnosti koji dozvoljava proizvođaču korištenje loga Wi-Fi koji je jamstvo da je uređaj sposoban komunicirati s drugim Wi-Fi uređajima.

1.3.4. FCC

FCC (eng. Federal Communications Commision) je agencija vlade SAD-a koja je u SAD-u utvrdila pravila koja definiraju dopustive frekvencije bežičnih mreža te izlaznu snagu na svakom frekvencijskom opsegu. FCC je definirala da WLAN-ovi mogu koristiti ISM (eng. Industrial, Scientfici and Medical) frekvencijske opsege koji su oslobođeni od plaćanja licenci. Uz navedene opsege FCC specificira i tri UNII (eng. Unlicensed National Information Infrastructure) opsega, a svaki od njih je u 5 GHz opsegu širine 100 MHz. U skladu sa FCC standardom on zahtijeva da proizvodi rade u UNII-2 i UNII-2 proširenom standardu (5, 25 – 5, 35 GHz i 5,47 – 5,725 GHz) te moraju podržavati DFS (eng. Dynamic Frequency Selection) kako bi detektirali i automatski prilagodili kanal i zaštitili WLAN komunikaciju od miješanja sa vojnim ili vremenskim sistemima/uređajima.[16]

1.3.5. WLANA

WLANA (eng. Wireless LAN Association) je neprofita obrazovna trgovinska firma, sastavljena od vodećih ljusi i tehnoloških inovatora u bežičnoj tehnološkoj industriji.

[16] Sveučilište Jurja Dobrile u Puli, Fakultet ekonomije i turizma „Dr. Mijo Mirković“, Završni rad: Bežične mreže, Pula 2015., str.15-17
https://repozitorij.unipu.hr/islandora/object/unipu%3A199/datastream/PDF/view

Kroz veliko znanje i iskustvo članova, WLANA pruža mnogo informacija o bežičnim lokalnim aplikacijama, problemima i trendovima.

1.3.6. ETSI

ETSI (eng. European Telecommunication Standard Institute) proizvodi globalno primjenjive standarde za ICT (eng. Information and Communications Technologies) uključujući fiksnu, mobilnu, radio i internet tehnologiju. Njihovi standardi omogućavaju tehnologije bitne za poslovanje i društvo i službeno su prepoznati u EU kao Europska Organizacija za standarde (eng. European Standards Organization). Inicijalno su utemeljeni za Europske potrebe, međutim ETSI je postao visoko poštovan kao proizvođač svjetskih tehničkih standarda. Standardi i izvještaji dizajnirani su da služe širokom spektru potreba i dostupni su svima bez naknade. ETSI je uspostavio standard HiperLAN/2 koji ima sličnu namjenu kao standard 802.11a kojeg je donio IEEE. Postoje intenzivni pregovori kako bi se uskladili standardi i područja bežičnih tehnologija između IEEE-a i ETSI-a.[17]

[17] Sveučilište Jurja Dobrile u Puli, Fakultet ekonomije i turizma „Dr. Mijo Mirković“, Završni rad: Bežične mreže, Pula 2015., str.17
https://repozitorij.unipu.hr/islandora/object/unipu%3A199/datastream/PDF/view

2. WLAN UREĐAJI

Kako bi znali na najbolji način iskorititi bežične mreže jedna od bitnih stvari jeste oprema koja nam stoji na raspolaganju. U nastavku ću da objasnim opermu koja se koristi za bežične mreže.

2.1. Pristupne tačke

Bežične pristupne tačke (AP ili WAP) su mrežni uređaji koji omogućavaju bežičnim Wi-Fi uređajima da se povežu na mrežu. Formiraju bežične lokalne mreže (WLAN) . Pristupna tačka deluje kao centralni predajnik i prijemnik bežičnih radio signala. Međusobni bežični AP-ovi podržavaju Wi-Fi i najčešće se koriste u kućama, kako bi podržali javne internetske vruće tačke i poslovne mreže kako bi se prilagodili proliferaciji bežičnih mobilnih uređaja koji su u upotrebi. Pristupna tačka može biti ugrađena u ruter ili može biti samostalni uređaj. Ako vi ili saradnik koristite tablet ili laptop za povezivanje na internet, prolazite kroz pristupnu tačku - ili hardver ili ugrađeni pristup Internetu bez povezivanja sa njim pomoću kabla.[18]

Bežične pristupne tačke unutar neke ustanove moraju se pažljivo razmjestiti, a da ne bi dolazilo do preklapanja područja komunikacije tamo gdje to nije poželjno preporučuje se svaku pristupnu tačku podesiti da radi na različitim frekvencijama te podesiti snagu predajnika na što manju vrijednost. Mehanizam bežične komunikacije suprotan je Ethernet mehanizmu komunikacije jer Ethernet koristi mehanizam detekcije kolizije signala (CSMA / CD - Carrier Sense Multiple Access / Collision Detect) dok WLAN koristi mehanizam izbjegavanja kolizije. Različite pristupne tačke imaju različite hardverske i softverske opcije, a najčešće su:

- fiksirane ili nefiksirane antene
- napredne sposobnosti filtriranja
- modularne radio-kartice
- promjenjiva izlazna snaga
- različiti tipovi ožičenih veza

Fiksirane ili nefiksirane antene odabiru se u zavisnosti od potreba organizacije. Pristupne tačke s nefiksiranim antenama omogućuju korištenje različitih antena i kablova različitih dužina kako bi se npr. korisniku koji je van objekta omogućio pristup mreži na pristupnu tačku koja se nalazi unutar objekta. Filtriranje se koristi kako bi se odbio pristup WLAN-u neovlaštenim korisnicima gdje kao osnovnu mjeru sigurnosti pristupnu tačku možemo konfigurisati za filtriranje uređaja koji nisu navedeni na MAC filter listi pristupne tačke.[19]

[18] http://mrezawifi.blogspot.com/2017/12/sta-je-bezicna-pristupna-tacka-wireless.html

[19] Sveučilište Jurja Dobrile u Puli, Fakultet ekonomije i turizma „Dr. Mijo Mirković“, Završni rad: Bežične mreže, Pula 2015., str.18
https://repozitorij.unipu.hr/islandora/object/unipu%3A199/datastream/PDF/view

Slika 7. Bežična pristupna tačka

https://i.stack.imgur.com/a0Bjk.jpg

2.2. Bežični mostovi

Bežični most (eng. Wireless Bridge) je uređaj koji povezuje udaljene mrežne segmente. Radi na drugom sloju OSI modela, tj. sloju veze podataka. Do sada smo vidjeli da u datom trenutku na mreži može da emituje samo jedna stanica. Ostale stanice osluškuju saobraćaj i kada zaključe da je medijum slobodan šalju svoje pakete. Može se zaključiti da bi bilo veoma zgodno logički podijeliti mrežu na segmente koji se sastoje iz stanica koje međusobno najviše komuniciraju. To bi značilo da po dvije stanice u različitim segmentima mogu da komuniciraju istovremeno. Ako stanica iz jednog segmenta šalje podatke stanici u drugom segmentu, tada ostalim stanicama nije dozvoljeno da komuniciraju. Segmentaciju mreže možemo izvršiti uređajem koji se zove mrežni most. Spolja je sličan ripiteru, a funkcionalno ima sve njegove osobine uz dodatak nekoliko novih koje su veoma značajne. Most provjerava sadržaj zaglavlja primljenog paketa da bi saznao MAC (fizičku) adresu izvora i odredišta. Na osnovu toga, on formira tabelu MAC adresa za svaki port. Pojedini segmenti mreže se nazivaju kolizioni domeni. Kada dobije broadcast paket (paket za sve računare u mreži), mrežni most ga samo prosljeđuje i ne pamti MAC adresu iz njegovog zaglavlja. Postoji pravilo u segmentiranju mreže po kome 80% saobraćaja treba da se odvija u okviru kolizionih domena, a 20% da ide preko mosta. To znači da ukoliko neke dvije stanice često međusobno komuniciraju (npr. neka radna stanica i određeni server), ne treba stavljati most između njih. Mrežni most unosi određeno kašnjenje kao posljedicu obrade paketa, ali se ono uglavnom ne osjeća.[20]

[20] Veionović, M., Jevremović, A.: Uvod u računarske mreže, Beograd, 2007.godine, str.33.

Slika 8. Mrežni most

http://bestwirelessroutersnow.com/wp-content/uploads/2016/11/Best-Wireless-Ethernet-Bridge.jpg

2.3. Bežični LAN uređaji

Bežični LAN uređaji su uređaji kojima je potrebna bežična veza do mrežne infrastukture koja se ostvaruje korištenjem WLAN radio-uređaja kao što su:

- PCMCIA, Compact Flash i Secure Digital Kartica
- Ethernet i serijski konvertor
- USB adapter
- PCI i ISA adapteri

Neki od LAN uređaja su: laptopi, PDA, bežični IP telefon, destkop, bežični printer serveri, Bežični prezentacijski gatewayi, IP kamere, itd...

2.4. PCMCIA, Compact Flash i Secure Digital Kartica

PCMCIA kartica koja je još poznata pod nazivom PC karica je najčešća komponenta bilo koje bežične mreže. To je uređaj koji povezuje računar sa računarskom mrežom. Često se naziva mrežni adapter ili mrežni interfejs, NIC. Jedan od važnijih elemenata mrežne kartice je MAC adresa koja čini da ovaj uređaj radi na 2. Sloju OSI modela. [21]

[21]Veinović, M., Jevremović, A.: Uvod u računarske mreže, Beograd, 2007.godine, str.31.

Slika 9. PCMCIA kartica
https://www.hrvatskitelekom.hr/ResourceManager/GetImage.aspx?imgId=521&fmtId=54

2.5. Ethernet i serijski konvertori

Ethernet i serijski konvektori koriste se sa uređajima koji imaju Ethernet ili 9-pinski serijski port s ciljem pretvorbe ovih mrežnih konektore. Bežični Ethernet konvertor spajamo sa uređajem Cat5 kablom. Serijski konvertori obično se koriste sa starijom opremom, koja koristi serijski priključak za mrežno povezivanje, kao što su terminali, telemetriska oprema i serijski štampači.

2.6. USB adapteri

USB klijenti veoma su popularni zbog jednostavnog povezivanja. USB klijenti podržavaju plug-n-play i ne zahtijevaju dodatnu snagu osim one koja je isporučena preko USB porta na računaru.[22]

Slika 10. WLAN USB
https://encrypted-tbn0.gstatic.com/images?q=tbn:ANd9GcRzWVdxdy_16B7bW3LHa1ddE4nOtC0XZqqQmI68MdaiMcEyV7FQ

[22] Hamidović, H.,Bežične lokalne računarske mreže, Zagreb, str 78-79
https://books.google.ba/books?id=7lOzfWDE8a8C&pg=PA78&lpg=PA78&dq=WLAN+PC+kartica&source=bl&ots=-QTZNcp5Cy&sig=ACfU3U0mSVjw1pWimwTSpYytQRX1Tp0QZw&hl=en&sa=X&ved=2ahUKEwixqKf6nNrkAhXqkosKHbQ5Cu8Q6AEwBXoECAkQAQ#v=onepage&q&f=false

2.7. PCI i ISA adapteri

PCI i ISA adapteri instaliraju se unutar destkop ili serverskog računara. Bežični PCO računari su također plug-n-olay kao i USB adapter za razliku od bežičnij ISA kartica koje najčešće nisu plug-n-play i zatijevaju ručnu konfiguraciju. Instaliranje WLAN klijentskih uređaja uključuje dva koraka- instalaciju drajvera i pomoćnih programa. [23]

2.8. Bežični gatewayi

Gateway hardverski uređaj i/ili softverski paket koji povezuje dva različita mrežna okruženja. Omogućava komunikaciju između različitih arhitektura i okruženja. Vrši prepakivanje i pretvaranje podataka koji se razmjenjuju između potpuno drugačijih mreža, tako da svaka od njih može razumijeti podatke iz one druge. Mrežni prolaz je obično namjenski računar, koji mora biti sposoban da podrži oba okruženja koja povezuje kao i proces prevođenja podataka iz jednog okruženja u format drugog. Svakom od povezanih mrežnih okruženja mrežni prolaz izgleda kao čvor u tom okruženju. Zahtjeva značajne količina RAM memorije za čuvanje i obradu podataka. Radi u sloju sesije i aplikativnom sloju. Kako povezuje različite mreže, mrežni prolaz mijenja format poruka da bi ih prilagodio krajnjim aplikacijama kojima su namjenjene, vrši prevođenje podataka.[24]

2.9. Antene

Antena je uređaj koji pretvara visoko frekventne elektromagnetske signale sa linije prijenosa u šireće RF valove i obrnuto. Svaka antena trebala bi pokrivati tri područja – osigurati pojačanje, usmjerenje i polarizaciju. Kada govorimo o pojačanju mislimo na iznos povećanja energije koju antena dodaje RF signalu, pod usmjerenjem mislimo na oblik odašiljanja vala i prekrivanje prostora signalom dok je polarizacija orijentacija električnog polja vala iz antene. Ove tri osobine vrlo su bitne i mogu dovesti do velikih razlika u karakteristikama antena. Odgovarajući izbor antene također može utjecati na sigurnost bežičnog LAN-a na način da je poveća. Isto tako dobro postavljena antena i dobro izabrana ima mogućnost umanjiti curenje signala van radnog prostora i otežati presretanje signala28. Sve bežične antene spadaju u tri osnovne kategorije: omni-direkcijske (dipol), semi-direkcijske i direkcijske. Omni direkcijske antene su najčešće, jednostavne su za dizajniranje i dio su standardne opreme na većini pristupnih točaka. Ove antene zrače oko svoje osi podjednako u svim pravcima osim uzduž same žice, a one čiji je dohvat velik nude više vodoravnih područja koje pokrivaju dok je okomito područje pokrivanja smanjeno. Zbog navedenog najbolje su za upotrebu za velika područja

[23] Sveučilište Jurja Dobrile u Puli, Fakultet ekonomije i turizma „Dr. Mijo Mirković“, Završni rad: Bežične mreže, Pula 2015., str.21
https://repozitorij.unipu.hr/islandora/object/unipu%3A199/datastream/PDF/view

[24] Veinović, M., Jevremović, A., Uvod u računarske mreže, Zagreb 2007., str 36.
https://muricmilorad.files.wordpress.com/2011/11/uvod-u-racunarske-mreze.pdf

pokrivanja oko središnje tačke. Kod vanjske upotrebe preporučuje se njihovo smještanje na vrh građevine, a pogodne su za sajmove i skladišta gdje je potrebno [25]pokrivanje od jednog do drugog kraja. Za razliku od omni-direkcijskih antena ove antene puno više usmjeravaju energiju od predajnika u jednom određenom smjeru. Semi-direkcijske antene idealne su za kratke i srednje udaljenosti koje treba premostiti kao npr. uredi u dvije zgrade razdvojene ulicom. Najčešći tipovi ovih antena korištenih u bežičnim LAN-ovima su Patch, Panel i Yagi antene. Treći tip antena odnosno direkcijske antene imaju najužu zraku signala i najveći dohvat od svih vrsta antena zbog čega su idealne za duge udaljenosti. Njima možemo bežično povezati dvije zgrade udaljene kilometrima bez prepreka u zračnoj liniji pri čemu treba paziti da budu precizno usmjerene jedna prema drugoj zbog uske zrake koju šalju.

[25] Sveučilište Jurja Dobrile u Puli, Fakultet ekonomije i turizma „Dr. Mijo Mirković“, Završni rad: Bežične mreže, Pula 2015., str.22-23.
https://repozitorij.unipu.hr/islandora/object/unipu%3A199/datastream/PDF/view

3. SIGURNOST BEŽIČNIH MREŽA

U ranim fazama razvoja tehnologija na kojima se baziraju računarske mreže fokus je bio postavljen na omogućavanje što veće brzine prenosa podataka sa što manjom mogućnošću greške. Mala baza korisnika (koju su uglavnom činila tehnički visoko-obrazovana lica) i retke praktične primjene omogućile su brz razvoj tehnologija i dovele računarske mreže do potencijala kojim prijete da u potpunosti zamijene ostale popularne sisteme komunikacije kao što su telefonija i televizija. Međutim, sa rastom popularnosti koja se bazira na povećanju baze korisnika računarske mreže su izašle iz čisto tehničko-tehnološkog domena i sve više na njihov razvoj i primjenu imaju ekonomski i socijalni faktori. Internet, kao najveća računarska mreža danas, se sastoji od miliona korisnika i stotina hiljada njima dostupnih servisa. Putem ove mreže se prenose lični podaci korisnika, obavljaju povjerljive poslovne video-konferencije i razgovori, obavljaju finansijske transakcije, prenose povjerljive vojne i državne informacije, obavljaju udaljeni hirurški zahvati i sl. Stoga, na primjeru Internet-a možemo zaključiti da se putem računarskih mreža prenose vrijednosti realnog sveta, daleko veće nego što je to slučaj kod telefonije i televizije. Međutim, svaka vrednost sa sobom nosi najčešće srazmeran rizik koga je, kako u realnom tako i u virtuelnom svetu računarskih mreža, cilj eliminisati ili u što većoj mjeri umanjiti. Postizanje ovog cilja pred inžinjere iterativno postavlja nove zadatke koji se rezultuju novim rješenjima. Ta rješenja mogu biti jednostavne tehničke izmjene nosećih protokola ili kompleksni inteligenti softverski sistemi koji uče i svoje odluke donose putem heurističkih metoda.

Greške koje se javljaju na računarskim mrežama i kod resursa koji su putem njih dostupni možemo podeliti u četiri kategorije na osnovu uzroka njihovog pojavljivanja:

- Greške koje se samoinicijativno pojavljuju uslijed propusta u definiciji hardverskih i softverskih komponenti računarskih mreža.
- Greške koje se javljaju kao posljedica neadekvatnog dizajniranja računarskih mreža i nenamjenske upotrebe korištenih komponenti.
- Greške koje se javljaju uslijed neadekvatnog korištjenja računarskih mreža od strane korisnika nedovoljno obučenih za rad.
- Greške koje se javljaju kao posledica iskorištenja propusta u definiciji hardverskih/softverskih komponenti računarskih mreža, njihovom dizajnu i/ili (ne)pažnji korisnika a od strane zlonamernih korisnika i u cilju ostvarivanje određene koristi od napada na računarsku mrežu ili resurs.[26]

[26] Veinović, M., Jevremović, A., Uvod u računarske mreže, Zagreb 2007., str 206. https://muricmilorad.files.wordpress.com/2011/11/uvod-u-racunarske-mreze.pdf

3.1. Napadi na bežične mreže

Postoji više načina neovlaštenog pristupa bežičnim mrežama. U nastavku donosimo neke od njih:

- slučajno povezivanje (*eng. Accidental Association*) – ako se u istom prostoru koristi više nezaštićenih bežičnih mreža, korisnik se slučajno može spojiti na krivu mrežu i time dovesti u opasnost sebe i tuđi sistem,
- zlonamjerno povezivanje (*eng. Malicious Association*) – izvodi se posebnim programima koji mrežnu karticu napadača predstavljaju kao legitimnu pristupnu tačku napadačeve mreže. Posljedica uspješnog napada je ta da se sav mrežni promet te bežične mreže preusmjerava kroz napadačevo računalo,
- ad - hoc mreže – budući da se u ovakvim mrežama komunikacija odvija bez pristupne tačke tj. izravno između dva računara (*eng. Peer-to-Peer*) i da se često ne koriste zaštitne metode kakve se mogu uvesti kroz pristupnu točku, sistem je osjetljiviji na lažno predstavljanje, otkrivanje podataka i druge vrste napada,
- netradicionalne mreže – podrazumijevaju Bluetooth i slične tehnologije čijoj se sigurnosti zbog kratkog dometa komunikacije često ne pridaje dovoljno pažnje. To otvara prostor napadačima za različite zlouporabe,
- krađa identiteta – ako je omogućeno prisluškivanje mrežnog prometa (podaci nisu kriptirani), napadač može saznati MAC (*eng. Medium Access Control*) adrese računala koje se koriste u lokalnoj mreži i pomoću nekog alata lažno se predstaviti kao ovlašteni korisnik mreže,
- napadi posredovanjem u komunikaciji (*eng. Man-In-The-Middle*) – ukoliko se primjerice uspješno izvede napad zlonamjernog povezivanja, napadač može saznati osjetljive podatke koje zatim može koristiti za posredovanje u komunikaciji tako da su krajnji korisnici nesvjesni da podatke šalju posredniku i primaju putem posrednika koji se predstavio kao pristupna točka,
- mrežno ubacivanje (*eng. Network Injection*) – ova vrsta napada cilja na izmjenu radnih postavki mrežnih uređaja kao što su usmjerivači i preklopni uređaji, a kojima se iz WLAN mreže pristupa pomoću pristupne točke. [27]

3.2. Sigurnosni mehanizmi 802.11 standarda

IEEE 802.11 standard za bežične mreže predviđa mehanizme kojima je cilj povećanje sigurnosti bežičnih mreža odnosno ostvarivanja povjerljivosti i integriteta podataka te mogućnost sigurne autentikacije. Podaci koji putuju bežičnom mrežom moraju biti zaštićeni od presretanja ili prisluškivanja i moraju nepromijenjeni stići na svoje odredište. [28]Najosnovniji ugrađeni sigurnosni mehanizmi standarda 802.11 su SSID (eng. Servise Set

[27] Sveučilište Jurja Dobrile u Puli, Fakultet ekonomije i turizma „Dr. Mijo Mirković“, Završni rad: Bežične mreže, Pula 2015., str.25
https://repozitorij.unipu.hr/islandora/object/unipu%3A199/datastream/PDF/view
[28] https://cuc.carnet.hr/cuc2007/program/radovi/pdf/c-6-rad.pdf

Identifier), autentikacija te statički WER ključ (eng. Wired Equivalent Privacy) koji spada u osnovne sigurnosne mehanizme.

3.2.1. SSID

SSID znači "Service Set Identifier". Prema standardu IEEE 802.11 za bežično umrežavanje, "skup usluga" odnosi se na skup bežičnih mrežnih uređaja s istim parametrima. Dakle, SSID je identifikator (ime) koji vam govori koji skup usluga (ili mreža) se pridružuje. SSID-ovi su dizajnirani kao jedinstveno ime za razlikovanje više Wi-Fi mreža u području tako da se možete povezati s ispravnim. Koriste ih sve vrste Wi-Fi pristupnih točaka, uključujući javne Wi-Fi mreže i vašu kućnu Wi-Fi mrežu. Proizvođači rutera često daju zadani SSID poput "Linksys" ili "Netgear", ali ga možete promijeniti u sve što vam se sviđa - ako upravljate Wi-Fi mrežom i imate administrativni pristup. SSID može imati najviše 32 znaka. Oni razlikuju velika i mala slova, tako da je "NetworkName" različiti SSID od "networkname". Dopušteni su i neki posebni znakovi, kao što su razmaci, donja crta, razdoblja i crtice. Bežični usmjerivač ili druga Wi – Fi bazna stanica emitira svoj SSID, omogućujući obližnjim uređajima prikaz popisa dostuonih mreža s imenima koja se čitaju. Ako je mreža otvorena, svako se može povezati samo sa SSID-om. Međutim, ako je mreža osigurana WPA2 ili nekom drugom vrstom šifriranja, ljudi će trebati šifru (password) prije nego što se mognu povezati. Nakon što se jednom povežete s Wi-Fi mrežom s određenim SSID-om, uređaj će se ubuduće općenito povezivati s SSID-ovima s tim nazivom. Stvari se kompliciraju ako postoji više Wi-Fi mreža s istim SSID-om. Ako se nalaze u istom području - na primjer, dvije mreže nazvane "Home" - neki uređaji pokušat će se automatski povezati s mrežom s najjačim signalom, dok će se neki pokušati spojiti na prvu mrežu koju vide. Naravno ako dvije Wi- Fi mreže pod nazivom „Home“ imaju različite šifre, uređaj će se moći uspješno povezati samo sa jednom od njih. Dakle, ako koristite isti SSID kao vač komšija, vjerovatno ćete oboje naići na neke probleme s vezom dok ga jedan od vas ne promijeni.[29]

3.2.2. Autentifikacija

Da bi dobili pristup nekoj mreži, moramo prvo proći kroz proces autentifikacije. U nastavku će biti objašnjena dva standarda koji definiraju provjeru korisnika:

- Autentifikacija otvorenog sistem (eng. Open System Authentication) – pvaj način autentifikacije se podrazumijeva u standardu 802.11. Kako i samo ime govori, ovaj način dopušta pridruživanje mreži svakome tko to traži. Dakle on ne predstavlja nikakvu metodu autentifikacije
- Autemntifikacija temeljena na tajni (eng. Shared Key Authentication) – ovaj način temelji se na pretpostavki da obje strane u procesu autentifikacije imaju jednako djeljiv ključ (eng. Shared Key), pretpostavka je da je taj ključ prenesen klijentu i pristupnoj tački sigurnosnim kanalom. Znači pristupna tačka šalje korisniku izazov koji korinik enkriptira svojim tajnim ključem i šalje natrag pristupnoj tački.

[29] Šta je SSID ili identifikator skupa usluga?
https://hr.digitalentertainmentnews.com/what-is-an-ssid-service-set-identifier-656869

Pristupna tačka dekriptira primljenu poruku svojim tajnim ključem i ukoliko se radi o istom tekstu koji je prvobitno poslala, korisniku se omogućuje spajanje. Ovaj nači autentifikacije se nikako ne preporučuje iz razloga ponovnog slanja upravljačkih okvira u neekriptiranom obliku preko nesigurnog medija. Napadač može uhavtiti upravljačke okvire s čistim tekstom kao i sa enkriptirani istim tekstom i na taj način doći do ključa koji se koristio.[30]

3.2.3. WEP

Wireless Encryption Protocol (WEP) je protokol, dio IEEE 802.11 standarda, namijenjen osiguranju bežičnih mreža. WEP protokol kriptira podatke koji putuju između korisnika i pristupne točke zajedničkim ključem. Korisnik mora imati odgovarajući WEP ključ kako bi mogao komunicirati s pristupnom točkom. WEP protokol za enkripciju koristi RC4 algoritam s 64 ili 128 bitnim ključem, a za osiguranje integriteta podataka koristi se CRC-32 algoritam. Pokazalo se da je takav sigurnosni mehanizam moguće probiti javno dostupnim alatima i ne preporuča se kao odgovarajuća mjera zaštite[31] Kao i ranije navedeni standardi i ovaj standard ima svoje ranjivosti. U komunikaciji pristupne točke i klijenta podaci se šalju u obliku okvira koji nisu enkriptirani, pa napadač može bez problema doći do inicijalizacijskog vektora koji se koristi u enkripciji. Isto tako postoje dvije osnovne vrste napada na WEP – pasivni i aktivni. U pasivnim napadima napadač prisluškuje komunikaciju korisnika sa mrežom, ali ne utječe na podatke koje razmjenjuju pristupna točka i klijent. U aktivnim napadima napadač aktivno utječe na podatke i to može raditi na više načina – ubacivati svoje podatke, neovlašteno koristiti mrežne resurse, zagušivati promet na mreži, lažirati komunikaciju klijenta i pristupne točke. Vrste pasivnih napada mogu biti analiza prometa što je najjednostavniji pasivni napad, a vrši se prisluškivanjem mreže kako bi se pratio broj i veličina paketa u mreži kao i pasivno prisluškivanje gdje napadač osluškuje mrežu, a jedini uvjet je da ima pristup signalu mreže. Od aktivnih napada možemo nabrojati napad ponavljanjem inicijalizacijskog vektora (eng. Initialization Vector Replay Attacks), napad obrtajem bitova podataka (eng. Bit-Flipping Attacks), napad čovjek-u-sredini (eng. Man-In-The-Middle attack), ARP napadi za čiji preduvjet je pristup mreži, krađa sjednica (eng. Session Hi-jacking) i napad ponavljanjem paketa (eng. Packet-Re-play Attack).[32]

---

[30] Veleučilište u Rijeci, Poslovni odjel , Stručni studij Informatika, završni rad: Sigurnost Bežičnih mreža, Rijeka 2015, str. 8
https://freslnet.com.hr/media/documents/SigurnostBezicnihMreza.pdf

[31] https://cuc.carnet.hr/cuc2007/program/radovi/pdf/c-6-rad.pdf

[32] Sveučilište Jurja Dobrile u Puli, Fakultet ekonomije i turizma „Dr. Mijo Mirković“, Završni rad: Bežične mreže, Pula 2015., str.29
https://repozitorij.unipu.hr/islandora/object/unipu%3A199/datastream/PDF/view

3.3. Sigurnosne nadogradnje 802.11 standarda

Zbog toga što je IEEE uočivši propuste u 802.11 standardu započelo rad na novim prijedlozima i rješenjima koja bi učinili bežične mreže sigurnijima. Plod toga rada je i 802.1X standard koji nastoji poboljšati sigurnost.

3.3.1. 802.1x standard

Kao što je već navedeno radi povećanja sigurnosti korisnika IEEE je otklanjanjem nedostataka standarda 802.11 uveo standard 802.1x koji kroz bolji autentikacijski okvir donosi nova rješenja. To je standard koji sigurnost donosi na razini porta i iako je njegova prva uloga trebala biti u svrsi sigurnosti na ožičenim mrežnim portovima pokazalo se da je također primjenjiv i na bežično umrežavanje. Standard 802.1x koristi EAP (eng. Extensible Autenthication Protocol) kao bazu u svrhu autentikacije. Navedena autentikacija zahtijeva postojanje tri entiteta:

- molitelj (eng. Supplicant) – nalazi se na WLAN klijentu,
- autentikator (eng. Authenticator) – nalazi se na pristupnoj točki,
- autentikacijski server (eng. Authentication server) – nalazi se na RADIUS serveru.

Bežični mediji zbog svojih karakteristika ne mogu osigurati dovoljnu povjerljivost podataka jer je nemoguće u potpunosti isključiti prisluškivanje od strane trećih osoba. Zbog mobilnosti korisnika, što je i svrha bežičnih mreža, potrebno je osigurati mogućnost autentikacije bez obzira u kojoj mreži se nalaze, a zbog širokog područja primjene dakle korištenja kako unutar velikih korporaciji tako i u obliku javnih mreža, standard mora biti fleksibilan kako bi se zadovoljile svačije potrebe. Zbog toga standard 802.1x pokušava ispuniti navedene sigurnosne ciljeve u što spadaju stroga povjerljivost podataka, fleksibilnost, skalabilnost, sveprisutna sigurnost, kontrola pristupa i mogućnost međusobne autentikacije. Međutim, i ovaj standard ima svoje ranjivosti. Najvažniji njegov dio je EAP koji je prvenstveno namijenjen za upotrebu u žičanim mrežama zbog čega se u bežičnim mrežama javljaju sigurnosni propusti zbog nemogućnosti u EAP protokolu da supplicant autenticira autentikatora. Supplicant koristi usluge autentikatora i autenticira se preko njega autentikacijskim poslužiteljem koji nalaže autentikatoru da dozvoli pristup mreži supplicantu. U ovoj komunikaciji dolazi do problema asimetričnosti na način da se na strani autentikatora kontrolira port u slučaju ispravne autentikacije klijenta dok je klijentov port stalno u stanju autenticiran što otvara mogućnost napada. Isto tako standard 802.1x nema odgovarajući mehanizam koji omogućava autentikaciju i provjeru integriteta svakog paketa. Zbog svega navedenog iako je standard 802.1x daleko prihvatljiviji na razini sigurnosti od standarda 802.11 i dalje postoje propusti koje je potrebno otkloniti.[33]

[33] Sveučilište Jurja Dobrile u Puli, Fakultet ekonomije i turizma „Dr. Mijo Mirković“, Završni rad: Bežične mreže, Pula 2015., str. 30-31.
https://repozitorij.unipu.hr/islandora/object/unipu%3A199/datastream/PDF/view

3.3.2. WEP2

Ovaj standard je još jedan od pokušaja povećanja sigurnosti bežičnih mreža. Kako se iz imena standarda dade naslutiti on je nastao nadograđivanjem WEP-a i s time je naslijedio neke slabosti u dizajnu. IEEE je načinio preinake u duljini ključa koji je proširen na 128 bita (prije 40 bita) te proširivanjem polja u kojemu se nalazi inicijalizacijski vektor koje je sada veliko 128 bita(prije 24 bita). Također donosi i podršku za Kerberos V protokol. No ostao je isti enkripcijski algoritam – RC4 i isti način upravljanja ključevima pa se može zaključiti da WEP2 ne donosi velik pomak u poboljšanju sigurnosti. Dobra stvar je da je WEP2 kompatibilan sa WEP protokolom tako da mrežna oprema uz određenu programsku nadogradnju može koristiti WEP2 protokol.[34]

3.4. WPA

WPA predstavlja certifikaciju, a ne protokol, odnosno sigurnosni standard. WPA uključuje samo jedan sigurnosni protokol TKIP. WPA je nastao prvenstveno zbog sigurnosnih nedostataka WEP enkripcije, odnosno nedostataka korištenjem inicijalizacijskog vektora. U kolovozu 2001. godine objavljena je kriptoanaliza WEP protokola i načina na koji se koriste RC4 tok za šifriranje i inicijalizacijski vektor.Navedena analiza je pokazala da je WPA enkripcijski protokol ranjiv na pasivne napade. Pasivni napadi imaju cilj otkrivanja RC4 ključa iz prikupljenih paketa podataka. Ovisno o količini prometa na mreži, odnosno broja uhvaćenih paketa dostupnih za analizu, za uspješno otkrivanje RC4 ključa može biti potrebno i samo nekoliko minuta. WPA i dalje koriste RC4 i CRC32 algoritmi. Uvedeni su TKIP (Temporal key integrity protocol), MIC (Message integrity code, izračunava se algoritmom Michael5) te 802.1x autentikacija. Kombinacijom dugačkog inicijalizacijskog vektora (IV) i TKIP protokola, sustav se može obraniti od napada kakvi se koriste za otkrivanje ključa kod primjene WEP protokola (Tanenbaum, Wetherall, 2011). Slabosti prethodnih sistema ležale su u premalom broju mogućih inicijalizacijskih vektora koji su uz isti tajni ključ davali nesigurne nizove podataka. To znači da je analizom tih nizova bilo moguće otkriti vrijednosti ključa. Na ovaj način opisani algoritam napada gotovo je nemoguće iskoristiti.[35]

3.5. WPA2

WPA2 je nadogradnja na WPA i jedina razlika među njima je što se kao enkripcijski algoritam koristi AES, a ne RC4. AES je prihvaćen kao službeni enkripcijski algoritam NIST-a (National Institute of Standards and Technology), ujedno kao i nasljednik DES-a. AES je simetrični algoritam i u ovom standardu se koristi u CCM (cipher-block chaining mode) načinu rada. Koristeći ga na taj način osigurano je da bude upotrebljiv i u IBSS(Independent Basic Service Set) načinu rada bežičnih mreža kada klijenti komuniciraju izravno jedan s drugim bez posredovanja pristupne točke. Duljina ključeva u AES-u je 128, 192 ili 256 bita. No WPA2 donosi i značajna materijalna

---

[34] Sveučilište u Zagrebu, Fakultet elektrotehnike i računarstva , Seminarski rad: Sigurnost bežičnih računalnih mreža, Zagreb 2004, str. 38
http://sigurnost.zemris.fer.hr/ns/wireless/2004_maric/sigurnost.pdf

[35] Skendžić, A., Stručni rad: Sigurnost infrastrukturnog načina rada bežične mreže standarda IEEE 802.11, str. 5
file:///C:/Users/korisnik/Downloads/12_sigurnost_rada_bezicne_mreze.pdf

ulaganja u novu mrežnu opremu jer je sadašnja preslaba da bi mogla bez značajnijeg pada performansi omogućiti rad korisnicima. Uzrok tome su veliki sklopovski zahtjevi AES-a. Svaka organizacija bi trebala procijeniti je li isplativo takovo ulaganje u mrežnu opremu.[36]

[36] Sveučilište u Zagrebu, Fakultet elektrotehnike i računarstva , Seminarski rad: Sigurnost bežičnih računalnih mreža, Zagreb 2004, str. 41
http://sigurnost.zemris.fer.hr/ns/wireless/2004_maric/sigurnost.pdf

ZAKLJUČAK

Danas je širenje bežičnih mreža u sve većem porastu. Glavne prednosi za njihovo korištenje jeste fleksibilnost, jednostavnost korištenja i implementacije, mobilnost, veliki izbor uređaja za korištenje, itd... Bežične mreže su veoma specifične i izložene su mnogim virusima zbog načina prijenosa podataka. I Zato je važno da nam je sigurnost bežičnih mreža prioritet. Da bi se zaštitila privatnost korisnika i komunikacija bežičnih mreža razvijeno je nekoliko protokola. Uz redovno praćenje razvoja tehnologije i primjenjivanje nanovijih sigurnosnih mehanizama te kroz edukaciju korisnika i administratora, moguće je sigurnosne rizike svesti na minimum.

U početku je korišten WEP protokol da donese jednaku zaštitu bežičnim mrežama kakvu imaju žičane, ali je s vremenom otkrio svoje nedostatke pa je zamijenjen sigurnijim protokolima WPA, a zatim i sa WPA2. WPA2 se danas smatra kao najbolji sistem za zaštitu uređaja. Da bi se postigla potrebna razina zaštite osim razvijenih standarda i protokola potrebno je educirati ne samo administratore nego i korisnike bežičnih mreža. Mali domen signala je i dalje nedostatak bežičnih mreža, te nemogućnost potpune zaštite.

LITERATURA

[1] Hamidović, H.,Bežične lokalne računarske mreže, Zagreb
https://books.google.ba/books?id=7lOzfWDE8a8C&pg=PA78&lpg=PA78&dq=WLAN+PC+kartica&source=bl&ots=-QTZNcp5Cy&sig=ACfU3U0mSVjw1pWimwTSpYytQRX1Tp0QZw&hl=en&sa=X&ved=2ahUKEwixqKf6nNrkAhXqkosKHbQ5Cu8Q6AEwBXoECAkQAQ#v=onepage&q&f=false

[2] Jeren, B., Pale, P.:Sustavi za vođenje i praćenje procesa
http://spvp.zesoi.fer.hr/predavanja%202008/WE_skripta.pdf

[3] Padarić D.,Kukec M.,Veleučilište u Varaždinu, Varaždin, Hrvatska: WiMax 802.16 standard
file:///C:/Users/korisnik/Downloads/TG_1_2_2009_Padaric_Kukec_WIMAX_802_16_standard.pdf

[4] Radovan, M.:Računalne mreže (1), Rijeka, 2010.godina.
file:///C:/Users/korisnik/Downloads/vdocuments.mx_racunalne-mreze-1-mario-radovan.pdf

[5] Ranjivosti Bluetooth tehnologije
https://www.cert.hr/wp-content/uploads/2019/04/NCERT-PUBDOC-2009-11-281.pdf

[6] Skendžić, A., Stručni rad: Sigurnost infrastrukturnog načina rada bežične mreže standarda IEEE 802.11
file:///C:/Users/korisnik/Downloads/12_sigurnost_rada_bezicne_mreze.pdf

[7] Sveučilište Jurja Dobrile u Puli, Fakultet ekonomije i turizma „Dr. Mijo Mirković“, Završni rad: Bežične mreže, Pula 2015.
https://repozitorij.unipu.hr/islandora/object/unipu%3A199/datastream/PDF/view

[8] Sveučilište u Zagrebu, Fakultet elektrotehnike i računarstva, Zavod za elektroničke sustave i obradu informacija, Seminarski rad iz kolegija: Sustavi za praćenje i vođenje procesa, ZigBee, Zagreb, 2006.
http://spvp.zesoi.fer.hr/seminari/2006/AndroBacan_ZigBee.pdf

[9] Sveučilište u Zagrebu, Fakultet elektrotehnike i računarstva , Seminarski rad: Sigurnost bežičnih računalnih mreža, Zagreb 2004.
http://sigurnost.zemris.fer.hr/ns/wireless/2004_maric/sigurnost.pdf

[10] Sveučilište u Zagrebu, Fakultet prometnih znanosti, Završni rad: Pregled mrežnih simulatora u funkciji analize bežičnih mreža, Zagreb 2018.
https://repozitorij.fpz.unizg.hr/islandora/object/fpz%3A1321/datastream/PDF/view

[11] Šta je SSID ili identifikator skupa usluga
https://hr.digitalentertainmentnews.com/what-is-an-ssid-service-set-identifier-656869

[12] Uvod u RFID tehnologiju
https://www.automatika.rs/baza-znanja/obrada-signala/uvod-u-rfid-tehnologiju.html

[13] Veinović, M., Jevremović, A.: Uvod u računarske mreže, Beograd, 2007.godine
file:///C:/Users/korisnik/Downloads/US%20-%20Uvod%20u%20ra%C4%8Dunarske%20mre%C5%BEe.pdf

[14] Veinović, M., Jevremović, A., Uvod u računarske mreže, Zagreb 2007.

https://muricmilorad.files.wordpress.com/2011/11/uvod-u-racunarske-mreze.pdf
[15] Veleučilište u Rijeci, Poslovni odjel , Stručni studij Informatika, završni rad: Sigurnost Bežičnih mreža, Rijeka 2015.
https://freslnet.com.hr/media/documents/SigurnostBezicnihMreza.pdf

Internet stranice:

[1]file:///C:/Users/korisnik/Downloads/vdocuments.mx_racunalne-mreze-1-mario-radovan.pdf (datum pristupa 10.09.2019.)
[2]https://www.cis.hr/www.edicija/LinkedDocuments/CCERT-PUBDOC-2008-04-225.pdf (datum pristupa 11.09.2019.)
[3]https://www.seminarski-diplomski.co.rs/INFORMATIKA/Bluetooth.html(datum pristupa 15.09.2019.)
[4] https://www.cert.hr/wp-content/uploads/2019/04/NCERT-PUBDOC-2009-11-281.pdf (datum pristupa 15.09.2019.)
[5]file:///C:/Users/korisnik/Downloads/TG_1_2_2009_Padaric_Kukec_WIMAX_802_16_standard.pdf (datum pristupa 15.09.2019.)
[6]http://mrezawifi.blogspot.com/2017/12/sta-je-bezicna-pristupna-tacka-wireless.html (datum pristupa 17.09.2019)
[7]https://cuc.carnet.hr/cuc2007/program/radovi/pdf/c-6-rad.pdf (datum pristupa 18.09.2019)