Univerza v Ljubljani
Fakulteta za računalništvo in informatiko

Jernej Oblak

Zmogljivostna analiza prenosa podatkov po standardu 802.11n

diplomsko delo

univerzitetni študijski program prve stopnje
računalništvo in informatika

Mentor: prof. dr. Miha Mraz

Ljubljana 2013

Besedilo je oblikovano z urejevalnikom besedil LaTeX.

Univerza *v Ljubljani*
Fakulteta *za računalništvo in informatiko*

Tržaška 25
1001 Ljubljana, Slovenija
telefon: 01 476 84 11
01 476 83 87
faks: 01 426 46 47
01 476 87 11
www.fri.uni-lj.si
e-mail: dekanat@fri.uni-lj.si

Št. naloge: 00094/2013
Datum: 09.04.2013

Univerza v Ljubljani, Fakulteta za računalništvo in informatiko izdaja naslednjo nalogo:

Kandidat: **JERNEJ OBLAK**

Naslov: **ZMOGLJIVOSTNA ANALIZA PRENOSA PODATKOV PO STANDARDU 802.11N**

DATA TRANSFER PERFORMANCE ANALYSIS ACCORDING TO THE 802.11N STANDARD

Vrsta naloge: Diplomsko delo univerzitetnega študija prve stopnje

Tematika naloge:

Kandidat naj v svojem delu predstavi osnove brezžičnih omrežij družine 802.11. V nadaljevanju naj vzpostavi testno okolje in izvede zmogljivostno analizo prenosa podatkov trenutno aktualne verzije 802.11n. Pridobljene rezultate naj primerja s starejšimi verzijami standarda.

Mentor:

prof. dr. Miha Mraz

Dekan:

prof. dr. Nikolaj Zimic

Fakulteta za računalništvo in informatiko • UNIVERZA V LJUBLJANI • 2

Izjava o avtorstvu diplomskega dela

Spodaj podpisani Jernej Oblak, z vpisno številko **63080113**, sem avtor diplomskega dela z naslovom:

Zmogljivostna analiza prenosa podatkov po standardu 802.11n

S svojim podpisom zagotavljam, da:

- sem diplomsko delo izdelal samostojno pod mentorstvom prof. dr. Mihe Mraza,
- so elektronska oblika diplomskega dela, naslov (slov., angl.), povzetek (slov., angl.) ter ključne besede (slov., angl.) identični s tiskano obliko diplomskega dela
- soglašam z javno objavo elektronske oblike diplomskega dela v zbirki "Dela FRI".

V Ljubljani, dne 3. septembra 2013 Podpis avtorja:

Zahvaljujem se mentorju prof. dr. Mihi Mrazu za strokovne popravke, nasvete in hitro odzivnost ter Marku Tišlerju za začetno usmeritev in pomoč. Navsezadnje se zahvaljujem družini, ki je trpela vso neurejenost in zmedenost v hiši v času pisanja.

Kazalo

Povzetek

Abstract

1 Uvod **1**

2 Družina omrežij 802.11 **3**

2.1 Zgodovina in razvoj 3

2.1.1 Koncept celic 6

2.1.2 1G, 2G ter 3G 7

2.1.3 ALOHA 7

2.2 Uporaba ter tipi brezžičnih omrežij 10

2.2.1 Uporaba 10

2.2.2 Lastnosti oz. prednosti brezžičnih omrežij 11

2.2.3 Tipi brezžičnih omrežij 12

3 Lastnosti brezžičnih omrežij ter standardi 802.11 **15**

3.1 Razlike med ožičenimi in brezžičnimi omrežji 15

3.2 Razmerje signal-šum 18

3.3 Problem skrite postaje 18

3.4 Atenuacija moči signala 18

3.5 CDMA 19

3.6 CSMA/CA 20

3.7 Varnost 21

3.8 Modulacije signalov 21
3.9 Uporaba frekvenčnih pasov 23
3.10 Osnovne verzije 802.11 24
3.11 Raznolikost anten pri 802.11n. 26
3.12 Več vhodov in izhodov - MIMO 27
3.12.1 Multipleksiranje v prostoru 28
3.12.2 Usmerjanje žarka 30
3.12.3 Združevanje prejetih signalov 30
3.13 Izboljšave na MAC nivoju 31

4 Izvedba in rezultati zmogljivostne analize 33
4.1 Meritve 33
4.1.1 Oprema in uporabljena programska orodja 34
4.1.2 Postopek meritev 35
4.2 Rezultati 44
4.2.1 Tabele in grafi meritev 44
4.2.2 Analiza in komentar rezultatov 50

5 Zaključek 55

Povzetek

V diplomskem delu predstavimo brezžična omrežja 802.11, njihov razvoj skozi čas in njihove lastnosti ter bistvene razlike v primerjavi z ožičenimi omrežji. Govorimo o specifičnih tipih omrežij in njihovi rabi. Ogledamo si protokole, na katerih so zasnovani standardi 802.11 ter navedemo in razložimo nekaj pomembnih pojmov, kot so razmerje signal-šum, atenuacija moči signala in interferenca. Na kratko razložimo modulacije signalov ter uporabo frekvenčnih pasov, navedemo glavne značilnosti in razlike med standardi 802.11 in se nato osredotočimo na 802.11n. Predstavimo izboljšave in metode, ki jih 802.11n standard uvaja in obljublja.

Nato kritično pristopimo k meritvam s katerimi izvedemo zmogljivostno analizo prenosa podatkov pri standardih 802.11g in 802.11n. Razložimo potek in postopke meritev ter predstavimo različne tehnologije, ki smo jih uporabili pri delu. Na koncu prikažemo rezultate in jih poskušamo čim bolje interpretirati ter obrazložiti. Navedemo dejavnike, ki so na rezultate najbolj vplivali, govorimo pa tudi o možnih izboljšavah meritev.

Ključne besede:

802.11n, meritve, primerjava, usmerjevalnik, prepustnost

Abstract

In this thesis we introduce the 802.11 wireless networks, their evolution, characteristics and main differences in comparison to wired networks. We discuss specific types of networks and their application. We take a look at the protocols, which serve as the foundation for the 802.11 standards and explain some of the more prominent notions, such as the signal-to-noise ratio, signal attenuation and interference. We briefly pay attention to signal modulations and the use of frequency bands, list the main aspects and differences between the 802.11 standards and finally focus on the 802.11n. We present the improvements and methods, which are introduced and promised by the standard.

We follow this up by taking a critical approach towards the tests, with which we performed the analysis of the 802.11g and 802.11n data transfer capability. We discuss the measuring procedures and present various technologies used during our research. We show, interpret and explain the results in the best way possible and conclude by listing the factors with the biggest influence on our results, as well as defining the possible improvements of our tests.

Keywords:

802.11n, measurements, comparison, router, throughput

Poglavje 1

Uvod

Dandanes si težko predstavljamo življenje brez interneta. Informacije so nam na ta način dostopne skoraj kjerkoli, kadarkoli, pa naj bo to doma, v javni knjižnici, gostilni, nakupovalnem središču ali na letališču. Ko pomislimo na internet, je danes že samoumevno in pričakovano, da je dostop omogočen tudi brezžično. Brezžičnost je običajno povezana z mobilnostjo, kar je tudi ena glavnih prednosti brezžičnih omrežij. Ko v nakupovalnem središču, v knjižnici ali na letališču dostopamo do interneta, smo običajno vsaj deloma mobilni; internetni dostop torej pričakujemo za vsako mizo, v vsakem kotičku, v vsakem nadstropju. Veliko naprav s katerimi vse bolj dostopamo do interneta pa pravzaprav sploh več ne podpira Ethernet vmesnikov. Pametni telefoni in tablice tako ali tako ne, pri novejših, super-lahkih in majhnih prenosnih računalnikih pa tudi vse več izpuščajo kabelske vmesnike. Vse to kaže na vse večjo uporabnost in prikladnost brezžičnih omrežij, če pa želimo le ta ohraniti učinkovita, varna in karseda optimalna, pa je potrebno upoštevati veliko pravil in napotkov.

V poglavju 2 razložimo kako se je brezžični prenos podatkov začel, in kako se je razvijal skozi čas. Govorimo o prvem uporabljenem brezžičnem omrežju in o tem kako je delovalo, o tem kakšni so dandanes tipi brezžičnih omrežij ter kakšne osnovne lastnosti imajo. Čim enostavneje poskušamo predstaviti zgodovino in razvoj brezžičnih omrežij in njihovih lastnosti, poleg tega pa

bralca spodbuditi k nadaljnjemu branju.

V poglavju 3 si pogledamo bolj podrobne lastnosti in značilnosti družine omrežij 802.11, predstavimo nekaj protokolov, nato pa tudi glavne standarde 802.11 in njihove teoretične prenosne hitrosti. Osredotočimo se na 802.11n, ki prinaša obilico zanimivih novosti, kot so 40 MHz širina kanala, izboljšana uporaba večih anten ter izboljšave na MAC nivoju. Kot lahko vidimo, nas zanimajo hitrosti prenosa podatkov po mediju, ki ga uporabljajo brezžična omrežja - zraku, osredotočimo pa se na izboljšave pri standardu 802.11n.

Večina standardov, ki jih bomo omenjali, obljublja določene prenosne hitrosti, ki pa so skoraj v vseh primerih teoretične. Zanimajo nas konkretne, realne vrednosti, ki jih lahko pridobimo samo iz meritev; te izvedemo za različne situacije in postavitve in jih nato predstavimo v poglavju 4. S tem v resnici izvedemo zmogljivostno analizo prenosa podatkov pri standardu 802.11n, predvsem v primerjavi z 802.11g standardom. Rezultate meritev tudi analiziramo in komentiramo, na koncu pa predlagamo še možne izboljšave pri izvajanju meritev.

V poglavju 4 se torej osredotočimo na testiranje konkretnih prenosnih hitrosti pri omenjenih standardih; v pomoč so nam programska orodja kot sta Iperf in Zap, najbolj realne hitrosti pa enostavno preverimo s FTP prenosom podatkov preko posameznega omrežja. Zanima nas za koliko se s prestopom na novejši standard 802.11n povečajo hitrosti pri prenosu podatkov glede na prejšnje standarde, predvsem 802.11g, pokazati pa želimo tudi, da se povečanje hitrosti precej pozna že z osnovno in poceni opremo.

V poglavju 5 samo še komentiramo celotno delo in postopek meritev ter predlagamo različne možnosti za nadaljnje delo.

Poglavje 2

Družina omrežij 802.11

V poglavju definiramo omrežja 802.11 ter predstavimo njihov razvoj skozi čas. Navedemo in obrazložimo tudi nekaj primerov takih omrežij, njihove prednosti, ter za kaj so se, oziroma se še danes vse bolj uporabljajo.

Omrežje 802.11 lahko enostavno definiramo kot računalniško omrežje, ki za prenos podatkov uporablja radijske zveze.

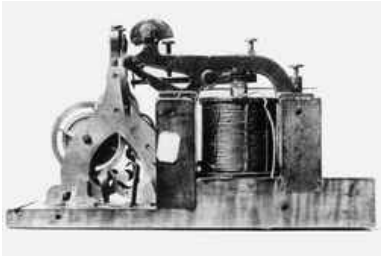
2.1 Zgodovina in razvoj

Že v 19. stoletju je precej znanstvenikov in inovatorjev začelo eksperimentirati na področju brezžičnih komunikacij in ustvarili so precej teorij na področju elektromagnetne radijske frekvence. Med najbolj znanimi so Michael Faraday, James Maxwell, Heinrich Hertz, Nikola Tesla ter še nekateri drugi.

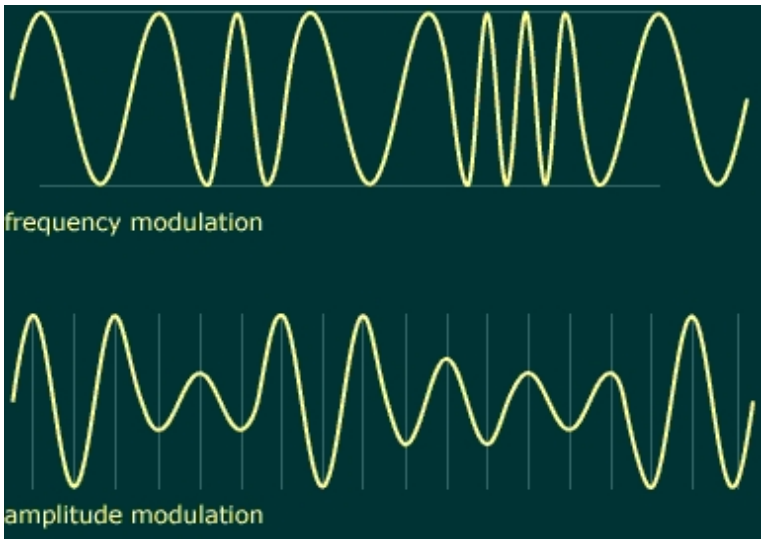
Konkreten korak naprej je uspel Heinrichu Hertzu [1857-1894], ko je leta 1886 odkril, da se lahko elektromagnetni valovi širijo po zraku. Bil je tudi prvi, ki je prikazal oddajanje ter sprejemanje elektromagnetnih valov po zraku in s tem je brezžična komunikacija počasi začela postajati realnost.

Okoli leta 1900 so se pojavili prvi brezžični komunikacijski sistemi - radijski telegrafi (glej sliko 2.1). Kmalu je bilo preko radijskega signala možno prenašati tudi zvok in ne samo telegrafskih signalov, s čimer se je začel tudi vzpon javnih radijskih postaj, ki so uporabljale modulacijo amplitude (angl.

AM - amplitude modulation) (glej sliko 2.2). Kmalu za javnimi radijskimi postajami je prišla televizija.



Slika 2.1: Eden prvih telegrafov, okoli leta 1900 [1].



Slika 2.2: Modulacija amplitude in frekvence [2].

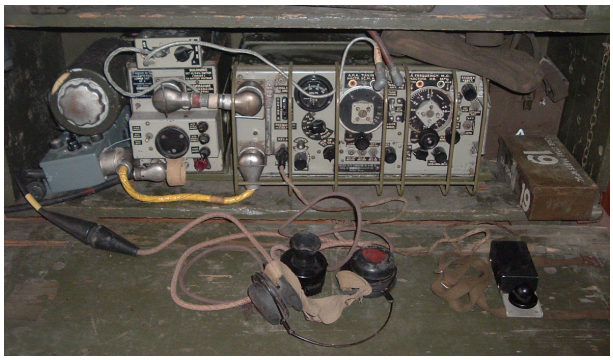
Dvosmerna komunikacija (angl. *two way person-to-person*) na daljše razdalje pa še vedno ni bila veliko v uporabi. Oba, radijske postaje ter televizija namreč uporabljata "broadcast" način oddajanja (angl. *one-to-many*) z močnimi oddajniki.

Leta 1938 je Al Gross izumil "walkie-talkie", telefonska podjetja pa niti v 50-ih letih še niso kazala zanimanja za povezovanje brezžičnosti ter telefonije. Brezžična omrežna tehnologija je bila uporabljena tudi že v času druge

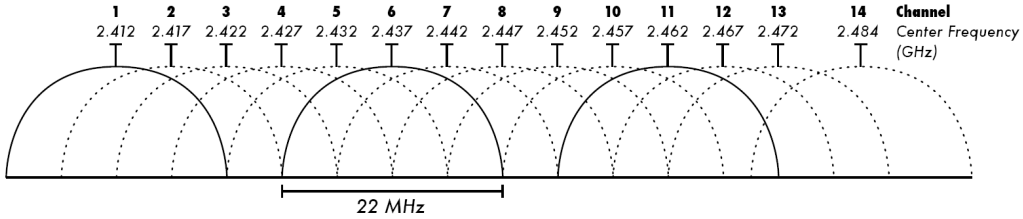
svetovne vojne za prenos šifriranih podatkov čez sovražnikovo črto, večinoma v obliki Morse-jeve abecede. Ena prvih naprav, ki so jo sprva uporabljali v tankovskih vozilih, je bil "wireless set no. 19" (glej sliko 2.3).

Precejšen korak naprej je bil koncept celic v poznih 70tih letih, kateremu je sledila prva generacija mobilnih sistemov (1G), ki so uporabljali ta koncept. Delovanje je nekoliko bolj podrobno razloženo kasneje v tem poglavju.

Istočasna uporaba brezžične komunikacije se je sicer izvajala že nekoliko pred tem, a so se za vsako uporabljali različni frekvenčni kanali. Frekvenčni kanali so frekvenčni pasovi, ki se uporabljajo za brezžično komunikacijo. Zaradi motenj, do katerih prihaja, če so kanali preveč skupaj, so le ti med seboj ločeni (glej sliko 2.4).



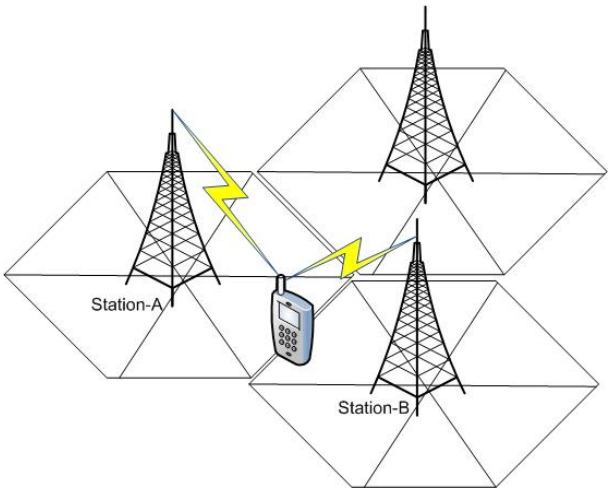
Slika 2.3: Eden prvih telegrafov v času druge svetovne vojne [3].



Slika 2.4: Frekvenčni kanali v 2.4 GHz spektru [4].

2.1.1 Koncept celic

V konceptu celic je uporabljenih veliko oddajnikov (seveda tudi sprejemnikov), a je pokritost območja, ki ga posamezen oddajnik pokriva, še vedno omejena. To omogoča vsaki celici uporabo istih parov kanalov iz drugih celic. Če so vse celice, ki uporabljajo iste pare frekvenc, dovolj ločene ena od druge, se lahko verjetnost interference kar precej zmanjša. Prednost takega koncepta je povečava kapacitete sistema (število uporabnikov) s ponovno uporabo frekvenc (glej sliko 2.5).



Slika 2.5: Primer koncepta celic [5].

Čeprav koncept celic predstavlja precejšen napredek v smislu obojestranske komunikacije, se pri njem pokaže tudi nov izziv: preklapljanje med osnovnimi postajami. Ker se uporabniki skoraj vedno premikajo med celicami, pokritost vsake izmed celic pa je omejena, se morajo seveda "preklopiti" iz ene v drugo celico. Ker to že presega obseg te diplomske naloge, si več o tem bralec lahko prebere v delu K. Daniel Wonga [6].

2.1.2 1G, 2G ter 3G

1G brezžični telekomunikacijski sistemi temeljijo na analogni telefonski tehnologiji - glas se prenaša po analognih vezjih. Po drugi strani, kasnejši 2G sistemi temeljijo na digitalni telefonski tehnologiji. Ti sistemi uporabljajo digitalno kodirane podatkovne tokove, prav tako pa procesiranje signalov ter digitalne kodirnike glasu. Pri 2G sistemih je izboljšan prehod med celicami, pri katerem sodelujejo tudi že mobilne naprave same. Leta 1998 je bilo več predlogov o 3G sistemu, ki pa se niso skladali. Ko je 3G le postal resničnost, je nudil hitrejše storitve, podporo multimediji v smislu istočasnega pošiljanja glasu in drugih podatkov ter seveda hitrejši prenos podatkov, vse do 2Mbps.

Kmalu za tem se je začelo povečevati povpraševanje po brezžičnih lokalnih omrežjih (WLANs - Wireless Local Area Network). Rezultat je standardiziral inštitut IEEE (Institute of Electrical and Electronics Engineers - http://www.ieee.org/about/index.html) v odprt standard, ki ga lahko uporabljajo vsi proizvajalci omrežne opreme, pod imenom 802.11 oz. kasneje kot blagovna znamka Wi-Fi, ki jo je določila "Wi-Fi zaveza" (Wi-Fi Alliance - http://www.wi-fi.org/).

2.1.3 ALOHA

Da pa se vrnemo nazaj na konkretne primere brezžičnih omrežij, moramo omeniti eno prvih delujočih primerov brezžične komunikacije.

Leta 1970 so na Havajski univerzi razvili prvo brezžično paketno omrežje pod imenom "ALOHAnet" oziroma na kratko kar "ALOHA". Omrežje ni bilo samo razvito, bilo je tudi v praktični uporabi. Prvotni cilj je bil z uporabo poceni komercialne radijske opreme povezati uporabnike na Havajskih otokih s centralnim računalnikom na glavnem kampusu na otoku Oahu.
Problem je bil pri skupni uporabi frekvenčnih pasov, tako, da med signali ni prihajalo do motenj. V tistih časih sta se za modulacijo signala uporabljali dve metodi, TDMA (angl. *time division multiple access*), ter FDMA (angl. *frequency division multiple access*). Prva, kot lahko razberemo iz imena,

uporablja razdeljevanje kanalov v časovne okvire oz. pasove, kar pomeni da vsakemu uporabniku dodeli celotno pasovno širino za določen čas. Druga metoda uporablja razdeljevanje v frekvečne pasove. Vsak kanal oz. del pasovne širine, je lahko dodeljen samo enemu uporabniku. Pri teh metodah se je vsak pas dodelil eni izmed postaj, ki so želele komunicirati. Slabost tega je seveda zmanjšanje hitrosti posameznih kanalov, zato so pri ALOHI uvedli drug način. Za svoje delovanje je ALOHA uporabljala izredno visoke frekvence (angl. *UHF - Ultra High Frequency*) – 400MHz, kajti frekvence za komunikacijo med računalniki takrat še niso bile dostopne v komercialne namene oz. v komercialnih aplikacijah.

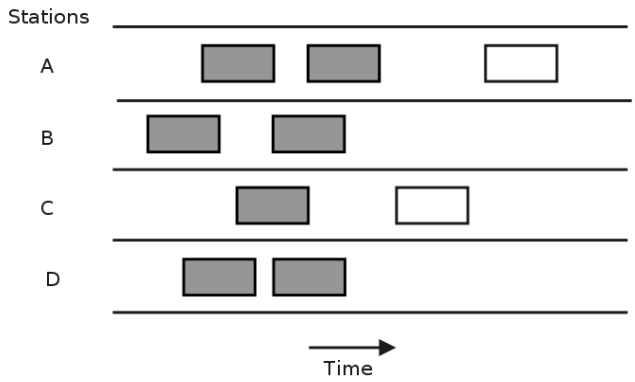
Razvita sta bila dva načina delovanja. Prvi, "Pure ALOHA" (glej sliko 2.6), je deloval na naslednji način:

- če ima pošiljatelj podatke, ki jih želi poslati, naj jih pošlje,
- če sporočilo trči z drugim prenosom sporočila (pride do kolizije), potem pošlji podatke kasneje;

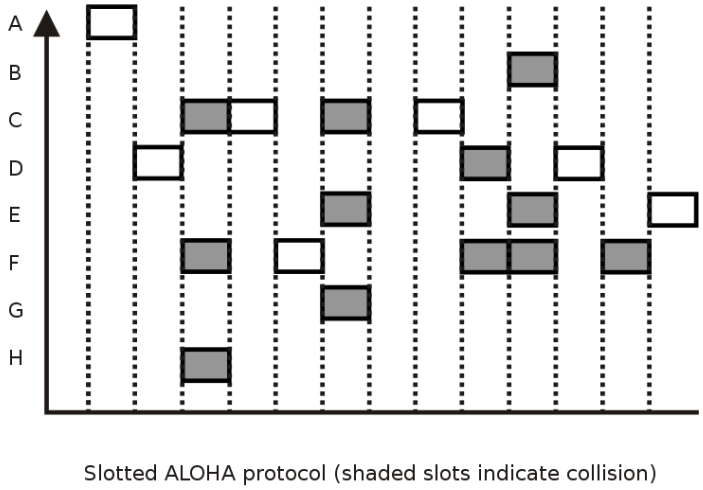
Ker so pri "Pure ALOHI" vse postaje lahko oddajale istočasno, kadarkoli so pač imele podatke, je seveda prihajalo do trkov. Teoretično dokazana maksimalna prepustnost tega protokola je 18.4%, kar pomeni da gre veliko časa za pošiljanje prvotno neuspešno poslanih sporočil.

"Slotted ALOHA" (glej sliko 2.7) je po drugi strani izboljšala prepustnost do največ 36.8%. Dvojno povečanje prepustnosti omogoči omejitev pri oddajanju sporočil in sicer so v tem primeru sporočila lahko poslana samo v začetku nekega časovnega okvira. Seveda smo predpostavili, da so podatkovni paketki istih dolžin.

Ker se ALOHA zaradi nedostopnih frekvenc ter slabe prepustnosti ni uspela razširiti v komercialne namene, so poiskali druge rešitve za njeno uporabnost. V 1970-tih letih se je začela širše uporabljati v omrežjih, ki so temeljila na Ethernet kablih, nato pa tudi v satelitskem omrežju Marisat, ki se zdaj imenuje Inmarsat. Več o ALOHI si bralec lahko prebere v [7], [8] ter [9].



Slika 2.6: Protokol “Pure ALOHA” [10].



Slika 2.7: Protokol “Slotted ALOHA” [10].

V 90. letih 20. stoletja so se na trgu začeli pojavljati prvi komercialni produkti, ki so uporabljali brezžična omrežja, ki so v večini delovala v 0.9 GHz (900 MHz) frekvenčnem pasu. Naj omenimo, da so bile hitrosti pri prvih produktih precej počasne (pod 1 Mbps).

Že leta 1991 so na že omenjenem inštitutu IEEE začeli razmišljati o standardizaciji brezžičnih lokalnih omrežij (WLANs). Med leti 1997 in 1999 je prišel v komercialno rabo osnovni 802.11 standard. V uporabi je bil predvsem v tovarnah in proizvodnjah za zbiranje podatkov z brezžičnimi skenerji črtnih kod.

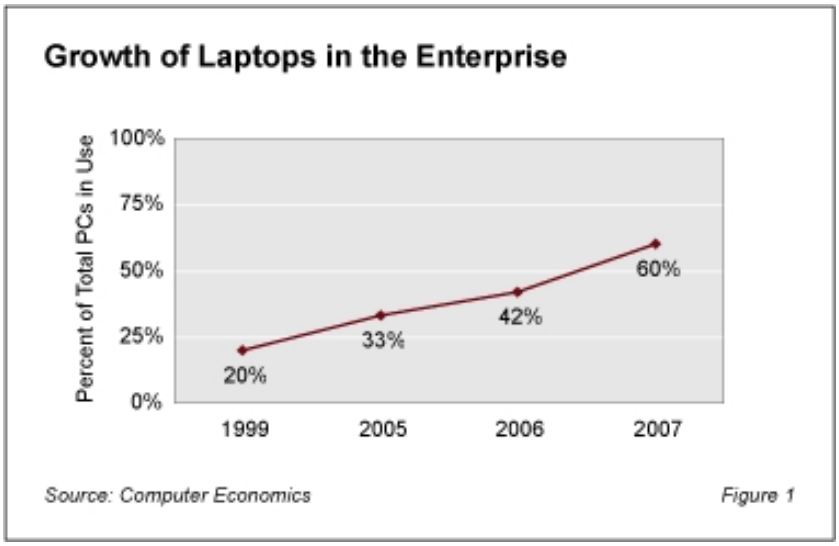
Leta 1999 so pri IEEE definirali višje hitrosti z nadgradnjo na 802.11b in sicer vse do 11Mbps. Znižale so se tudi cene in s tem se je počasi začel vzpon 802.11 standardov tudi v domačih ter drugih službenih okoljih. Leta 2009 naj bi bilo po svetu že več kot 450 milijonov uporabnikov brezžičnih omrežij [6], [11], [12].

Več podrobnosti o posameznih 802.11 standardih je strnjenih v poglavju 3, zdaj pa se bomo osredotočili na uporabo brezžičnih omrežij in predstavili nekaj primerov.

2.2 Uporaba ter tipi brezžičnih omrežij

2.2.1 Uporaba

Brezžična omrežja se dandanes uporabljajo skoraj povsod. Najbolj se to kaže pri povečanem številu mobilnih telefonov in drugih mobilnih naprav z možnostjo uporabe takih omrežij, kar nam pride prav tako rekoč vsak dan, ter nam omogoča lažjo in v veliko primerih tudi cenejšo komunikacijo. Seveda se skupaj s številom mobilnih naprav povečuje tudi število aplikacij za take naprave. Da o prenosnih računalnikih ne govorimo – proti koncu leta 2008 je število izdelanih ter poslanih prenosnikov po svetu prvič večje v primerjavi z stacionarnimi računalniki. Število takih prenosnikov omenjenega leta je bilo več kot 38 milijonov [13], [14], [15]. Naraščanje števila prenosnih računalnikov od leta 1999 naprej se lahko vidi na sliki 2.8.



Slika 2.8: Naraščanje števila prenosnih računalnikov [16].

2.2.2 Lastnosti oz. prednosti brezžičnih omrežij

Prednosti brezžičnih omrežij pred ožičenimi omrežji se kažejo tudi pri raznih javnih ustanovah, knjižnicah, policijskih postajah, bolnišnicah, gostilnah itd. Nekatere izmed glavnih lastnosti oz. prednosti so opisane v nadaljevanju.

- *Mobilnost*
  Mobilnost je glavna in najpomembnejša karakteristika brezžičnih omrežij. Ko naletimo na okolje, kjer bi le s precej težav postavili ožičeno omrežje, se precej pokažejo prednosti brezžižnih omrežij. Ceste, reke, velika industrijska skladišča, letališča, vse to so lokacije, kjer ožičena omrežja ne pridejo v poštev ali pa bi za tako postavitev omrežja porabili preveč denarja in časa. Prihranek prostora se pozna tudi v domačih okoljih z znižanjem števila žic in napeljav, pa tudi z vse večjo uporabo brezžičnih tiskalnikov, skenerjev in drugih naprav, ki vse bolj uporabljajo 802.11 tehnologije.

- *Cena*
  Tudi cena je lahko velik faktor, ko govorimo o brezžičnih omrežjih. Koa-

ksialni ter optični kabli lahko stanejo kar precej, kar se pozna predvsem ko moramo pokriti srednje veliko ali precej veliko področje.

- *Hitrost instalacije ter enostavnost*
  Instalacija oziroma nastavitev domačega ali manjšega službenega brezžičnega omrežja sta precej enostavni, izognemo pa se lahko tudi potrebi po vstavljanju kablov skozi zidove ter ostalim nevšečnostim, ki pridejo s kablovjem.

- *Skalabilnost*
  Konfiguracije naprav v brezžičnih omrežjih se da relativno hitro prilagoditi na spremembe omrežja, npr. povečavo ali pa velik narast števila uporabnikov.

Tudi pri brezžičnih omrežjih seveda naletimo na težave oz. probleme. Prva in zelo pomembna stvar so motnje signala, torej nasploh motnje pri prenosu podatkov. Težave se lahko pojavijo pri uporabi določenih frekvenc v različnih državah, saj ima vsaka država svoje nacionalne predpise glede uporabe specifičnih frekvenc. Problem so lahko še zakasnitve ter razmeroma nizka hitrost prenosa podatkov, predvsem pri obremenjenem omrežju. Stvar na katero moramo vedno misliti je tudi varnost - tudi to je težje implementirati v brezžičnih omrežjih, kot v tistih, ki uporabljajo kable.

2.2.3 Tipi brezžičnih omrežij

Brezžični sistemi lahko uporabljajo licenčni ali pa ne-licenčni radijski spekter. Imajo lahko različne propagacijske lastnosti, kar pomeni, da nekateri lahko uspešno oddajajo na daljših razdaljah kot drugi. Omogočajo lahko večje ali manjše hitrosti pretoka podatkov. Nekateri so zmožni pretakati zvok, nekateri podatke, tretji pa oboje.

V naslednjih odstavkih so naštete glavne oblike brezžičnih omrežij ter njihove glavne lastnosti:

- *PAN (Wireless personal area networks):*
  Povezuje naprave znotraj relativno majhnega področja. Primer WPAN-a sta npr. "Bluetooth" ter "infrared" (glej tudi sliko 2.9).

- *LAN (Wireless local area networks):*
  Povezuje dve ali več naprav preko kratke razdalje. Običajno se vmes postavi dostopna točka (angl. *access point*), ki omogoča uporabo in dostop do Internet-a. WLAN je v bistvu samo ime za skupino 802.11 standardov.

- *Mesh (Wireless mesh networks):*
  Več dostopnih točk povezanih ena z drugo z dinamično hierarhijo, ki omogoča več možnih poti za prenos podatkov in s tem varnost ob izpadu katerekoli izmed točk. Pomembne so radijske zveze med njimi in pa moč signala, ki se v prvi vrsti ohranja s krajšimi razdaljami med vključenimi napravami. Primer takega omrežja se lahko vidi na sliki 2.10.

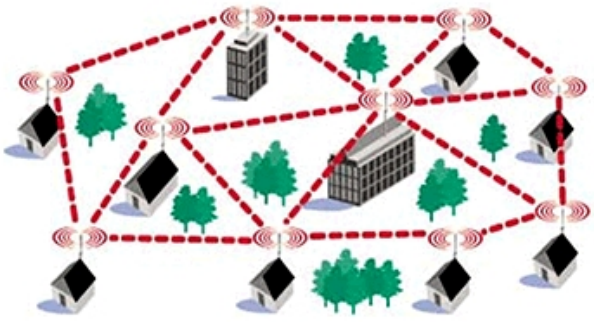
- *MAN (Wireless metropolitan area networks):*
  Brezžično omrežje, ki povezuje več brezžičnih omrežij tipa LAN. Primer MAN-a je WiMAX (802.16).

- *WAN (Wireless wide area networks):*
  Omrežja, ki omogočajo priključitev na širokem geografskem področju. Običajno namenjena večjim oz. razpršenim podjetjem, kjer omogočajo povezovanje oddaljenih pisarn s centralnimi deli podjetja.

- *Telefonska omrežja (cellular or mobile networks):*
  Radijsko omrežje sestavljeno iz več delov - tako imenovanih celic, ki se ločijo po frekvencah oddajanja in se tako izognejo interferenci ter nudijo zagotovljeno pasovno širino znotraj vsake celice. Te celice lahko skupaj pokrijejo precej velika geografska območja (za razlago celic glej poglavje 2.1). Osnovna in najbolj znana brezžična telefonska tehnologija danes je GSM (angl. *Global System for Mobile communications*), ki nudi več vrst storitev, kot so pogovor, faks ter pogovorna sporočila

(angl. *SMS - short message service*), po GSM pa je prišlo že kar nekaj novih nadgradenj oz. novejših protokolov kot so npr. GPRS (angl. *General Packet Radio Service*), UMTS (angl. *Universal Mobile Telecommunications System*) ali LTE (angl. *Long-Term Evolution*) [17], [18].

Slika 2.9: "Personal Area Network" [19].



Slika 2.10: "Mesh Network" [20].

Poglavje 3

Lastnosti brezžičnih omrežij ter standardi 802.11

V tem poglavju najprej naštejemo glavne razlike med žičnimi in brezžičnimi omrežji. Razložimo nekaj osnovnih pojmov in protokolov, kar nam bo koristilo pri nadaljnjem branju, nato pa naštejemo glavne standarde 802.11 in opišemo njihove značilnosti, prednosti ter slabosti. Podamo primere uporabe vsakega od njih, na koncu pa se osredotočimo na standard 802.11n.

3.1 Razlike med ožičenimi in brezžičnimi omrežji

Če se želimo osredotočiti na razlike med ožičenimi in brezžičnimi omrežji, moramo poznati plasti OSI (Open Systems Interconnection) modela (glej sliko 3.1). Pri primerjavi imejmo v mislih drugo, tako imenovano povezovalno oz. povezavno plast (angl. *data link layer*), na kateri definiramo naslednje pomembne razlike:

- *Propagacija radijskega signala:*
  Že zaradi fizikalnih lastnosti kot sta frekvenca in amplituda radijskega signala se s povečevanjem razdalje med pošiljateljem in prejemnikom manjša moč signala. Pri oddajanju pri višjih frekvencah se signali bolj absorbirajo in zato jih je težje sprejemati na enaki razdalji, kot

tiste, ki so oddani pri manjših frekvencah. Problem so tudi ovire na katere naleti signal na svoji poti do prejemnika, kot so npr. rastje, trdne površine in pa seveda absorbiranje in odboji od njih. Telesa in predmeti, ki vsebujejo vodo, so še posebej problematični, saj voda v človeškem telesu predstavlja 60% telesne teže, hkrati pa je frekvenca 2.4GHz resonančna frekvenca molekul vode. Posledično se energija radijskega signala pri potovanju skozi telesa, ki vsebujejo vodo, troši za segrevanje, kar povzroča visoko atenuacijo signala. Voda je ključni gradnik tudi v primeru rastlin, zato zaradi velike vsebnosti spomladi in poleti, ko rastline ozelenijo, zaznavamo večje izgube v moči signalov.

- *Interference:*
  Med napravami, ki oddajajo v istem frekvenčnem pasu prihaja do motenj, ki jih lahko povzroči npr. bližnja mikrovalovna pečica, mobilni telefon ali katerakoli druga naprava, ki uporablja enak frekvenčni pas. Večina omenjenih naprav uporablja nelicenčne frekvenčne pasove, tako kot standardi 802.11, zato interference niso tako redek pojav. Do interference v praksi pride, ko dve napravi oddajata signal v istem frekvenčnem pasu. Signal se v večini primerov oslabi, kar oteži nadaljnjo komunikacijo.

- *Več možnih poti (angl. Multipath Propagation):*
  Elektromagnetni valovi se lahko odbijajo od sten, tal in drugih trdnih objektov, ki so na poti med pošiljateljem in prejemnikom ter tako prepotujejo različno dolge poti preden prispejo na cilj. Večji problem je lahko še rastje, stavbe itd. Prejemnik ima zaradi tega lahko probleme pri sprejemanju signala.

Glede na zgornje odstavke lahko sklepamo, da je pri brezžičnih omrežjih več težav s prenosom podatkov, kot pri žičnih. Kot pa bomo videli kasneje, brezžični protokoli oz. standardi uporabljajo potrebne varnostne mehanizme za preprečevanje težav, kot so CRC (angl. *Cyclic Redundancy Check*) zaznavanje ter zanesljivo ponovno pošiljanje "okvarjenih" okvirov.

Layer	Layer Name	Function
Layer 7	Application	The level seen by users; the user interface
Layer 6	Presentation	Control functions requested by the user; data is restructured from other standard formats; code and data conversion
Layer 5	Session	System-to-system connection; log-in and log-off controlled here; establishes connections and disconnections
Layer 4	Transport	Provides reliable data transfer between end devices; network connections for a given transmission are established by protocol
Layer 3	Network	Outgoing messages are divided into packets; incoming packets are assembled into messages for higher levels, establishing connections between equipment on the network
Layer 2	Data link	Outgoing messages are assembled into frame and acknowledgements; error detection or error correction is perfomed
Layer 1	Physical	Parameters, such as signal voltage swing, bit duration, and electrical connections, are established in this layer plcmanual.com

Slika 3.1: Plasti OSI modela [21].

3.2 Razmerje signal-šum

O razmerju signal-šum govorimo zaradi prej omenjene izgube signala. Prejemnik mora namreč znati razbrati radijski signal, pa čeprav je le ta lahko precej atenuiran. Razmerje signal-šum je mera, ki pove moč prejetega signala upoštevajoč izgube oziroma šum, ki nastane pri prenosu. Enota, s katero jo običajno predstavljamo, so decibeli (dB). Večji kot je SNR, lažje je prejemniku razbrati prejeti signal. SNR v formuli predstavimo z izrazom

$$SNR = \frac{P_s}{P_n}, \tag{3.1}$$

kjer P_s predstavlja moč signala, P_n pa moč šuma signala.

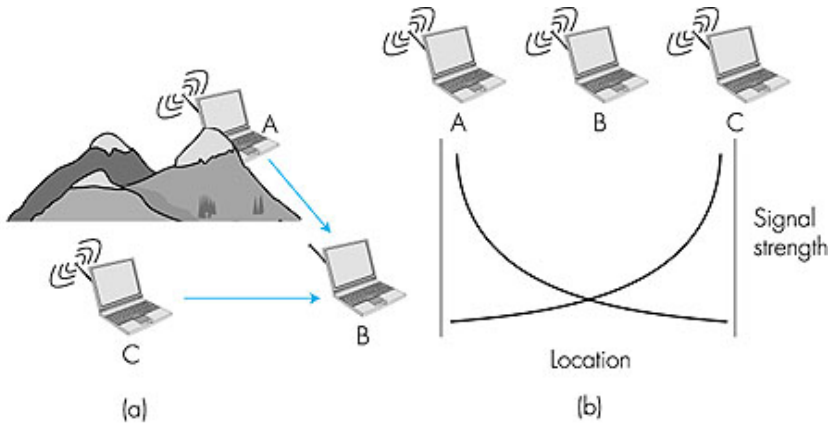
3.3 Problem skrite postaje

O problemu skrite postaje (angl. *hidden node problem*) govorimo, ko je med pošiljateljem in prejemnikom neka fizična ovira, bodisi gora, stavba, zid itd. (glej sliko 3.2a), kar onemogoča njuno komunikacijo, pa čeprav njuna signala vplivata en na drugega v skupni točki B.

3.4 Atenuacija moči signala

Brezžični signali so v resnici radijski valovi. Tako kot vir svetlobe pojenja s podaljševanjem razdalje od njega, tudi brezžični signali izgubljajo svojo moč oz. atenuirajo. Atenuacija ali slabljenje moči signala se konkretno vidi v primeru, ko dva oddajnika zaradi slabega signala ne vidita prenosov en drugega (glej sliko 3.2b). Po drugi strani sta njuna signala lahko dovolj močna, da vplivata en na drugega v neki drugi točki.

Problem skrite postaje in atenuacija moči signala sta precejšna ovira za sočasni dostop (angl. *multiple access*) v brezžičnih omrežjih, kar je velika razlika v primerjavi z omrežji, ki kot glavni medij za prenos podatkov uporabljajo fiksno ožičenje.



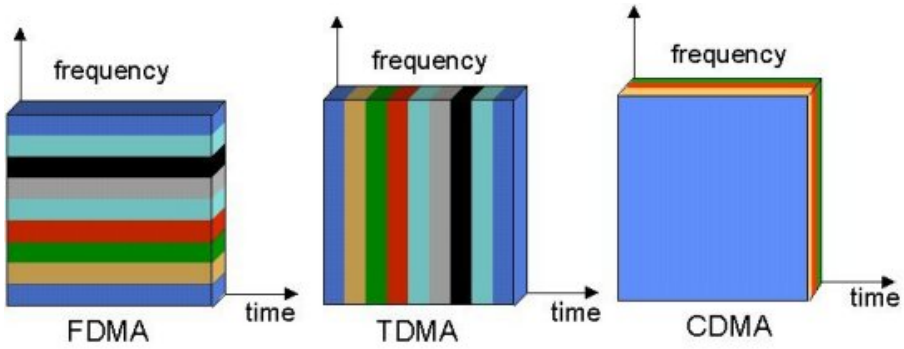
Slika 3.2: Problem skritega terminala ter zmanjševanje moči signala [22].

3.5 CDMA

Samo za razumevanje in kot primerjavo z aktualnim protokolom (glej poglavje 3.6) v brezžičnih omrežjih omenimo njegovega predhodnika - CDMA (*Code Division Multiple Access*).

Če dva, ali več pošiljateljev želi istočasno poslati sporočilo nekemu prejemniku po istem komunikacijskem kanalu, ima ta pri prejemanju signala lahko velike težave. CDMA to rešuje z uporabo "razširjenega spektra" (angl. *spread-spectrum*) in posebnega kodiranja bitov, ki vsakemu pošiljatelju dodeli kodo. Na podlagi omenjenih metod je lahko hkrati na kanalu več uporabnikov oz. signalov, brez porajanja interferenc. Ker kompleksnost in celotna metodologija CDMA protokola segata čez okvire tega dela, si več o tem bralec lahko prebere v [23], [24].

CDMA spada v prvo izmed treh skupin protokolov za istočasno dostopanje (angl. *multiple access protocols*) in sicer tako imenovano "razdeljevanje kanala" (angl. *channel partitioning*). Druga in tretja skupina sta imenovani "naključni dostop" (angl. *random access*) ter "izmenjave" (angl. *taking turns*). CDMA v primerjavi z v prejšnjem poglavju omenjenima metodama TDMA in FDMA lahko vidite na sliki 3.3.



Slika 3.3: Metode sočasnega dostopa do medija z razdeljevanjem kanala [25].

3.6 CSMA/CA

Razvijalci so se pri 802.11 standardih odločili za metodo naključnih dostopov, ker je le ta dobro uveljavljena tudi v Ethernet protokolu (CSMA/CD - *Carrier Sense Multiple Access with Collision Detection*) in pa seveda najbolj primerna. Konkretno, v 802.11 standardih je uporabljen CSMA/CA (*Carrier Sense Multiple Access with Collision Avoidance*). Z imena lahko razberemo, da pošiljatelj (naprava opremljena z 802.11) preden pošlje podatke najprej "zaznava" kanal, nato pa se na podlagi tega odloči ali bo nadaljeval pošiljanje. Če zazna, da je kanal zaseden, podatkov ne bo oddajal. Za zahtevo do medija mora naprava, ki želi poslati podatke, najprej poslati prošnjo za pošiljanje (angl. *RTS - Request To Send*), nato pa mu prejemnik odgovori z "prosto pošiljaj" (angl. *CTS - Clear To Send*). Če katerakoli druga naprava sprejme tako sporočilo (pa ji le to ni namenjeno), mora počakati vnaprej predvideno periodo časa. Ta perioda je določena v obeh, RTS in CTS okvirih. Za potrditvijo pošiljanja se seveda pošljejo podatki (DATA) in pa ACK (angl. *acknowledge*) iz strani prejemnika, če je podatke ustrezno prevzel. Potrebni koraki so lažje predstavljeni s kombinacijo okrajšav RTS-CTS-DATA-ACK. Opisan postopek se ne zgodi v vsakem primeru pošiljanja, kajti večino časa deluje samo fizično "tipanje" nosilne frekvence (angl. *Physical carrier sensing*). To je prvi izmed dveh tipov preverjanja zasedenosti medija in deluje

na fizični plasti OSI modela. Drugi tip deluje na MAC (angl. *Medium Access Control*) nivoju.

3.7 Varnost

Varnost v brezžičnih omrežjih predstavlja večji problem, kot v žičnih. Ker je zrak oz. prostor skupen medij, po katerem se v tem primeru prenašajo signali, je potrebno za vsako poslano sporočilo zagotoviti določeno stopnjo varnosti. Pri varnosti v brezžičnih omrežjih se uporabljajo metode za zagotavljanje zasebnosti podatkov, overjanje, avtorizacijo (pooblastilo oz. dovoljenje za dostop) ter sledenje (kdo je uporabil kaj), segmentacijo, monitoriranje oz. nadzor, ter razne varnostne politike. Osnovni standard za šifriranje vpeljan v 802.11 protokole že z osnovnim standardom leta 1999 je WEP (angl. *Wired Equivalent Privacy*), ki pa je zdaj že zastarel. WPA in WPA2 (angl. *Wi-Fi Protected Access*) sta novejši tehnologiji, ki pa jih ni težko zaobiti, če ima nek uporabnik nastavljeno šibko geslo. Po drugi strani, če je geslo naključno izbrano in vsebuje dovolj črk oz. besed, je WPA protokola zelo težko obiti. Med bolj uporabljanimi varnostnimi protokoli je EAP (angl. *Extensible Authentication Protocol*), ki omogoča overjanje, kot lahko razberemo iz imena. V EAP vključujemo veliko število metod, ki ga dopolnjujejo, vsaka pa ima specifične lastnosti in načine uporabe. Več o varnosti in varnostnih protokolih v brezžičnih omrežjih si lahko bralec prebere v [26] in [27], dobro pa si je zapomniti, da sta glavna sklopa za zagotavljanje varnosti v brezžičnih omrežjih overjanje in šifriranje.

3.8 Modulacije signalov

802.11 tehnologije oz. protokoli/standardi določajo specifične lastnosti na fizični plasti ter na MAC podplasti povezavne plasti OSI modela. Govorimo o treh različnih specifikacijah na fizični plasti:

- *Infrared (IR)* je zastarela tehnologija o kateri nekaj več lahko preberete

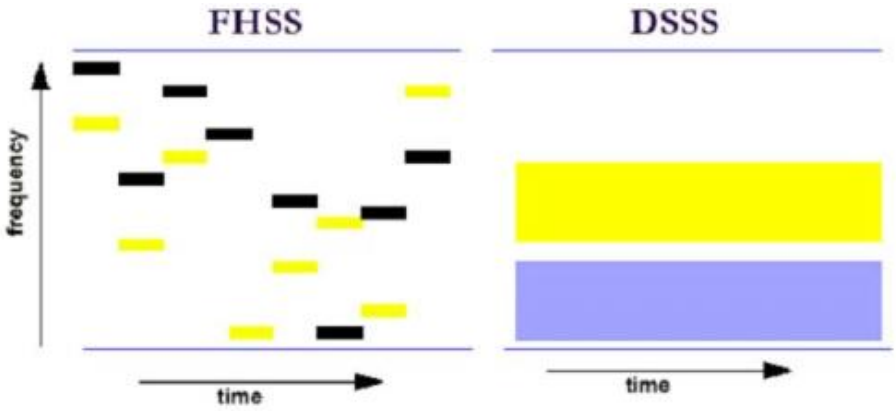
na www.irda.org.

- *Frequency hopping spread spectrum (FHSS)* signal je bil prvič uporabljen v času druge svetovne vojne. Signal "razširjenega spektra" (angl. *spread-spectrum*) je signal, ki ima pasovno širino večjo kot tisto, ki je potrebna za prenos podatkov. Poznamo tudi "ozkopasovni" (angl. *narrowband*) signal, ki kot ime pove, za prenos podatkov uporabi kolikor se le da malo pasovne širine. FHSS deluje po načelu menjave frekvenc in sicer uporablja določeno frekvenco samo določeno periodo časa. Ko se čas izteče, se premakne (hop) na drugo frekvenco in nadaljuje oddajanje. To seveda zmanjša možnosti interference. Krajšanje periode časa lahko še bolj zmanjša možnost interference, podaljševanje pa lahko poveča prepustnost (angl. *throughput*).

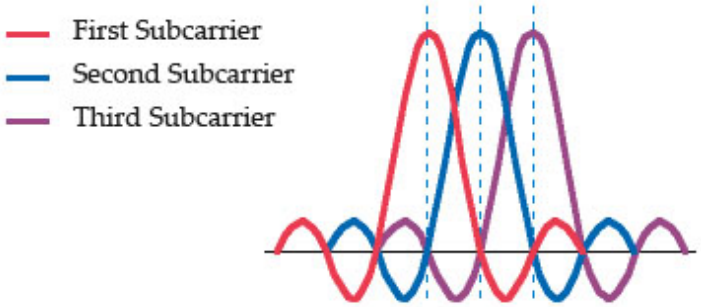
- *Direct sequence spread spectrum (DSSS)* naprave ne morejo pošiljati podatkov s FHSS. Pri DSSS se uporablja samo en kanal ter je bolj pogosto uporabljena metoda in tudi lažja za implementacijo. Pri pošiljanju se tu osnovnim podatkom dodajo dodatni podatki, torej namesto npr. enega bita, se pošljejo še dodatni, redundantni (kodiranje). To se sprva zdi nesmiselno, a nam v resnici izboljša odpornost podatkov na zunanje vplive. DSSS je sprva uporabljala vojska, ker je zaradi širjenja poslanega signala čez večje območje le tega bilo težko oslabiti. Razlika med FHSS in DSSS se lepo vidi na sliki 3.4.

Poznamo tudi OFDM (angl. *Orthogonal Frequency Division Multiplexing*) tehnologijo, ki je bila uporabljena že v ožičenih omrežjih. Za razliko od FHSS in DSSS, OFDM ni metoda razširjenega spektruma (angl. *spread spectrum*), čeprav ima nekaj podobnih lastnosti kot je npr. uporaba večje pasovne širine, kot je je v resnici potrebno za prenos neke količine podatkov. Pri OFDM se za prenos podatkov uporablja 52 ločenih frekvenc (angl. *subcarriers*), ki so med seboj oddaljene 25 MHz (glej sliko 3.5). Čeprav se posamezna frekvenca prenaša počasneje, je končna oz. skupna hitrost višja. Na

koncu lahko še povemo, da se na fenomen večih možnih poti OFDM odziva bolje kot prej omenjeni "spread spectrum" metodi.



Slika 3.4: Razlika med FHSS in DSSS [28].



Slika 3.5: OFDM nosilci [29].

3.9 Uporaba frekvenčnih pasov

Radijski signali se uporabljajo v veliko različnih namenov, zato se je pri uporabi posameznih frekvenc potrebno držati določenih pravil. V ta namen ima vsaka država točno definirane predpise za uporabo posameznih frekvenc. Če nekdo (radio, ponudniki storitev, radioamaterji ...) želi uporabljati frekvenco, potrebuje za to licenco. Obstaja pa tudi ožji pas, za katerega ni

potrebno imeti licence - ISM (angl. *Industrial Scientific and Medical*) pas, ki pa ima zato omejeno moč oddajanja. Vsi 802.11 standardi delujejo v ISM frekvenčnem pasu.

3.10 Osnovne verzije 802.11

- *802.11b*:
  Standard je bil sprejet leta 1999. Prenos podatkov poteka pri največ 11 Mbps, deluje pa v frekvenčnem pasu od 2.4 Ghz do 2.485 GHz. Za doseg večjih hitrosti uporablja CCK (angl. *Complimentary Code Keying*). Ker tudi nekateri mobilni telefoni ter mikrovalovne pečice delujejo v 2.4 GHz pasu, ima 802.11b več težav z interferenco. Omeniti moramo tudi, da se "hitrost prenosa podatkov" (angl. *data rate*) ne sme mešati s "prepustnostjo" (angl. *throughput*), ki je končna in aktualna hitrost.

- *802.11a*:
  Objavljen istega leta kot 802.11b. Deluje na višjih frekvencah - od 5.1 do 5.8 GHz in s tem ima tudi precej visoko hitrost pretoka podatkov, kar vse do največ 54 Mbps. Zaradi višje frekvence in s tem večjega absorbiranja v okolico ima 802.11a slabši domet pri katerem lahko uspešno oddaja signal, slabost pa je tudi pri večih možnih poteh, ki jih lahko uberejo signali, kar se pri 802.11a precej pozna. Izguba signala glede na razdaljo je seveda lahko tudi prednost, saj težje pride do medsebojnih motenj sosednjih omrežij, torej do prekrivanj kanalov oz. frekvenčnih pasov. Uporablja zgoraj omenjeno metodo OFDM. Glavna prednost 802.11a je delovanje v manj zasedenem frekvenčnem pasu. 802.11a ne more komunicirati z napravami, ki uporabljajo b ali g standard. Za to obstajata dva razloga: uporaba različne "spread spectrum" metode in različnih frekvenčnih pasov.

- *802.11g*:

Sprejet leta 2003, 802.11g deluje v istem pasu kot 802.11b, torej 2.4-2.485 GHz. Izboljšana je hitrost prenosa podatkov in sicer do največ 54 Mbps, omogoča pa tudi kompatibilnost z napravami, ki uporabljajo samo starejši, 802.11a standard. Istočasna uporaba večih standardov pomeni za novejši standard podrejanje starejšim, torej če je v omrežju naprava, ki ne podpira novejših standardov, se morajo vse kontrolne informacije prenašati tako, da jih lahko sprejmejo vse naprave. Pri skupni uporabi je seveda zaželjeno, da je prenosov z nizkimi hitrostmi čim manj. V praksi to zgleda tako, da naprave med prenosom spreminjajo hitrost in način modulacije. 802.11g še vedno uporablja OFDM.

- *802.11n*:
  Prvotni cilj 802.11n je izboljšava prepustnosti ter pretoka podatkov v 2.4 GHz in 5GHz pasu. 802.11n omogoča tudi nov način delovanja: visoko prepustnost (angl. *high throughput*), ki prinaša v primerjavi s prejšnjimi 802.11 standardi zelo visoke hitrosti. Uporablja se lahko 40 MHz široki kanal, kar je dvakrat več kot pri prejšnih 802.11 standardih. Širina kanala 40 MHz je v resnici sestavljena tako, da se uporabljata dva, primarni ter sekundarni kanal, razmaknjena za 20 MHz. Primarni kanal se uporablja za komunikacijo s klienti, ki niso sposobni delovanja v 40 MHz širokem pasu. Tako imenovana dvakratna širina kanala pri 802.11n naj bi tako pohitrila prenos podatkov za nekoliko več kot dvakrat [30]. Uporaba MIMO (Multiple input multiple output) tehnologije v kombinaciji s prej omenjeno OFDM še izboljša delovanje. 802.11n oblublja tudi zanesljivejši prenos podatkov in povečan doseg, tako v prostoru kot tudi izven prostora, prav tako pa omogoča sobivanje s starejšimi, zgoraj omenjenimi standardi. Zakaj in kako 802.11n pride do večjih hitrosti, koliko se to pozna v praksi in metode, ki jih uporablja, bomo opisali na naslednjih straneh.

	802.11b	802.11a	802.11g
hitrost (Mbps)	do 11	do 54	do 54
frekvenčni pas (GHz)	2.4-2.485	5.1-5.8	2.4-2.485
modulacija	DSSS ali CCK	OFDM	OFDM, CCK ali DSSS
širina kanala (MHz)	20	20	20

Tabela 3.1: Primerjava osnovnih lastnosti 802.11 standardov pred 802.11n

3.11 Raznolikost anten pri 802.11n.

Brezžične omrežne naprave, kot so naprimer dostopne točke, imajo v veliko primerih implementirano tako imenovano raznolikost anten (angl. *antenna diversity*). To pomeni, da uporabljajo za prenos in prejemanje signalov več kot eno samo anteno. Ker zaradi več možnih poti (glej poglavje 3.1) in interferenc prihaja do izgub moči signala, uporaba tehnike večih anten v takih primerih izboljša zanesljivost povezave oz. prenosov med različnimi napravami v omrežju.

Vsak proizvajalec omrežne opreme lahko implementira svoj način uporabe večih anten, zato bomo tukaj razložili samo osnovne principe.

Kot smo že omenili, se več anten sprva uvede predvsem zaradi problema večih možnih poti. Ker se signal na svoji poti do prejemnika lahko lomi oz. odbija od sten ali drugih površin, to pomeni, da prejemnik lahko vidi več signalov, ki pa se razlikujejo v fazi in amplitudi. Vsi ti signali se "nalagajo" na prejemnikovo anteno, kar privede do pojava, ki mu pravimo izginevanje oz. slabljenje signala (angl. *fading*).

Pri uporabi večih anten lahko vidimo, da se slabljenje signala omeji, kajti le malo verjetno je, da bodo vse antene istočasno prejemale zelo oslabljen signal. Z več antenami seveda ni nujno, da se izognemo posledicam izgubljanja signala in interferencam, v vsakem primeru pa lahko le te zmanjšamo. V praksi to zgleda tako, da naprava primerja signala na obeh antenah (če ima dve anteni), ter uporabi tistega, ki ima večjo moč. Ta primerjava in izbira signala poteka za vsak prejet okvir posebej.

Poslušanje signala na večih antenah se imenuje preklopna raznolikost (angl. *switched diversity*), metoda izbire tistega z največjo močjo ter ignoriranje ostalih pa sprejemna raznolikost (angl. *receive diversity*). Prispeli signali so seveda kopije istega signala z nekoliko drugačno amplitudo. "Switched diversity" se uporablja tudi pri pošiljanju, ampak se v tem primeru uporabi samo ena antena in sicer tista, ki je nazadnje prejela najmočnejši signal. Postopek pošiljanja skozi anteno, ki je nazadnje prejela oz. slišala najboljši signal, se imenuje prenosna raznolikost (angl. *transmit diversity*).

Glavno je, da si zapomnimo, da je pri tem načinu delovanja v vsakem trenutku aktivna (za prejem in pošiljanje) samo ena antena. Torej če prva antena ravnokar pošilja podatke, ni možno da jih druga istočasno prejema.

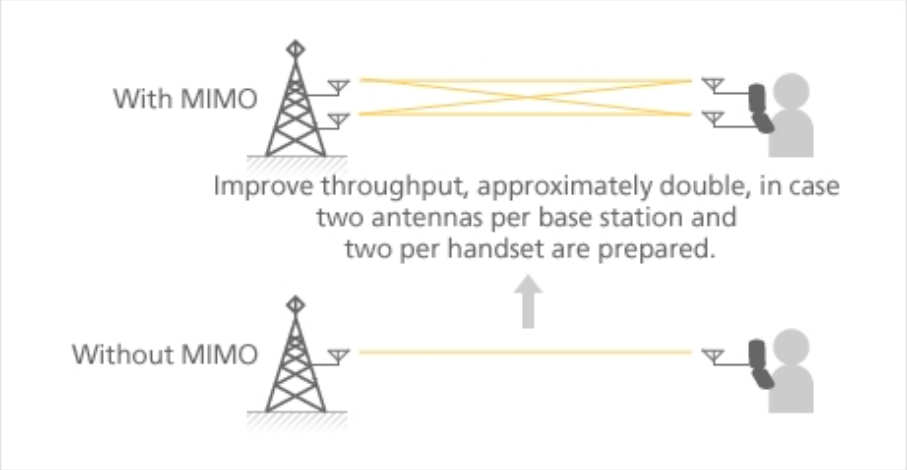
3.12 Več vhodov in izhodov - MIMO

Več vhodov in več izhodov oz. MIMO (angl. *Multiple Input Multiple Output*) je bolj napredna oblika uporabe večih anten. Raznolikost anten se sooča z že večkrat omenjenim problemom večih poti (angl. *multipath propagation*), kar pa se pri MIMO načinu delovanja pokaže ravno nasprotno. MIMO namreč izkoristi problem večih možnih poti z različnimi metodami, ki lahko celo izboljšajo delovanje in sam prenos podatkov. Glavne metode bomo opisali nekoliko kasneje.

Najprej povejmo, kaj MIMO sploh je. To je tehnologija oz. radio-frekvenčni komunikacijski sistem, ki za delovanje uporablja več anten na obeh straneh komunikacijske povezave, kot bi lahko sklepali iz imena. Pomembno je dejstvo, da se tukaj antene lahko uporabljajo hkrati, torej istočasno lahko več anten sprejema in oddaja. Ker je MIMO glavna novost, ki je prišla z 802.11n standardom in tudi najbolj pomembna, ji posvetimo kar nekaj časa.

802.11n standard definira maksimalno število oddajnikov (angl. *transmitters*) in sprejemnikov (angl. *receivers*) in sicer štiri (4x4), uradno pa so za uporabo dovoljene samo tri antene (3x3). Na sliki 3.6 je prikazana prednost uporabe tehnologije MIMO, na sliki 3.7 pa možne kombinacije uporabe

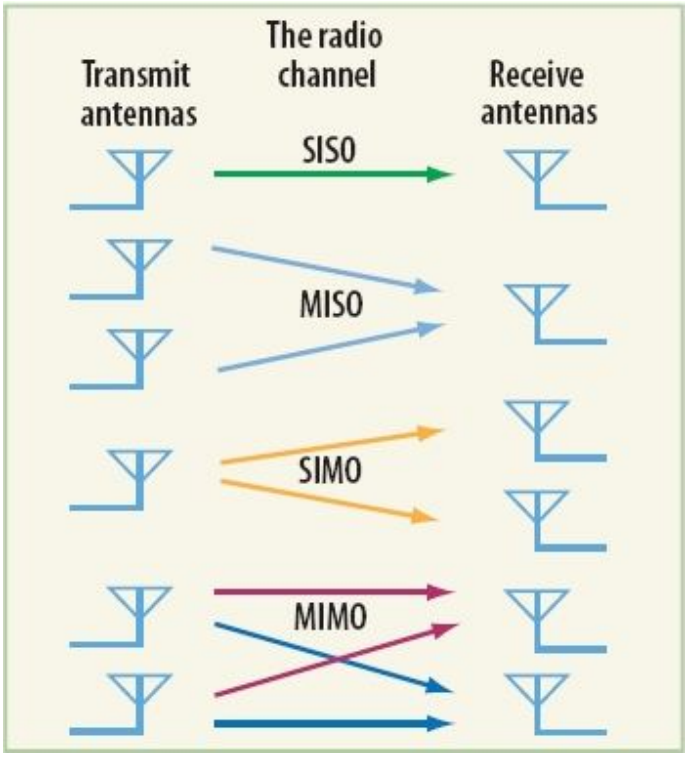
anten.



Slika 3.6: Prednosti uporabe MIMO [31].

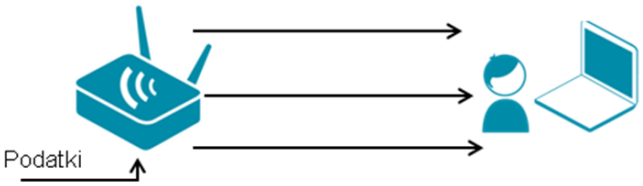
3.12.1 Multipleksiranje v prostoru

Multipleksiranje v prostoru (angl. *spatial multiplexing*) je ena izmed metod (ki jih omogoča MIMO), ki fenomen večih možnih poti uporabi v svojo korist. V praksi to zgleda tako, da oddajnik istočasno oddaja več različnih signalov iz večih anten, sprejemnik pa s pomočjo večih anten te iste signale tudi prejema. Ta metoda torej deluje, ko imata oba, oddajnik ter prejemnik več (2 ali več) anten, ki delujejo v načinu MIMO. Če odjemalec nima podpore za standard 802.11n, multipleksiranje v prostoru ni mogoče. Prednost oddajanja oz. pošiljanja večih edinstvenih (angl. *unique*) tokov podatkov se kaže v velikem povečanju prepustnosti. Če torej neka dostopna točka pošlje dva taka toka podatkov nekemu prejemniku, ki je zmožen oba toka sprejeti, se prepustnost poveča za 2x. Enako velja za prenos treh ali štirih tokov, prepustnost se v teh dveh primerih poveča za trikrat oziroma štirikrat. Če razumemo delovanje multipleksiranja v prostoru, lahko povzamemo, da če več signalov, ki jih pošlje oddajnik, istočasno prispe do sprejemnika, se bodo



Slika 3.7: Kombinacije anten vse do MIMO [32].

ti signali med seboj motili (prihajalo bo do interferenc) in učinkovitost takega prenosa ni nič boljša kot pri sistemih, ki ne uporabljajo MIMO tehnologije.



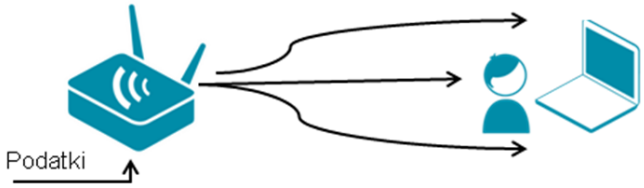
Slika 3.8: Multipleksiranje v prostoru.

3.12.2 Usmerjanje žarka

Usmerjanje žarka (angl. *transmit beamforming*) omogoči oddajniku, ki uporablja MIMO, da s pomočjo večjega števila anten signale pošlje usmerjeno proti nekemu prejemniku (kolikor se da dobro v njegovi smeri). Z dodatno uporabo digitalnega procesiranja signalov je rezultat usmerjanja žarka povečanje razmerja signal-šum na prejemnikovi strani, kar pomeni, da prejemnik lažje razbere oz. prejme poslani signal. Poveča se tudi amplituda prejetega signala, kar pomeni, da lahko posamezni odjemalci komunicirajo na daljši razdalji od oddajnika (običajno dostopne točke). Povečanje razmerja signal-šum na prejemnikovi strani omogoči uporabo bolj kompleksnih metod za modulacijo signala, ki lahko zakodirajo več podatkovnih bitov, kar pomeni, da se s tem poveča tudi prepustnost. Torej končni rezultat uporabe usmerjanja radijskega signala je boljši sprejem in manj motenj drugih sosednjih naprav.

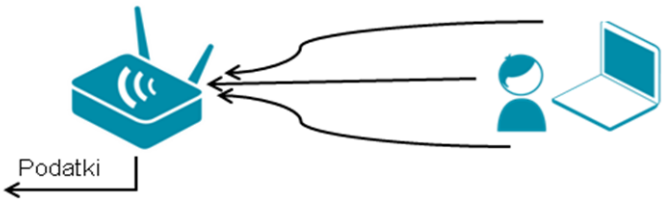
3.12.3 Združevanje prejetih signalov

Zaradi večjega števila sprejemnih anten lahko uporabimo združevanje sprejetih signalov (angl. *maximal ratio combining*) tako, da je končni signal



Slika 3.9: Usmerjanje žarka.

močnejši, kot bi bil, če bi sprejemali z samo eno anteno. Ta metoda se lahko uporablja tudi, ko ima oddajnik samo eno anteno.



Slika 3.10: Združevanje prejetih signalov.

3.13 Izboljšave na MAC nivoju

Pri 802.11n se pojavi tudi nekaj izboljšav na MAC (angl. *Media Access Control*) nivoju, kot so npr. združevanje paketov, kjer se paketi na MAC nivoju združujejo (angl. *frame aggregation*) in pošljejo kot en sam paket na fizičnem nivoju. Zaradi združevanja je bilo potrebno uvesti tudi nov način potrjevanja paketov, kar nas pripelje do naslednje izboljšave - skupinsko potrjevanje paketov, kjer ne zahtevamo potrditve po vsakem prejetem paketku in s tem zmanjšamo število poslanih ACK. Pri vseh že omenjenih metodah in izboljšavah je potrebno misliti tudi na porabo energije, kajti uporaba MIMO

jo sama po sebi le povečuje. Zato je bil omogočen način delovanja, kjer naprava uporablja samo eno anteno v načinu majhne porabe, ko pa je potrebno, se aktivirajo še ostale antene.

Torej skupne prednosti, ki jih 802.11n združuje v omenjene metode, so hkratna uporaba dveh kanalov, boljša izraba frekvenčnega pasu ter optimalna raba večjega števila anten. Vse to omogoča, da podatke pošljemo zanesljivejše in hitreje. 802.11n obljublja večji domet in izkoriščanje naravnih ovir v svoj prid ter hitrejše in bolj zanesljivejše prenose. Koliko je temu res tako, bomo preverili v naslednjem poglavju z meritvami.

Poglavje 4

Izvedba in rezultati zmogljivostne analize

V poglavju predstavimo meritve, ki smo jih izvedli in opišemo postopke, metode in uporabljena programska orodja. Podamo in predstavimo rezultate meritev, nato pa jih komentiramo in na kratko analiziramo.

4.1 Meritve

V tem podpoglavju preverimo, kakšne so izboljšave 802.11n pri prenosu podatkov glede na prejšnje 802.11 standarde, predvsem 802.11g. V ta namen uporabimo različna programska orodja in opremo, s katerimi pridobimo potrebne podatke. Uporabljena oprema in tehnologije morda niso najboljše, prostora za izboljšave je seveda vedno na pretek. Na hitrost prenosa podatkov vplivajo odboji, lomi ter slabljenje signala, poleg tega pa tudi izgubljeni paketki in "jitter" (neželjena odstopanja v zakasnitvah), kar lahko povzroča velike raznolikosti pri meritvah. Poleg omrežja je pomembna tudi procesorska moč naprav, hitrost brezžičnih kartic ter velikost pomnilnikov; temu se v tem delu nismo podrobno posvečali.

4.1.1 Oprema in uporabljena programska orodja

Za izvedbo meritev potrebujemo različne omrežne naprave, kot so usmerjevalniki, računalniki ter morebitne druge brezžične uporabljene naprave, ki vplivajo na hitrost in zanesljivost prenosa podatkov po brezžičnem omrežju. Tako smo uporabili dva brezžična usmerjevalnika, kjer prvi podpira standard 802.11g (Belkin F5D7231-4), drugi pa že 802.11n (TP-LINK WR841ND). Od tu naprej se bomo nanju sklicevali kot usmerjevalnika G in N. Oba imata dve zunanji anteni ter 4 LAN vmesnike, kar pa ni tako pomembno za naše meritve. Uporabili smo tudi dva računalnika, prvi je prenosnik Macbook Pro z Airport Extreme NIC (angl. *Network Interface Card*), ki podpira vse standarde, vključno z 802.11n, torej a/b/g/n. Prenosnik uporablja najnovejši operacijski sistem Mountain Lion. Drugi računalnik je stacionaren ter s kablom povezan na usmerjevalnik, a mu kasneje dodamo brezžično USB omrežno kartico, ki omogoča 802.11n (TP-Link TL-WN821N) z do 300Mbps prenosa. Ko bomo omenjenemu računalniku dodali USB omrežno kartico, mu bomo seveda izklopili direktno kabelsko povezavo z usmerjevalnikom (več o postopku meritev bomo povedali v naslednjem poglavju).

	`standardi`	`širina kanala`	`teoretične hitrosti`
`Belkin F5D7231-4`	b/g	20MHz	do 54Mbps
`TP-Link WR841ND`	b/g/n	20 ali 40MHz	do 300Mbps

Tabela 4.1: Uporabljena usmerjevalnika.

Za merjenje moči signala ter preverjanje okoliških omrežij uporabimo zastonjsko različico programa inSSIDer [34]. Koristi nam tudi za preverjanje morebitnih interferenc, do katerih lahko pride zaradi bližnjih omrežij. Na Macbook računalniku lahko moč signala (prav tako tudi moč šuma) preverimo s pogledom v System Information (Network→Wi-Fi), ali pa SNR preverjamo s podatki, ki se prikazujejo v realnem času s pomočjo Wireless Diagnostics→Utilities. Pri prvem načinu je potrebno, da vsakič, ko računalnik premaknemo, ponovno zaženemo tudi System Information, saj se

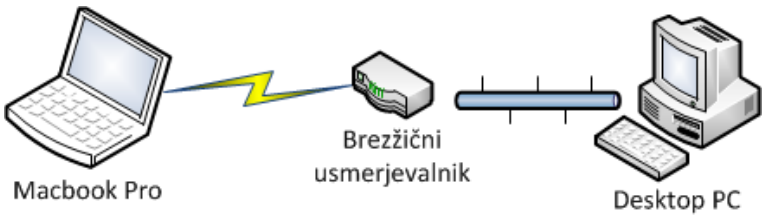
podatki ne spreminjajo dinamično, pač pa so prikazani statično po vsakem ponovnem zagonu.

Za pridobivanje podatkov o prepustnosti povezave uporabimo odprtokodno programsko orodje napisano v programskem jeziku C++ IPERF [35], ki omogoča merjenje prepustnosti povezav preko različnih platform (Windows, Linux, OS X), prav tako pa simuliranje porabe linije, ko se na dostopno točko poveže več uporabnikov. Enostavno preverimo tudi izgubo podatkovnega prometa z UDP (angl. *User Datagram Protocol*) testi ter neželjena odstopanja v zakasnitvah (angl. *jitter*).

Za dodatno primerjavo in ugotavljanje prepustnosti smo uporabili prav tako odprtokodni program Zap [36], ki s pošiljanjem večjega števila paketkov med dvema napravama v ugotavlja prepustnost omrežne povezave med njima.

4.1.2 Postopek meritev

Za namen meritev potrebujemo različne situacije oz. postavitve omrežja. V prvem primeru smo izvajali meritve v relaciji prenosnik→stacionaren računalnik(angl. *Desktop PC*), enkrat z uporabljenim usmerjevalnikom G, drugič pa z N. V drugi situaciji oz. postavitvi pa stacionarnemu računalniku dodamo USB brezžično omrežno kartico in mu izključimo ethernet kabel, ki ga direktno povezuje z usmerjevalnikom. Tako simuliramo dva računalnika, oba brezžično povezana v neko omrežje, na isto dostopno točko. Ponovimo meritve in jih zapišemo, zopet ločeno za primer usmerjevalnika G in N. Obe uporabljeni postavitvi sta prikazani na slikah 4.1 in 4.2.



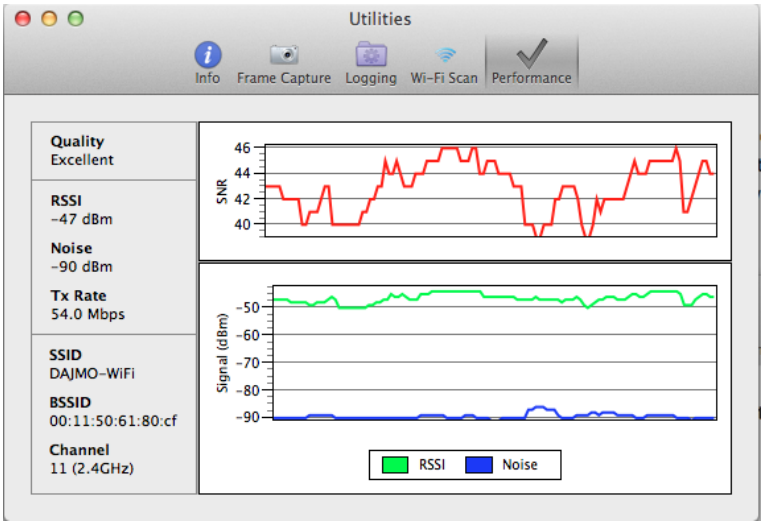
Slika 4.1: Postavitev 1.

Slika 4.2: Postavitev 2.

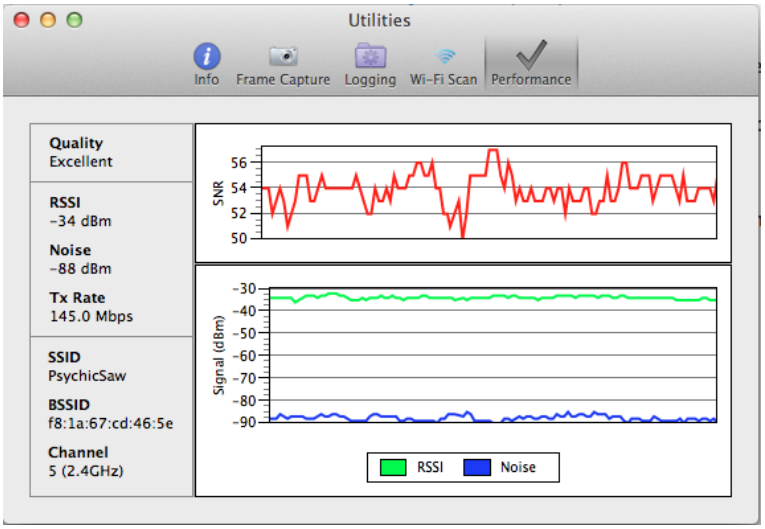
Ker je pri brezžičnih omrežjih zelo pomembna oddaljenost od dostopne točke, smo seveda upoštevali tudi to. Za oba zgoraj omenjena primera (postavitvi), smo enkrat meritve izvedli na razdalji 1-2m od usmerjevalnika, v ostalih primerih pa v določeni oddaljenosti, kar bolj točno povemo nekoliko kasneje. Prav tako smo meritve izvedli izven prostorov, torej v primeru da je klient izven prostora, kjer se nahaja dostopna točka. Stacionarni računalnik je bil vedno na isti razdalji od obeh usmerjevalnikov - 1m.

Testirali smo tudi ping med prenosnikom ter stacionarnim računalnikom, seveda z obema usmerjevalnikoma in pri obeh postavitvah. Prenosnik je bil ves čas brezžično povezan v omrežje testiranega usmerjevalnika, ter na podobni razdalji. Tu je potrebno povedati, da smo razdaljo prenosnika od usmerjevalnika nekoliko prilagajali (približno 3 metre, a izven prostora kjer je usmerjevalnik), kajti želeli smo vsaj približno enak SNR pri meritvah, tako z G, kot z N usmerjevalnikom. To velja tudi za prej omenjene meritve z IPERF. Primer pogleda v Utilities na prenosniku, kjer preverjamo moč signala ter šum, lahko vidimo na slikah 4.3, 4.4 in 4.5. Prva in druga slika prikazujeta podatke za G in N usmerjevalnik na enaki oddaljenosti od prenosnika (1m), tretja pa prikazuje podatke za N usmerjevalnik, ko je prenosnik nekoliko oddaljen (3m, izven prostora), kajti samo tako lahko dosežemo približno enako moč prejetega signala za oba usmerjevalnika (N usmerjevalnik ima očitno boljše antene in večjo oddajno moč).

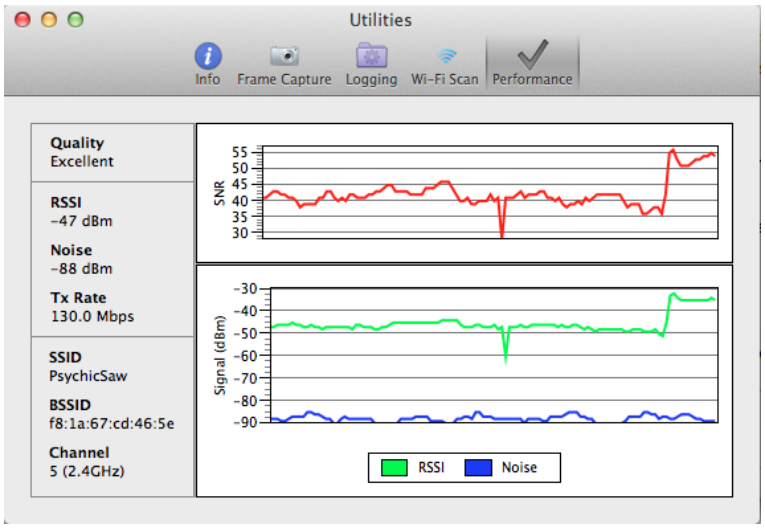
Z IPERF lahko izvajamo več različnih meritev. Prva, ki smo jo izvedli je TCP meritev prepustnosti povezave; en od računalnikov igra vlogo strežnika, kar dosežemo z vpisom ukaza “iperf -s” v ukazno vrstico (glej



Slika 4.3: SNR na prenosniku, usmerjevalnik G.



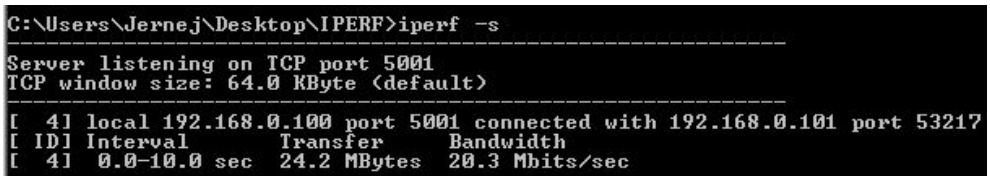
Slika 4.4: SNR na prenosniku, usmerjevalnik N.



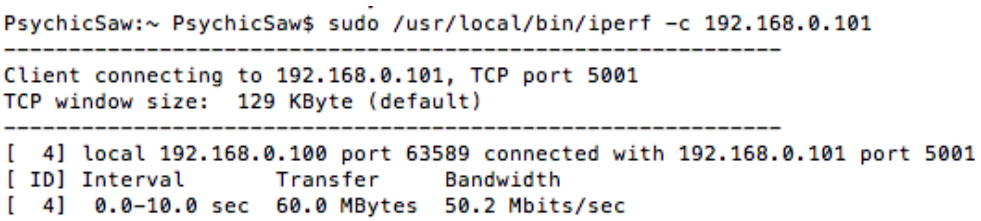
Slika 4.5: Oddaljitev prenosnika za dosego približno enakega SNR kot pri usmerjevalniku G, usmerjevalnik N.

sliko 4.6), v našem primeru je to CMD (angl. *Command Prompt*) na Windows računalniku. Nato na drugem računalniku, ki je povezan v isto omrežje izvedemo ukaz "iperf -c IP" (glej sliko 4.7), kjer IP nadomestimo z ustreznim IP-jem strežniškega računalnika. Za ukaze je potrebno imeti administratorske pravice, izvedemo pa jih seveda na lokaciji, kjer se nahaja IPERF. Z opisanim postopkom se izvede meritev prepustnosti s pošiljanjem čim večjega števila podatkov naenkrat. Na tem mestu naj razjasnimo razliko med prepustnostjo (angl. *throughput*) in pasovno širino (angl. *bandwidth*), kajti oba pojma se velikokrat mešata. Pasovna širina je maksimalna hitrost prenosa podatkov na neki povezavi, torej koliko podatkov (oz. bitov ali paketkov) lahko največ pošljemo v nekem trenutku. Prepustnost po drugi strani je povprečna hitrost prenosa podatkov in je izmerjena in konkretna vrednost, ki jo občuti uporabnik. Pasovna širina je torej bolj teoretična vrednost, prepustnost pa bolj realna oziroma izmerjena, praktična vrednost.

Druga meritev, ki smo jo izvedli s pomočjo IPERF UDP testov, je meritev neželjenih odstopanj v zakasnitvah (angl. *jitter*). Najbolje bi bilo, če bi bil "jitter" kar 0, kar pa v realnih okoljih običajno ni mogoče, zato je vre-



Slika 4.6: IPERF, strežniška stran.



Slika 4.7: IPERF, klientova stran.

dnost "jitter" v omrežjih lahko pomemben faktor, ki vpliva na odzivnost in delovanje omrežja. Za izvajanje UDP testov je potrebno na strežniški strani izvesti ukaz "iperf -s -u", na klientovi strani pa "iperf -c IP -u".

Še zadnja meritev, ki smo jo izvedli z IPERF, je test povezave, ko se poveže več uporabnikov hkrati (paralelno). To dosežemo z ukazom "iperf -c IP -P X", kjer X nadomestimo s številom istočasnih povezav, ki naj se poskusijo vzpostaviti. Testirali smo 5, 10, 20, 30, 40, 50 in 100 istočasnih prenosov. Primer testa z več hkratnimi prenosi lahko vidimo na slikah 4.8 in 4.9.

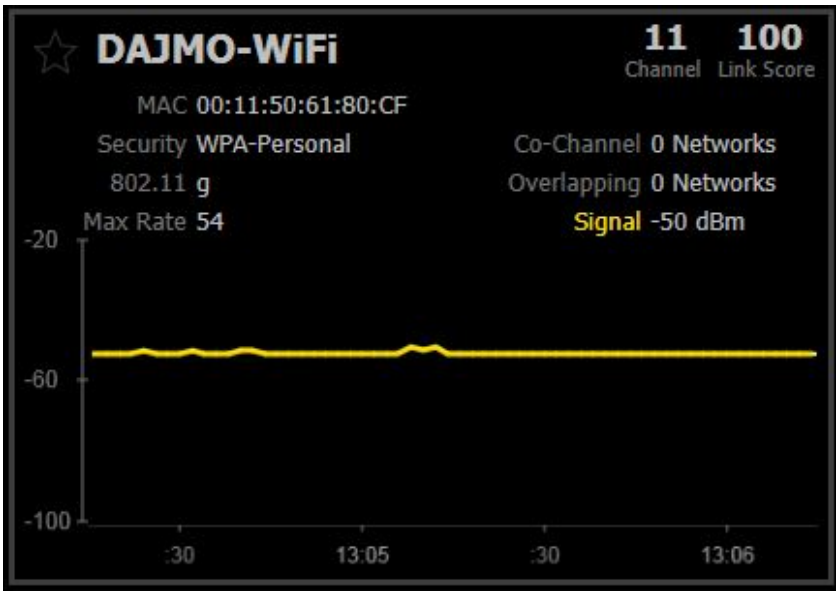
Kot omenjeno smo izvedli tudi meritve s ping-i, ki nam povejo čas ki je potreben, da paketki prepotujejo iz ene naprave na drugo in nazaj. Vsakič smo iz prenosnika poslali 100 paketkov zapored z ukazom "ping -c 100 IP". Pri vseh meritvah smo seveda pazili na RSSI (angl. *Received Signal Strength Indicator*) oz. SNR, kar se lahko vidi na slikah 4.10, 4.11 in 4.12, ki prikazujejo podatke z inSSIDer-ja. Na zadnji se vidi sprememba prejetega signala in hitrosti pri 20Mhz širini kanala; maksimalna teoretična hitrost (angl. *Max Rate*) se kar razpolovi.

```
PsychicSaw:~ PsychicSaw$ sudo /usr/local/bin/iperf -c 192.168.0.100 -P 5
------------------------------------------------------------
Client connecting to 192.168.0.100, TCP port 5001
TCP window size:  129 KByte (default)
------------------------------------------------------------
[  8] local 192.168.0.101 port 57448 connected with 192.168.0.100 port 5001
[  4] local 192.168.0.101 port 57445 connected with 192.168.0.100 port 5001
[  5] local 192.168.0.101 port 57444 connected with 192.168.0.100 port 5001
[  6] local 192.168.0.101 port 57446 connected with 192.168.0.100 port 5001
[  7] local 192.168.0.101 port 57447 connected with 192.168.0.100 port 5001
[ ID] Interval       Transfer     Bandwidth
[  8]  0.0-10.0 sec  22.5 MBytes  18.8 Mbits/sec
[  4]  0.0-10.0 sec  22.5 MBytes  18.8 Mbits/sec
[  5]  0.0-10.0 sec  22.5 MBytes  18.8 Mbits/sec
[  6]  0.0-10.0 sec  22.5 MBytes  18.8 Mbits/sec
[  7]  0.0-10.0 sec  22.5 MBytes  18.8 Mbits/sec
[SUM]  0.0-10.0 sec   112 MBytes  94.0 Mbits/sec
PsychicSaw:~ PsychicSaw$
```

Slika 4.8: IPERF - klientova stran, paralelno pošiljanje petih uporabnikov, 802.11n.

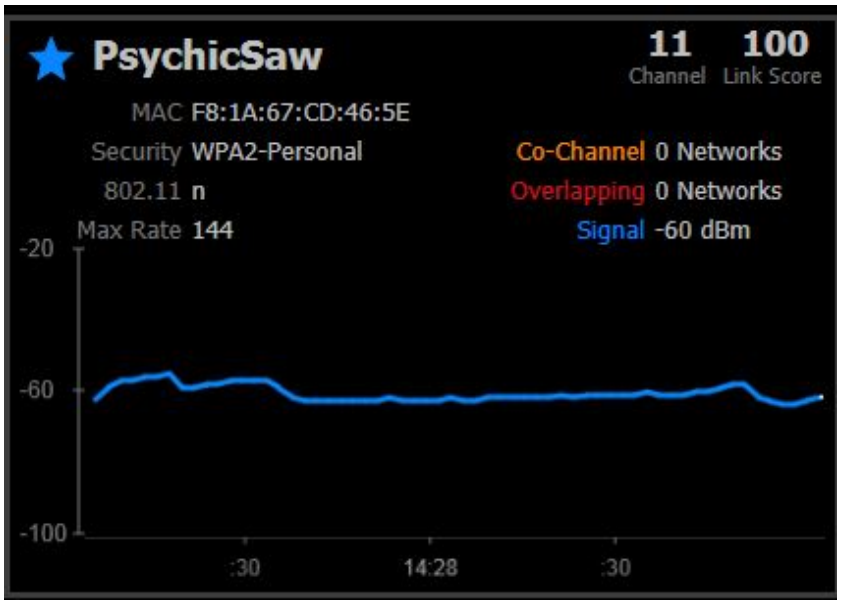
```
^CPsychicSaw:~ PsychicSaw$ sudo /usr/local/bin/iperf -c 192.168.2.4 -P 5
------------------------------------------------------------
Client connecting to 192.168.2.4, TCP port 5001
TCP window size:  129 KByte (default)
------------------------------------------------------------
[  8] local 192.168.2.3 port 57319 connected with 192.168.2.4 port 5001
[  6] local 192.168.2.3 port 57317 connected with 192.168.2.4 port 5001
[  4] local 192.168.2.3 port 57315 connected with 192.168.2.4 port 5001
[  5] local 192.168.2.3 port 57316 connected with 192.168.2.4 port 5001
[  7] local 192.168.2.3 port 57318 connected with 192.168.2.4 port 5001
[ ID] Interval       Transfer     Bandwidth
[  6]  0.0-10.0 sec  4.50 MBytes  3.77 Mbits/sec
[  8]  0.0-10.1 sec  4.00 MBytes  3.34 Mbits/sec
[  5]  0.0-10.2 sec  4.00 MBytes  3.30 Mbits/sec
[  4]  0.0-10.3 sec  4.00 MBytes  3.25 Mbits/sec
[  7]  0.0-10.4 sec  3.88 MBytes  3.13 Mbits/sec
[SUM]  0.0-10.4 sec  20.4 MBytes  16.5 Mbits/sec
PsychicSaw:~ PsychicSaw$
```

Slika 4.9: IPERF - klientova stran, paralelno pošiljanje petih uporabnikov, 802.11n.



Slika 4.10: inSSIDer, 802.11g omrežje.

Slika 4.11: inSSIDer, 802.11n omrežje, 40Mhz.



Slika 4.12: inSSIDer, 802.11n omrežje, 20Mhz.

S prav tako odprtokodnim programom (več ali manj se dobi kar skripta napisana v programskem jeziku C++) Zap, ki mora biti naložen na obeh straneh (pošiljatelj in prejemnik), smo ponovno preverjali prepustnost povezave. Tu naj povemo, da smo na prenosniku uporabili virtualno Windows okolje, kajti na OS X operacijskem sistemu bi imeli nekoliko več dela in preglavic. Korektnost meritev smo kasneje preverili tudi na ločenem Windows računalniku. Na obeh računalnikih mora biti najprej zagnan zapd, ki ga poženemo enostavno z vpisom "zapd" v ukazno vrstico CMD (seveda na lokaciji kjer se zapd nahaja). Nato lahko izvedemo test prepustnosti z ukazom "zap -sIP1 -dIP2", kjer je IP1 IP pošiljatelja, IP2 pa prejemnika. Zap začne pošiljati veliko število paketkov in sproti izračunava statistiko, ki jo tudi prikazuje. Pri hitro poslanih paketkih sproti izračunava in meri izgubo paketkov ter vmesne čase, poda pa tudi podrobne statistike prepustnosti - podane so vrednosti pri katerih je 50%, 90%, 95%, 99% in 99.9% časa prepustnost vsaj taka kot podana. Te vrednosti koristijo pri določanju kvalitete povezave za prenos videa, slik in ostalih multimedijskih vsebin [37].

Preverili smo tudi kako se izkaže posamezen usmerjevalnik pri prenosu datotek v omrežju. Na prenosniku smo aktivirali možnost FTP (angl. *File Transfer Protocol*) prenosov z ukazom
`sudo -s launchctl load -w /System/Library/LaunchDaemons/ftp.plist`,
nato pa smo s pomočjo FTP prenesli 25.9 MB veliko datoteko iz prenosnika na Windows računalnik. Na Windows računalniku smo kot FTP klienta uporabili program WinSCP in tako spremljali čas in hitrost prenosa pri obeh usmerjevalnikih. Pozoren je treba biti na nastavitev prenosnega protokola v WinSCP, kajti FTP ni privzeta vrednost. Prenos smo zaradi morebitnih napak in statistike ponovili večkrat.

Za vse omenjene meritve in teste, ki smo jih izvedli, smo poskrbeli, da smo imeli približno enako delovno okolje tako za G, kot za N usmerjevalnik. To pomeni enake postavitve računalnikov ter usmerjevalnikov, isti prostor in stavba, iste ovire, ki bi lahko ovirale signal, ter enako število klientov povezanih v omrežje. Vsakič smo tudi preverili SNR ustreznega usmerjevalnika, ter ga primerjali s prejšnjim. Za potrebe enakih pogojev G in N usmerjevalnika, smo, kot že omenjeno, pomikali prenosnik nekoliko stran od N usmerjevalnika. Za vse meritve podane v naslednjem poglavju je bil RSSI pri stacionarnem računalniku v postavitvi 2 vedno okoli -50 dBm (max 3 dBm odstopanja). Pri prenosniku je bilo to nekoliko težje doseči, a vseeno smo se vedno potrudili doseči čim bližjo vrednost, razen pri posebej omenjenih rezultatih. SNR je bil v primerih kjer ni drugače napisano vedno med 38-45 dBm, pri "oddaljenih" meritvah pa okoli 10 dBm (RSSI je bil v slednjem primeru okoli -80 dBm in je tak tudi vedno ko omenjamo "slabši" signal v nadaljnjih straneh).

Večino meritev smo zaradi morebitnih odstopanj izvedli vsaj desetkrat. Rezultati so prikazani in komentirani v naslednjem poglavju.

4.2 Rezultati

V tem poglavju predstavimo rezultate in jih komentiramo ter analiziramo. Primerjamo tiste, ki smo jih dobili z G usmerjevalnikom in tiste, ki smo jih dobili za omrežje z N usmerjevalnikom. Poglavje je razdeljeno na dva dela, in sicer na tabele meritev ter analizo rezultatov. V prvem so predstavljeni pridobljeni podatki meritev, v drugem pa podatke komentiramo in analiziramo.

4.2.1 Tabele in grafi meritev

Tu se nahajajo tabele z meritvami, pri vsaki pa je zapisano na kaj se nanaša. Prve tabele predstavljajo podatke pridobljene z IPERF, nato sledijo podatki, ki smo jih pridobili s pomočjo ping-a, nato pa še podatki pridobljeni s pomočjo programa Zap. Na koncu smo vpisali še rezultate hitrosti in čase pri prenosu datoteke s pomočjo FTP. Če ni posebej napisano, je pri tabelah za IPERF vrednost velikosti prenešenih podatkov (angl. *Transfer*) vedno predstavljena v MBytes, vrednost za prepustnost pa v Mbps. "Jitter" je vsakič predstavljen v mili-sekundah (ms). Podrobnejši opisi in razlage ter komentarji rezultatov se nahajajo v poglavju 4.2.2.

`Transfer`	14.0	19.5	19.2	16.2	16.8	16.1	14.8	14.4	21.2	19.5
`Bandwidth`	11.6	16.2	16.0	13.5	13.9	13.4	12.2	12.0	17.7	16.2

Tabela 4.2: IPERF - meritve prepustnosti iz prenosnika na stacionaren računalnik (postavitev 1), usmerjevalnik G.

`Transfer`	78.6	82.5	70.9	85.9	84.5	83.6	79.9	89.0	70.9	81.2
`Bandwidth`	65.9	69.1	59.3	71.8	70.8	70.1	66.9	74.5	59.2	68.1

Tabela 4.3: IPERF - meritve prepustnosti iz prenosnika na stacionaren računalnik (postavitev 1), usmerjevalnik N.

`Transfer`	11.5	10.1	5.12	5.25	4.25	5.12	9.25	5.38	3.50	4.00
`Bandwidth`	9.34	8.04	4.08	4.20	3.35	4.02	7.64	4.09	2.80	3.19

Tabela 4.4: IPERF - meritve prepustnosti iz prenosnika na stacionaren računalnik (postavitev 2), usmerjevalnik G.

`Transfer`	59.2	55.6	61.6	62.1	63.1	62.9	63.0	63.1	63.0	60.0
`Bandwidth`	49.6	46.5	51.6	52.0	52.9	52.6	52.8	52.8	52.7	50.2

Tabela 4.5: IPERF - meritve prepustnosti iz prenosnika na stacionaren računalnik (postavitev 2), usmerjevalnik N-40Mhz.

`Transfer`	49.2	30.1	49.5	49.4	49.8	49.8	49.4	50.2	49.8	49.5
`Bandwidth`	41.2	25.2	41.4	41.3	41.6	41.6	41.3	42.0	41.6	41.4

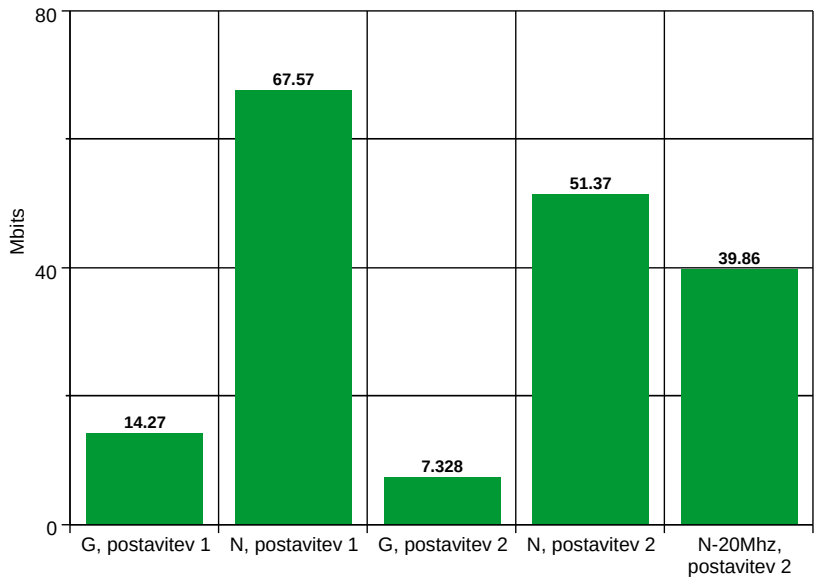
Tabela 4.6: IPERF - meritve prepustnosti iz prenosnika na stacionaren računalnik (postavitev 2), usmerjevalnik N-20Mhz.

`Transfer`	10.5	10.5	10.6	7.75	10.8	10.8	10.4	10.4	10.5	10.2
`Bandwidth`	8.76	8.75	8.83	6.47	8.99	8.92	8.46	8.66	8.71	8.52

Tabela 4.7: IPERF - meritve prepustnosti iz prenosnika na stacionaren računalnik (postavitev 2), usmerjevalnik G - slabši signal.

`Transfer`	47.8	43.0	45.0	33.2	29.9	48.2	51.5	35.2	58.2	52.2
`Bandwidth`	40.0	36.0	37.6	10.8	13.3	13.5	10.8	9.40	12.8	10.8

Tabela 4.8: IPERF - meritve prepustnosti iz prenosnika na stacionaren računalnik (postavitev 2), usmerjevalnik N - slabši signal.



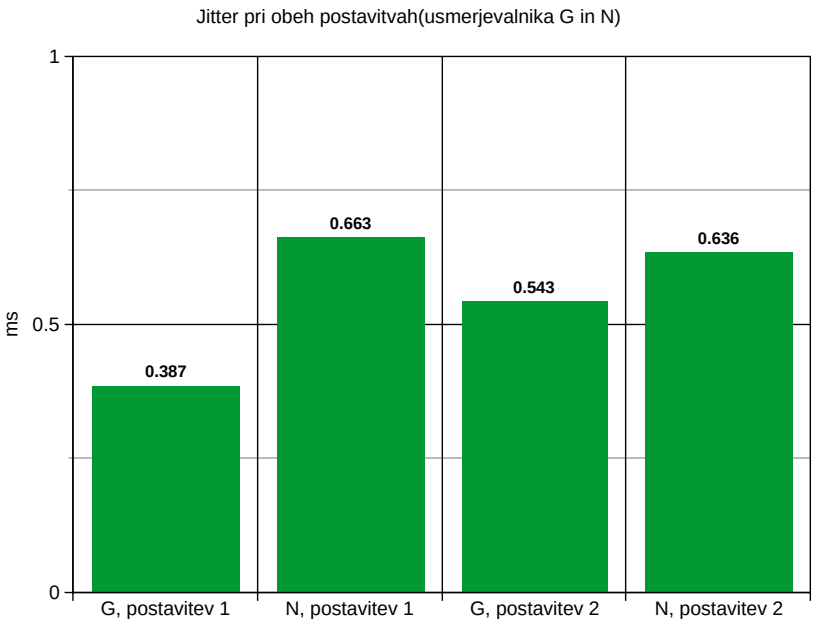
Slika 4.13: Primerjava povprečnih izmerjenih prepustnosti pri obeh usmerjevalnikih.

G	0.375	0.563	0.420	0.364	0.355	0.379	0.345	0.415	0.307	0.347
N	0.467	0.887	0.833	0.633	0.616	0.958	0.429	0.419	0.835	0.553

Tabela 4.9: Meritve IPERF UDP - "jitter" iz prenosnika na stacionaren računalnik, postavitev 1.

G	0.525	0.706	0.518	0.427	0.400	0.557	0.600	0.742	0.359	0.593
N	0.470	0.488	0.641	0.666	0.730	0.579	0.946	0.733	0.571	0.531

Tabela 4.10: Meritve IPERF UDP - "jitter" iz prenosnika na stacionaren računalnik, postavitev 2.



Slika 4.14: Primerjava povprečnih izmerjenih vrednosti "jitter" pri obeh usmerjevalnikih.

št. povezav	Interval	Transfer	Bandwidth
5	10.2 s	14.1 MBytes	11.8 Mbps
10	10.8 s	16.1 MBytes	12.5 Mbps
20	11.1 s	17.5 MBytes	13.2 Mbps
30	14.0 s	14.0 MBytes	8.36 Mbps
40	20.6 s	14.8 MBytes	6.00 Mbps
50	29.9 s	13.5 MBytes	3.78 Mbps
100	68.7 s	25.0 MBytes	3.05 Mbps

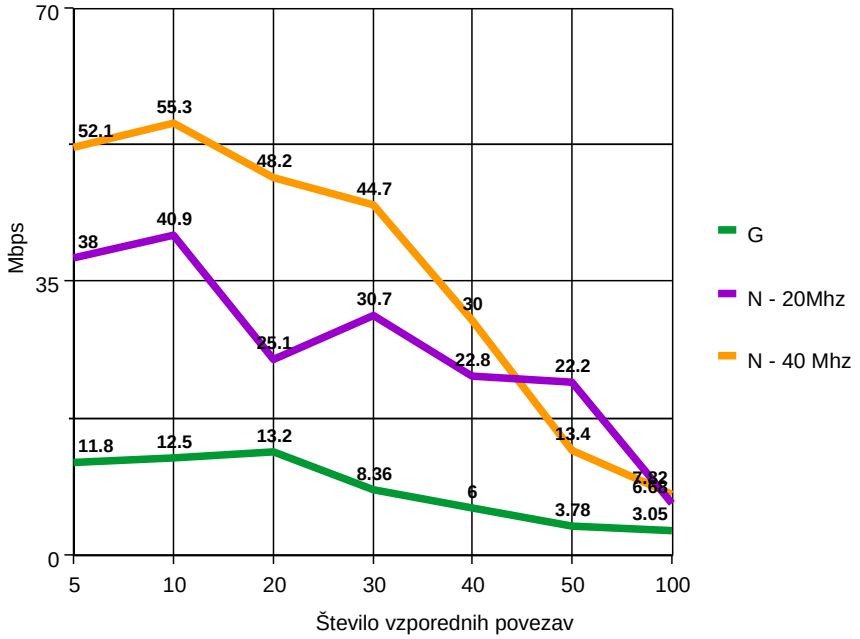
Tabela 4.11: IPERF - paralelne povezave v 802.11g omrežju.

št. povezav	Interval	Transfer	Bandwidth
5	10.1 s	45.9 MBytes	38.0 Mbps
10	10.3 s	50.1 MBytes	40.9 Mbps
20	16.1 s	48.0 MBytes	25.1 Mbps
30	14.4 s	52.6 MBytes	30.7 Mbps
40	14.7 s	39.9 MBytes	22.8 Mbps
50	15.2 s	40.1 MBytes	22.2 Mbps
100	56.6 s	45.1 MBytes	6.68 Mbps

Tabela 4.12: IPERF - paralelne povezave v 802.11n (20Mhz) omrežju.

št. povezav	Interval	Transfer	Bandwidth
5	10.1 s	62.6 MBytes	52.1 Mbps
10	10.2 s	67.5 MBytes	55.3 Mbps
20	11.2 s	64.2 MBytes	48.2 Mbps
30	12.6 s	67.0 MBytes	44.7 Mbps
40	14.9 s	53.2 MBytes	30.0 Mbps
50	29.8 s	47.7 MBytes	13.4 Mbps
100	56.9 s	53.1 MBytes	7.82 Mbps

Tabela 4.13: IPERF - paralelne povezave v 802.11n (40Mhz) omrežju.



Slika 4.15: Primerjava vzporednih prenosov več uporabnikov pri obeh usmerjevalnikih.

	povp. čas - postavitev 1	povp. čas - postavitev 2
802.11g	4.153 ms	10.482 ms
802.11n	3.364 ms	9.703 ms

Tabela 4.14: Ping iz prenosnika na stacionaren računalnik.

	povprečen čas(100 poslanih paketkov, 5 ponovitev)
802.11g	4.260 ms
802.11n	3.772 ms

Tabela 4.15: Ping iz prenosnika na usmerjevalnik.

	prejeti paketi	izgubljeni paketi	povp. prepustnost
802.11g	60406	0	13.8 Mbps
802.11n	428770	246	98.4 Mbps

Tabela 4.16: Zap - prepustnost iz prenosnika na stacionaren računalnik(postavitev 2).

	hitrost[mbps]	čas prenosa[s]	postavitev
802.11g	14.7-22.1	9-14	1
802.11n	45.9-81.1	2-3	1
802.11g	5.7-10.7	18-30	2
802.11n	40.1- 58.9	3-5	2
802.11n(20Mhz)	27.9-43.4	5-8	2

Tabela 4.17: FTP - testiranje hitrosti pri prenosu 25.9 MB datoteke.

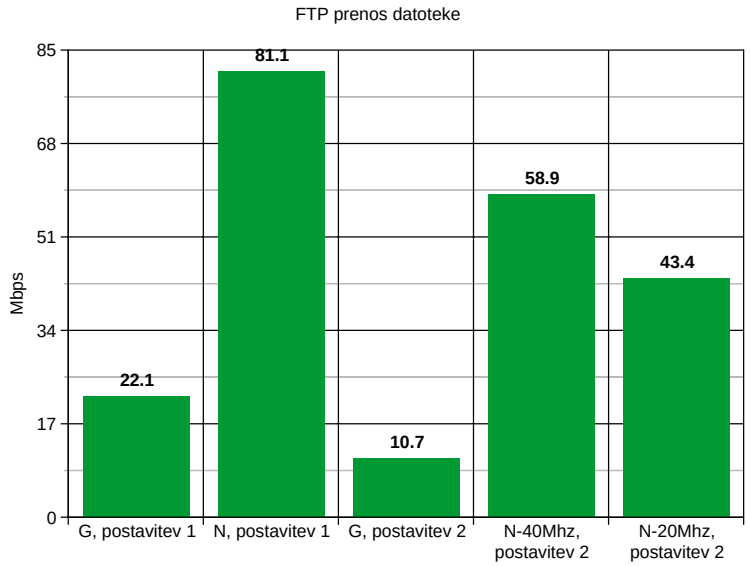
4.2.2 Analiza in komentar rezultatov

Rezultati, kot po pričakovanjih, odražajo prednosti 802.11n standarda pred 802.11g. Zanimivo pa je, za koliko so se spremenile hitrosti z nadgradnjo na novejši standard, kar smo preverili na konkretnem primeru. Obljubljene teoretične hitrosti 802.11n standarda so vse do 300 Mbps, ponekod pa tudi do 600 Mbps. Seveda se jim reče "teoretične" z namenom; ne upoštevajo namreč omrežnih zastojev in zakasnitev, interferenc ter obdelave prometa, ki jo izvaja vsak usmerjevalnik nekoliko drugače.

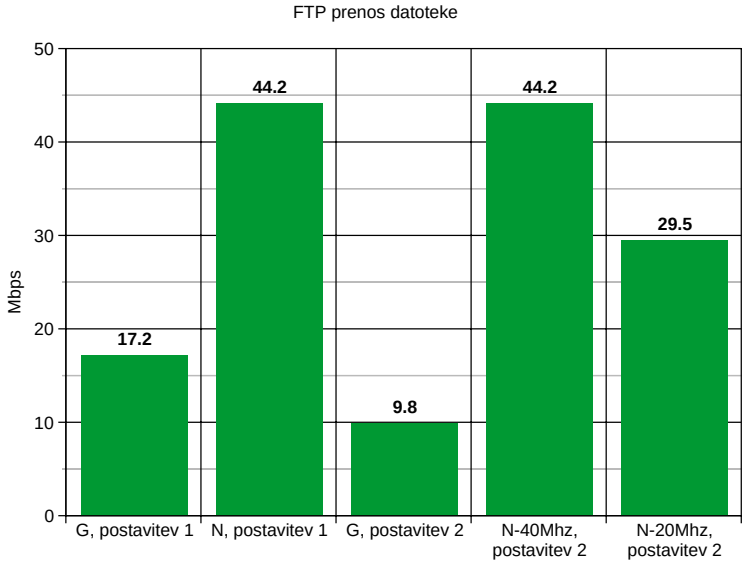
Prve IPERF meritve so nam podale prepustnost povezave v podanih situacijah. Na sliki 4.13 lahko jasno vidimo veliko razliko med 802.11g in 802.11n omrežjem. Slednje je glede na rezultate približno pet do sedemkrat hitrejše, upoštevajoč postavitev 2. Z uporabo 20 MHz širine kanala je 802.11n omrežje prehitelo predhodnika za petkrat. V tabelah 4.7 in 4.8

	hitrost[mbps]	čas prenosa[s]	postavitev
802.11g	6.6-17.2	14-40	1
802.11n	25.4-44.2	4-7	1
802.11g	6.6-9.8	21-25	2
802.11n	16.4-44.2	5-10	2
802.11n(20Mhz)	22.9-29.5	7-9	2

Tabela 4.18: FTP - testiranje hitrosti pri prenosu 25.9 MB datoteke pri slabšem signalu.



Slika 4.16: Primerjava hitrosti pri prenosu datoteke s FTP.



Slika 4.17: Primerjava hitrosti pri prenosu datoteke s FTP pri slabšem signalu.

lahko vidimo zmanjšanje prepustnosti pri obeh usmerjevalnikih zaradi večje razdalje med prenosnikom in usmerjevalnikom. S prenosnikom smo se premaknili eno nadstropje nižje, še vedno pa smo poskrbeli za približno enak RSSI (kot že omenjeno okoli -80 dBm) in SNR (malo pod 10 dBm) pri obeh usmerjevalnikih.

Druge IPERF meritve so bile usmerjene v odstopanja v zakasnitvah oz. "jitter". Slika 4.14 nam pokaže primerjavo povprečnih vrednosti "jitter" v različnih postavitvah za oba usmerjevalnika. V tem primeru se je G usmerjevalnik odrezal nekoliko bolje - v obeh postavitvah smo v 802.11g omrežju izmerili manjši "jitter", razlika pa sploh pri postavitvi 2, ki nas najbolj zanima, ni ravno velika. Odstopanja v meritvah "jitter" so bila iz dneva v dan (da, meritve smo ponovili tudi na različne dni) različna, kar za "jitter" niti ni tako neobičajno.

Tretje IPERF meritve so se posvetile sočasnim oziroma vzporednim povezavam in testiranju prepustnosti v takšni situaciji. Več vzporednih povezav

simulira večje število uporabnikov, ki hkrati pošiljajo podatke skupnemu prejemniku. Prepustnost se seveda razdeli med pošiljatelje, čas, ki je potreben za pošiljanje enake kvote podatkov, pa se povečuje glede na število pošiljateljev. V tabelah 4.11, 4.12 in 4.13 se lepo vidi povečevanje intervala v katerem so poslani podatki. Prav tako lahko opazimo zmanjševanje skupne prepustnosti pri večjem številu uporabnikov, kar se še najbolje vidi na sliki 4.15. Pri vzporednih prenosih je maksimalna prepustnost povezave pri G usmerjevalniku več kot štirikrat manjša, kot pri usmerjevalniku N. Zanimivo pa je, kako pada prepustnost s povečevanjem števila vzporednih sej; pri N usmerjevalniku je padanje precej bolj razvidno, pri 100 vzporednih prenosih se usmerjevalnik N skoraj približa usmerjevalniku G. Tu bi torej lahko sklepali, da je G usmerjevalnik bolj skalabilen, res pa je, da so to rezultati naših specifičnih meritev. Zelo verjetno je, da bi z drugim usmerjevalnikom, v drugem okolju, dobili precej drugačne rezultate, vseeno pa je zanimivo opazovati razlike.

Pri vseh IPERF meritvah je pomembna velikost TCP (angl. *Transmission Control Protocol*) okna (angl. *TCP Window Size*), ki pove kolikšno količino podatkov lahko pošiljatelj pošlje, brez da bi dobil potrditveni paket iz strani prejemnika. Pri Windows računalnikih je privzeta vrednost 64 KB, pri OS X pa 129 KB; teh vrednosti nismo spreminjali. Velikost TCP okna in RTT (angl. *Round Trip Time*) direktno vplivata na prepustnost povezave med dvema točkama v omrežju.

Ping testi nam povedo koliko časa potrebuje naprava na drugi strani usmerjevalnika, da se odzove na neko prošnjo prve naprave - pošiljatelja. Rezultati so bili pri 802.11n usmerjevalniku nekoliko boljši, ni pa bilo zaznati ogromnih razlik. Sklepamo, da večjih razlik med G in N usmerjevalnikom tu ni, ker se RTT času direktno prišteva čas, ki ga potrebuje vsaka naprava za odziv, ta pa je pri obeh meritvah približno enak. Razlika je torej v hitrejši prenosni poti po zraku pri usmerjevalniku N - časi so za približno 7-11% krajši.

Tudi s programom ZAP smo poskusili izmeriti prepustnost povezave med klientoma v omrežjih. Ker Zap deluje na nekoliko drugačen način kot Iperf,

smo dobili tudi drugačne rezultate, v več meritev pa se nismo poglabljali, zato smo izvedli samo meritev za postavitev 2. V podrobnosti se tu ne bomo spuščali, osredotočili se bomo samo na primerjavo G in N usmerjevalnika pri tem delu meritev posebej. V tabeli 4.16 lahko vidimo prepustnosti, ki jih vrne Zap pri posameznem usmerjevalniku; N usmerjevalnik doseže kar sedemkrat večjo prepustnost.

S pomočjo FTP smo dobili še eno primerjavo obeh usmerjevalnikov. Ta test je skoraj najboljši približek realnim rezultatom, kajti podobni prenosi se lahko dogajajo dnevno. Na stacionarnem računalniku smo preko WinSCP pri različnih postavitvah prenesli 25.9 MB veliko datoteko iz prenosnika. Zapisovali smo si hitrosti in končne čase, ki se lahko vidijo v tabelah 4.17 in 4.18. Zopet lahko opazujemo zanimive razlike med G in N usmerjevalnikom pri različnih postavitvah; maksimalna hitrost, ki smo jo dosegli s prvim je 22.1 Mbps, pri drugem pa 81.1 Mbps. Ti dve hitrosti sta bili izmerjeni pri postavitvi 1, pri postavitvi 2 pa sta maksimalni hitrosti (pri RSSI -50 dBm in SNR okoli 40 dBm) 10.7 in 58.9 Mbps. Pot po zraku torej konkretno zmanjša hitrost oziroma efektivnost prenosa, bolj pa se to pozna pri G usmerjevalniku. Meritve smo izvedli tudi pri slabšem signalu, rezultati se najbolje vidijo na sliki 4.17, kjer jih lahko primerjamo s tistimi na sliki 4.16. Enostavno je razbrati podobnost. V primeru G usmerjevalnika se prepustnost zmanjša za skoraj polovico, ko postavitev 1 zamenjamo za postavitev 2. Pri usmerjevalniku N ta razlika ni tako velika. Omenimo pa naj, da so na obeh grafih vpisane samo najvišje hitrosti, povprečne bi bile nekoliko manjše.

Nasploh lahko rečemo, da je ena večjih prednosti standarda 802.11n, uporaba 40 MHz kanala. Širši kanal omogoča direktno povečanje hitrosti za več kot dvakrat. Zmanjšanje širine na osnovno, 20 MHz, je povzročilo takojšnji upad hitrosti za približno 22-34%. Uporaba MIMO in izboljšave na MAC plasti k povečanju hitrosti samo še pripomorejo.

Poglavje 5

Zaključek

Brezžična omrežja so zanimivo in precej statistično naravnano področje. Težko je namreč izmeriti in določiti točne hitrosti prenosa podatkov po omrežju, kajti le te varirajo in so odvisne od veliko dejavnikov. Vseeno pa smo se v tem delu lotili pregleda, primerjave in številk, ki jih ponujajo take meritve. Četudi lahko brez slabe vesti rečemo, da 802.11n standard nudi štiri do sedemkrat večje hitrosti prenosa podatkov kot 802.11g, bi bolj točno trditev, glede na opravljene meritve, le stežka sprejeli. Še enkrat je nujno povedati, da bi meritve lahko bile boljše. Nudili bi lahko točno določeno okolje, brez sprememb pri posameznih meritvah. Meritve bi lahko ponovili večkrat, statistika je seveda velik pokazatelj. Upoštevati bi morali vsakodnevne spremembe faktorjev, kot so mikrovalovna pečica in brezžični domači telefoni, ki delujejo v 2.4 GHz omrežju, kar lahko povzroča nezaželjene interference. Seveda so te enkrat lahko večje, drugič manjše. Če bi nudili izoliran prostor, bi bile meritve natančnejše.

Pri meritvah smo se osredotočali na primerjavo hitrosti med 802.11g in 802.11n standardom pri različnih postavitvah, nismo pa se posvečali specifičnim lastnostim strojne opreme, ki je lahko pomemben faktor pri določanju le te. Vseeno smo dobili neko realno primerjavo, ki bi seveda vedno lahko bila še boljša.

Leta 2014 pričakujemo hitrejše uvajanje novejših standardov kot sta 802.11ac

in 802.11ad. Obljubljata še večje hitrosti prenosa podatkov, vse do in tudi nad 1 Gbps. Pa take hitrosti res potrebujemo za domačo uporabo? Najvišja hitrost je v vsakem primeru namreč podrejena pasovni širini, ki jo imamo na voljo, 1 Gbps pa je precej nad trenutno dosegljvo mejo.

Literatura

[1] "http://www.toptenz.net"

[2] "http://www.jjgifford.com/expressions/geometry/img/"

[3] "http://www.cbeagle.co.uk"

[4] "http://wndw.net/download.html"

[5] "http://yawlay.webs.com"

[6] K. Daniel Wong, "Wireless Internet Telecommunications", *Artech House mobile communications series*, poglavje 6, od str. 91, 2005.

[7] R. Binder, N. Abramson, F. Kuo, A. Okinaka, D. Wax, "ALOHA packet broadcasting - A retrospect",1975. Dostopno na: http://www.computer.org

[8] N. Abramson, "The ALOHAnet-Surfing for Wireless Data", December 2009. Dostopno na: http://dl.comsoc.org/livepubs/ci1/public/2009/dec/pdf/abramson.pdf

[9] Roberts, Lawrence G. "ALOHA Packet System With and Without Slots and Capture", *Computer Communications Review*, str. 28-42 (April 1975).

[10] "http://en.wikipedia.org/wiki/ALOHAnet"

[11] "http://arstechnica.com/gadgets/2011/10/cutting-the-cord-how-the-worlds-engineers-built-wi-fi/"

[12] David D. Coleman, David A. Westcott, "CWNA-Certified Wireless Network Administrator", Official study guide

[13] "http://www.computereconomics.com/article.cfm?id=1084"

[14] "http://www.nytimes.com/2009/04/19/business/19digi.html?_r=2&ref=technology&"

[15] "http://www.reghardware.com/2008/04/17/intel_laptop_desktop_crossover/"

[16] "http://www.computereconomics.com"

[17] K. Daniel Wong, "Wireless Internet Telecommunications", *Artech House mobile communications series*, str. 40, 2005.

[18] Jim Geier,Wireless Network Industry Report, Dostopno na: http://www.wireless-nets.com/resources/downloads/wireless_industry_report_2007.pdf

[19] "http://www.personalareanetwork.net"

[20] "http://www.scansourcesecurity.com/MicroSites/ScanSourceSecurity/quickstart/wireles

[21] "http://www.plcmanual.com/isoosi-model"

[22] "http://netlab.ulusofona.pt/rc/book/5-link/5_07/index.htm"

[23] R. Pickholtz, D. Schilling, L. Milstein, "Theory of Spread Spectrum Communication - a Tutorial", *IEEE Transactions on Communications*, Vol 30, No. 5, str. 855-884 , Maj 1982.

[24] A. Viterbi, "CDMA: Principles of Spread Spectrum Communication", Addison-Wesley, Reading, MA , 1995. Dostopno na: http://www.scribd.com/doc/46022718/CDMA-Principles-of-Spread-Spectrum-Communication

[25] "http://www.umtsworld.com/technology/cdmabasics.htm"

[26] Syngress, Eric Ouellet, Neal O'Farrell, "Hackproofing Your Wireless Network", 2002

[27] "http://www.hjp.at/doc/rfc/rfc3748.txt "

[28] "http://www.helifreak.com/showthread.php?t=347351"

[29] "http://www.wirelesstut.com/ccna-wireless-knowledge/basic-terminologies"

[30] "http://en.wikipedia.org/wiki/IEEE_802.11n-2009#40.C2.A0MHz_in_2.4.C2.A0GHz"

[31] "http://www.softbank.co.jp/en/news/press/2006/20061211_01/"

[32] "http://mwrf.com/test-and-measurement/analyze-antenna-approaches-lte-wireless-systems"

[33] James F. Kurose, Keith W. Ross "Computer Networking a top-down approach", fifth edition

[34] "http://www.metageek.net/products/inssider/"

[35] "http://openmaniak.com/iperf.php"

[36] "https://code.google.com/p/zapwireless/"

[37] "http://www.ruckuswireless.com/press/releases/20100104-zap-wireless-tool"