Bežične mreže

Bajtl, Saša

Sveučilište Jurja Dobrile u Puli
Fakultet ekonomije i turizma
"Dr. Mijo Mirković"

Saša Bajtl

BEŽIČNE MREŽE

ZAVRŠNI RAD

Pula, 2015.

Sveučilište Jurja Dobrile u Puli
Fakultet ekonomije i turizma
"Dr. Mijo Mirković"

Saša Bajtl
Matični broj : 2790 - E, izvanredni student
Smjer: Informatika

BEŽIČNE MREŽE

ZAVRŠNI RAD

Predmet : Elektroničko poslovanje
Mentor: Prof.dr.sc. Vanja Bevanda

Pula, rujan 2015.

IZJAVA O AKADEMSKOJ ČESTITOSTI

Ja, dolje potpisani Saša Bajtl, kandidat za prvostupnika Informatike ovime izjavljujem da je ovaj Završni rad rezultat isključivo mojega vlastitog rada, da se temelji na mojim istraživanjima te da se oslanja na objavljenu literaturu kao što to pokazuju korištene bilješke i bibliografija. Izjavljujem da niti jedan dio Završnog rada nije napisan na nedozvoljen način, odnosno da je prepisan iz kojega necitiranog rada, te da ikoji dio rada krši bilo čija autorska prava. Izjavljujem, također, da nijedan dio rada nije iskorišten za koji drugi rad pri bilo kojoj drugoj visokoškolskoj, znanstvenoj ili radnoj ustanovi.

Student:

U Puli, 18. 09. 2015. _____

SADRŽAJ

UVOD

U današnje doba svaki prosječan korisnik susreo se barem jednom sa nekim od uređaja koji koristi bežičnu tehnologiju. U svakodnevnici svi se služimo pametnim telefonima kojima se putem Wi-Fi-ja spajamo na internet bilo da se spajamo na kućnu mrežu ili na javno dostupne besplatne mreže. Danas malo tko nije čuo za Internet i svi žele njime „surfati“ . Putem njega besplatno nam je dostupna velika količina informacija, možemo pristupati društvenim mrežama, slušati muziku, gledati filmove, čitati knjige, učiti kroz razne online edukacije – mogućnosti su neograničene. Stoga ne čudi činjenica da svatko danas želi biti „online“.

Bežična tehnologija omogućava nam mobilnost i jednostavnost korištenja, ali pri tome većina korisnika ne razmišlja o sigurnosti. U većini slučajeva korisnici su nedovoljno informirani o potencijalnim opasnostima koje donosi spajanje na Internet pogotovo ako pristupaju važnim podacima, bankovnim računima, svom e-mailu ili ostalim sadržajima za koje je bitno da ostanu izvorno sačuvani i skriveni od trećih osoba. U medijima se sve više govori o zlonamjernim napadima na račune banaka gdje tzv. hakeri raznim sofisticiranim metodama i naprednim tehnologijama „upadaju“ u račune korisnika i bez većih poteškoća zaobilaze sve zaštite.

Stoga je danas pitanje sigurnosti jedan od prioriteta za svakog korisnika Interneta. Bežična komunikacija je zbog svojih karakteristika posebno izložena napadima zbog načina na koji se podaci odašilju pri čemu se otvara mogućnost presretanja informacija koje se razmjenjuju. U standardima koji definiraju bežične računalne mreže postoje određeni elementi sigurnosti, ali oni ne garantiraju uvijek da je postignuta potrebna razina zaštite. U drugim slučajevima ti elementi nisu dovoljno iskorišteni.

Predmet istraživanja ovog rada su su bežične mreže pri čemu su razrađeni svi bitni elementi, prednosti i nedostaci kao i mogućnosti poboljšanja radi veće sigurnosti korisnika. Rad je podijeljen na četiri poglavlja u kojima ćemo razraditi strukturu bežičnih mreža i bitne poveznice. Prvi dio je uvodni u kojem dajemo osvrt na temu rada i osnovne probleme koje istražujemo. U drugom poglavlju upoznajemo se sa pojmom bežičnih mreža, objasniti ćemo njihove elemente i karakteristike, najpoznatije vrste bežičnih tehnologija te prikazati postojeće standarde. U trećem poglavlju bavimo se vrstama bežičnih uređaja koji koriste bežičnu tehnologiju. U četvrtom

poglavlju obraditi ćemo sigurnost bežičnih mreža gdje ćemo objasniti ugrađene sigurnosne mehanizme najraširenijeg standarda 802.11, mogućnosti njegove nadogradnje te ostale naprednije sigurnosne standarde koji pružaju veću razinu zaštite. U posljednjem petom dijelu donosimo zaključak na sve iznesene činjenice i zaključne postavke.

1. BEŽIČNE MREŽE, UMREŽAVANJE I BEŽIČNI PRIJENOS

Bežične mreže (*eng. Wireless Networking*) su računalne mreže koje povezuju jedno ili više računala, a veze uspostavljaju pomoću elektromagnetskih signala ili valova. Elektromagnetski valovi nastaju gibanjem elektrona u prostoru nekim brojem oscilacija u sekundi što se naziva frekvencija. Količina informacija koju elektromagnetski signal može nositi ovisi o rasponu frekvencija (*eng. Frequency Band*). Spektar elektromagnetskih signala vrlo je širok pri čemu signali iz različitih dijelova spektra imaju i različite frekvencije i svojstva. Tako razlikujemo radijske signale ili radijske valove, mikrovalove, infracrvene signale, X i Gama zrake i vidljivu svjetlost. S obzirom da elektromagnetski valovi imaju različita svojstva neki su kao nosioci podataka pogodniji od drugih u zavisnosti od uvjeta u kojima dolazi do prijenosa podataka. Kao primjer možemo navesti infracrvene signale koji ne prolaze kroz zidove te se stoga koriste za prijenos podataka na vrlo malim udaljenostima, npr. unutar iste prostorije, a ukoliko bi se koristile za prijenos podataka između dvije fiksne točke uvijek treba voditi računa da između njih ne postoje nikakve zapreke kao što treba voditi računa i o upitnosti sigurnosti takvog načina prijenosa.

Bežični prijenos podataka počeo se koristiti i prije razvoja računalnih komunikacijskih sustava i to za prijenos televizijskih i radijskih programa. Osnovna razlika između prijenosa navedenih programa i prijenosa podataka je u tome što se kod prvih žele prenijeti informacije što većem broju primatelja dok se kod drugih podaci žele prenijeti samo jednom primatelju, a pri tome onemogućiti dostupnost sadržaja drugim osobama. Kada se prijenos vrši putem čvrstih veza podatke je daleko lakše zaštititi nego što je to moguće kod prijenosa podataka bežičnim putem pri čemu treba voditi računa da podaci budu dostupni samo primatelju kojem su i namijenjeni, što znači da moraju biti nerazumljivi trećim osobama te mora postojati otpornost na zlonamjerna ometanja. Rješenje ovih problema pojavljuje se u vidu različitih frekvencija prema određenim zemljopisnim područjima i ograničavanjem snage signala. Naime, signali slabe sa porastom udaljenosti pri čemu je moguće da se komunikacije odvijaju na istoj frekvenciji, a da pri tom ne ometaju jedna drugu. Da bi se onemogućilo prisluškivanje ili kopiranje sadržaja prijenosa ili ometanje i iskrivljavanje koriste se različite metode zapisivanja i prijenosa signala. Najpoznatije takve metode zovu se metode raširenog spektra frekvencija (*eng. Spread Spectrum Techniques*) kojima je osnovno načelo da se za zapis i prijenos sadržaja koristi znatno širi frekventni pojas od

potrebnog. Takav način kodiranja i prijenosa sadržaja omogućava zaštitu tajnosti sadržaja i smanjenje osjetljivosti prijenosa na vanjske smetnje. Među najpoznatije metode raširenog spektra spadaju metoda skakutanja frekvencija (*eng. Frequency Hopping*) i metoda izravne sekvencije (*eng. Direct Sequence*).

Nadalje, u bežičnoj komunikaciji također postoji više tehnologija zapisivanja i prijenosa sadržaja od kojih možemo navesti temeljne FDMA, TDMA i CDMA[1]. Ove metode nazivaju se metodama fizičkog prijenosa podataka, a osim u bežičnim mrežnim sustavima mogu se koristiti i u žičanim sustavima.

FDMA (*eng. Frequency Division Multiple Access*) znači višestruki pristup s podjelom frekvencija pri čemu se frekvencije šireg pojasa dijele na više užih pojaseva (kanale) pri čemu se svakoj komunikaciji dodjeljuje jedan kanal te se istovremeno u više dodijeljenih kanala odvija više komunikacija unutar istog frekventnog pojasa. FDMA metoda pogodna je za prijenos kod analognih komunikacijskih sustava u što spadaju mobilni telefoni prve generacije (1G) te također za prijenos digitalnih signala.

TDMA (*eng. Time Division Multiple Access*) znači višestruki pristup s podjelom vremena pri čemu se jedan frekventni pojas (kanal) dijeli na vremenske intervale ili otvore (*eng. Slots*) u kojima se u nekom trenutku vrši prijenos sadržaja jedne komunikacije, a svakoj pojedinoj komunikaciji dodjeljuje se neki vremenski interval kako bi se omogućio višestruki pristup za više komunikacija u različitom vremenu. TDMA metoda pogodna je za prijenos digitalnih sadržaja i bila je dominantna za prijenos kod mobilnih telefona druge generacije (2G).

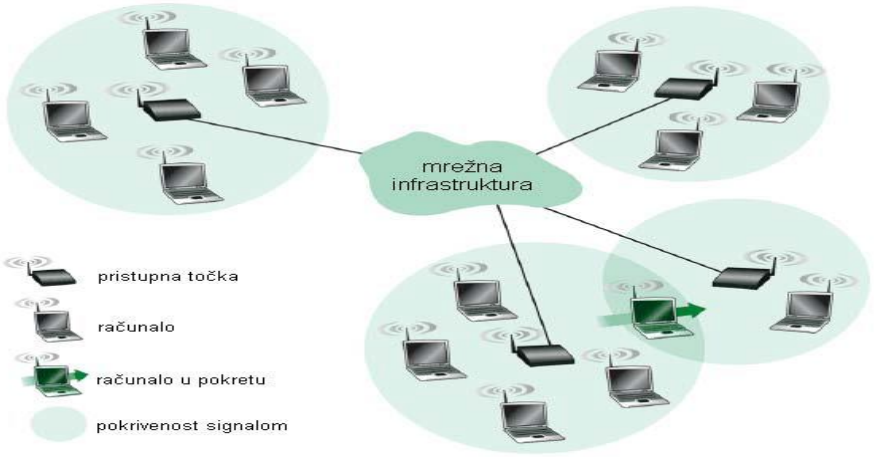
CDMA (*eng. Code Division Multiple Access*) znači višestruki pristup sa podjelom koda pri čemu se koristi raširen spektar frekvencija, a ova metoda spada u metodu izravne sekvencije. Kod ovog načina prijenosa za prijenos sadržaja više komunikacija na jednom kanalu ostvaruje se tako da svaka komunikacija koristi poseban slučajni niz bitova pomoću kojeg kodira svoje sadržaje. Sadržaji svih komunikacija zapisuju se na isti kanal jedan iza drugog i razlikuju se po tome što su kodirani pomoću različitih nizova bitova. CDMA metoda koristi se za prijenos sadržaja treće generacije mobilnih telefona (3G).

[1] Radovan, M. (2010): Računalne mreže 1 – povezivanje računala i mreža, sveučilište u Rijeci, odjel za informatiku, Rijeka, str. 163 - 164

1.1. Elementi bežične mreže

Osnovni elementi bežične mreže i njihove funkcije u okviru mreže su[2]:

1. **čvor bežične mreže** (*eng. Host*) - krajnji uređaji na kojima se izvršavaju aplikacije, kao npr. stolna, prijenosna i džepna računala,
2. **bazna stanica** – najbitniji element bežične mrežne infrastrukture čiji je zadatak predaja i prijem podatkovnih paketa ka ili od pojedinih računala unutar mreže kao i koordiniranu predaju podataka većem broju računala koja su pridružena toj baznoj stanici. Tipični primjer baznih stanica su pristupne točne (*eng. Access Points – AP*) koje kontroliraju pristup mediju, a djeluju i kao mostovi prema drugim bežičnim i ožičenim mrežama,
3. **bežične veze** – računala se s baznom stanicom ili drugim računalima unutar mreže povezuju preko bežične komunikacijske veze. Različite tehnologije bežičnih veza karakteriziraju različite brzine prijenosa i različite domete.



Slika 1 . Elementi bežične mreže
Izvor: http://www.cis.hr/www.edicija/LinkedDocuments/CCERT-PUBDOC-2008-04-225.pdf

Slika 1. prikazuje osnovne elemente bežične mreže gdje je vidljivo da su pristupne točke spojene na mrežnu infrastrukturu dok su računala na mrežu spojena putem pristupnih točaka. Računala u pokretu spajaju se na onu pristupnu točku koja ima najbolju pokrivenost signalom.

[2] Wireless forenzika, CARNet CCERT-PUBDOC-2008-04-225, str. 5

Bazna stanica najčešće je povezana s nekom većom mrežom kao npr. Internet, javne telefonske mreže i sl., a djeluje kao poveznica između računala u bežičnoj mreži i ostatka svijeta. Računala koja su pridružena nekoj baznoj stanici rade u infrastrukturnom režimu rada jer se svi mrežni servisi ostvaruju preko mreže na koju je to računalo povezano preko bazne stanice.

Drugi način povezivanja nalazimo kod neovisne ili ad-hoc mreže gdje pojedina računala ne koriste infrastrukturu već svaki čvor može izravno komunicirati sa svim drugim čvorovima koristeći bežične adaptere. Takva mreža pogodna je za jednostavnu i brzu implementaciju prema potrebama korisnika.

Slika 2. Ad-hoc mreža
Izvor: http://spvp.zesoi.fer.hr/predavanja%202008/WE_skripta.pdf

Slika 2. prikazuje Ad-hoc topologiju gdje računala međusobno komuniciraju putem bežičnih adaptera. Nedostatak ad-hoc topologije je što svi sudionici moraju biti u dometu radio signala. U nedostatku infrastrukture čvorovi sami osiguravaju usluge poput usmjeravanja, dodjeljivanja i dr. zbog čega su puno složeniji od čvorova infrastrukturno bazirane bežične mreže. U slučaju da pokretno računalo prijeđe iz dometa jedne bazne stanice u područje pokrivenosti druge bazne stanice tada ono mijenja svoju pristupnu točku u odnosu na veću mrežu prilikom čega treba riješiti problem određivanja položaja takvog računala u mreži te problem usmjeravanja podataka kako bi se izbjegao prekid veze[3].

[3] http://spvp.zesoi.fer.hr/predavanja%202008/WE_skripta.pdf

1.2. Vrste bežičnih tehnologija

S obzirom na činjenicu da postoji više vrsta bežičnih tehnologija sukladno tome postoji niz specifičnih elemenata koje treba definirati kao i problema koje treba riješiti. Neki od tih problema su određivanje frekvencije odnosno frekventnog pojasa koji će se koristiti za prijenos podataka, zatim potrebno je ishodovati licencu nadležne institucije za određene frekventne pojaseve, odrediti snagu signala koji će se koristiti čime se automatski određuje i maksimalna udaljenost čvorova mreže. Među specifične elemente bežičnog prijenosa spada pitanje interferencije signala (međusobnog utjecaja) i ometanja komunikacije kao i pitanje zaštite sadržaja. Svaka bežična mreža ima svoje specifičnosti koje donosimo u nastavku.

1.2.1. Wi – Fi

IEEE (*eng. Institute of Electrical and Electronics Engineers*) proizveo je set standarda i specifikacija za bežične mreže po nazivom IEEE 802.11 koji definira format i strukturu signala relativno kratkog dometa koje pruža Wi-Fi usluga. Originalni 802.11 standard lansiran je 1997. godine. Naziv Wi-Fi je ime za obitelj bežičnih lokalnih mreža (eng. *wireless LAN-WLAN*) koje su definirane sa više varijanti IEEE standarda 802.11[4].

Slika 3. Wi-Fi mreža
Izvor: http://www.computerhint.com/software-guide/what-is-a-wlan-wireless-lan-or-wifi/

Slika 3. prikazuje pristupnu točku na koju se računala mogu spajati bežično putem Wi-Fi ja ili žičano putem kabla. Wi-Fi je tehnologija pristupa i priključenja IP uređaja na žičnu mrežu korištenjem bežične tehnologije radio uređaja. Korisnički IP uređaji imaju radio (bežični adapter)

[4] http://cdn.ttgtmedia.com/searchNetworking/downloads/wireless_sample.pdf

sa kojim se priključuju na pristupnu točku. Navedeni radio uređaj odašilje signale na frekventnom pojasu za koji nije potrebna dozvola za rad – na 2, 4 GHz ili 5 GHz. Svaka točka pristupa omogućava da preko nje bežičnim putem međusobno komuniciraju oni uređaji koji su vezani na tu točku pristupa. Točke pristupa međusobno su povezane preko žičanog distribucijskog sustava koji je obično lokalnih razmjera – to može biti jedna mreža tipa Ethernet zbog čega se mreže iz Wi-Fi obitelji mogu nazivati i bežičnim Ethernetom. Isto tako distribucijski sustav može biti i neki od opsežnijih kao npr. neki od oblika proširenog LAN-a. Distribucijski sustav najčešće je vezan na Internet mrežu tako da spajanjem na neku točku pristupa nekog WLAN-a računalo dobije mogućnost komunikacije u globalnoj Internet mreži[5].

1.2.2. Bluetooth

Razvoj Bluetooth tehnologije započela je tvrtka Ericsson 1994. godine. Svrha istraživanja bila je pronaći troškovno i tehnološki učinkovito radio sučelje niske potrošnje za mobilne uređaje za male udaljenosti. Naziv Bluetooth dat je prema imenu danskog kralja Haralda Bluetootha (940.-986.) koji je poznat u povijesti kao kralj koji je ujedinio Dansku i Norvešku. Za razvoj i standardizaciju Bluetooth sučelja formirana je posebna grupa 1998.godine koja danas ima više od 4.000 članova, a predvode je tvrtke Ericsson, Nokia, Toshiba, Intel i IBM. Specifikacija Bluetooth tehnologije objavljena je 1999.godine, a 2002.godine IEEE usvojio je IEEE 802.15.1 standard za bežične privatne mreže PAN (*eng. Personal Area Network*) zasnovan na Bluetooth specifikaciji[6]. Bluetooth bežična tehnologija prvobitno je razvijena kao tehnologija za bežično povezivanje mobilnih aparata. Danas ova tehnologija omogućuje povezivanje prijenosnih i stolnih računala, računalne opreme, mobilnih telefona, kamera i drugih digitalnih uređaja upotrebom bežičnih veza na relativno malim udaljenostima. Ova tehnologija se koristi i kao zamjena za kabel, stvaranje privatnih ad-hoc mreža te ostvarivanje pristupnih točaka za povezivanje korisničkih terminala na postojeće mreže za prijenos govora i podataka. Glavne

[5] Radovan, M.: op. cit. pod. 1, str. 165
[6] Restović A., Stojan I., Ćubić I. (2005): Bluetooth bežična tehnologija i njezine primjene, http://www.ericsson.com/hr/etk/revija/Br_1_2005/bluetooth.pdf

karakteristike Bluetooth tehnologije su robusnost te značajna troškovna učinkovitost kao i ekonomičnost u potrošnji energije i snage[7].

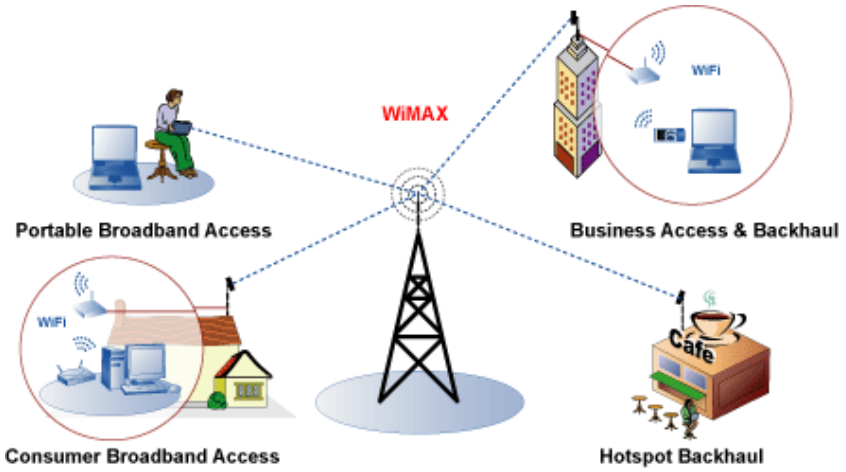
Slika 4. Bluetooth povezivanje uređaja
Izvor: http://blog.tonerboss.com/tips-on-using-a-bluetooth-enabled-printer/

Slika 4. prikazuje različite uređaje koji se koristeći bluetooth tehnologiju mogu međusobno bežično povezati. Na ovaj način moguć je prijenos podataka, slušanje muzike, slanje dokumenata putem mobitela na printanje, povezati tipkovinicu gdje treba voditi računa o udaljenosti koje ne mogu biti velike.

1.2.3. WiMax

WiMax (*eng. Worldwide Interoperability for Microwave access*) je bežična tehnologija koja omogućava širokopojasni bežični pristup Internetu uz upotrebu radio frekvencijskog spektra[8]. WiMax tehnologiji zasnovana je na Ethernetu, obitelji normi IEEE 802. Standard 802.16 razvijen je od strane IEEE i predstavlja bežičnu tehnologiju dizajniranu i optimiziranu za tzv. gradske računalne mreže (*eng. Metropolitan Area Networks - MAN*). Tehnologija 802.16 komplementarna je sa bežičnom tehnologijom 802.11 dizajniranom i optimiziranom za lokalne računalne mreže (*eng. Local Area Networks - LAN*). Standard 802.16 omogućava isporuku širokopojasnog pristupa te predstavlja alternativu kablovskom i DSL širokopojasnom pristupu. WiMax tehnologiju odlikuje velika pokrivenost od 15 do 50 km, a slična je Wi-Fi tehnologiji uz razliku u navedenom dometu.

[7] Hamidović, H. (2009): WLAN bežične lokalne računalne mreže, Priručnik za brzi početak, BiH, str. 196
[8] Padarić, D., Kukec, M. (2009): WiMAX 802.16 standard, Tehnički glasnik, Časopis veleučilišta u Varaždinu, str. 54



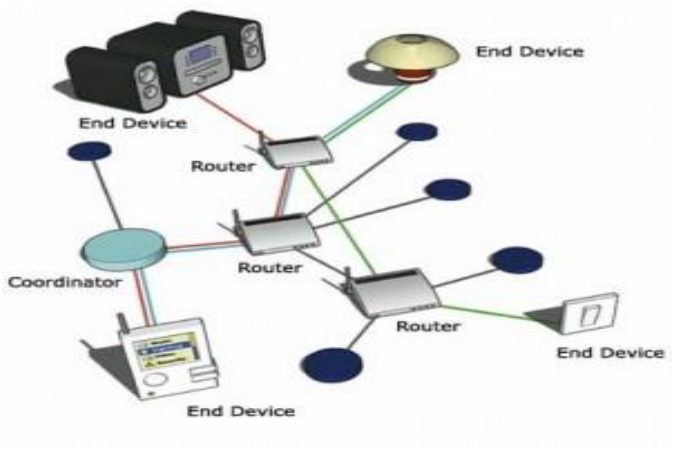
Slika 5. Prikaz uloge WiMax mreže
Izvor: http://www.gemtek.com.tw/pro_odu_230S.html

Slika 5. prikazuje mogućnost spajanja različitih korisnika putem WiMax bazne stanice. Svaki bežični korisnik unutar dometa bazne stanice trebao bi biti u mogućnosti pristupiti WiMax servisu. Metoda rada WiMax tehnologije različita je od metode rada Wi-Fi tehnologije jer se putem Wi-Fi-ja spajanje može vršiti putem rutera ili hot-spot-a dok se spajanje u WiMax mreži sastoji od dva dijela od kojih je jedan WiMax toranj (*eng. WiMax tower*) poznat i kao WiMax bazna stanica (*eng. Wimax base station*) dok je drugi dio WiMax resiver (*eng. WiMax receiver*) ili WiMax CPE (*eng. WiMax Customer Premise Equipment*). Postoje dvije primjene u kojima WiMax može pokazati svoje prednosti i obje su vezane uz širokopojasni pristup Internetu. S jedne strane omogućiti će se implementacija broad banda na području gdje je gradnja žičane infrastrukture kompliciranа ili neisplativa ili ju je teško izgraditi. S druge strane daje se mogućnost konkurentskim operaterima da ponude širokopojasni Internet po nižim cijenama uz veće brzine. WiMax tehnologija udovoljava potrebama i interesima potrošača, a ima za krajnji cilj povećanje prihoda, poboljšanje konkurentnosti i povećanje produktivnosti.

1.2.4. ZigBee

IEEE institut je u travnju 2003.godine odobrio IEEE 802.15.4 standard namijenjen za stvaranje bežičnih privatnih mreža s malom propusnošću LR-WPAN (*eng. Low Rate Wireless Personal Area Networks*). Navedeni standard osim male propusnosti mreže određuje i malu potrošnju energije i malu složenost. Ova bežična komunikacija temeljena na ZigBee tehnologiji

namijenjena je elektroničkim uređajima razmjerno malih dimenzija i niske potrošnje energije[9]. Porijeklo imena ove bežične mreže potječe od engleskog naziva „*ZigBee principle*“ kojim se označava tehnika koju koriste pčele kako bi ostale članove zajednice obavijestile o pronalasku hrane. ZigBee tehnologiju na fizičkom sloju definiraju dva tipa uređaja – FFD (*eng. Full Function Device*) i RFD (*eng. Reduced Function Device*).



Slika 6. Uređaji povezani u ZigBee mrežu
Izvor: http://www.mobilenetx.com/what-is-zigbee-technology

Slika 6. prikazuje tipičnu ZigBee mrežu koja se sastoji od tri vrste uređaja, a to su ZigBee koordinator ZC (*eng. ZigBee Coordinator*), ZigBee ruter ZR (*eng. ZigBee Router*) i ZigBee ZED (*eng. ZigBee End Device*). ZigBee koordinator i ZigBee ruter moraju biti FFD uređaji dok su krajnji uređaji obično RFD tipovi uređaja. Uređaji u mreži imaju ulogu ili „roditelja“ ili „djeteta“ u zavisnosti da li se drugi uređaji spajaju na njih. Mogućnosti upotrebe ZigBee mreže su brojne – od automatizacije zgrada, korištenja u sigurnosnim sustavima u kućama, senzorskim mrežama, industrijskim mrežama, daljinskim mjerenjima do povezivanja raznih periferija na osobna računala.

1.2.5. IrDA

U današnje doba infracrvena tehnologija koristi se gotovo svakodnevno u kućanstvima. Primjeri takvog korištenja su daljinski upravljači za upravljanje televizorima kao i za upravljanje čitavim nizom elektroničkih uređaja, a signale šalju putem infracrvene svjetlosti. Osim za upravljanje

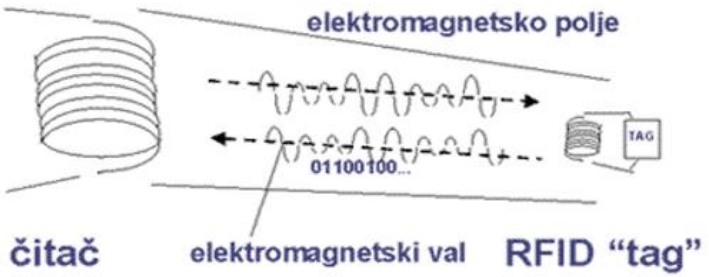
[9] Hamidović, H.: op. cit. pod. 7, str 200

televizorima, DVD playerima, TV tunerima i drugim elektroničkim uređajima, infracrvena svjetlost može se koristiti i za bežično povezivanje računala. Za otkriće infracrvenog zračenja zaslužan je fizičar William Herschel (1738.-1822.) koji je zapazio kako svjetlo koje prolazi kroz različito obojene filtere zagrijava stvari. Jedno od važnijih područja primjene infracrvenog zračenja je i u vatrogastvu jer omogućava vatrogascima gledanje u dimu što je problem koji danas na niti jedan drugi način nije moguće riješiti. IrDA uređaji koriste RF spektar koji obuhvaća elektromagnetsko zračenje valnim duljinama većim od valne duljine vidljive crvene svjetlosti, a manjim od valne duljine radio – valova. Najbolja povezanost uređaja postiže se na udaljenostima do 1 metra. IrDA tehnologija obično se koristi za sinkronizaciju podataka ili prijenos datoteka. Nove IrDA specifikacije omogućavaju i siguran prijenos financijskih informacija. Tijekom IrDA komunikacije jedan uređaj je primarni dok je drugi sekundarni. Početna brzina komunikacije uspostavlja se brzinom od 9.600 bps te nakon početnog pregovaranja uređaji usklađuju brzinu kojom će nastaviti komunicirati[10].

1.2.6. RFID

RFID (*eng. Radio Frequency Identification*) znači prepoznavanje pomoću radio-valova. Osnovni RFID sustav sastoji se od tagova, čitača tagova i softvera za procesiranje. Podaci koje tag može slati o objektu na kojem se nalazi mogu biti beskonačno različiti – cijena, boja, datum proizvodnje, datum isteka roka trajanja itd. Informacije dobivene s taga RFID čitač može obrađivati interno ili slati središnjem uređaju na daljnju obradu. RFID sustavi grupiraju se u tri frekvencijska područja - Low Frequency, High Frequency i Ultra High Frequency. Prednosti korištenja RFID sustava u odnosu na bar-kod sustav su mogućnost primjene u vlažnoj, prašnjavoj i prljavoj okolini, za očitavanje nije potrebna izravna optička vidljivost između čitača i taga, čitanje i pisanje podataka vrši se bez ikakvog kontakta s objektom, tag može imati veliki kapacitet memorije za pohranu podataka. Bez obzira na navedene prednosti RFID tehnologija ne smatra se boljom od tehnologije bar-koda. Prednost tehnologije bar-koda je niža cijena naljepnica, a općeprihvaćeni standardi na tom području čine je globalno upotrebljivom.

[10] Ibidem, str 202 - 205



Slika 7. RFID princip rada
Izvor: http://www.gs1hr.org/djelatnosti/prikupljanje/rfid

Slika 7. prikazuje interakciju u elektromagnetskom polju između čitača i taga gdje tag putem elektromagnetskog vala šalje povratnu informaciju pohranjenu u sebi natrag čitaču. RFID se danas upotrebljava u kontroli pristupa, evidenciji prisutnosti, evidenciji masovnih prolazaka (autoceste, skijališta), evidenciji životinja, a sve veću primjenu nalazi u proizvodnji i skladištenju roba. Razvoj RFID tehnologije rezultira sve jeftinijom proizvodnjom opreme (tagova, čitača), sve većom memorijom, širim dometom prijenosa signala i bržom obradom. Uz sve navedeno nije izgledno da će RFID tehnologija skroz zamijeniti bar-kod. Njeno veliko širenje omogućila bi uspješna standardizacija koja bi omogućila kompatibilnost RFID opreme različitih proizvođača i pad cijena[11].

1.2.7. HomeRF

HomeRF (*eng. Home Radio Frequency*) koristi se za prijenos zvuka, slike i podataka unutar ureda. Služi ne samo za komunikaciju između PC-a već i za povezivanje pokretnih uređaja (npr. telefoni), printera, kontrolnih uređaja, audio i video uređaja s PC-om. Jedna od glavnih primjena HomeRF-a je „*Resource Sharing*"dijeljenje odnosno zajedničko korištenje periferne infrastrukture (printera, interneta, veza) između više PC-a. HomeRF jedinice koriste SWAP protokol (*eng. Shared Wireless Access Protocol*) koji je kombinacija CSMA (korištenog u lokalnim računalnim mrežama) i TDMA (korištenog u mobilnim telefonima) protokola. SWAP je hibrid između 802.11 i DECT standarda i razvijen je od strane HomeRF radne grupe. HomeRF uređaji smatraju se sigurnijima od 802.11 uređaja koji koriste WEP. HomeRF koristi frekvencijsko područje od 2,4 GHz-a i oba koriste tehnologiju „*Spread Spectrum*". To je

[11] Ibidem, str. 206 - 208

tehnologija kod koje se koristi veći frekvencijski pojas zbog povećanja efikasnosti. Neke od osobina HomeRF su 50 skokova u sekundi, 2, 4 GHz ISM opseg, brzina prijenosa do 10 Mbps, kompatibilnost unatrag itd.[12]

1.3. Karakteristike bežičnih mreža

Glavna prednost bežičnih mreža je mogućnost kretanja klijentskih računala unutar nje tj. bez prekida veze na mrežu što se većinom postiže posebnim postupkom, tzv. roaming-om koji omogućuje prijelaz s jedne pristupne točke na sljedeću najbližu tijekom slanja ili primanja podataka. Klijenti se u bežičnim mrežama prespajaju na sljedeću pristupnu točku u trenutku kada mrežna kartica zaključi kako je signal trenutne pristupne točke preslab za daljnju pouzdanu komunikaciju. Prilikom prijelaza često se dešava promjena radio kanala na kojem se provodi komunikacija[13]. Uz uobičajena izobličenja signala koja su prisutna u svim vrstama prijenosa (žični, optički, bežični) kod bežičnih mreža pojavljuju se i smetnje kojih nema u drugim vrstama prijenosa od kojih možemo navesti sljedeće[14]:

- **gubitak snage elektromagnetskog zračenja uslijed prostiranja** *(eng. Path Loss)*
  Snaga EM zračenja opada približno sukladno eksponencijalnom zakonu sa povećanjem udaljenosti odašiljača. Prigušenje signala ovisi o udaljenosti i snazi odašiljača, fizičkim preprekama (npr. razni objekti) od kojih se zračenje reflektira te o količini međudjelovanja s ostalim čvorovima koji odašilju signale,
- **višestazno prostiranje** *(eng. Multipath Propagation)*
  Nastaje kada se EM zrake iz jednog izvora reflektiraju od objekata na svom putu do odredišta. Zbog toga na odredište stiže originalni signal i njegove zakašnjele verzije koje mogu biti više ili manje prigušene. Višestazno prostiranje uzrokuje povećanje kašnjenja i u konačnici intersimbolnu interferenciju (ISI) koja se manifestira neželjenim proširenjem simbola u prijemu uslijed čega simboli ometaju jedni druge,
- **iščezavanje signala uslijed zasjenjenja** *(eng.shadow fading)*

[12] Ibidem, str. 208 - 209
[13] Wireless forenzika: op. cit. pod. 2, str. 7
[14] Jeren, B., Pale, P.: Sustavi za vođenje i praćenje procesa, http://spvp.zesoi.fer.hr/predavanja%202008/WE_skripta.pdf

Uzrokuju ga fizičke prepreke na putu prostiranja EM zraka, a prigušenje signala u ovom slučaju ovisi o dielektričnim svojstvima materijala prepreke,

- **kašnjenje signala uslijed prostiranja prijenosnim medijem**
  Iz gore navedenog možemo zaključiti da su bežične komunikacije daleko nepouzdanije od žičanih.

1.4. 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.

1.4.1. IEEE 802.11

IEEE (*eng. Institute of Electrical and Electronics Engineers*) razvio je najznačajnije standarde za bežične mreže. Međutim, najšire prihvaćen standard bio je IEEE 802.11 poznati i kao Wi-Fi. Postoji puno njegovih varijacija, a tri najvažnije su 802.11a, 802.11b, 802.11g[15].

802.11 specifikacija	Širina kanala	Frekvencijski opseg	Modulacija	Maksimalna brzina prijenosa
802.11a	20 MHz	5160-5330 MHz	OFDM (eng. *Orthogonal Frequency Division Multiplexing*)	54 Mbps
802.11b	22 MHz	2401-2495 MHz	DSSS (eng. *Direct Sequence Spread Spectrum*)	11 Mbps
802.11g	22/20 MHz	2401-2495 MHz	DSSS/OFDM	54 Mbps

Slika 8. Prikaz standarda i njihovih karakteristika
Izvor: http://www.cert.hr/sites/default/files/CCERT-PUBDOC-2008-04-225.pdf

Slika 8. donosi pregled varijacija standarda 802.11, njegove širine kanala, frekvencijskog opsega, modulacije te maksimalne brzine prijenosa. Svi navedeni standardi koriste Ethernet protokol i CSMA/CA i razlikuju se međusobno po brzini prijenosa i broju kanala. Na tržištu prevladavaju WLAN-ovi bazirani na standardu 802.11 b. Sva tri standarda podržavaju dva načina rada mreže i to ad-hoc i infrastrukturni, a smanjenjem brzine prijenosa moguće je ostvariti prijenos na veće

[15] Hamidović, H.: op. cit. pod. 7, str. 141

daljine. Glavne razlike uočavamo na fizičkom nivou. 802.11b WLAN-ovi koriste brzinu prijenosa do 11 Mbps što je dovoljna brzina za većinu mreža i radi u frekventnom opsegu od 2,4 do 2,485 GHz koji se koristi od strane bežičnih mobilnih telefona. Bežične mreže mogu raditi i sa većim brzinama prijenosa i pri višim frekvencijama kao npr.802.11a (brzina prijenosa do 54 Mbps, frekvencija 5,15- 5,72 GHz) no razmaci u prijenosu su kraći, a smetnje zbog multipath propagacije veće[16].

1.4.2. 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[17].

1.4.3. FFC

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[18]. Sukladno FCC

[16] http://www.webopedia.com/TERM/8/802_11.html
[17] http://www.wi-fi.org/
[18] Hamidović, H.: op. cit. pod. 7, str. 146

standardu 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[19]

1.4.4. 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[20].

1.4.5. WLANA

WLANA (*eng. Wireless LAN Association*) je neprofitna obrazovna trgovinska udruga sastavljena od vodećih ljudi i tehnoloških inovatora u bežičnoj tehnološkoj industriji. Misija WLANA-e je da educira i promiče bežične mrežne tehnologije i bežičnu industriju. Svatko tko o WLAN-ovima želi naučiti nešto više najbolji edukacijski izvor je upravo WLANA. Ona također može pomoći u potrazi za određenim proizvodom ili servisom za bežične mreže.

[19] http://www.cisco.com/c/en/us/products/collateral/wireless/aironet-1300-series/prod_white_paper0900aecd801c4a88.html
[20] http://www.etsi.org/

2. WLAN UREĐAJI

Kako bi na najbolji način mogli implementirati i koristiti bežične mreže jedna od bitnih stvari je znati karakteristike opreme koja nam stoji na raspolaganju. U nastavku će biti objašnjene hardverske komponente koje su osnova bežičnih LAN-ova.

2.1. Pristupne točke

Pristupne točke (*eng. Access Point – AP*) osiguravaju točku pristupa mreži za bežične klijente. One komuniciraju s drugim pristupnim točkama, s bežičnim klijentima i ožičenom mrežom, a mogu biti konfigurirane za rad u tri moda – korijenski mod, most mod i ponavljački mod. Standardne operacije pristupnih točaka rade u korijenskom modu, a druga dva moda su proširenje funkcionalnosti. Bežične pristupne točke unutar neke ustanove moraju se pažljivo razmjestiti, a da ne bi dolazilo do preklapanja područja komunikacije tamo gdje to nije poželjno preporuča se svaku pristupnu točku 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 točke imaju različite hardverske i softverske opcije, a najčešće su[21]:

- 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 točke s nefiksiranim antenama omogućuju korištenje različitih antena i kablova različitih duljina kako bi se npr. korisniku koji je van objekta omogućio pristup mreži na pristupnu točku koja se nalazi unutar objekta. Filtriranje se koristi kako bi se odbio pristup WLAN-u neovlaštenim korisnicima

[21] Hamidović, H.: op. cit. pod. 7, str. 69 - 70

gdje kao osnovnu mjeru sigurnosti pristupnu točku možemo konfigurirati za filtriranje uređaja koji nisu navedeni na MAC filter listi pristupne točke.

Slika 9. Bežična pristupna točka
Izvor: http://www.informatika.buzdo.com/s930-intranet-bezicna-komunikacija.htm

Slika 9. prikazuje bežičnu pristupnu točku. Modularne radio kartice mogu raditi na način da jedna radio kartica djeluje kao pristupna točka, a druga kao most ili da svaka od radio kartica djeluje kao neovisna pristupna točka. Promjenjiva izlazna snaga omogućava kontrolu razine snage koju pristupna točka koristi za slanje podataka, a kontrola snage izlaza bitna je u situaciji kada udaljeni čvorovi ne mogu locirati pristupnu točku. Kontroliranje izlazne snage na pristupnoj točki i anteni bitno je i zbog ograničenja koja postavljaju regulatori, a pravilan mrežni dizajn i metode povezivanja služe da pristupna točka ne postane usko mrežno grlo[22].

2.2. Bežični mostovi

Bežični mostovi (*eng. Wireless Bridges*) služe za bežično povezivanje ožičenih LAN segmenata. Koriste se u konfiguracijama točka-točka ili točka-više točaka. Mogu biti konfigurirani za rad u jednom od četiri moda i to[23]:

- korijenski mod
- nekorijenski mod

[22] http://www.informatika.buzdo.com/s930-intranet-bezicna-komunikacija.htm
[23] Hamidović, H.: op. cit. pod. 7, str. 72

- pristupna točka mod
- ponavljački mod

Kod korijenskog moda jedan od mostova u svakoj grupi mora biti konfiguriran za rad u korijenskom modu rada dok se u nekorijenskom modu mostovi spajaju bežično na mostove u korijenskom modu rada. Nekorijenski mod rada je poseban mod jer u njemu most djeluje simultano i kao pristupna točka i kao most. Kod moda pristupna točka most dobije funkcionalnost pristupne točke kako i sam naziv kaže, te most može u potpunosti biti pretvoren u pristupnu točku. U ponavljačkom modu rada mostovi su korijenski i nekorijenski, a ovaj mod rada postavlja se između druga dva mosta s ciljem produžetka segmenta koji se bežično premošćuje. Hardverske i softverske opcije za bežične mostove slične su onima koje nalazimo u pristupnim točkama i imaju većinom istu svrhu[24].

2.3. Bežični LAN klijentski uređaji

Bežični LAN klijentski uređaji su uređaji krajnjih korisnika od kojih možemo navesti laptop, PDA, bežični IP telefon, desktop, bežične printer servere, bežični prezentacijski gatewayi, IP kamere i sl. Navedenim uređajima potrebna je bežična veza do mrežne infrastrukture koja se ostvaruje korištenjem nekog od niže navedenog WLAN radio – uređaja[25]:

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

[24] Ibidem, str. 75
[25] Ibidem, str. 78

Slika 10. WLAN PC kartica
Izvor: http://www.index.hr/vijesti/clanak/nova-generacija-siemens-gigaseta-predstavljena-na-cebitu/254828.aspx

Slika 10. prikazuje WLAN PC karticu. Najčešća komponenta bilo koje bežične mreže je PCMCIA kartica koja je još poznata pod nazivom PC kartica. Koristi se u laptopima i PDA uređajima, a komponenta je koja osigurava vezu između mreže i klijentskog računala. Svaka PC kartica ima antenu koje se razlikuje ovisno o proizvođaču, a neke imaju i višestruke antene.

Ethernet i serijski konvertori koriste se s uređajima koji imaju Ethernet ili 9-pinski serijski port s ciljem da se navedeni mrežni konektori pretvore u WLAN konektore. Serijski konvertori se najčešće koriste sa starijom opremom koja koristi serijski priključak za mrežno povezivanje. USB adapteri vrlo 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 računalu.

Slika 11. WLAN USB klijent
Izvor:http://www.tigerdirect.com/applications/SearchTools/item-details.asp?EdpNo=5265581

PCI i ISA adapteri instaliraju se unutar desktop ili serverskog računala. Bežični PCI uređaji su također plug-n-play kao i USB adapteri za razliku od bežičnih ISA kartica koje najčešće nisu plug-n-play i zahtijevaju ručnu konfiguraciju. Instaliranje WLAN klijentskih uređaja uključuje dva koraka – instalaciju drajvera i pomoćnih programa[26].

[26] Ibidem, str. 79

2.4. Bežični gatewayi

Bežične gateway-e možemo podijeliti na gateway-e za male tvrtke i kuće i gateway-e za korporacije. Bežični gatewayi za male tvrtke i kuće služe sa spajanje manjeg broja bežičnih čvorova na jedan uređaj radi povezivanja na Internet ili druge mreže i obično uključuju ugrađeni hub ili preklopnik i potpuno podesivu pristupnu točku. WAN port na bežičnim gatewayima najčešće je Ethernet port namijenjen vezi s Internetom preko kablovskog modema, xDSL modema, analognog modema ili satelitskog. Korporacijski bežični gateway pogodan je za velika okruženja i može osigurati specijalizirane usluge autentikacije i povezivost za bežične klijente. Korporacijski bežični gatewayi moraju imati snažne CPU-ove i brza sučelja kako bi mogli podržavati više pristupnih točaka[27].

2.5. 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 signala[28]. 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 pokrivanja oko središnje točke. Kod vanjske upotrebe preporuča se njihovo smještanje na vrh građevine, a pogodne su za

[27] Ibidem, str. 81 - 83
[28] Iskratrade d.o.o., Ruckus – Osnovno o Wi – Fi antenama, lipanj 2012., http://iskratrade.hr/Portals/0/datasheets/ITR-%20Ruckus-antene.pdf

sajmove i skladišta gdje je potrebno 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 odašilju[29].

2.6. PoE

PoE (*eng. Power Over Ethernet*) je tehnologija koja omogućava napajanje električnom energijom pristupnim točkama bežičnog LAN-a kao i primanje podataka preko istih postojećih LAN kablova bez modifikacije Ethernet infrastrukture. U telekomunikacijama već postoji primjena prijenosa električne energije mrežnim vezama, međutim PoE tehnologija omogućava integriranje podataka, glasa i energije preko standardne Ethernet infrastrukture te uz centraliziran sustav za neprekidno napajanje UPS (*eng. Uninterrupted Power supply*) osigurava neprekinuto napajanje tijekom prekida napona sustava. Zbog svega navedenog PoE tehnologija štedi novac i vrijeme jer nema potrebe za instalacijom dodatnih napojnih kablova, utičnica te nema niti potrebe za dodatnim UPS uređajima za svaki pojedinačni mrežni uređaj. Također ukoliko dođe do prestanka funkcioniranja neke od pristupnih točaka potrebno ju je resetirati (inače je potrebno povremeno resetirati sve pristupne točke) što se kod primjene PoE tehnologije može obaviti iz ureda bez potrebe za fizičkim obilaskom lokacije gdje se pristupne točke nalaze. Nadalje ukoliko dođe do promjene lokacije pristupne točke nije potrebno vršiti promjene na elektro - naponskim instalacijama već je moguće eksperimentirati s različitim pozicijama sa svrhom dobijanja najbolje pokrivenosti[30].

[29] Ibidem, str. 86 – 88
[30] Ibidem, str. 91

3. SIGURNOST BEŽIČNIH MREŽA

U današnje vrijeme teško je zamisliti svakodnevni život bez računalne tehnologije. Ona je prisutna u svim segmentima društva. Među računalnim tehnologijama vrlo važno mjesto zauzimaju bežične tehnologije čija se upotreba rapidno širi. Danas postoji veliki broj uređaja koji koriste bežičnu tehnologiju kao npr. bluetooth slušalice, bežični printeri, routeri, Wi-Fi stickovi koje možemo naći u svakom prosječnom domaćinstvu. Popularnosti bežičnih mreža doprinijela je jednostavnost implementacije, veliki izbor uređaja, fleksibilnost u radu te smanjenje troškova u odnosu na klasične lokalne mreže. Stoga ne čudi da su one u upotrebi u većini javnih i privatnih organizacija, a sve popularniji je i trend postavljanja tzv. vrućih točaka (*eng. Hot Spot*) putem kojih je dozvoljen besplatan pristup Internetu sa bilo kojim uređajem koji podržava bežičnu mrežu.

Međutim, paralelno sa njihovom ekspanzijom postavlja se pitanje njihove sigurnosti. Neovlašten pristup mreži određenog korisnika može izazvati mnoge probleme – povredu privatnosti, krađu podataka, onemogućiti rad korisnikove mreže, izvesti napad na neki treći sustav, uzrokovati direktnu financijsku štetu, pa i objavljivanje u javnosti nekih tajnih podataka što može dovesti do raznih sukoba, javnog sramoćenja pogotovo ukoliko se radi o politički izloženim osobama ili bilo kojoj javnoj osobi. Dakle, sigurnost bežičnih mreža od vrlo velike je važnosti svakoj osobi koja se koristi ovakvim načinom spajanja na Internet. Kako se ovo područje jako brzo mijenja zbog velikog napretka računalne tehnologije, vrlo je bitno pratiti trendove jer se sa novim mogućnostima pojavljuju i nove prijetnje i ranjivost.

U standardima koji definiraju bežične računalne mreže postoje razni elementi sigurnosti, međutim oni su u većini slučajeva nedovoljno iskorišteni, ali i kada se koriste upitno je da li je postignuta dovoljna razina sigurnosti zbog čega dolazi zbog nedostataka samog standarda kao i zbog nekih drugih razloga. Osnovni sigurnosni zahtjevi u bežičnoj komunikaciji su tajnost podataka koji se prenose, besprijekornost podataka odnosno sigurnost da nisu mijenjani u prometu, autentičnost pošiljatelja što znači da onaj koji je naveden kao pošiljatelj to doista i jeste te neporecivost što znači da onaj koji je poslao poruku ne može to kasnije poreći[31]. Početni WEP standard koji se koristio pokazao se neučinkovit zbog lakog „probijanja“ zaštite uslijed čega je

[31] http://www.cert.hr/sites/default/files/CCERT-PUBDOC-2009-06-267.pdf

stvoren novi WPA standard te WPA2 standard kao konačni oblik. U nastavku ovog poglavlja objasniti ćemo razlike u sigurnosnim standardima te prikazati sadašnje stanje u području sigurnosti bežičnih tehnologija.

3.1. Napadi na bežične mreže

Postoji više načina neovlaštenog pristupa bežičnim mrežama. U nastavku donosimo neke od njih[32]:

- 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 sustav,
- zlonamjerno povezivanje (*eng. Malicious Association*) – izvodi se posebnim programima koji mrežnu karticu napadača predstavljaju kao legitimnu pristupnu točku 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 točke tj. izravno između dva računala (*eng. Peer-to-Peer*) i da se često ne koriste zaštitne metode kakve se mogu uvesti kroz pristupnu točku, sustav 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 pak 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,

[32] Ibidem

- 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.

3.2. Sigurnosni mehanizmi 802.11 standarda

Standard IEEE 802.11 sadrži određeni broj ugrađenih sigurnosnih mehanizama kako bi se minimalizirala zloupotreba i neovlašten pristup mreži. Međutim, čak i u slučaju aktivacije tih sigurnosnih mehanizama to nužno ne znači da je postignuta potrebna razina sigurnosti, a bežične mreže su najslabiji aspekti sigurnosti svake organizacije. Najveći problem je taj što standardi i njihovi mehanizmi ne zadovoljavaju tri najbitnija sigurnosna uvjeta – autorizacija korisnika, zaštita privatnosti i pouzdana autentikacija korisnika. Najosnovniji ugrađeni sigurnosti mehanizmi standarda 802.11 su SSID (*eng. Service Set Identifier*), autentikacija te statički WEP ključ (*eng. Wired Equivalent Privacy*) koji spada u osnovne sigurnosne mehanizme. U nastavku ćemo obrazložiti svaki od navedenog sigurnosnog mehanizma.

3.2.1. SSID

SSID predstavlja identifikator skupa usluga te predstavlja niz znakova koji daju jedinstveno ime bežičnom LAN-u. SSID ponekad predstavlja ime mreže koje omogućava stanicama spajanje na željenu mrežu kada veći broj nezavisnih mreža operira u istom fizičkom prostoru. Svaki set bežičnih uređaja komunicira direktno međusobno što se naziva osnovni skup usluga (*eng. Basic Service Set – BSS*). Nekoliko BSS-ova može biti udruženo zajedno tvoreći jedan logički WLAN segment koji se tada naziva proširen skup usluga (*eng. Extended Service Set – ESS*). SSID pojednostavljeno rečeno je 1-32 byte-no alfanumeričko ime koje dobija svaki ESS. Jedan ESS ili

WLAN segment može se sastojati od nekoliko pristupnih točaka (*eng. Access Point-AP*) i stanica koje koriste isti SSID.

Druga organizacija u istoj zgradi može operirati putem svog WLAN segmenta koji je sastavljen od pristupnih točaka i stanica koje koriste drugi SSID. Svrha SSID-a je da pomogne stanicama u jednom WLAN segmentu pronalaženje i spajanje na pristupne točke u istom segmentu istovremeno ignorirajući pristupne točke koje spadaju drugom WLAN segmentu. Svaka pristupna točka oglašava se nekoliko puta u sekundi šaljući upravljačke okvire (*eng. Beacon Frames*) koji nose ime ESS-a odnosno SSID. Stanice mogu otkriti pristupne točke osluškivanjem upravljačkih okvira ili mogu slati testne okvire u svrhu aktivnog traženja pristupnih točaka za željenim SSID-om. Nekim okvirima dozvoljeno je da nose SSID nulte duljine (*eng. Zero Length*) koji se nazivaju odašiljući SSID-ovi (*eng. Broadcast SSID*).

U tom slučaju stanica može poslati testni zahtjev koji nosi odašiljući SSID – pristupna točka u tom slučaju mora vratiti svoj stvarni SSID kao odgovor. Neke pristupne točke mogu biti konfigurirane za slanje SSID nulte duljine u upravljačkim okvirima umjesto slanja svog aktualnog SSID-a. Međutim, nije moguće sačuvati vrijednost SSID-a tajnom jer se njena stvarna vrijednost nalazi u više okvira. Ovaj sigurnosni mehanizam može se na prvu činiti kao dobar način kontrole pristupa podacima – međutim, u praksi nije tako. S obzirom da se svi okviri ne šalju u enkripcijskom obliku napadač može lako doći do naziva SSID-a i neovlaštenog pristupa mreži osluškivanjem komunikacije unutra mreže tj. hvatanjem kontrolnih okvira koje odašilju sve pristupne točke.

3.2.2. Autentikacija

Da bi korisnik mogao pristupiti mreži prvi korak je autentikacija. To je proces koji osigurava verifikaciju bežičnih čvorova od strane mreže na koju se čvorovi žele povezati. Ugrađen sigurnosni mehanizam standarda definira dva načina provjere korisnika – autentikaciju otvorenog sustava (*eng. Open System Autentication*) te autentikaciju temeljem dijeljenog ključa (*eng. Shared Key Autentication*).

Autentikacija otvorenog sustava u standardu 802.11 zadana je kao defaultna te je svakome tko zatraži dopušteno pridruživanje mreži (zato i naziv otvorena). U ovom načinu autentikacije može

biti korištena WEP (*eng.Wired Eqiuvalent Privacy*) enkripcija pri čemu ne dolazi do verifikacije WEP ključa već se on koristi samo za enkripciju podataka. Ranjivost autentikacije otvorenog sustava je u tome što ova autentikacija ne osigurava provjeru valjanosti klijenta čime se otvara mogućnost prijetnje sigurnosti mreže.

Autentikacija temeljena na dijeljenom ključu bazira se na tome da obje strane u procesu autentikacije imaju jednak dijeljeni ključ (*eng. Shared Key*). U ovom procesu postoji nekoliko koraka[33]:

- klijent zahtijeva asocijaciju s pristupnom točkom,
- pristupna točka šalje izazov (*eng. Challenge*) klijentu – izazov je nasumce generiran tekst kojeg pristupna točka šalje u čistom obliku,
- klijent odgovara na izazov – klijent enkriptira tekst izazova korištenjem klijentskog WEP ključa i šalje ga natrag pristupnoj točki,
- pristupna točka odgovara na klijentski odgovor – pristupna točka dekriptira enkriptirani klijentski odgovor. Na ovaj način pristupna točka može ustanoviti ima li klijent odgovarajući WEP ključ. Ako je klijentski WEP ključ odgovarajući pristupna točka će odgovoriti pozitivno i autenticirati klijenta. Ako klijentski WEP ključ nije odgovarajući pristupna točka će odgovoriti negativno i neće autenticirati klijenta te klijent ostaje neautenticiran i neasociran.

Autentikacija dijeljenog ključa također ima svoju ranjivost te se ne preporučuje. Naime, u procesu razmjene tekstovi se razmjenjuju u čistom i u enkripcijskom obliku putem bežične veze te mogu biti izloženi napadačima. Također, ovaj način autentikacije također kao ni autentikacija otvorenog pristupa ne osigurava provjeru valjanosti klijenta koji se spaja na mrežu čime se otvara mogućnost prijetnje.

3.2.3. WEP

WEP spada među prve standarde za zaštitu podataka i definiran je u standardu 802.11. U početku je smatrano da je ovaj standard dovoljno siguran za prijenos podataka u bežičnim

[33] Hamidović, H.: op. cit. pod. 7, str. 126

mrežama, međutim ova pretpostavka ispostavila se kao netočna zbog određenih nedostataka koji su naknadno otkriveni. Radi zaštite podataka tijekom prijenosa WEP se koristi na podatkovnom sloju OSI modela. Ovaj simetrični algoritam oslanja se na tajnost ključa koji se koristi između pristupne točke i klijenta, a istim ključem koristi se enkripcija i dekripcija. Enkripcija se odvija u dva koraka – prvi korak je zaštitno kodiranje (*eng. Checksumming*) CRC32 (*eng. Cyclic Redundancy Check*) polinomom koje se vrši radi zaštite integriteta poruke. CRC32 je 32-bitni polinom koji služi u WEP-u za očuvanje integriteta podataka u komunikacijskom kanalu. Drugi korak je enkripcija čistog teksta iz prethodnog koraka pomoću RC4 algoritma. RC4 je algoritam koji se najčešće koristi u softverskim aplikacijama.

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*).

3.3. Sigurnosne nadogradnje 802.11 standarda

S obzirom da standard 802.11 zbog nedostataka ne pruža dovoljnu zaštitu korisnika, IEEE je odlučio naći nova rješenja radi veće sigurnosti bežičnih mreža. Tako je nastao novi standard –

802.1x s ciljem povećanja sigurnosti. Osim njega možemo spomenuti i standard WEP2 kao nastavak nadogradnje standarda WEP.

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[34]:

- 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[35].

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

[34] Ibidem, str. 137
[35] RADIUS (Remote Authentication Dial-In User Service) – mrežni protokol koji omogućava centralizirano upravljanje autentikacijom, autorizacijom i administracijom korisnika (*eng. AAA – Authentication, Authorization, Accounting*)

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.

3.3.2. WEP2

Standard WEP2 nastao je razvijanjem standarda WEP kao pokušaj povećanja sigurnosti bežičnih mreža. Razlika u odnosu na standard WEP iz kojeg je nastao je u dužini ključa koji je proširen na 128 bita i povećanu vrijednost inicijalizacijskog vektora IV, međutim koristi isti RC4 enkripcijski algoritam uz isti način upravljanja ključevima. Još jedan problem koji se javlja je što zahtijeva veliku procesorsku snagu te ga svi proizvođači ne podržavaju. Stoga standard WEP2 ne donosi značajan pomak u sigurnosti, ali je kompatibilan sa WEP protokolom tako da mrežna oprema uz nadogradnju može koristiti i ovaj poboljšani standard.

.

3.4. WPA

WPA (*eng. Wi-Fi Protected Access*) je razvijen u okviru Wi-Fi Alliance udruženja. Nastao je kao posljedica nedovoljne sigurnosti WEP-a pri čemu se pazilo da se eliminiraju sve ranije pogreške, a istovremeno da se zadrži sukladnost sa postojećom mrežnom opremom. WPA kao i WEP koristi RC4 sustav za enkripciju i inicijalizacijski vektor (IV), ali poboljšanje je u korištenju TKIP protokola (*eng. Temporal Key Integrity Protcol*) koji služi za dinamičko mijenjanje ključeva za vrijeme korištenja sustava. Nadalje, WPA protokol koristi i sigurniji sustav provjere besprijekorne poruke u odnosu na CRC sustav koji koristi WEP protokol . Spomenuti sigurniji sustav zove se MIC (*eng. Message Integrity Check tzv.“Michael“*), a isključuje mogućnost promjene sastava poruka u komunikacijskom kanalu za razliku od CRC provjere kod koje postoji takva opasnost. Prednost WPA je mogućnost ugradnje u postojeću mrežnu opremu bez većih ulaganja. Ovaj standard eliminirao je slabosti prethodnog sustava uvođenjem dugačkog incijalizacijskog vektora (IV) i TKIP protokola radi obrane od napada kakvi se koriste za otkrivanje ključa u WEP protokolu. Međutim, i ovdje su otkrivene određene ranjivosti u dijelu TKIP komponente koju napadači mogu iskoristiti za otkrivanje niza bitova kojima je paket kriptiran. Napad se može izvesti samo na kratkim porukama kod kojih je sadržaj uglavnom poznat. Ranjivost se pri tome odnosi samo na WPA protokol, ali ne i na WPA2 protokol o kojem ćemo nešto reći u nastavku.

3.5. WPA2

WPA2 predstavlja nadogradnju na WPA i jedina razlika je što se za enkripciju ne koristi RC4 algoritam već AES. AES je napredni enkripcijski standard koji je odobrio NIST (*eng. National Institute od Standards and Technology*), a ovaj algoritma poznat je i kao Rijndael algoritam. WPA2 sustav je ujedno i najrašireniji sustav zaštite bežičnih mreža koji je također kao i WPA razvijen u okviru Wi-Fi Alliance udruženja. WPA2 sustav koristi CCMP (*eng. Counter Mode with Cipher Block Chaining Message Authentication Code Protocol*) enkripciju za sigurnu razmjenu poruka kako bi se onemogućila njihova izmjena u komunikacijskom kanalu. WPA i WPA2 protokoli mogu se koristiti na dva načina i to PSK (*eng. Pre-Shared Key*) koji

podrazumijeva prethodnu razmjenu ključeva između pristupne točke i svih klijenata, te Enterprise koji podrazumijeva zaseban ključ između pristupne točke i svakog klijenta.

PSK način rada naziva se još i privatni (*eng. Personal*) i namijenjen je privatnim mrežama ili manjim poslovnim mrežama. Jednostavniji je za izvedbu od Enterprise sustava jer ne zahtijeva autentikacijski poslužitelj već se definira kroz jedinstveni 256 bitni ključ (sastoji se od niza znakova ili riječi od 8 do 63 slova preko kojeg se izračunava ključ) koji se koristi za svu komunikaciju u mreži u čemu leži i ranjivost WPA2 certifikacije. U praksi korisnici koriste razne fraze ili izraze, a napad na ključ podrazumijeva isprobavanje svih potencijalnih kombinacija od strane napadača. Problem takvih vrsta napada je u vremenskom trajanju i često je neizvediv u vremenskom okviru. Enterprise način nudi bolju zaštitu jer se svaki uređaj u mreži mora autenticirati (identificirati i ovjeriti identitet lozinkom), ali uvođenje i održavanje takvog sustava zahtijeva puno više posla. Ako uspoređujemo WPA i WPA2 protokol osim razlike u primjeni sigurnijeg i robusnijeg algoritma enkripcije u WPA2 protokolu (CCMP) ova dva protokola vrlo su slična.

ZAKLJUČAK

Trend širenja bežičnih mreža je u sve većem porastu. Fleksibilnost, jednostavnost korištenja i implementacije, mobilnost, veliki izbor uređaja koji koriste bežičnu tehnologiju i niži troškovi glavne su prednosti za njihovo korištenje. Bez obzira kojim uređajem se spajamo na Internet sigurnost nam uvijek mora biti prioritet. Bežične mreže vrlo su specifične i posebno izložene zbog načina prijenosa podataka. U standardima koji definiraju bežične mreže postoje ugrađeni sigurnosni mehanizmi koji često nisu dovoljno iskorišteni ili se koriste sa nedovoljnom razinom sigurnosti. Kako bi se zaštitila komunikacija u bežičnim mrežama i onemogućio zlonamjeran pristup informacijama razvijeno je nekoliko protokola.

U početku je korišten WEP protokol sa idejom da donese jednaku razinu zaštite bežičnim mrežama kakvu imaju žičane. Međutim, WEP protokol je s vremenom otkrio svoje nedostatke, pa je zamijenjen sigurnijim protokolima WPA te u konačnici WPA2 koji se danas smatra najboljim sustavom zaštite bežičnih mreža. On uključuje zaštitu integriteta poruka, kriptiranje podataka i autentikaciju uređaja. Da bi se postigla potrebna razina zaštite osim razvijenih standarda i protokola potrebno je educirati ne samo administratore već i korisnike bežičnih mreža. Nedostatak bežičnih mreža je još uvijek mali domet signala te nemogućnost stopostotne zaštite. Iako nije izgledno da će u potpunosti zamijeniti žičane mreže za kojima zaostaju u sigurnosti i brzini, bežične mreže su svakako stvar budućnosti.

LITERATURA

Knjige:

Hamidović, H. (2009). *WLAN bežične lokalne računalne mreže*: *Priručnik za brzi početak*, Zagreb: Impresum, Info press

Radovan, M. (2010). *Računalne mreže (1): Povezivanje računala i mreža*, Rijeka: Digital point

Članci:

CARNET CCERT-PUBDOC-2008-04-225 (Revizija 1.03), *Wireless forenzika*, http://www.cert.hr/sites/default/files/CCERT-PUBDOC-2008-04-225.pdf (18.07.2015.)

CARNET CCERT-PUBDOC-2009-06-267 (Revizija 1.04), *WPA2 zaštita*, http://www.cert.hr/sites/default/files/CCERT-PUBDOC-2009-06-267.pdf (23.07.2015.)

Padarić, D., Kukec, M. (2009). WiMAX 802.16 standard, *Tehnički glasnik*, 3(5), str 54 – 57 http://www.unin.hr/data/knjiznica/tehnicki_glasnik/tehnickiglasnik_1_2_2009.pdf (11.07.2015.)

Restović A., Stojan I., Ćubić I. (2005). Bluetooth bežična tehnologija i njezine primjene, *Ericsson Nikola Tesla*, 18(1), str. 59 – 73 http://www.ericsson.com/hr/etk/revija/Br_1_2005/bluetooth.pdf (12.07.2015.)

Web:

CISCO, http://www.cisco.com/c/en/us/products/collateral/wireless/aironet-1300-series/prod_white_paper0900aecd801c4a88.html (20.06.2015.)

European Telecommunications Standards Institute (ETSI) , http://www.etsi.org/ (29.06.2015.)

802.11 IEEE wireless LAN standards, http://www.webopedia.com/TERM/8/802_11.html (07.08.2015.)

Introduction to wireless network, http://cdn.ttgtmedia.com/searchNetworking/downloads/wireless_sample.pdf (12.07.2015.)

Iskratrade d.o.o. (lipanj 2012), Osnovno o Wi – Fi antenama, *Ruckus*, http://iskratrade.hr/Portals/0/datasheets/ITR-%20Ruckus-antene.pdf (11.08.2015.)

Jeren, B., Pale, P., Sustavi za vođenje i praćenje procesa, http://spvp.zesoi.fer.hr/predavanja%202008/WE_skripta.pdf (02.06.2015.)

Informatička abeceda, *Bežična komunikacija*, http://www.informatika.buzdo.com/s930-intranet-bezicna-komunikacija.htm (09.06.2015.)

POPIS SLIKA

SAŽETAK

U doba ekspanzije informacijske i komunikacijske tehnologije bežične mreže zauzimaju vrlo važno mjesto. Njihova upotreba je u porastu u svim segmentima društva. Iz tog razloga tema mog završnog rada je „Bežične mreže“ u kojem se nastoji upoznati sa pojmom bežičnih mreža, njihovom primjenom, prednostima i nedostacima te smjernicama za budućnost. Težište rada je na pitanju sigurnosti bežičnih mreža s obzirom da je to njihov najveći nedostatak. U konačnom zaključku dolazimo do činjenice da danas mnoge tvrtke i institucije kao i velik broj prosječnih korisnika sve više koristi uređaje za bežično spajanje na Internet prvenstveno zbog prednosti bežičnih mreža - mobilnosti, fleksibilnosti, jednostavnosti korištenja te niskih troškova pri čemu je pitanje sigurnosti i zaštite podataka imperativ za svakog korisnika.

Ključne riječi: bežične mreže, Internet, sigurnost

SUMMARY

In time of the expansion of information and communication technologies wireless networks take a very important place. Their use is increasing in all segments of society. For this reason, the topic of my thesis is „Wireless networks “which tries to show the concept of wireless networks, their use, advantages and disadvantages and also guidelines for the future. Focus in this thesis is about wireless networks security considering that this is their biggest disadvantage. In the final conclusion we come to the fact that today many companies and institutions as well as a large number of average users are increasingly using devices to wirelessly connect to the Internet primarily due to benefits of wireless networks – mobility, flexibility, simplicity and low costs with the issue of security and data protection as an imperative for each user.

Key words: wireless networks, Internet, security