UNIVERZA V LJUBLJANI
FAKULTETA ZA RAČUNALNIŠTVO IN INFORMATIKO

Samo Vodopivec

ANALIZA PRENOSA PODATKOV PRI PREHAJANJU MED DOSTOPNIMI TOČKAMI V BREZŽIČNEM OMREŽJU

DIPLOMSKO DELO NA
UNIVERZITETNEM ŠTUDIJU

Mentor: prof. dr. Nikolaj Zimic
Somentor: doc. dr. Iztok Lebar Bajec

Ljubljana, 2010

Univerza
v Ljubljani

Fakulteta za računalništvo
in informatiko

Tržaška 25
1000 Ljubljana, Slovenija
telefon: 01 476 84 11
faks: 01 426 46 47
www.fri.uni-lj.si
e-mail: dekanat@fri.uni-lj.si

Št. naloge: 01611/2009
Datum: 15.10.2009

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

Kandidat: **SAMO VODOPIVEC**

Naslov: **ANALIZA PRENOSA PODATKOV PRI PREHAJANJU MED DOSTOPNIMI TOČKAMI V BREZŽIČNEM OMREŽJU**

ANALYSIS OF DATA TRANSFER DELAYS IN WIRELESS NETWORKS SUBJECT TO ROAMING

Vrsta naloge: Diplomsko delo univerzitetnega študija

Tematika naloge:

Mobilne naprave postajajo vedno bolj priljubljene in tudi število aplikacij, ki so s stališča prenosa podatkov zelo zahtevne, se povečuje. Brezžična lokalna omrežja so zelo zanimiva, ker omogočajo dokaj velike prenosne hitrosti pri razmeroma nizki ceni. Posledica lokalnosti pa je zahteva po prehajanju med dostopnimi točkami brezžičnega omrežja.

V nalogi analizirajte možnosti prehoda med dostopnimi točkami za brezžična omrežja, ki temeljijo na standardu IEEE 802.11. Svoje ugotovitve potrdite z meritvami časov v laboratorijskem okolju ter v brezžičnem omrežju Eduroam, ki je dostopno na fakulteti. Posebej bodite pozorni na zakasnitve prenosa paketov oziroma njihovo morebitno izgubo.

Mentor:

prof. dr. Nikolaj Zimic

Fakulteta za računalništvo in informatiko
2
UNIVERZA V LJUBLJANI

Dekan:

prof. dr. Franc Solina

Somentor:

doc. dr. Iztok Lebar Bajec

Namesto te strani vstavite original izdane teme diplomskega dela s podpisom mentorja in dekana ter žigom fakultete, ki ga diplomant dvigne v študentskem referatu, preden odda izdelek v vezavo!

I Z J A V A O A V T O R S T V U

diplomskega dela

Spodaj podpisani Samo Vodopivec,

z vpisno številko 63020178,

sem avtor diplomskega dela z naslovom:

ANALIZA PRENOSA PODATKOV PRI PREHAJANJU MED DOSTOPNIMI TOČKAMI V BREZŽIČNEM OMREŽJU

S svojim podpisom zagotavljam, da:

- sem diplomsko delo izdelal samostojno pod mentorstvom

  prof. dr. Nikolaja Zimica

  in somentorstvom

  doc. dr. Iztoka Lebarja Bajca,

- 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 12.4.2010 Podpis avtorja:

Zahvala

Zahvaljujem se svojim staršem, ki so mi študij omogočili, ter vsem prijateljem, ki so mi stali ob strani in pomagali v času celotnega študija.

Zahvaljujem se mentorju prof. dr. Nikolaju Zimicu in somentorju doc. dr. Iztoku Lebarju Bajcu, ki sta mi izdatno svetovala ter me usmerjala pri izdelavi diplomskega dela.

Za podatke o brezžičnem omrežju Eduroam ter pomoč pri izvajanju meritev v njem se zahvaljujem g. Damirju Metelku in g. Igorju Čarmanu.

Lektoriranje diplomskega dela je opravila gdč. Andreja Molan, za kar se tudi njej iskreno zahvaljujem.

Kazalo vsebine

ZAHVALA ..... **I**

KAZALO VSEBINE ..... **III**

SEZNAM UPORABLJENIH KRATIC ..... **V**

SEZNAM UPORABLJENIH ENOT ..... **VII**

POVZETEK ..... **IX**

ABSTRACT ..... **XI**

1. UVOD **1**

2. BREZŽIČNO OMREŽJE PO STANDARDU IEEE 802.11 ..... **3**

2.1. STANDARD IEEE 802.11G 4
2.2. TOPOLOGIJA BREZŽIČNIH OMREŽIJ 4
2.3. DOSTOPNA TOČKA 5
2.4. PREPROSTO BREZŽIČNO OMREŽJE 6
2.5. RAZŠIRJENO BREZŽIČNO OMREŽJE 6

3. DELOVANJE BREZŽIČNEGA OMREŽJA **9**

3.1. OSNOVNE ZAKONITOSTI DELOVANJA 9
3.1.1. Dostop do medija *9*
3.1.2. Zgradba okvirjev *11*
3.1.3. Prenos okvirjev po omrežju *11*
3.1.4. Tipi okvirjev *12*
3.1.5. Distribucija sporočil *12*
3.1.6. Integracija *13*
3.1.7. Kvaliteta storitve *13*
3.2. DOSTOPNA TOČKA 13
3.2.1. Svetilni okvirji *13*
3.2.2. Odziv na aktivno iskanje *14*
3.2.3. Upravljanje z energijo *15*
3.2.4. Zasedenost medija ter dostopne točke *16*
3.3. ODJEMALEC 17
3.3.1. Problemi pri iskanju dostopnih točk *17*
3.3.2. Postopka iskanja dostopnih točk *18*
3.3.3. Avtentifikacija *19*
3.3.4. Asociacija *20*
3.3.5. Reasociacija *20*
3.3.6. Deasociacija *21*
3.3.7. Posebnosti pri IEEE 802.1X načinu avtentifikacije *21*
3.3.8. Standard IEEE 802.11r *22*
3.4. PREHAJANJE 22
3.4.1. Prehod na drugo dostopno točko *22*

4. TESTNO OKOLJE **25**

4.1. STROJNA OPREMA 25
4.1.1. Nastavitev dostopnih točk *25*
4.1.2. Nastavitev odjemalca *26*
4.1.3. Nastavitev vohljačev *26*

4.1.4. Testno omrežje *26*
4.1.5. Omrežje Eduroam *28*
4.2. PROGRAMSKA OPREMA 29
4.2.1. Generator prometa pktgen *29*
4.2.2. Nadgrajen MadWifi gonilnik *30*
4.2.3. Nadgrajen gonilnik vmesnika Intel WiFi Link 5100 ..... *30*
4.2.4. Programski paket Linux WPA Supplicant *31*
4.2.5. Programa za vohljanje CommView for WiFi ter Wireshark *31*
4.2.6. Kombinacija gonilnika Intelovega vmesnika ter CommView for WiFi *33*

5. TESTNI SCENARIJI IN REZULTATI 35

5.1. OSNOVNI PODATKI O MERITVAH 35
5.2. PREHODI V NEOBREMENJENEM OMREŽJU BREZ ŠIFRIRANJA IN GENERIRANEGA PROMETA 37
5.3. PREHODI V NEOBREMENJENEM OMREŽJU BREZ ŠIFRIRANJA 37
5.4. PREHODI V NEOBREMENJENEM OMREŽJU BREZ ŠIFRIRANJA Z DOSTOPNO TOČKO NA PASIVNEM KANALU 38
5.5. PREHODI V NEOBREMENJENEM OMREŽJU Z WPA ŠIFRIRANJEM 38
5.6. PREHODI V NIZKO OBREMENJENEM OMREŽJU Z WPA ŠIFRIRANJEM 39
5.7. PREHODI V MOČNO OBREMENJENEM OMREŽJU Z WPA ŠIFRIRANJEM 39
5.8. PREHODI V NEOBREMENJENEM EDUROAM OMREŽJU 40
5.9. PREHODI V OBREMENJENEM EDUROAM OMREŽJU 41
5.10. REZULTATI MERITEV ČASOV ISKANJ 41

6. UGOTOVITVE IN ZAKLJUČEK 43

6.1. MOŽNE IZBOLJŠAVE 43

PRILOGE 45

TABELE Z REZULTATI OPRAVLJENIH MERITEV 45
Prehodi v neobremenjenem omrežju brez šifriranja in generiranega prometa *45*
Prehodi v neobremenjenem omrežju brez šifriranja *46*
Prehodi v neobremenjenem omrežju brez šifriranja z dostopno točko na pasivnem kanalu *47*
Prehodi v neobremenjenem omrežju z WPA šifriranjem *48*
Prehodi v lahno obremenjenem omrežju z WPA šifriranjem *49*
Prehodi v močno obremenjenem omrežju z WPA šifriranjem *50*
Prehodi v neobremenjenem Eduroam omrežju *51*
Prehodi v obremenjenem Eduroam omrežju *52*

SEZNAM TABEL 53

SEZNAM SLIK 55

SEZNAM UPORABLJENE LITERATURE IN VIROV 57

Seznam uporabljenih kratic

AES	Advanced Encryption Standard blokovni algoritem, ki je leta 2002 nadomestil DES kot ameriški standard
AIFS	Arbitration InterFrame Space dogovorjeni medokvirski čas
AP	Access Point dostopna točka
ARP	Address Resolution Protocol protokol za prepoznavanje naslovov
ATM	Asynchronous Transfer Mode protokol za prenos enako dolgih podatkovnih paketov, namenjen večjim prenosnim hitrostim
BSS	Basic Service Set osnovni nabor storitev
CSMA/CA	Carrier Sense Multiple Access with Collision Avoidance večkratni dostop s prepoznavanjem nosilca in izogibanjem kolizij
CSMA/CD	Carrier Sense Multiple Access with Collision Detection večkratni dostop s prepoznavanjem nosilca in detekcijo kolizij
CTS	Clear To Send dovoljenje za pošiljanje
DCF	Distributed Coordination Function porazdeljena koordinacijska funkcija
DHCP	Dynamic Host Configuration Protocol protokol za dinamično konfiguracijo gostitelja
DIFS	DCF InterFrame Space DCF medokvirski čas
DS	Distribution System distribucijski sistem
DSM	Distribution System Medium medij distribucijskega sistema
DTIM	Delivery Traffic Indication Message obvestilo o dostavi čakajočih okvirjev
EIFS	Extended InterFrame Space razširjen medokvirski čas
ESS	Extended Service Set razširjen nabor storitev
HTTP	HyperText Transfer Protocol protokol za prenos hiperteksta
IEEE	Institute of Electrical and Electronics Engineers Inštitut inženirjev elektrotehnike in elektronike
IFS	InterFrame Space medokvirski čas
IP	Internet Protocol internetni protokol
ISM	Industrial, Scientific and Medical industrijski, znanstveni in medicinski

ISO	International Organization for Standardization mednarodna organizacija za standardizacijo
LAN	Local Area Network lokalno omrežje
OFDM	Orthogonal Frequency-Division Multiplexing ortogonalno frekvenčno multipleksiranje
OSI	Open System Interconnection referenčni model za razvoj in oblikovanje komunikacijskih protokolov in protokolov računalniških omrežij
PCF	Point Coordination Function točkovna koordinatna funkcija
PIFS	PCF InterFrame Space PCF medokvirski čas
QoS	Quality of Service kakovost storitve
RAM	Random Access Memory pomnilnik z naključnim dostopom
RTP	Real-Time Protocol realno-časovni protokol
RTS	Request To Send zahteva za pošiljanje
SIFS	Short InterFrame Space kratek medokvirski čas
SSID	Service Set IDentifier ime brezžičnega omrežja
TCP	Traffic Control Protocol protokol za nadzor transporta
TIM	Traffic Indication Map obvestilo o čakajočih okvirjih
TKIP	Temporal Key Integrity Protocol Protokol za zagotavljanje začasne integritete ključa
UDP	User Datagram Protocol uporabniški datagramski protokol
VoIP	Voice over Internet Protocol govor po internetnem protokolu
WEP	Wired Equivalent Privacy zasebnost kot v žičnem omrežju
WLAN	Wireless Local Area Network brezžično lokalno omrežje
WPA	Wi-Fi Protected Access zaščiteni brezžični dostop

Seznam uporabljenih enot

Bit je osnovna in hkrati najmanjša enota informacije, ki se uporablja v računalništvu in teoriji informacij. Oznaka za bit je b.

Ime	Simbol	Desetiška uporaba	Dvojiška uporaba
kilobit	kb	10^3	2^{10}
megabit	Mb	10^6	2^{20}
gigabit	Gb	10^9	2^{30}

Zavedati se moramo, da se desetiška in dvojiška vrednost med seboj razlikujeta. Tako je $10^3 = 1000$ in $2^{10} = 1024$, pri višjih potencah pa je absolutna razlika še ustrezno večja. Enaka razlika velja tudi pri enoti bajt oziroma pri vseh enotah, kjer uporabljamo tako desetiško kot dvojiško predstavitev.

Bajt (ang. »byte«) je manjša enota za količino podatkov oziroma velikost pomnilnika. 1 bajt je 8 bitov. Oznaka za bajt je B.

Ime	Simbol	Desetiška uporaba	Dvojiška uporaba
kilobajt	kB	10^3	2^{10}
megabajt	MB	10^6	2^{20}
gigabajt	GB	10^9	2^{30}

Hertz je izpeljana enota za frekvenco. En hertz ustreza enemu dogodku na sekundo, izraženo v osnovnih enotah je to s^{-1}. Oznaka za hertz je Hz.

Ime	Simbol	Desetiška uporaba
kilohertz	kHz	10^3
megahertz	MHz	10^6
gigahertz	GHz	10^9

Sekunda je osnovna enota časa. Oznaka za sekundo je s, uporablja pa se tudi sec ali sek.

Ime	Simbol	Desetiška uporaba
milisekunda	ms	10^{-3}
mikrosekunda	μs	10^{-6}
nanosekunda	ns	10^{-9}

Povzetek

Brezžična omrežja postajajo vse večja po številu uporabnikov in količini podatkov, ki se prenašajo preko njih. V želji, da bi uporabnikom zagotovili čim boljše delovne pogoje, vanje dodajamo nove dostopne točke. Te sestavljajo razširjeno brezžično omrežje, njihova skupna lastnost pa je enako ime omrežja. Fizično so postavljene na različnih lokacijah, zaradi izogibanja medsebojnim motnjam pa delujejo na različnih kanalih. Uporabniku želimo zagotoviti kvalitetno delovanje omrežja ne glede na to, kako se znotraj območja omrežja giblje.

Prehajanje je postopek, ki uporabnika na avtomatiziran način povezuje z bližnjimi dostopnimi točkami. Za izbiro nove (boljše) dostopne točke mora odjemalec poznati svojo okolico, kar stori z iskanjem. Ta postopek zahteva prekinitev podatkovnega toka uporabnika, saj odjemalec išče po različnih kanalih. Podatkovni tok je prekinjen tudi med samo menjavo dostopne točke, saj se takrat izvaja postopek asociacije ter avtentifikacije.

V diplomski nalogi sem predstavil delovanje razširjenega brezžičnega omrežja ter s prehajanjem povezane lastnosti dostopnih točk in odjemalcev, predvsem postopka iskanja in prehoda. Predstavljeno je tudi omrežje Eduroam ter strojna in programska oprema, ki sem jo uporabljal za izvajanje meritev, vključno s parametri testiranj. Meritve so bile izvedene v različnih konfiguracijah v testnem omrežju ter delujočem omrežju Eduroam.

Rezultati kažejo, da uporaba prehajanja v najbolj preprosti obliki ni primerna za storitve, ki zahtevajo minimalne prekinitve podatkovnih tokov. Tako storitev VoIP, ki lahko tolerira prekinitve do največ 50ms, ne moremo uporabljati v kombinaciji s prehajanjem. Podane so tudi ideje za določene izboljšave, ki bi postopek iskanja ter prehajanja nekoliko skrajšale.

Ključne besede: brezžična omrežja, prehajanje, prenos podatkov, Eduroam

Abstract

Wireless networks are constantly increasing in size, both in the number of users as well as in the amount of data being transmitted through them. In an effort to provide users with better working conditions we constantly increase the number of access points within a network. These access points form the basis of a wireless network, their common feature being the same network name. Physically they are placed at various locations, and in order to avoid mutual interference, they operate on different channels. The goal is to ensure the highest quality of network operation, regardless of movement of the user within the network's coverage area.

Roaming is the process which connects a user with closer access points in an automated way. In order to choose a new (better) access point, the network client must be familiar with its neighborhood, which is explored by searching. A suspension of the users data stream is required while the network client is searching through different channels. Data flow is also interrupted during the roaming, because the processes of association and authentication are being performed.

In the thesis I presented the operation of an extended wireless network and properties of access points and clients related to switching access points, in particular the processes of searching and roaming. I also presented the Eduroam network as well as the network hardware and software that I used for measurements, including the testing parameters. Measurements in different configurations were made in a test network and the Eduroam network.

The results show that the use of roaming in its simplest form is not appropriate for services requiring minimal interruptions of data flows. Thus, VoIP services that can tolerate interruptions of up to 50ms, cannot be used in combination with roaming. Also provided are some ideas for certain improvements to shorten the search and roaming processes.

Keywords: wireless networks, roaming, data transfer, Eduroam

1. Uvod

Uporaba lokalnih brezžičnih omrežij (WLAN) se je v zadnjih nekaj letih močno razširila. Tehnologija, ki je bila sprva namenjena predvsem zmanjševanju odvisnosti prenosnih računalnikov od žičnega omrežja, je danes prisotna tudi v napravah z visoko stopnjo mobilnosti, kot so prenosni telefoni in dlančniki. Povečale so se tudi hitrosti prenosa podatkov znotraj brezžičnih omrežij, kar je zaradi fizikalnih zakonov privedlo do uporabe večjega števila dostopnih točk v posameznem omrežju.

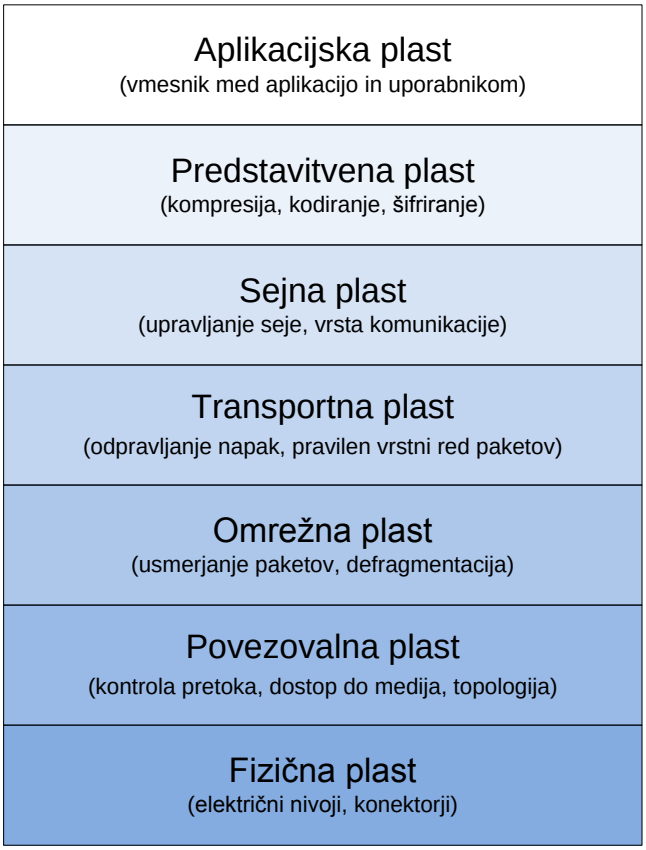
S povečevanjem mobilnosti naprav ter večanjem brezžičnih omrežij nastajajo tudi novi tehnološki problemi, ki jih pri uporabi žičnih povezav ni bilo. Eden izmed njih je zagotavljanje za uporabnika neopazno prehajanje (roaming) med dostopnimi točkami v omrežju, ki je zelo pomemben faktor pri zagotavljanju kvalitetne storitve uporabniku.

Neopazno prehajanje med dostopnimi točkami lahko definiramo različno strogo, odvisno od uporabljene storitve. Tako je nekajsekundni izpad prenosa podatkov pri nalaganju spletne strani še povsem sprejemljiv, saj uporabnik slednje občuti samo kot zmanjšanje hitrosti prenosa (stran se naloži v nekoliko daljšem času). Podobno velja tudi pri poslušanju spletnega radia – uporabnik ne bo opazil prehoda, če le ima predvajalnik dovolj velik vmesni pomnilnik. Nekoliko drugače pa je pri uporabi storitev, ki za svoje delovanje potrebujejo bolj ali manj stalen prenos podatkov z minimalno zakasnitvijo, kot recimo VoIP, video konference ter igranje iger. Pri slednjih nam lahko že zakasnitve občutno krajše od ene sekunde povzročajo motnje ali celo prekinejo zvezo, zato je zaželeno, da je prehod med dostopnima točkama časovno čim krajši.

Z namenom zmanjševanja zakasnitev pri prehodih med dostopnimi točkami so v preteklih letih razvili določene izboljšave. Tako je nastal standard IEEE 802.11r, ki lahko pri uporabi IEEE 802.1X načina avtentifikaje, s pomočjo hranjenja dela ključa v dostopnih točkah nekoliko pospeši prehajanje. Druge izboljšave pa so doletele predvsem algoritma, ki igrata ključno vlogo pri prehajanju – algoritem za iskanje dostopnih točk v okolici ter algoritem za odločitev o izvedbi prehoda. Pri prvem so izboljšali strategijo iskanja, pri drugem pa zmanjšali število nepotrebnih prehodov med dostopnimi točkami. Kolikšni so realni časi prehajanja ter kako vplivajo na storitve, ki potrebujejo minimalne zakasnitve, pa bom poizkušal ugotoviti v svojem diplomskem delu.

2. Brezžično omrežje po standardu IEEE 802.11

Standard IEEE 802.11 je množica standardov, ki definirajo lokalna brezžična omrežja v 2,4 GHz, 3,6 GHz ter 5 GHz frekvenčnem območju radijskih valov [3].



Slika 1: ISO/OSI model.

Po ISO/OSI modelu se brezžična povezava uvršča v fizično plast (Slika 1), kar omogoča popolno združljivost z IEEE 802.3 (ethernet) standardom, najbolj razširjenim standardom za povezovanje v žičnih lokalnih omrežjih. Za brezžične naprave v primerjavi z žičnimi veljajo sledeče razlike na nivoju fizične plasti [2]:

- medij za prenos nima absolutnih in jasno določenih prostorskih mej, znotraj katerih je brezžična komunikacija mogoča;
- medij je deljen z drugimi napravami in posledično nezaščiten pred njihovimi signali;
- brezžični medij je občutno manj zanesljiv od žičnega;
- topologija omrežja se dinamično spreminja med delovanjem;
- pomanjkanje polne povezljivosti – vsaka postaja ne more direktno komunicirati z vsako drugo;
- širjenje signala je asimetrično ter časovno spremenljivo.

Standard zahteva tudi podporo prenosnim in mobilnim postajam. Za prenosno postajo je značilno, da se med uporabo fizično ne premika, lahko pa se premika, kadar je izključena. Za razliko od nje pa mobilne postaje dostopajo do omrežja tudi med gibanjem. Z vidika omrežja ni praktične razlike med prenosnimi in mobilnimi postajami. Zaradi sprememb v okolju, ki

vplivajo na širjenje radijskih valov, se namreč prenosne postaje obnašajo enako kot mobilne [2].

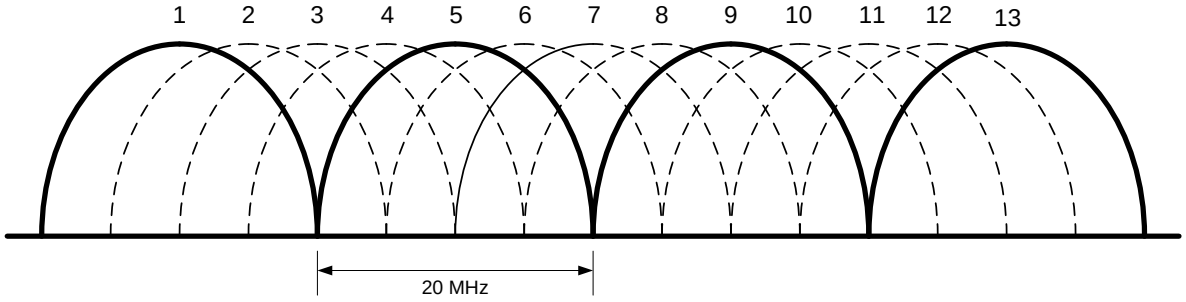
Brezžično omrežje mora za višje plasti v ISO/OSI modelu delovati kot žično omrežje. Od tod posledično izvira tudi zahteva, da je celoten postopek mobilnosti postaj transparentno izveden na fizični plasti [2].

2.1. Standard IEEE 802.11g

Bil je sprejet junija 2003 in je trenutno najbolj razširjen standard za brezžična lokalna omrežja na svetu. Deluje na 2,4 GHz frekvenčnem območju ter uporablja OFDM (ang. »Orthogonal Frequency-Division Multiplexing«) oddajno shemo. Njegova signalna hitrost znaša 54 Mbit/s, tipična povprečna hitrost prenosa pa 22 Mbit/s. Združljivost s predhodnikom, standardom 802.11b, mu je zagotovila hiter in množičen prodor do uporabnikov [3].

2,4 GHz frekvenčno območje sodi med frekvenčna območja, ki so registrirana za uporabo v industrijske, znanstvene in medicinske namene. Njegova uporaba je ob upoštevanju določenih omejitev (maksimalna oddajna moč, odpornost na motnje drugih naprav itd.) dovoljena brez licence, zato ga uporablja veliko število med seboj zelo različnih si naprav. Obsega frekvenčno območje od 2400 MHz do 2500 MHz in je standardizirano skoraj po celem svetu. V strokovni literaturi se označuje tudi kot 2,4 GHz ISM (ang. »Industrial, Scientific and Medical«) frekvenčno območje [6].

Frekvenčno območje je razdeljeno na 13 (v Ameriki na 11) kanalov s pasovno širino 20 MHz, ki pa so med seboj oddaljeni 5 MHz, kar pomeni, da se delno prekrivajo med seboj (Slika 2). Posledično obstajajo samo štirje neprekrivajoči se kanali, kar se v urbanih območjih izkaže za precej veliko omejitev, saj prihaja do motenj med posameznimi omrežji ter posledično slabših zmogljivosti. Poleg lastne interference brezžičnih omrežij med sabo pa motnje izvirajo tudi s strani drugih naprav, ki prav tako delujejo v 2,4 GHz frekvenčnem območju, kot so mikrovalovne pečice ter ZigBee in Bluetooth naprave [3].



Slika 2: Prekrivanje kanalov na 2.4 GHz frekvenčnem področju.

2.2. Topologija brezžičnih omrežij

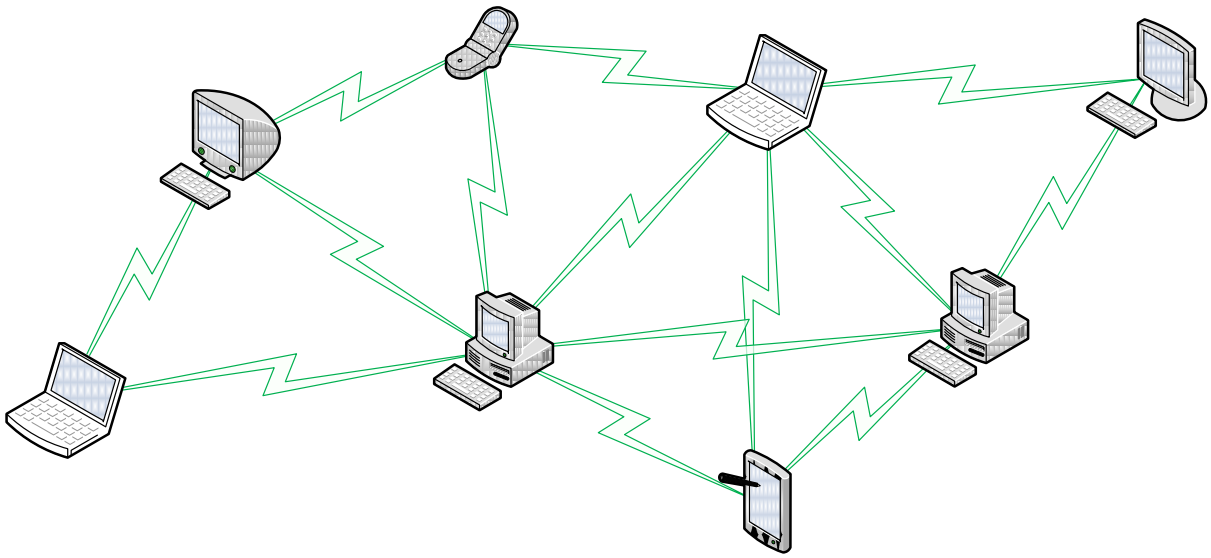
Brezžična omrežja lahko topološko razdelimo v dve skupini:

- decentralizirana (ad-hoc) omrežja (Slika 3) – so najpreprostejša omrežja in za svoje delovanje ne potrebujejo dodatne infrastrukture, kot so brezžične dostopne točke in usmerjevalniki. Vsi odjemalci (postaje) so enakovredni in sodelujejo pri usmerjanju s

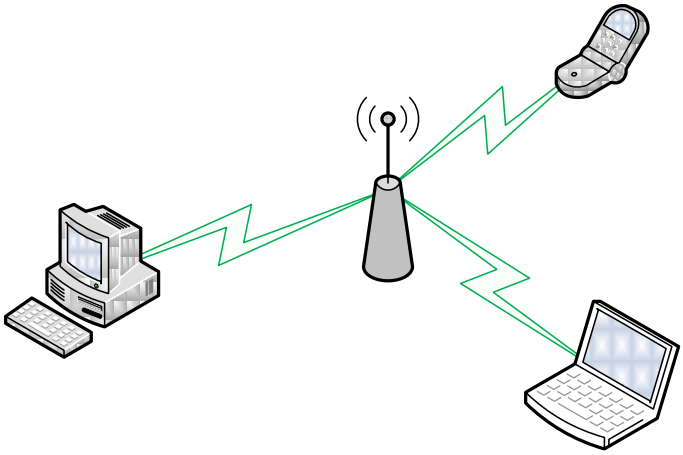
posredovanjem sporočil za druge odjemalce v omrežju. Na izbiro poti sporočil vpliva predvsem povezljivost odjemalcev med sabo;

- centralizirana omrežja (Slika 4) – v teh omrežjih lahko odjemalci komunicirajo samo preko dostopnih točk, ki skrbijo za ustrezno usmerjanje sporočil. V primeru izpada dostopne točke postane omrežje neuporabno.

Diplomska naloga se omejuje zgolj na centralizirana brezžična omrežja.



Slika 3: Decentralizirano (ad-hoc) omrežje.



Slika 4: Centralizirano brezžično omrežje.

2.3. Dostopna točka

Dostopna točka (ang. »access point«) je brezžična postaja, ki v centraliziranem brezžičnem omrežju skrbi za delovanje omrežja. Njene naloge so:

- povezovanje brezžičnih postaj (odjemalcev) med sabo;
- kontrolo dostopa postaj do brezžičnega omrežja ter njegovih virov;
- usmerjanje prometa med brezžičnimi postajami.

Če je dostopna točka namenjena tudi povezovanju z žičnim omrežjem (LAN) pa je njena naloga dodatno še:

- usmerjanje prometa med brezžičnim in žičnim omrežjem.

2.4. Preprosto brezžično omrežje

Preprosto centralizirano brezžično omrežje je prikazano na sliki (Slika 4). Sestavlja ga dostopna točka ter en ali več odjemalcev. Odjemalci se morajo nahajati znotraj dosega radijskih valov dostopne točke, da omrežje deluje. Meja dosega ni enolično določena, ampak variira glede na mikrolokacijo dostopne točke ter posameznega odjemalca. Na širjenje radijskih valov v prostoru namreč vplivajo fizične ovire (stene, vegetacija itd.), motnje s strani drugih naprav ter motnje, ki so posledica širjenja radijskega signala (npr. odboji).

V angleški literaturi [2] se za preprosto brezžično omrežje uporablja kratica BSS oziroma izraz »basic service set.«

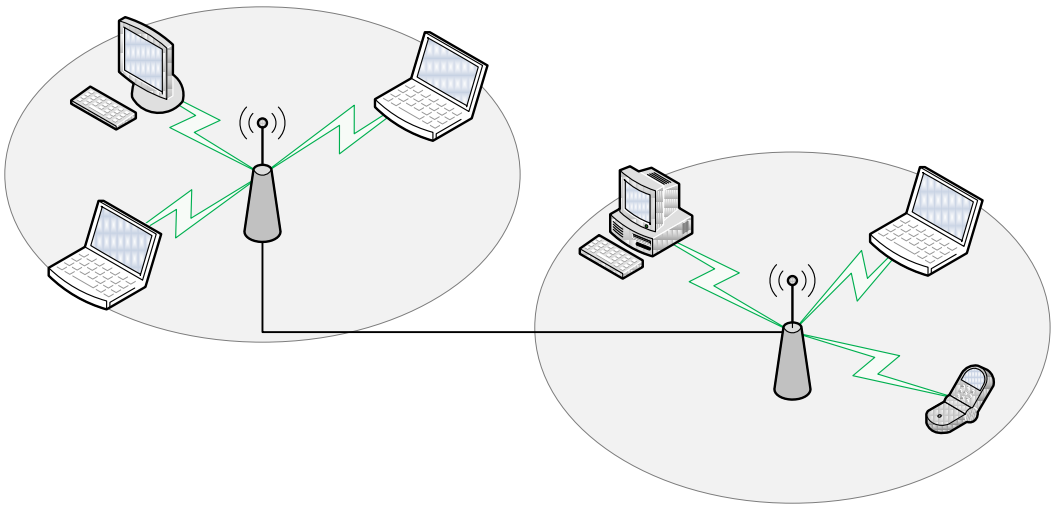
2.5. Razširjeno brezžično omrežje

Ker nam brezžična omrežja z eno dostopno točko hitro ne zadostujejo več, jih moramo razširiti. Obstaja več razlogov za povečevanje brezžičnih omrežij:

- pokrivanje večjega območja s signalom,
- zagotavljanje kvalitetnih storitev za večje število odjemalcev,
- odprava naravnih ovir.

V večini primerov je razlog za širitev kombinacija vseh zgoraj naštetih razlogov.

Nekoliko večje brezžično omrežje je prikazano na sliki (Slika 5). Sestavlja ga več preprostih brezžičnih podomrežij (BSS), ki skupaj tvorijo razširjeno, a vseeno enotno brezžično omrežje (ESS), ki ga povezuje distribucijski sistem (DS). Brezžične postaje se lahko znotraj dosega radijskih valov omrežja neomejeno gibljejo, saj je prehod med dostopnimi točkami izveden transparentno. Primer takega omrežja iz realnega sveta je brezžično omrežje Eduroam, ki je prisotno tudi na Fakulteti za računalništvo in informatiko v Ljubljani.



Slika 5: Primer razširjenega brezžičnega omrežja.

V angleški literaturi [2] se za razširjeno brezžično omrežje uporablja kratica ESS oziroma izraz »extended service set.«

Združevanje preprostih brezžičnih omrežij nam omogoča gradnjo brezžičnih omrežij različnih velikosti ter kompleksnosti. Z vidika odjemalcev ni pomembno, na katero dostopno točko je kateri izmed njih vezan, saj distribucijski sistem zanje deluje popolnoma transparentno.

3. Delovanje brezžičnega omrežja

Razen kjer je drugače navedeno, se vsebina celotnega poglavja nanaša na IEEE 802.11g standard (ERP-OFDM način delovanja) ter brezžične postaje, delujoče po tem standardu. Ta način delovanja ni združljiv z napravami, delujočimi po predhodnem IEEE 802.11b standardu.

Čeprav se dolžine podatkov praviloma izražajo v bitih ali bajtih, je v sledečih poglavjih dolžina izražena v času, ki ga podatek potrebuje za prenos po brezžičnem mediju. Slednje je posledica dejstev:

- da se podatki po mediju lahko prenašajo z različnimi hitrostmi in posledično dolžina v bitih ali bajtih ne omogoča direktne primerjave,
- da časovno označevanje dolžin uporablja tudi standard [2], ki je služil kot vir ter
- da se diplomska naloga ukvarja z merjenjem časovnih zakasnitev.

3.1. Osnovne zakonitosti delovanja

3.1.1. Dostop do medija

Brezžična omrežja za prenos okvirjev uporabljajo skupni medij, katerega si postaje na nekem geografskem območju delijo med seboj – so v isti kolizijski domeni. Znotraj kolizijske domene obstaja pravilo, ki zagotavlja uspešno komunikacijo med postajami: naenkrat lahko oddaja samo ena postaja, vse ostale pa morajo poslušati. Če se kdaj zgodi, da oddajata dve ali več postaj istočasno, pride do kolizije. V tem primeru morajo vse postaje, ki so v času kolizije oddajale, oddajanje kasneje ponoviti (druga za drugo), zato se v prenos vpleteni okvirji dodatno zakasnijo. Tudi čas, ki so ga na mediju porabili okvirji, vpleteni v kolizijo, je z vidika omrežja nesmotrno porabljen, saj se takrat ni prenesla nobena koristna informacija. Ker število kolizij narašča s količino prometa in številom postaj znotraj kolizijske domene, je za optimalno delovanje omrežja ključnega pomena preprečevanje kolizij v čim večji meri. Zaradi dveh lastnosti brezžičnih postaj [1, 2]:

1. postaja ne more oddajati in poslušati istočasno ter
2. vse postaje znotraj kolizijske domene se ne slišijo med sabo.

Odpove algoritem za detekcijo kolizij CSMA/CD, zato je v uporabi algoritem za izogibanje kolizijam CSMA/CA [1, 2].

Algoritem za izogibanje kolizijam CSMA/CA je za uporabo v brezžičnih omrežjih še nekoliko dodatno prilagojen in med drugim [1, 2]:

- daje prednost pri dostopu do medija kontrolnim in upravnim okvirjem ter fragmentom delno že poslanega paketa,
- zmanjšuje čakalni čas za dostop do medija postajam, ki že dlje časa čakajo nanj,
- povečuje čakalni čas za dostop do medija postajam, ki so imele v zadnjih oddajanjih kolizije ter
- omogoča rezervacijo medija za določen čas preko RTS/CTS mehanizma.

Pred pričetkom oddajanja okvirja se mora postaja prepričati, da je medij res prost. To naredi s poslušanjem na mediju ter analizo dogajanja na njem. Postaja lahko prične s postopkom priprave na oddajanje, ko:

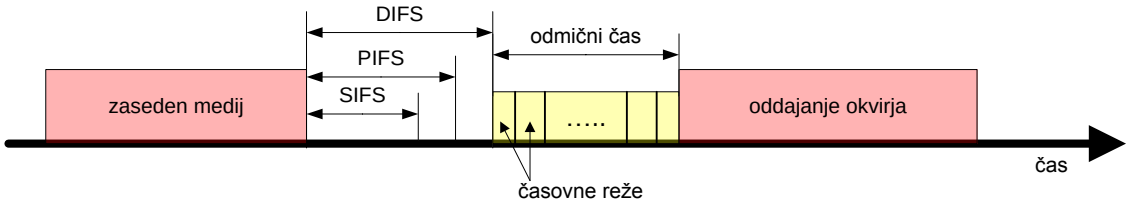
- se je iztekla časovna rezervacija medija oziroma
- zaznava prost medij.

Algoritem za izogibanje kolizijam ni agresiven pri zasedanju medija, zato mora preteči nekaj časa med oddajanjem dveh okvirjev. Ta vmesni čas se imenuje IFS (ang. »inter frame space«) in je različen za različne tipe okvirjev [1, 2]:

- SIFS vmesni čas se uporablja za kontrolna okvirja RTS/CTS mehanizma ter pozitivne potrditvene okvirje;
- PIFS vmesni čas je v uporabi za upravljalne okvirje [7];
- DIFS vmesni čas se uporablja za podatkovne okvirje pod pogojem, da je bil predhodno sprejeti okvir sprejet brez napak;
- AIFS je spremenljiv vmesni čas, ki je v uporabi pri storitvi QoS;
- EIFS vmesni čas se uporablja za podatkovne okvirje v primeru, da je bil predhodno sprejeti okvir napačno sprejet.

Različne dolžine čakalnih časov, prikazane na sliki (Slika 6), definirajo tudi prioritetni seznam pri oddajanju oziroma zasedanju medija. Za okvirje, ki potrebujejo krajši čakalni čas, lahko postaja namreč prej poizkusi zasesti medij [1, 2].

Za podatkovne okvirje, ki v vsakodnevnih komunikacijah predstavljajo večino, se uporablja DIFS vmesni čas. Ker je ta čas konstanten, bi po njegovem izteku prišlo do večjega števila kolizij, saj bi vse postaje pričele z oddajanjem istočasno. Ta neželena situacija je rešena tako, da mora po izteku DIFS vmesnega časa na vsaki postaji preteči še nek naključno izbran odmični čas (ang. »backoff time«), večkratnik časa reže (ang. »slot time«). Ta čas se odšteva, dokler je medij prost. Če v tem času medij zasede druga postaja, se odštevanje začasno ustavi ter nadaljuje po preteku naslednjega DIFS intervala. S tem je zagotovljeno, da ima postaja, ki je v predhodnem poizkusu izpadla, verjetno krajši odmični čas ter s tem večjo možnost, da si zagotovi dostop do medija. Namesto DIFS vmesnega časa je po istem principu lahko v uporabi tudi EIFS vmesni čas – izbira je prepuščena posamezni postaji in je odvisna od (ne)uspešnosti sprejema zadnjega okvirja [1, 2].



Slika 6: Prikaz različnih medokvirskih časov.

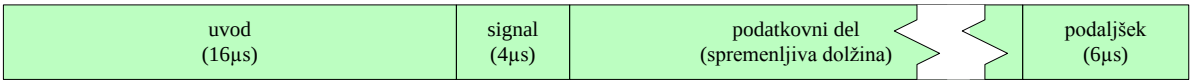
Po standardu [2] so za IEEE 802.11g omrežje v uporabi naslednje vrednosti:

- čas reže (»slot time«): 9 µs
- SIFS čas: 10 µs
- PIFS čas: 19 µs
- DIFS čas: 28 µs

Za večkratnik pri času reže se uporablja celoštevilski faktor med 15 in 1023, kar posledično pomeni čase med 135 µs in 9207 µs oziroma 9,207 ms [2].

3.1.2. Zgradba okvirjev

Na sliki (Slika 7) je predstavljena splošna struktura okvirja na fizičnem nivoju, ki se uporablja v brezžičnih omrežjih.



Slika 7: Prikaz fizične strukture okvirja.

Okvir sestavlja [1, 2]:

- uvod (ang. »preamble«) dolg 16 µs, ki služi sinhroniziranju sprejemnika, nastavitvi ojačevalnika signala itd;
- polje z imenom »signal«, dolgo 4 µs, ki podaja tehnične podatke (dolžina, hitrost, modulacija) o prenosu podatkovnega dela okvirja;
- podatkovni del, dolg od 0 do 4095 bajtov, ki nosi okvir višjega nivoja;
- prazen podaljšek okvirja (ang »signal extension«), dolg 6 µs, ki sprejemnikom zagotavlja dodaten čas za procesiranje prejetega okvirja.

Uvod in polje »signal«, ki tvorita glavo, se prenašata s tako imenovano osnovno hitrostjo (ang. »basic rate«). Ta je občutno nižja od hitrosti prenosa podatkovnega dela okvirja. Slednje omogoča sprejem glave tudi bolj oddaljenim postajam, ki s pomočjo parametrov hitrosti in dolžine za ustrezen čas označijo brezžični medij kot zaseden (četudi samega podatkovnega dela zaradi oddaljenosti ne morejo sprejeti). Vsebina oziroma pomen okvirja (kontrolni, upravljalni ali podatkovni) ter vsi ostali parametri, kot sta npr. izvor in ponor, pa se razberejo iz višjenivojskega (podatkovnega) dela okvirja. Določeni upravljalni okvirji (npr. svetilni okvirji) se morajo prenašati z nižjo hitrostjo, saj je pomembno, da jih sprejmejo vse postaje – tudi tiste s šibkejšim signalom [2].

3.1.3. Prenos okvirjev po omrežju

Ko postaja dobi v uporabo prenosni medij, lahko prične z oddajanjem okvirja. Njegova dolžina (merjena v bajtih) lahko znatno variira, saj okvir nosi poljubno število podatkov višjenivojskega sloja v mejah od 1 do vključno 4095 bajtov. Poleg tega na dolžino vpliva tudi dolžina kontrolnih podatkov (npr. uvod), ki se od standarda do standarda nekoliko razlikuje. Dolžina okvirja pa ni direktno povezana s tem, koliko časa bo okvir potreboval za prenos po omrežju. Brezžična omrežja namreč omogočajo prenos podatkov z različnimi hitrostmi, ki se lahko tudi dinamično prilagajajo glede na kakovost signala, število kolizij (zasedenosti omrežja) itd. Zato za izračunan časa, ki ga potrebujemo za prenos enega okvirja preko brezžičnega omrežja, uporabljamo enačbo [2]:

$$T = T_{PREAMBLE} + T_{SIGNAL} + T_{SYM} + \lceil (16 + 8 * L_{DATA} + 6) / N_{DBPS} \rceil + T_{SE} \quad \textbf{(1)}$$

Pri tem je [2]:

- čas uvoda ($T_{PREAMBLE}$) – 16 µs,
- čas polja SIGNAL v glavi (T_{SIGNAL}) – 4 µs,
- čas simbolnega intervala (T_{SYM}) – 4 µs,
- $L_{PODATKI}$ dolžina podatkovnega bloka znotraj okvirja v bajtih,

- N_{DBPS} število podatkovnih bitov na simbol (konstantno za posamezno hitrost prenosa),
- podaljšek okvirja (T_{SE}) – 6 µs.

Tako lahko izračunamo, da za prenos 1000 B dolgega višjenivojskega bloka pri hitrosti 24 Mbit/s potrebujemo 16 µs + 4 µs + 4 µs + ⌈83,5625⌉ µs + 6 µs = 114 µs.

K tej vrednosti je potrebno prišteti še čas, ki ga signal potrebuje za širjenje po prostoru, pri čemer standard predpostavlja čas 1 µs za vsakih 300 m poti. Torej 300 m oddaljena postaja sprejme zgornji okvir po 115 µs od začetka oddajanja. Če predpostavimo, da mora sprejemna postaja poslati še pozitiven odgovor sprejema, se čas zasedenosti omrežja še nekoliko podaljša:

- pred oddajo potrditvenega okvirja je potrebno počakati SIFS časovni interval (10 µs),
- prenos potrditvenega okvirja zahteva 16 µs + 4 µs + 4 µs + ⌈1,396⌉ µs + 6 µs = 32 µs,
- zakasnitev zaradi širjenja signala v prostoru pa ponovno znaša 1 µs.

Tako skupen čas od začetka oddaje okvirja do prejema potrditve njegovega sprejema znaša 114 µs + 1 µs + 10 µs + 32 µs + 1 µs = 158 µs. Preden se lahko na mediju pojavi naslednji okvir (s katerekoli brezžične postaje v omrežju), pa mora preteči vsaj še en SIFS interval (lahko tudi daljša PIFS ali DIFS, odvisno od tipa naslednjega okvirja), kar pomeni, da prenos 1000 B dolgega višjenivojskega bloka skupaj s potrditvijo prejema zasede prenosni medij za 168 µs.

3.1.4. Tipi okvirjev

V standardu so definirane tri glavne vrste okvirjev, ki se prenašajo znotraj brezžičnega omrežja [2]:

1. upravljalni (ang. »management«) okvirji se uporabljajo pri izvajanju povezovanja v omrežje (asociiranje, avtentifikacija itd.);
2. kontrolni (ang. »control«) okvirji skrbijo za kontrolo prenosa po omrežju (potrjevanje, RTS, CTS itd.);
3. v podatkovnih (ang. »data«) okvirjih pa se prenašajo uporabniški podatki.

3.1.5. Distribucija sporočil

Glavni namen brezžičnega omrežja je podpora računalniškim komunikacijam, posledično je njegova primarna naloga distribucija sporočil med odjemalci, za kar skrbi distribucijski sistem. DS za distribucijo sporočil med različnimi dostopnimi točkami uporablja medij distribucijskega sistema (DSM oziroma ang. »distribution system medium«). V večini omrežij je DSM kar ethernet oziroma LAN, ni pa nujno. V določenih scenarijih se namreč uporabljajo tudi druge alternative, npr. ATM [2].

Standard IEEE 802.11 ne predpisuje poteka distribucije sporočil znotraj DS. Zagotoviti pa mora dovolj informacij, s pomočjo katerih lahko DS nedvoumno določi izvor in ponor sporočila. Storitve brezžičnega omrežja, ki DS zalagajo s potrebnimi informacijami, so [2]:

- asociacija (association),
- reasociacija (reassociation) in
- deasciacija (disassociation).

3.1.6. Integracija

Je storitev, ki skrbi za komunikacijo med brezžičnim in LAN omrežjem. Zadolžena je za izvedbo vseh akcij, ki jih potrebujemo za prenos sporočila iz DSM v LAN in obratno, vključno z morebitnimi spremembami naslovov, protokola in prenosnega medija [2].

3.1.7. Kvaliteta storitve

V angleščini »quality of service« (kratica QoS) označuje storitev, ki skrbi za upoštevanje prioritet posameznih tipov prometa glede na določene parametre. Njena naloga je izbira naslednjega paketa za pošiljanje iz čakalne vrste [2].

3.2. Dostopna točka

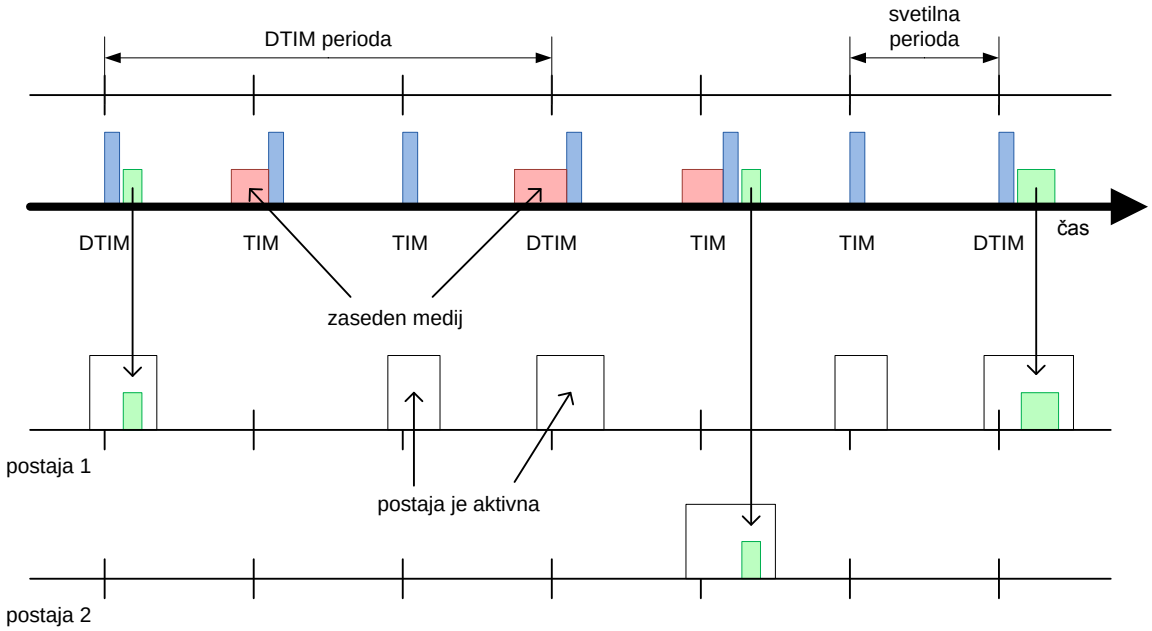
3.2.1. Svetilni okvirji

Spadajo v kategorijo upravljalnih okvirjev. V centraliziranih brezžičnih omrežjih jih periodično, tipično vsakih 100 ms, razpošiljajo dostopne točke. Njihova naloga je okoliške postaje obveščati o prisotnosti brezžičnega omrežja ter njegovih parametrih, asociirane postaje pa tudi o čakajočih podatkih, sinhronizaciji ure itd. Vsebujejo vse informacije, ki jih odjemalec potrebuje za vzpostavitev asociacije z določeno dostopno točko. Zaradi velike količine informacij, ki jih nosijo svetilni okvirji, so tu predstavljene samo tiste, ki vplivajo na proces prehajanja med dostopnimi točkami [1, 2]:

- **ime omrežja** (SSID) – poleg tega, da podaja uporabniku prijazno ime brezžičnega omrežja, je pomemben tudi pri prehajanju. Alternativne dostopne točke morajo namreč imeti enak SSID kot trenutno uporabljena dostopna točka;
- **svetilna perioda** (ang. »beacon interval«) – določa, kako pogosto dostopna točka pošilja svetilne okvirje. Standard je ne predpisuje, v praksi pa se večinoma uporablja perioda 100 ms. Perioda igra pomembno vlogo pri pasivnem iskanju dostopnih točk, pri katerem odjemalci čakajo in poslušajo za svetilnimi okvirji. Odjemalci morajo namreč poslušati dovolj časa, da ujamejo svetilne okvirje, kar pri tipični periodi svetilnih okvirjev 100 ms pomeni vsaj 120 ms dolg interval poslušanja (zaradi morebitnega časovnega zamika pri oddajanju svetilnih okvirjev itd.);
- **TIM in DTIM** – podatka odjemalcu sporočata, ali ga na strani dostopne točke čakajo okvirji, ki so se nabrali v času njegovega spanja. Perioda TIM je individualno dogovorjena s posameznim odjemalcem, perioda DTIM pa je skupna za vse in določena s strani dostopne točke. Odjemalec mora sprejeti vsaj svetilne okvirje, ki nosijo njegov del TIM informacije ter svetilne okvirje z DTIM informacijo (če njihovega prejemanja ni izklopil), saj v nasprotnem primeru lahko pride do izgube okvirjev. Dostopna točka namreč lahko zbrane okvirje, če jih odjemalec v določenem času ne prevzame, zavrže. Slednje od odjemalca zahteva, da se vrne iz energijsko varčnega spanja v sprejemni način delovanja. Posledično to pomeni, da odjemalec v času oddajanja svetilnega okvirja s TIM (ali pogojno DTIM) informacijo ne more iskati dostopnih točk na drugih kanalih;
- **perioda DTIM** (Delivery Traffic Indication Message) – določa, kateri izmed svetilnih okvirjev nosi informacije o morebitnih čakajočih okvirjih za vse odjemalce (ang. »broadcast«) dostopne točke;

- **obremenjenost BSS** (ang. »BSS Load«) – sporoča zasedenost brezžičnega medija ter obremenjenost dostopne točke (število asociiranih odjemalcev), kar lahko odjemalci uporabijo kot vhodna parametra pri izbiri nove dostopne točke.

Svetilni okvirji se sicer pošiljajo periodično, vendar samo v primeru, da je brezžični medij prost. V nasprotnem primeru mora postaja pred njegovim pošiljanjem počakati na sprostitev medija, kar vnese določen zamik pri pošiljanju. Slednji se, če je možno (medij prost ob pravem času), kompenzira pri naslednjem svetilnem okviru, tako da se vzdržuje prvotno periodo. Morebitni zamiki igrajo pomembno vlogo pri pasivnem iskanju omrežij, saj lahko prekratek interval poslušanja odjemalca povzroči, da le-ta ne sliši svetilnih okvirjev določene dostopne točke [1, 2].



Slika 8: Periodično pošiljanje svetilnih okvirjev.

Na sliki (Slika 8) je prikazano pošiljanje svetilnih okvirjev s TIM in DTIM informacijami. DTIM se pošilja vsake tri svetilne okvirje. Postaja 1 deluje v zmernem energijsko varčevalnem načinu in sprejema vse DTIM okvirje ter večino TIM okvirjev. Postaja 2 pa se nahaja v ekstremnem energijsko varčevalnem načinu, saj ne sprejema vseh DTIM okvirjev ter tudi zelo poredko TIM okvirje.

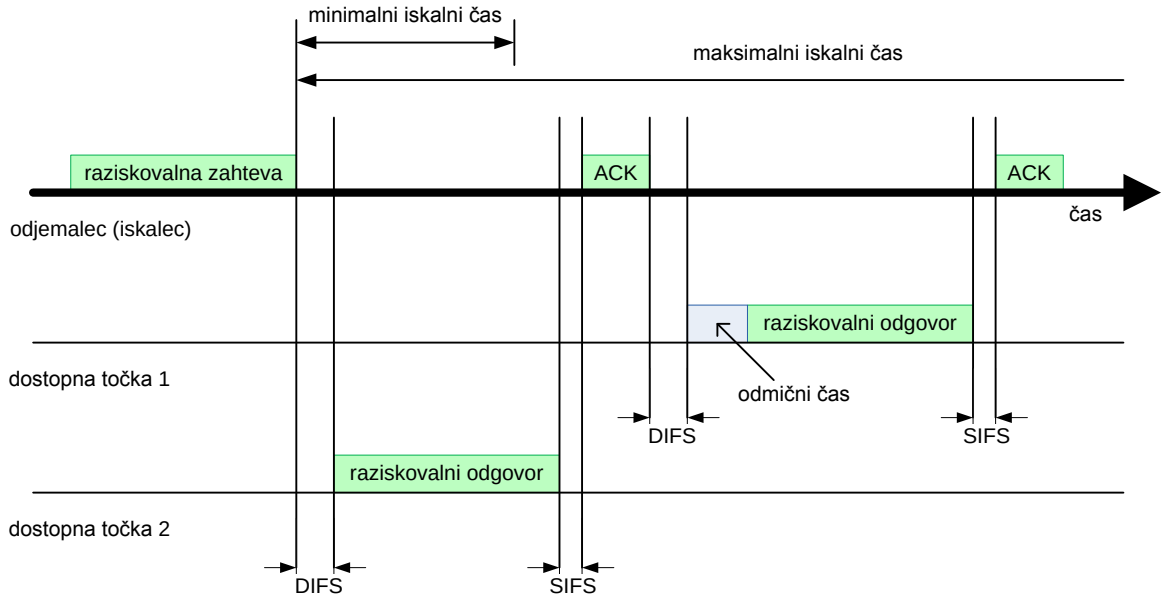
3.2.2. Odziv na aktivno iskanje

Dostopna točka se mora na aktivno iskanje z raziskovalnimi zahtevami (ang. »probe request«) odzvati z raziskovalnim odgovorom (ang. »probe response«) pod pogojem, da [2]:

- iskalec išče vsa omrežja ali pa je SSID v raziskovalni zahtevi enak SSID-ju dostopne točke in
- iskalec išče vse dostopne točke ali pa je BSSID v raziskovalni zahtevi enak BSSID-ju dostopne točke in
- je raziskovalna zahteva naslovljena na vse postaje ali direktno na to dostopno točko.

Raziskovalni odgovor je poslan brez prioritete (DIFS čakalni čas itd.), naslovljen direktno na postajo, ki izvaja iskanje. Postaja mora prejem raziskovalnega odgovora potrditi. V odgovoru

se, prav tako kot v svetilnih okvirjih, nahajajo vse informacije, ki jih odjemalec potrebuje za vzpostavitev asociacije z dostopno točko [2].



Slika 9: Prikaz iskanja z raziskovalnimi zahtevami in odgovori.

3.2.3. Upravljanje z energijo

Ena izmed bistvenih razlik med dostopnimi točkami in odjemalci se pokaže pri upravljanju z energijo. Dostopne točke so praviloma postavljene statično, kar jim omogoča boljšo ter lažjo preskrbo z električno energijo kot odjemalcem, ki se lahko poljubno premikajo. Zaradi tega se od dostopnih točk zahteva, da ves čas delujejo v aktivnem načinu (oddajanje oziroma sprejemanje), odjemalci pa lahko poleg aktivnega načina izberejo tudi energijsko bolj varčno spanje. Najpreprostejši in najučinkovitejši način varčevanja je ugašanje določenih naprav ali njenih delov v času, ko jih ne potrebujemo. To spoznanje je bilo eno izmed vodilnih pri nastanku brezžičnih omrežij, ki so zasnovana tako, da imajo lahko mobilne postaje večino prostega časa sprejemno-oddajni del izklopljen. Poraba energije je namreč največja pri oddajanju, občutno manjša je pri sprejemanju ter obdelavi prejetih okvirjev, najmanjša pa pri ugasnjenem brezžičnem vmesniku.

V aktivnem načinu delovanja odjemalec deluje kot polnopravni član omrežja – sprejema ter, v skladu s pravili za dostop do medija, tudi pošilja. V spanju pa ne spremlja dogajanja na mediju, kar pomeni, da ne more sprejeti okvirjev, ki so mu namenjeni. Zato v tem času dostopna točka zanj shranjuje okvirje ter mu jih posreduje, ko se vrne v aktivni način delovanja. Prisotnost shranjenih okvirjev za posameznega odjemalca dostopna točka sporoča preko svetilnih okvirjev oziroma TIM ter DTIM podatkovnih polj v svetilnem okvirju.

Preklop med spanjem ter aktivnim načinom delovanja lahko sproži odjemalec kadarkoli, dostopna točka pa mora seznanjenje s to menjavo odjemalcu potrditi. S potrditvijo se prepreči težave, ki bi lahko nastale zaradi neusklajenosti odjemalca in dostopne točke [1, 2]:

- odjemalec spi, dostopna točka pa ga označuje kot aktivnega – dostopna točka mu pošilja okvirje, ki pa jih odjemalec ne sprejme. V tem primeru bi prišlo do zmanjšanja prepustnosti omrežja, saj je določen del časa na mediju porabljen nesmotrno. Stanje

dodatno poslabša še ponovno pošiljanje okvirjev, saj dostopna točka predvideva, da jih odjemalec ni prejel pravilno ter zaradi tega ne potrdi njihovega sprejema. V končni fazi pa to privede do izgube okvirja, saj dostopna točka po določenem številu ponovitev pošiljanj obupa ter okvir zavrže;

- odjemalec je aktiven, dostopna točka pa ga označuje kot spečega – dostopna točka shranjuje okvirje za odjemalca, čeprav to ne bi bilo potrebno. S tem se vnaša dodatna zakasnitev v dostavo okvirjev.

Zakasnitve pri dostavi okvirjev, ki nastanejo v času spanja odjemalca, so relativno velike in znašajo povprečno vsaj nekaj 10ms.

Predpostavimo, da odjemalec sprejema vse svetilne okvirje ter začne z izpraševanjem dostopne točke takoj, ko ugotovi, da je to potrebno. Tako se pri tipični periodi svetilnih okvirjev (100 ms) določen okvir v najslabšem primeru lahko zakasni tudi več kot 100 ms:

1. dostopna točka sprejme okvir (preko žičnega omrežja) za odjemalca v času oddajanja svetilnega okvirja, v katerem mu sporoča, da nima podatkov zanj;
2. odjemalec po prejemu tega svetilnega okvirja nadaljuje s spanjem do naslednjega svetilnega okvirja, torej najmanj 100 ms, v primeru zamika svetilnega okvirja pa tudi ustrezno dlje;
3. po sprejemu novega svetilnega okvirja, ki mu sporoča, da ga na dostopni točki čakajo podatki, začne s postopkom izpraševanja dostopne točke – prične tekmovati za dostop do brezžičnega medija. V najslabšem primeru ga pri zasedanju prehiti drug odjemalec, kar pri 1000 B velikem drugonivojskem okvirju pomeni dodatnih 168 µs zakasnitve. Pri večji količini podatkov (ali pri zasegu medija s strani tretjega odjemalca) se ta čas ustrezno poveča, lahko tudi čez 1 ms;
4. ko odjemalec dobi dostop do medija ter začne izpraševati dostopno točko tudi ta postopek traja nekaj časa. Odvisen je predvsem od količine podatkov na strani dostopne točke ter hitrosti prenosa, tipično pa se giblje od nekaj 10 µs navzgor (lahko tudi preseže 1 ms).

Iz zgoraj opisanega primera lahko vidimo, da v najslabšem primeru samo v brezžičnem omrežju pridelamo več kot 100 ms dodatne zakasnitve. V primeru, da odjemalec spremlja samo vsak drugi svetilni okvir (in ne vseh), pa dodatne zakasnitve lahko presežejo tudi 200 ms. Pri vsakem tretjem svetilnem okvirju presegajo 300 ms in podobno naprej. Statistično gledano so povprečne zakasnitve sicer približno pol manjše od teh iz najslabšega primera, a vendar ne smemo pozabiti, da nam to nič ne koristi. 100 ms dolgo prekinitev v telefonskem pogovoru namreč že zaznamo (slišimo), pri daljših prekinitvah pa je ta motnja še toliko bolj opazna in moteča.

3.2.4. Zasedenost medija ter dostopne točke

Dostopna točka lahko, če je funkcionalnost podprta in vklopljena, odjemalcem sporoča podatke o zasedenosti medija ter obremenjenosti dostopne točke (parameter »BSS Load« v svetilnih okvirjih). Zasedenost medija je predstavljena kot vrednost, normalizirana z 255, in predstavlja procentualno zasedenost kanala, kot ga vidi dostopna točka. Časovni interval, v katerem se meri zasedenost medija, je celoštevilčni večkratnik dolžine svetilnih period. Privzeta vrednost je 50 svetilnih period, uporabnik pa jo lahko nastavi na poljubno vrednost od 1 do 100. Obremenjenost dostopne točke pa se izraža kot število na njej asociiranih odjemalcev [2].

S pomočjo teh podatkov lahko odjemalec lažje izbere novo, zanj optimalno dostopno točko. Podatki so pomembni predvsem za postaje, katerim je bolj pomembna zmogljivost omrežja

kot pa varčevanje z energijo. Tako lahko izberejo sicer bolj oddaljeno, a manj obremenjeno dostopno točko, ki ji teoretično zagotavlja večje hitrosti prenosa.

Časovni interval, na katerem se v praksi meri zasedenost kanala, pa znaša po privzetih nastavitvah dostopnih točk 5 sekund. Slednje preprosto izračunamo iz podatkov o svetilni periodi (privzeto 100 ms oziroma 0,1 s) ter večkratniku svetilnih period za merjenje (privzeto 50) [2].

3.3. Odjemalec

3.3.1. Problemi pri iskanju dostopnih točk

Vsaka brezžična postaja ima vgrajen sprejemnik in oddajnik, ki lahko zaradi fizikalnih omejitev deluje samo na enem kanalu. Posledica te fizikalne omejitve sta dve neprijetni lastnosti, ki vplivata na hitrost ter učinkovitost iskanja dostopnih točk.

Prva vpliva predvsem na čas, ki ga porabimo za iskanje brezžičnih dostopnih točk. Iskanje namreč lahko poteka samo strogo zaporedno en kanal naenkrat, kar poglavitno vpliva na količino časa, ki ga potrebujemo za izvedbo iskanja. Slednje bi potekalo veliko hitreje, če bi odjemalec lahko iskal dostopne točke vzporedno na večih kanalih hkrati.

Druga, veliko bolj neprijetna lastnost, pa je dejstvo, da mora odjemalec v času iskanja brezžičnih dostopnih točk po različnih kanalih, zapustiti kanal, na katerem poteka komunikacija s trenutno asociirano dostopno točko. Slednje v času iskanja na drugem kanalu popolnoma onemogoči vsakršno komunikacijo z asociirano dostopno točko, kar pomeni tudi prekinitev podatkovnega toka od ali k odjemalcu. Ta prekinitev pa ima lahko negativne posledice za storitve, ki potrebujejo zanesljivo povezavo s čim manj prekinitvami (npr. storitve VoIP, ki lahko tolerirajo prekinitev do 50 ms [4]), saj lahko pride do motenj ali celo prekinitve delovanja storitve.

Ker je druga omejitev (prekinitev podatkovnega toka) veliko bolj kritična od prve (daljši čas iskanja brezžičnih dostopnih točk), je večina proizvajalcev pri izdelavi algoritma za iskanje brezžičnih dostopnih točk izbrala rešitev, ki te prekinitve kar se da minimizira. Najpreprostejši algoritem namreč preišče vse kanale naenkrat (zaporedno enega za drugim), kar posledično pomeni sicer redke, a dolge prekinitve, v času katerih je komunikacija odjemalca v brezžičnem omrežju onemogočena. Veliko bolj učinkovit pa je algoritem, ki sproži iskanja bolj pogosto, vendar v vsakem izmed iskanj preišče zgolj enega izmed kanalov. S tem se sicer čas iskanja dostopnih točk občutno podaljša, saj lahko traja tudi nekaj sekund, preden odjemalec uspe preiskati vse kanale, vendar pa so posamezne prekinitve podatkovnega toka tudi do desetkrat krajše kot v prvem primeru.

Prekinitev podatkovnega toka brez izgube podatkov odjemalcu omogočajo funkcije upravljanja z energijo. Odjemalec namreč dostopni točki sporoči, da odhaja v spanje, ta pa med tem zanj shranjuje podatkovne okvirje v svoj vmesni pomnilnik. Seveda pa odjemalec v tem času ne spi, temveč išče dostopne točke na drugih kanalih. Po končanem iskanju (vrnitvi iz spanja) pa prevzame v tem času zbrane okvirje in nadaljuje s komunikacijo.

3.3.2. Postopka iskanja dostopnih točk

Vsak odjemalec mora pred prvim priklopom v omrežje ali pred menjavo dostopne točke poznati svojo okolico. Leto spozna v procesu iskanja dostopnih točk, kjer z aktivnim ali pasivnim iskanjem dostopnih točk pridobi ustrezne informacije o okoliških brezžičnih omrežjih [2].

Pri pasivnem iskanju brezžičnih omrežij odjemalec določen čas posluša na posameznem kanalu ter išče svetilne okvirje (ang. »beacon frame«), ki jih oddajajo dostopne točke. Ta način iskanja je primeren predvsem za naprave, ki se napajajo z baterij, saj je energijsko varčen – napravi med iskanjem ni potrebno oddajati. Žal pa na račun varčevanja z energijo odjemalec za iskanje porabi več časa – večina dostopnih točk namreč oddaja svetilne okvirje vsakih 100 ms, kar pomeni, da mora odjemalec na posameznem kanalu poslušati več kot 100 ms v enem kosu, da zazna večino svetilnih okvirjev z okolice. Aktivno iskanje pa poteka tako, da odjemalec pošilja raziskovalne zahteve (ang. »probe request«) na posamezen kanal ter čaka raziskovalne odgovore (ang. »probe response«) brezžičnih dostopnih točk nanje. Ker standard zahteva, da so dostopne točke ves čas aktivne, ni bojazni, da bi bila posamezna raziskovalna zahteva preslišana. Lahko je kvečjemu izgubljena v koliziji, zato postaje praviloma pošljejo več raziskovalnih zahtev na posameznem kanalu. Tako pri pasivnem kot tudi aktivnem iskanju lahko odjemalec uporabi filter po SSID, kar pri aktivnem iskanju manj obremenjuje omrežje, saj na raziskovalne zahteve odgovarjajo samo dostopne točke z ustreznim SSID. Pri pasivnem iskanju odjemalec omrežja dodatno ne obremenjuje, je pa pri uporabi filtra porabljenih manj virov na odjemalcu, saj mora obdelati samo svetilne okvirje z ustreznim SSID [2].

Za oba načina iskanja velja skupna lastnost, da mora odjemalec preiskati vse kanale enega za drugim. Porabljen čas na posameznem kanalu se med metodama razlikuje, skupen pa jima je čas menjave kanala. Po specifikacijah čas za eno menjavo kanala znaša 224 μs, kar pomeni, da je pri vsakem iskanju porabljenih 448 μs časa samo za skok na iskalni kanal ter vrnitev na trenutno delujoč kanal. Postopek iskanja definira še tri različne časovne periode, za katere pa ne predpisuje privzetih vrednosti, tako da se med posameznimi izdelki razlikujejo. Časovne periode so [2]:

- ProbeDelay – čakalni čas pred oddajo iskalne zahteve;
- MinChannelTime – minimalni čas iskanja na določenem kanalu, enak ali večji od ProbeDelay;
- MaxChannelTime – maksimalni čas iskanja na določenem kanalu, enak ali večji od MinChannelTime.

Pri aktivnem iskanju so v uporabi vse tri časovne periode, pri pasivnem pa samo najdaljši MaxChannelTime [2].

Postopek pasivnega iskanja je s strani odjemalca zelo preprost [2]:

1. sporoči dostopni točki, da odhaja v spanje;
2. premakne se na kanal, na katerem želi iskati dostopne točke;
3. na kanalu posluša MaxChannelTime časa, nato vrne rezultat iskanja;
4. vrne se na kanal trenutno asociirane dostopne točke.

Časi korakov 1, 2 in 4 se merijo v mikrosekundah in sešteti skupaj le izjemoma presežejo čas 1ms. Povsem drugače pa je s porabljenim časom pri 3. koraku – odjemalec mora na vsakem kanalu poslušati dovolj dolgo, da sprejme vse oziroma večino svetilnih okvirjev. Izbira časa poslušanja je prepuščena razvijalcem strojne in programske opreme, za optimalno delovanje pa morajo upoštevati [3]:

- interval naj bo kar se da kratek (čim krajša prekinitev delovanja);
- večina svetilnih okvirjev ima periodo 100 ms, vendar jo lahko skrbniki brezžičnih omrežij tudi podaljšajo;
- perioda svetilnih okvirjev se lahko zaradi zasedenosti kanala nekoliko podaljša.

Konkretne periode v različnih gonilnikih na Linux platformi so sledeče:

- MadWifi gonilnik za Atheros brezžične vmesnike uporablja periodo 150 ms;
- gonilnik za Intelove brezžične vmesnike uporablja periodo 120 ms kadar ni asociiran z dostopno točko. V nasprotnem primeru je perioda linearno odvisna od svetilnega intervala asociirane dostopne točke, najdaljša perioda pa lahko znaša 88ms.

Aktivno iskanje, katerega princip je predstavljen na sliki (Slika 9), pa z vidika odjemalca poteka tako [2]:

1. sporoči dostopni točki, da odhaja v spanje,
2. premakne se na kanal, na katerem želi iskati dostopne točke,
3. počaka periodo ProbeDelay ter pošlje raziskovalno zahtevo,
4. če v času MinChannelTime ne zazna brezžičnega medija kot zasedenega, predpostavi, da je kanal prazen (na njem ni dostopnih točk) ter konča postopek iskanja,
5. v nasprotnem primeru posluša na kanalu MaxChannelTime ter vrne rezultat iskanja,
6. vrne se na kanal trenutno asociirane dostopne točke.

Podobno kot v primeru pasivnega iskanja sta tudi tu največja porabnika časa koraka 4 in 5, vendar pa sta v primerjavi z njim občutno krajša. MaxChannelTime se lahko med aktivnim in pasivnim načinom iskanja namreč razlikuje. Tako se aktivni način iskanja v primeru praznega kanala lahko zaključi v času od 4 ms do 7 ms, pri nepraznem kanalu pa v 50 ms [8].

3.3.3. Avtentifikacija

Je postopek, s katerim se odjemalec nedvoumno identificira dostopni točki pred asociacijo ter vstopom v omrežje. Edini način avtentifikacije, ki ga zahteva standard, je odprti način avtentifikacije – dostopna točka avtentificira vsakega odjemalca, ki se želi povezati nanjo. Poleg odprtega načina je možna tudi uporaba WEP šifriranja, ki pa se zaradi šibkosti in ranljivosti praktično ne uporablja več - nadomestila sta ga standarda WPA in IEEE 802.1X. Zaradi sprememb v načinu avtentifikacije brezžičnih odjemalcev, ki so nastale evolucijsko, se avtentifikacija pred asociacijo sedaj smatra zgolj kot predhodno rokovanje odjemalca z dostopno točko, večinoma pa je v uporabi odprt sistem avtentifikacije. Za zaščito podatkov ter njihove integritete pa so v uporabi drugi sistemi, ki se vzpostavijo po asociaciji, vezani pa so na uporabnika (oseba) in ne na odjemalca (postajo). Slednje omogoča ohranjanje pravic uporabnikov ne glede na to, kje se fizično nahajajo v omrežju. Odjemalec je lahko istočasno avtentificiran na večih brezžičnih dostopnih točkah, kar mu omogoča uporaba predavtentifikacije. Slednje pomeni, da se odjemalec avtentificira na novi dostopni točki že v času, ko aktivno deluje še na stari [1, 2].

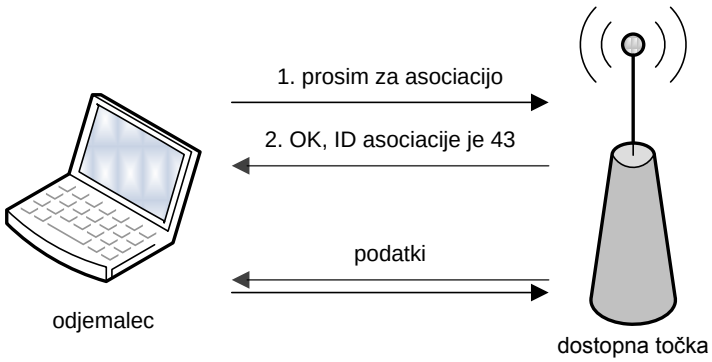
3.3.4. Asociacija

Za dostavljanje sporočil znotraj DS mora distribucijski servis vedeti preko katere dostopne točke lahko dostopa do določenega brezžičnega odjemalca. Ta preslikava med dostopno točko in odjemalcem se ustvari v procesu asociacije. Asociacija je nujna za zagotavljanje mobilnosti znotraj ESS, ni pa zadostna. Zadostuje namreč samo prenosnim postajam, ne pa tudi mobilnim. Odjemalec ne more pošiljati podatkovnih sporočil v omrežje, dokler ni asociiran z dostopno točko. Proces asociacije vedno sproži odjemalec, naenkrat pa je lahko asociiran samo z eno dostopno točko. Slednje zagotavlja nedvoumen odgovor DS na vprašanje: »Katera dostopna točka servisira odjemalca X?« V obratni smeri pa velja, da je posamezna dostopna točka lahko asociirana tudi z večimi odjemalci [1, 2].

Za proces asociacije velja, da ni vedno uspešen, saj lahko dostopna točka asociacijo zavrne. Razlogi za zavrnitev so različni, med drugim tudi:

- dosežena zgornja meja števila odjemalcev,
- kršenje politike dostopa.

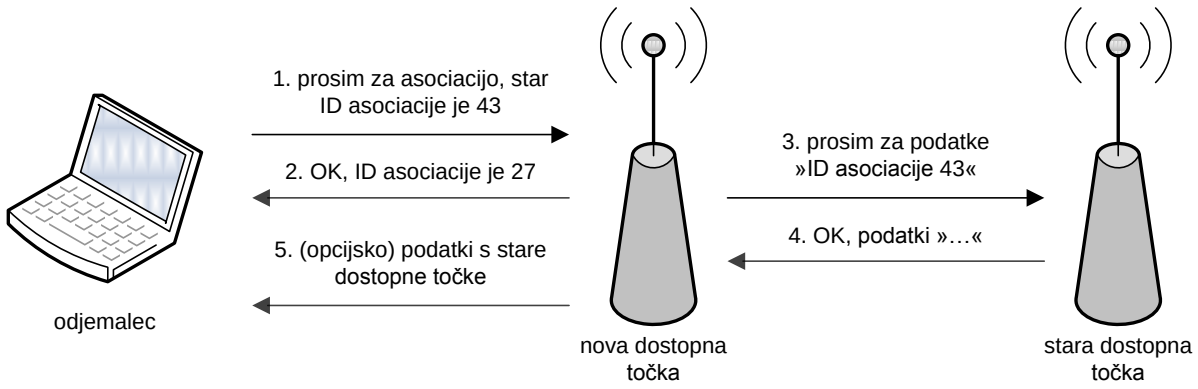
Primer vzpostavitve asociacije z dostopno točko je prikazan na sliki (Slika 10).



Slika 10: Primer asociacije odjemalca z dostopno točko.

3.3.5. Reasociacija

Ker storitev asociacije zadostuje samo prenosnim postajam ne pa tudi mobilnim, je za mobilnost v omrežju potrebna dodatna funkcionalnost. Leto zagotavlja storitev reasociacije, ki odjemalcem omogoča prenos asociacije z ene dostopne točke na drugo, kar prikazuje slika (Slika 11) Slednje zagotavlja DS aktualno preslikavo med odjemalcem in dostopno točko, kadar odjemalec menja dostopne točke znotraj ESS. Storitev omogoča tudi spremembo parametrov že obstoječe asociacije med dostopno točko in odjemalcem. Pri menjavi dostopnih točk prav tako poskrbi, da odjemalec preko nove dostopne točke dobi dostavljena vsa sporočila, ki so se v času poteka reasociacije nabrala v vmesnem pomnilniku stare dostopne točke. Analogno z asociacijo lahko tudi reasociacijo sproži samo odjemalec [1, 2].



Slika 11: Primer prenosa asociacije (reasociacija) na novo dostopno točko.

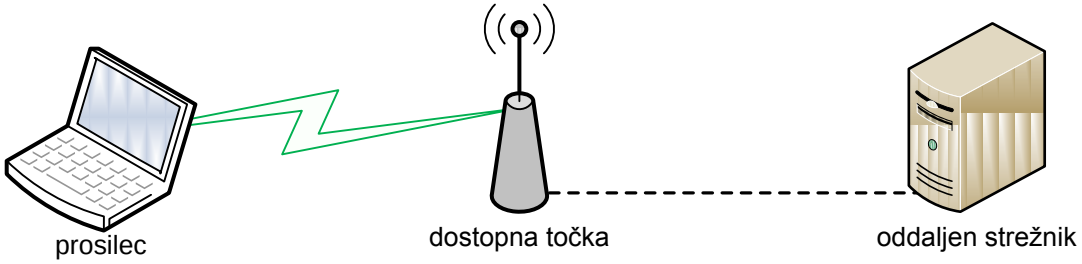
3.3.6. Deasociacija

Je storitev, ki odstrani preslikavo med dostopno točko in odjemalcem. Čeprav v tesni povezavi z asociacijo in reasociacijo, se deasociacija nekoliko razlikuje od njiju [2]:

1. storitev ne izda zahteve temveč obvestilo – ni ga možno zavrniti,
2. obvestilo lahko pošlje tudi dostopna točka in ne samo odjemalec,
3. razpošiljanje obvestila je zaželeno, ni pa nujno. Protokol je namreč zasnovan tako, da ni odvisen od storitve deasociacije. Slednje omogoča pravilno delovanje omrežja tudi v primeru, da odjemalec nenapovedano zapusti omrežje (premik izven dosega omrežja, prazna baterija itd.).

3.3.7. Posebnosti pri IEEE 802.1X načinu avtentifikacije

Zgoraj opisani postopek prehoda na drugo dostopno točko je povsem točen samo za brezžična omrežja z odprtim načinom avtentifikacije ali za omrežja z avtentifikacijo s skupnim geslom. Slednje je povsem zadostno za domačo ali pisarniško uporabo, pri večjih brezžičnih omrežjih, v katerih je lahko tudi nekaj 100 različnih uporabnikov z različnimi pravicami dostopv, pa se zaradi praktičnosti uporablja 802.1X način avtentifikacije. Primer takega omrežja je brezžično omrežje Eduroam. V tem načinu je začetna faza prehoda na drugo dostopno točko povsem enaka zgoraj opisani, vendar pa ima odjemalec (v tem primeru imenovan prosilec oziroma ang. »supplicant«) na koncu dostop samo do upravljalnega omrežja, ne pa tudi do podatkovnega. Za dostop do podatkovnega omrežja mora namreč izvesti še avtentifikacijo po IEEE 802.1X standardu, ki mu ob uspešni izvedbi zagotovi dostop. Posledično je zaradi dodatne avtentifikacije čas prehoda občutno daljši, saj postopek zahteva komunikacijo z avtentifikacijskim strežnikom, ki se lahko nahaja tudi na drugem koncu sveta, kar prikazuje slika (Slika 12) [1].



Slika 12: Primer avtentifikacije odjemalca (prosilec) po standardu IEEE 802.1X.

3.3.8. Standard IEEE 802.11r

Bil je objavljen 15. julija 2008, v njem pa so definirali zmožnost hranjena dela odjemalčevega ključa v brezžičnem omrežju (dostopnih točkah), kar zmanjša število zahtev, ki so usmerjene proti avtentifikacijskemu strežniku. S tem so uspeli nekoliko pospešiti prehajanje med dostopnimi točkami pri uporabi IEEE 802.1X avtentifikacije, saj lahko vsi prehodi znotraj določenega časovnega okvira koristijo shranjen del ključa. Ključ se na dostopni točki shrani ob prvem vstopu v omrežje oziroma prvem prehodu med dostopnimi točkami po poteku časovne omejitve hranjenja ključa. V primerih, ko ključ še ni shranjen na dostopni točki, se mora izvesti daljša različica avtentifikacije [4].

3.4. Prehajanje

Prehajanje (ang. »roaming«) je proces, v katerem odjemalec prenese asociacijo z ene dostopne točke na drugo znotraj brezžičnega omrežja. Pogoj za zmožnost prehajanja je omrežje z vsaj dvema dostopnima točkama (razširjeno brezžično omrežje). Prenos asociacije vedno sproži odjemalec [2].

Vsi odjemalci v omrežju imajo isti cilj – optimalno delovanje povezave z njihovega vidika. Pojem optimalnega delovanja pa se med posameznimi odjemalci lahko močno razlikuje.

1. Mobilna naprava z omejeno kapaciteto baterije bo izbrala dostopno točko, s katero bo lahko komunicirala s čim manj porabljene energije (nižja oddajna moč mobilne naprave, daljši časi spanja).
2. Odjemalec na skrajnem robu omrežja lahko praviloma izbere samo eno dostopno točko, s katero še lahko komunicira, saj so ostale že izven njegovega dosega.
3. Postaja, ki ne potrebuje intenzivnega varčevanja z energijo, lahko v nasprotju z mobilno (1. primer) izbere tudi nekoliko bolj oddaljeno, a manj obremenjeno dostopno točko. S tem uporabniku zagotovi bolj stabilno delovanje omrežja ter večje hitrosti prenosa podatkov.

3.4.1. Prehod na drugo dostopno točko

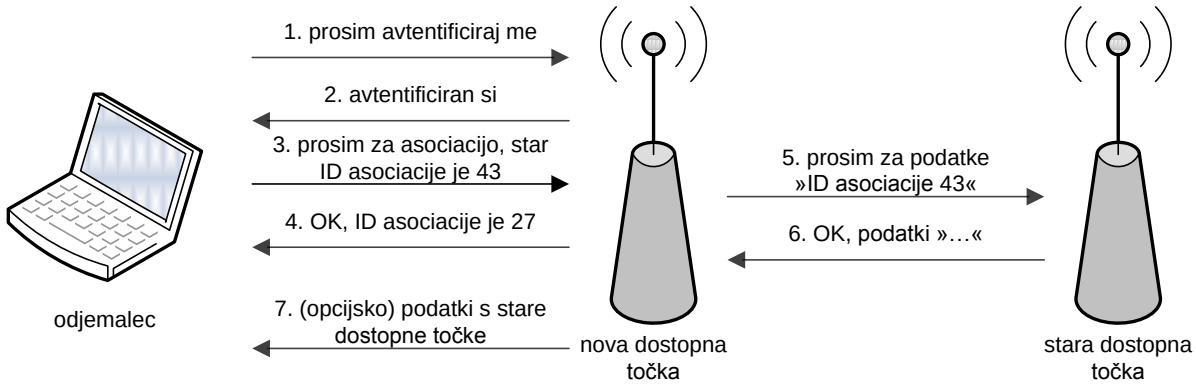
Predpogoj za izvedbo prehoda na drugo dostopno točko je poznavanje dostopnih točk v okolici. Slednje odjemalec spozna v postopku iskanja dostopnih točk, opisanem v predhodnem poglavju. Po uspešno izvedenem iskanju dostopnih točk ter odločitvi odjemalca, da bo izvedel prehod na novo dostopno točko, sledi preprost postopek, ki je shematsko prikazan tudi na sliki (Slika 13) [1, 2]:

1. odjemalec se avtentificira na novi dostopni točki. To lahko stori tudi predhodno, še v času uporabe stare dostopne točke, tako da to ne vpliva neposredno na zakasnitev, ki se zgodi ob prehodu;
2. novi dostopni točki pošlje zahtevo za reasociacijo, katere del je tudi podatek o njegovi trenutni (stari) dostopni točki;
3. nova dostopna točka na stari preveri, ali je uporabnik tam res avtentificiran:
    a. če je odgovor negativen, se poizkus reasocijacije zaključi z obvestilom o deavtentifikaciji s strani dostopne točke,
    b. v nasprotnem primeru dostopna točka nadaljuje z obdelavo zahteve za reasociacijo na podoben način kot v primeru asociacije – preveri se politika dostopa odjemalca do dostopne točke itd.;
4. ob odobritvi reasociacije odjemalcu pošlje pozitivno potrditev asociacije, staro dostopno točko pa obvesti o prehodu odjemalca. Stara dostopna točka nato kot

odgovor novi posreduje vse podatkovne okvirje za odjemalca, ki so se med tem nabrali v njenem vmesnem pomnilniku;

5. nova dostopna točka posreduje podatkovne okvirje odjemalcu na način, ki je opisan v podpoglavju »Upravljanje z energijo.«

Po uspešno končanem postopku lahko odjemalec nadaljuje z delom v brezžičnem omrežju preko nove dostopne točke.



Slika 13: Primer prehoda na novo dostopno točko.

4. Testno okolje

4.1. Strojna oprema

Pri izvajanju meritev v testnem omrežju bo v uporabi sledeča strojna oprema:

- dostopni točki La Fonera FON2100 [9]:
  - 100 Mbit/s ethernet vmesnik
  - 32 bit MIPS CPE serije R4000 delujoč na 183,5 MHz
  - 16 MB spomina z naključnim dostopom (RAM)
  - IEEE 802.11b/g kompatibilen vmesnik Atheros AR2315
- dostopne točke v omrežju Eduroam
  - Cisco AIR-AP1131AG-E-K9
  - Cisco AIR-AP1252AG-E-K9
  - Cisco AIR-AP1220
- vohljača ter obremenjevalec Asus EEE PC model 701
  - 100 Mbit/s ethernet vmesnik
  - Intel Celeron 900 MHz (delujoč na 630 MHz)
  - 512 MB spomina z naključnim dostopom (RAM)
  - IEEE 802.11b/g kompatibilen vmesnik Atheros AR5BXB63
- odjemalec IBM ThinkPad R500
  - 1000 Mbit/s ethernet vmesnik (delujoč na 100 Mbit/s)
  - CPE Intel Core 2 Duo P8400 2,6 GHz
  - 2 GB spomina z naključnim dostopom (RAM)
  - Brezžična mrežna kartica Intel WiFi Link 5100
- generator prometa – osebni računalnik
  - 1000 Mbit/s ethernet vmesnik (delujoč na 100 Mbit/s)
  - CPE Intel Core 2 Duo E8400 3 GHz
  - 4 GB spomina z naključnim dostopom (RAM)
- spletni strežnik – prenosni računalnik
  - 100 Mbit/s ethernet vmesnik
  - CPE Intel Celeron 466 MHz
  - 160 MB spomina z naključnim dostopom (RAM)
- stikalo Level One FSW-2218 z osem 100 Mbit/s ethernet porti

4.1.1. Nastavitev dostopnih točk

Dostopne točke v testnem omrežju so nastavljene:

- SSID: test-ssid
- Svetilna perioda: 100ms
- Perioda DTIM: 1
- Kratek uvod (short preamble): vklopljen
- Kratka časovna reža (short slot): vklopljena
- Podprte hitrosti: 1, 2, 5'5, 11, 6, 9, 12, 18, 24, 36, 48, 54 Mbit/s
- Avtentifikacija: odprti tip

Pri testnih scenarijih z uporabo šifriranja pa dodatno še:

- Avtentifikacija: šifriranje s skupnim ključem
- Šifrirni algoritem: AES

Dostopne točke brezžičnega omrežja Eduroam so nastavljene:

- SSID: eduroam
- Svetilna perioda: 100ms
- Perioda DTIM: 2
- Kratek uvod (short preamble): izklopljen
- Kratka časovna reža (short slot): vklopljena
- Podprte hitrosti: 1, 2, 5'5, 6, 9, 11, 12, 18, 24, 36, 48, 54 Mbit/s
- Šifrirni algoritem: TKIP (WPA)
- Avtentifikacija: po standardu IEEE 802.1X

4.1.2. Nastavitev odjemalca

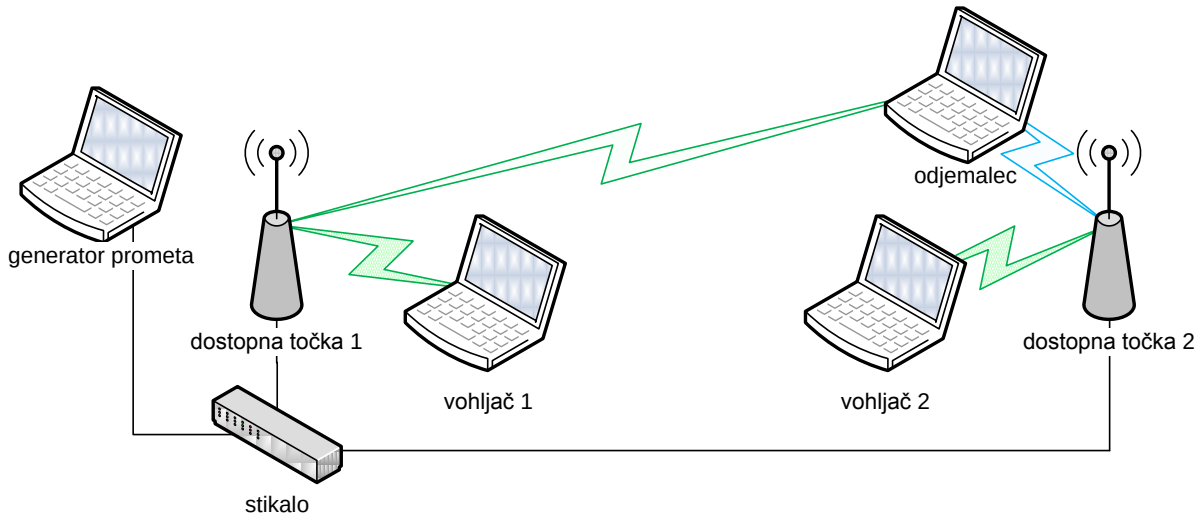
Odjemalec je, z izjemo IP naslovov, nastavljen na popolnoma avtomatsko delovanje s privzetimi nastavitvami, razen kjer v posameznem testnem scenariju ni zahtevana določena izrecna nastavitev. Zaradi avtomatskih nastavitev odjemalec samodejno prilagaja hitrost ter svoje nastavitve dostopnima točkama. Za izvajanje meritev sta bila uporabljena Linux distribucija BackTrack 4 z individualno nadgrajenim gonilnikom (glej poglavje »Nadgrajen gonilnik Intel«) ter programskim paketom Linux WPA Supplicant, ki kontrolira postopek prehajanja.

4.1.3. Nastavitev vohljačev

Vohljača delujeta na Windows XP SP3 operacijskem sistemu ter uporabljata programu CommView for WiFi priložen gonilnik za brezžični vmesnik. Vse nastavitve razen kanala, ki je ročno nastavljen na fiksno vrednost, so privzete.

4.1.4. Testno omrežje

Postavitev testnega omrežja prikazuje slika (Slika 14):

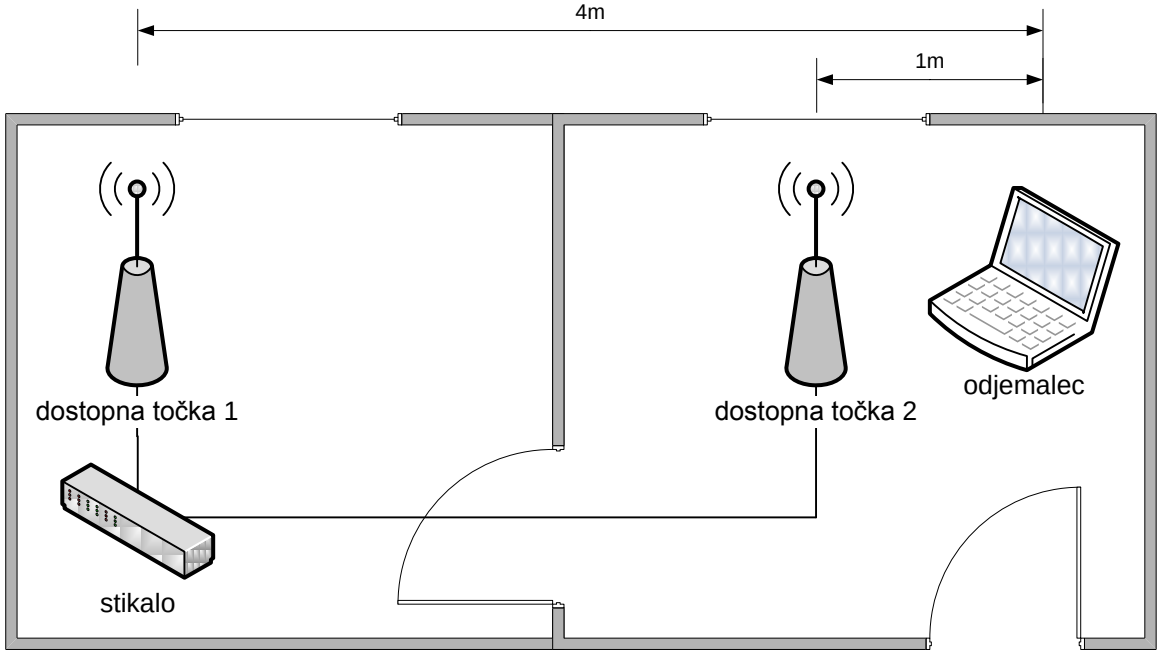


Slika 14: Topologija testnega omrežja.

Na sliki predstavljeni dostopni točki se nahajata v ločenih prostorih, saj je tako zagotovljen zadosten upad jakosti signala. S tem je odjemalec prisiljen, da poišče drugo dostopno točko (z boljšim signalom, modra oznaka) ter nanjo prenese asociacijo.

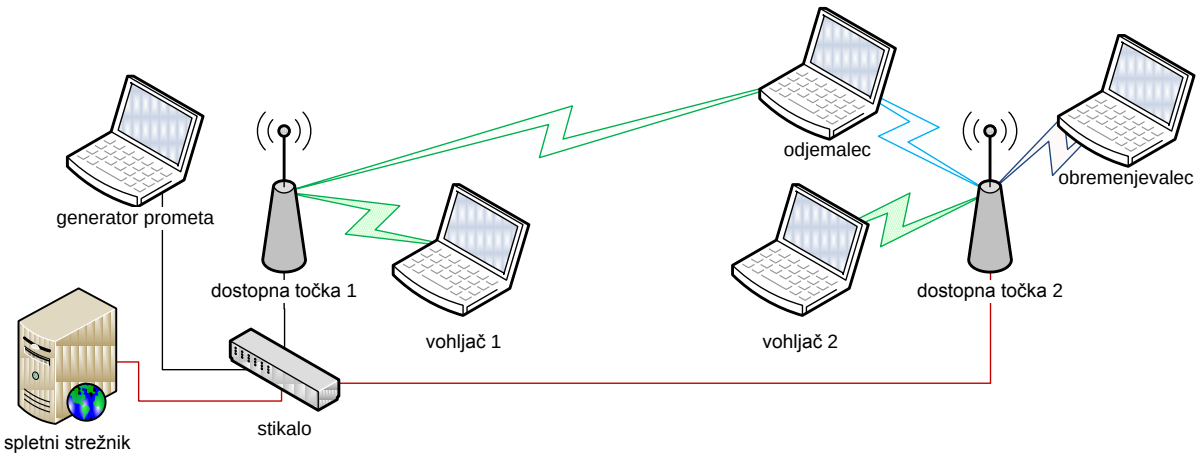
Dostopni točki ter generator prometa so med seboj povezani preko 100 Mbit stikala v LAN (ethernet) omrežju. Vse naprave se nahajajo znotraj istega podomrežja, vse IP številke so nastavljene ročno na statično vrednost. V neposredni bližini vsake izmed dostopnih točk se nahaja po en brezžični vohljač (ang. sniffer), ki je statično nastavljen na kanal bližnje dostopne točke. Tako zaznava ves promet dostopne točke ter odjemalca na tem kanalu. Dostopna točka 1 deluje na kanalu 1 (2,412 GHz), dostopna točka 2 pa na kanalu 11 (2,462 GHz).

Odjemalec je prenosni računalnik, delujoč po principu mobilne postaje, ki se v času testiranja ne premika. Nahaja se približno 4 metre (zračna razdalja) od dostopne točke 1 ter približno 1 meter od dostopne točke 2. S tem je zagotovljeno, da je v času testiranja signal dostopne točke 2 boljši, kar prisili odjemalca k izvedbi prehoda. Poenostavljeno skico fizične postavitve testnega omrežja prikazuje slika (Slika 15).



Slika 15: Skica fizične postavitve testnega omrežja.

Obremenjevalec (brezžični odjemalec, namenjen obremenitvi brezžičnega omrežja) je nastavljen na privzete nastavitve delovanja, IP naslov pa je nastavljen ročno. Na njem teče Linux distribucija BackTrack 3, promet pa je generiran s pomočjo programa wget na obremenjevalcu ter spletnega strežnika Apache 2.2 na drugem koncu. Spletni strežnik je v omrežje povezan preko 100 Mbit ethernet povezave, obremenjevalec pa preko svojega brezžičnega vmesnika delujočega po IEEE 802.11g standardu. Shemo testnega omrežja z dodanim obremenjevalcem predstavlja slika (Slika 16).



Slika 16: Shema testnega omrežja z dodanim obremenjevalcem ter spletnim strežnikom. Obremenjene povezave so označene z rdečo barvo.

V testnem omrežju se pojavljajo trije tipi prometa:

- obremenilni promet, ki ga povzročata spletni strežnik in obremenjevalec,
- promet generatorja prometa proti odjemalcu,
- ter promet podpornih protokolov (npr. ARP), ki skrbijo za delovanje omrežja.

Pred začetkom izvajanja meritev je odjemalcu bližja izmed dostopnih točk ugasnjena. S tem je preprečeno, da bi odjemalec že med prvim povezovanjem v brezžično omrežje zaznal obe dostopni točki, kar bi lahko pokvarilo rezultate meritev. Ko odjemalec vzpostavi asociacijo z oddaljeno dostopno točko, pa vklopim še bližjo ter izvedem posamezno meritev.

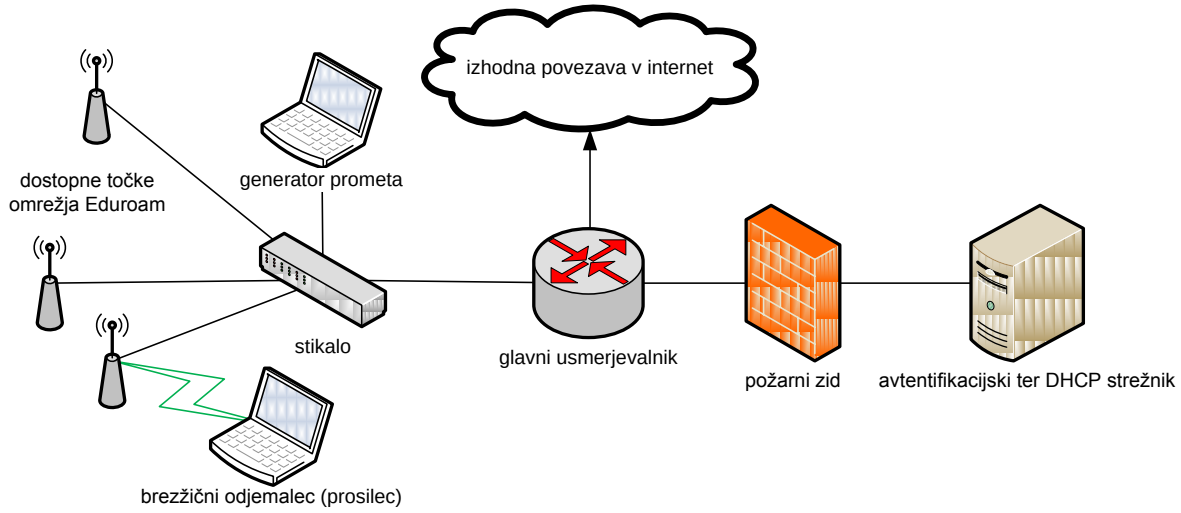
Vsa testiranja v testnem omrežju so izvedena v hiši, kjer živim. Okolje je zaradi nerazširjenosti brezžičnih omrežij v okolici popolnoma čisto (pri iskanju ne zaznam nobene druge dostopne točke). Brezžična dostopna točka, ki jo imam v uporabi doma, pa je bila med izvedbo testiranj fizično ugasnjena.

4.1.5. Omrežje Eduroam

Poenostavljen prikaz brezžičnega omrežja Eduroam na Fakulteti za računalništvo in informatiko v Ljubljani prikazuje slika (Slika 17). Omrežje je združljivo z napravami delujočimi še po starem IEEE 802.11b standardu, standard IEEE 802.11r (pohitreno prehajanje) pa ni v uporabi.

Dostopne točke so z generatorjem prometa povezane preko 100 Mbit ethernet povezave. Generator prometa ter brezžični odjemalec se nahajata znotraj istega podomrežja. IP naslov generatorja je nastavljen ročno na statično vrednost, IP naslov odjemalca pa je dodeljen dinamično s strani DHCP strežnika. V neposredni bližini vsake izmed dostopnih točk se nahaja po en brezžični vohljač (ang. sniffer), ki je statično nastavljen na kanal bližnje dostopne točke. Tako zaznava ves promet dostopne točke ter odjemalca na tem kanalu.

Odjemalec je prenosni računalnik, delujoč po principu mobilne postaje, ki ga med testiranjem premikamo po prostoru, saj dostopnih točk ne moremo poljubno prižigati in ugašati. S tem premikom odjemalcu poslabšamo signal trenutne dostopne točke ter izboljšamo signal dostopne točke, na katero želimo, da odjemalec izvede prehod.



Slika 17: Poenostavljena shema omrežja Eduroam na Fakulteti za računalništvo in informatiko v Ljubljani.

Testiranja na omrežju Eduroam so bila izvedena na Fakulteti za računalništvo in informatiko, Tržaška 25, v Ljubljani. Za avtentifikacijo v omrežju sem uporabljal svoje uporabniško ime, ki mi ga je izdala fakulteta. Posledično se je celoten postopek avtentifikacije vršil na lokalnem strežniku – komunikacija s strežniki zunaj fakultetnega omrežja ni bila potrebna.

Zaradi želje po nezasičenem okolju je bil izbran popoldanski čas (16.00) ter del zgradbe, kjer se nahajajo laboratoriji (2. nadstropje v bližini prehoda med starim in novim delom fakultete), saj se v tem času drugi brezžični odjemalci tam praviloma ne zadržujejo več. Za testiranje pri obremenjenem omrežju je bila izbrana avla fakultete v najbolj obremenjenem delu dneva – odmor ob 12.00.

4.2. Programska oprema

4.2.1. Generator prometa pktgen

Pktgen je v jedro Linux operacijskega sistema vgrajen generator prometa. Zaradi delovanja v jedru ima najbolj neposreden dostop do mrežnega vmesnika, kar mu omogoča generiranje prometa z največjo možno časovno natančnostjo. Generira IP/UDP promet, kateremu lahko poljubno nastavljamo različne parametre: obseg izvornih in ponornih IP naslovov, obseg izvornih in ponornih vrat (UDP protokol), število in velikost paketov itd. Če generatorju namesto ene številke podamo obseg števil le ta naključno izbira med njimi, vendar pri testiranju obsegi (ter posledično naključen izbor števil) niso bili uporabljeni. To pomeni, da je generirani promet ves čas enak.

Pri meritvah zakasnitev v omrežju je zelo pomemben časovno natančen generator prometa, zato je bila njegova natančnost pred izvedbo meritev preverjena. Pri tej meritvi je bil generator prometa (izvor) preko kabla direktno povezan z odjemalcem (ponorom) brez nepotrebnih vmesnih naprav, kot je npr. stikalo. Generiran promet je imel sledeče parametre:

- velikost paketa: 60 B (minimalna velikost, ki jo lahko generiramo),
- zakasnitev med paketi: 2 ms (500 paketov na sekundo),
- število paketov: 100000,

- sistem je bil obremenjen z istimi programi, kot bo obremenjen v času izvajanja testov v brezžičnem omrežju.

Z vohljanjem na strani odjemalca so bili ugotovljeni naslednji statistični parametri generatorja prometa:

- povprečna zakasnitev: 2,007 ms,
- standardna deviacija: 0,04 ms.

Glede na ugotovljeno natančnost generatorja prometa ocenjujemo, da nam le-ta omogoča merjenje zakasnitev ter izpadov podatkovnega toka do ±2 ms natančno.

Generator prometa zaradi tehničnih omejitev ne more delovati istočasno z wpa_supplicant-om na istem mrežnem vmesniku, zato bo brezžični odjemalec obremenjen samo enosmerno, in sicer kot ponor podatkovnega toka.

Spletna stran projekta: http://www.kernel.org/

4.2.2. Nadgrajen MadWifi gonilnik

Izvedba meritev na odjemalcu je bila zaradi dostopnosti izvorne kode predvidena na Linux platformi z uporabo gonilnika MadWifi za Atheros brezžične kartice, različica 0.9.4 (revizija 4100). Zaradi potrebe po merjenju časov posameznih dogodkov, česar gonilnik sam po sebi ne podpira, je bila izvorna koda na določenih mestih nadgrajena – dodana je bila koda za izpis trenutnega sistemskega časa.

Pred izvedbo meritev je bilo delovanje gonilnika preverjeno v podobnih konfiguracijah, v kakršnih se je kasneje izvajalo meritve. Žal pa se je izkazalo, da je gonilnik preveč nezanesljiv ter nezrel za resno uporabo, saj je imel določene dokaj resne probleme pri delovanju:

1. aktivno iskanje dostopnih točk ni delovalo v primeru, ko je bil tudi odjemalec izvor prometa. Pri pravilnem delovanju bi moral namreč odjemalec zamenjati kanal, poslati raziskovalne zahteve ter v tišini čakati na raziskovalne odgovore. Žal pa zaradi nedelujočega gonilnika odjemalec ni bil tiho, ampak je izhodni promet oddajal tudi na iskani kanal in to celoten čas iskanja. Posledično dostopna točka ni dobila dostopa do medija in ni mogla pravočasno oddati raziskovalnih odgovorov, ki bi jih odjemalec sprejel. Raziskovalni odgovori so bili namreč poslani šele takrat, ko je odjemalec zaključil iskanje na tem kanalu ter posledično nanj tudi nehal oddajati izhodni promet. Zaradi te napake odjemalec z izhodnim prometom nikoli ni našel alternativne dostopne točke;
2. gonilnik je v podatkovni tok v času asociacije in reasociacije vnašal več kot 110 ms dolgo prekinitev. S pomočjo vohljačev je bilo ugotovljeno, da sama (re)asociacija (izmenjava upravljalnih okvirjev) poteka približno 6 ms. Zaradi velike razlike med časoma, kjer 6 ms predstavlja izrazito manjši del, je merjenje časov prehoda s takim gonilnikom žal nemogoče.

Spletna stran projekta: http://www.madwifi-project.org/

4.2.3. Nadgrajen gonilnik vmesnika Intel WiFi Link 5100

Ker zgoraj omenjeni gonilnik za brezžične vmesnike Atheros ni bil primeren za opravljanje meritev, je bil namesto njega izbran brezžični vmesnik Intel WiFi Link 5100. Tudi tu je bila zaradi dostopnosti izvorne kode izbrana platforma Linux, kar je omogočilo nadgradnjo gonilnika z izpisovanjem trenutnega časa ob želenih dogodkih. Poleg dodatnih izpisov časa je

bil v izvorni kodi ostranjen tudi del za iskanje dostopnih točk v 5 GHz področju (802.11a). Gonilnik namreč ne omogoča selektivnega izklopa preko kontrolnega vmesnika.

Že med popravljanjem izvorne kode se je gonilnik izkazal za bistveno bolj dovršenega, o njegovi kvaliteti pa govori tudi dejstvo, da je (od različice 2.6.24 naprej) vgrajen v Linux jedro. Na testnem sistemu je bila v uporabi različica jedra 2.6.30.9.

Spletna stran projekta: http://www.kernel.org/

4.2.4. Programski paket Linux WPA Supplicant

Sestavlja ga več med seboj dopolnjujočih se programov, ki skrbijo za avtentifikacijo odjemalca in/ali uporabnika (vloga prosilca pri IEEE 802.1X protokolu) v brezžičnih omrežjih. Najpomembnejši izmed programov je servis wpa_supplicant, ki praviloma teče v ozadju in skrit pred uporabnikom skrbi za nemoteno delovanje odjemalca v omrežju. Podpira praktično vse tipe avtentifikacije, modularna zgradba pa omogoča sprotno razširjanje programske opreme v skladu z razvojem tehnologij. O njegovi zrelosti govori podatek, da se neprekinjeno razvija že od leta 2003 naprej.

Programom iz paketa je preko univerzalnega programskega vmesnika Linux Wireless Extension omogočeno delovanje z veliko večino brezžičnih vmesnikov, podprtih na Linux platformi. Uporaba univerzalnega vmesnika omogoča večjo efektivnost pri razvoju, saj ena rešitev deluje na vseh brezžičnih vmesnikih, ki podpirajo univerzalni vmesnik.

Tekom let se je iz prvotne vloge prosilca pri IEEE 802.1X načinu avtentifikacije paket razvil v dokaj napreden vmesnik za upravljanje z brezžičnimi omrežji. V teku je tudi vgradnja sistema za nadzor prehajanja med dostopnimi točkami v brezžičnem omrežju, kar sem izkoristil pri opravljanju meritev. Sistem prehajanja je trenutno še zelo preprost, kontroliramo pa ga preko dveh vhodnih parametrov: interval prehajanja ter prag jakosti signala.

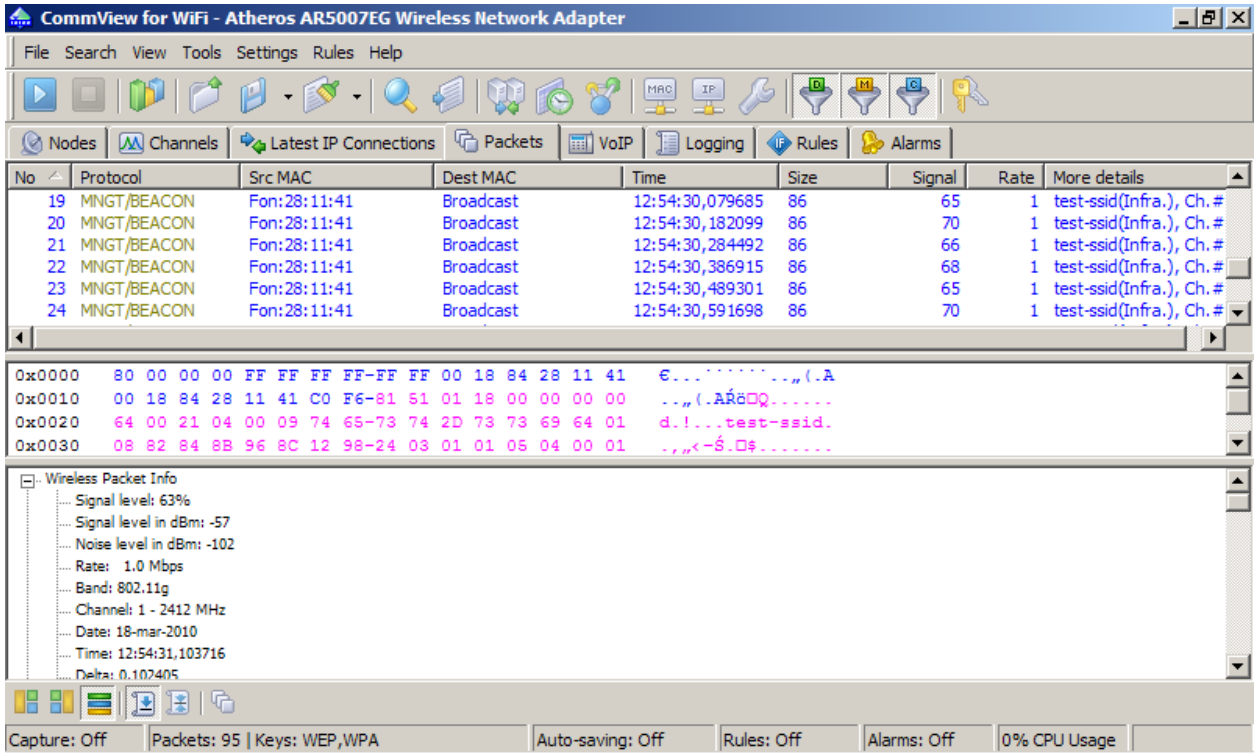
Interval prehajanja, podan v milisekundah, določa čas med dvema preverjanjema pogoja ali naj odjemalec poizkuša izvesti prehod ali ne. Rezultat pogoja pa določa parameter praga jakosti signala, ki je podan kot celo število na intervalu od 1 do 100. Dokler je jakost trenutnega signala večja od praga jakosti, odjemalec nadaljuje z normalnim delovanjem. Ko pa jakost trenutnega signala pade pod podan prag, se sproži iskanje alternativnih dostopnih točk v okolici. Če je najdena dostopna točka z boljšim signalom, odjemalec izvede prehod nanjo, drugače pa nadaljuje z uporabo trenutne. Ta postopek iskanja se nato ponavlja po vsakem preteku intervala prehajanja, dokler odjemalec ali ne izvede prehoda na dostopno točko ali pa se (zaradi spremembe parametrov v omrežju) signal s trenutne dostopne točke dvigne nad podan prag jakosti.

Spletna stran projekta: http://hostap.epitest.fi/wpa_supplicant/

4.2.5. Programa za vohljanje CommView for WiFi ter Wireshark

Za vohljanje na brezžičnem mediju je bil uporabljen program CommView for WiFi, katerega zaslonski prikaz prikazuje slika (Slika 18). Deluje na Microsoft Windows platformi, omogoča pa pasivno spremljanje dogajanja na določenem kanalu brezžičnega omrežja - nivo fizične plasti ISO/OSI modela. Njegova prednost je uporabniku prijazen prikaz vseh parametrov okvirja (zaglavje) ter beleženje natančnega časa sprejema okvirja. V primeru izklopljenega

šifriranja ali šifriranja s poznanim ključem pa nam omogoča tudi vpogled v višjenivojski (podatkovni) del okvirja.



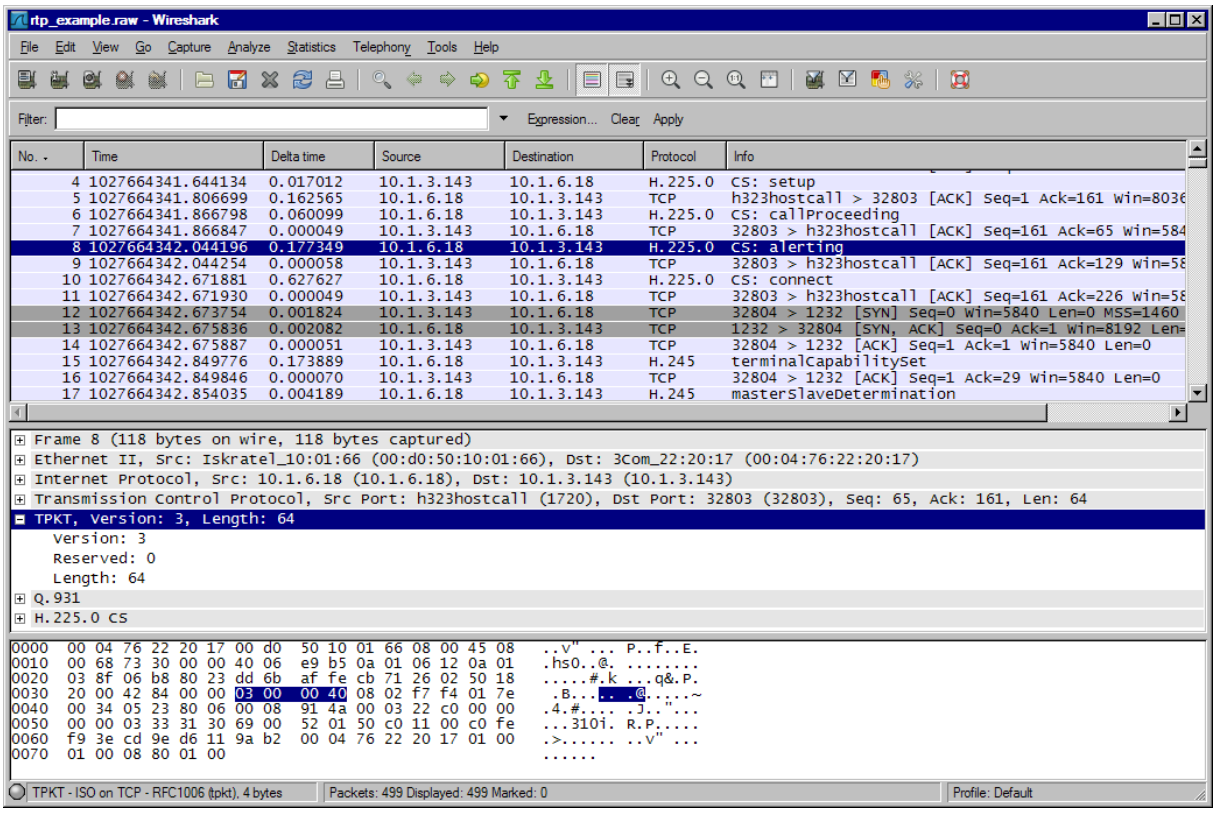
Slika 18: Zaslonska slika programa CommView for WiFi.

Brezplačno orodje Wireshark, katerega zaslonska slika je prikazana na sliki (Slika 19), s svojo funkcionalnostjo dopolnjuje CommView, saj deluje od povezovalne plasti navzgor. Velik poudarek je dan dekodiranju različnih protokolov, kar nam omogoča vpogled v notranjost podatkovnega dela paketov na različnih nivojih.

Ker deluje od povezovalne plasti navzgor, ga lahko uporabljamo direktno na odjemalcu – ne potrebujemo ločenega računalnika za poslušanje kot za CommView. Deluje nad nivojem kriptiranja v brezžičnih omrežjih, zato tudi brez težav vidimo ves promet med odjemalcem in dostopno točko.

Spletna stran programov:

http://www.tamos.com/products/commwifi/
http://www.wireshark.org/



Slika 19: Zaslonska slika programa Wireshark.

4.2.6. Kombinacija gonilnika Intelovega vmesnika ter CommView for WiFi

Vse meritve so bile izvedene istočasno z uporabo prilagojenega gonilnika za Intelov brezžični vmesnik WiFi Link 5100 na odjemalcu ter CommView for WiFi na vohljačih. Slednje nam omogoča dva različna pogleda na dogajanje:

- prvi pogled (gonilnik Intelove brezžične kartice) nam omogoča vpogled v odjemalca ter razumevanje zakasnitev, ki so posledica njegovega notranjega delovanja (delovanje gonilnika ter v njem uporabljenih algoritmov);
- drugi pogled preko vohljačev (CommView for Wifi) pa nam omogoča vpogled v dogajanje na brezžičnem mediju. Z njegovo pomočjo lahko izmerimo točne čase posameznih okvirjev na mediju, kar nam olajša delitev zakasnitev med odjemalca in dostopno točko. Ta način meritev namreč dosti bolj točno podaja razmerja med časi, ki jih drugače ne moremo dovolj natančno izmeriti. Zakasnitev, ki jo vohljaču vnese strojna in programska oprema, je namreč konstantna za vse okvirje, ne glede na njihov izvor, česar pri ločenih meritvah na odjemalcu in dostopni točki ne bi mogli zagotoviti. Poleg tega nam pogled preko vohljača omogoča tudi analizo delovanja brezžičnega vmesnika odjemalca in dostopne točke (izmenjave različnih tipov okvirjev itd.) ter odkrivanje morebitnih nepravilnosti v njunem delovanju.

Dodatna prednost združenih meritev je tudi v povsem identičnih testih. Določen testni scenarij sicer lahko ponovimo poljubnokrat, vendar žal ne s popolnoma enakimi parametri, zato je vsak test zase edinstven. Pri uporabi obeh načinov merjenja istočasno pa ta problem elegantno zaobidemo.

5. Testni scenariji in rezultati

5.1. Osnovni podatki o meritvah

V okviru diplomske naloge so bile izvedene meritve časa, potrebnega za prehod na novo dostopno točko. Ker mora odjemalec pred prehodom obvezno opraviti tudi proces iskanja dostopnih točk, je v sklopu vsake meritve časa prehoda izmerjen tudi čas iskanja. Uporaba aktivnega iskanja na kanalih 12 in 13 je prepovedana, zato gonilnik zanju samodejno izbere pasivni način iskanja. Ta lastnost nam omogoča poenostavitev meritev, saj dobimo podatke o obeh tipih iskalnih časov s pomočjo ene meritve.

Z meritvami je bilo izmerjenih več različnih časov, njihov pomen pa je sledeč:

1. čas iskanja dostopnih točk na aktiven način (T_{ISK-A}) merjen od začetka izvajanja iskanja do njegovega zaključka. Začetek predstavlja odločitev gonilnika za izvedbo iskanja na določenem kanalu, zaključek pa vrnitev na kanal s trenutno asociirano dostopno točko ter ponovna vzpostavitev komunikacije z njo (vrnitev odjemalca iz navidezno energijsko varčnega načina);
2. čas iskanja dostopnih točk na pasiven način (T_{ISK-P}) merjen na enak način kot pri aktivnem iskanju.
3. čas za izvedbo prehoda na novo dostopno točko (T_{ROAM}) merjen od poslanega deavtifikacijskega okvirja trenutni dostopni točki ali prvega poslanega upravljalnega okvirja novi dostopni točki (prvega od obeh, ki se pojavi na mediju) do zaključka prenosa asociacije. Zaključek predstavlja sprejeta pozitivna potrditev prenosa asociacije s strani nove dostopne točke oziroma, v primeru Eduroam brezžičnega omrežja, sprejet zadnji okvir iz sklopa IEEE 802.1X avtentifikacije.

Pri scenarijih, kjer je bil do odjemalca vzpostavljen podatkovni tok (enosmerna povezava proti odjemalcu), so pri rezultatih podani še trije časi, ki predstavljajo čas trajanja prekinitve podatkovnega toka na strani odjemalca. Začetek prekinitve je definiran kot čas sprejema zadnjega podatkovnega okvirja pred posamezno prekinitvijo, konec prekinitve pa kot čas sprejema prvega podatkovnega okvirja po koncu prekinitve. Kot podatkovni okvir se smatra okvir iz generiranega podatkovnega toka in ne morebitni upravljalni paketi IEEE 802.1X avtentifikacije (pri Eduroam omrežju). Zaradi analogije z zgoraj opisanimi tremi merjenimi časi so tudi ti poimenovani po enakem ključu: $T_{ISK-A-D}$, $T_{ISK-P-D}$ ter T_{ROAM-D}.

Parametri generiranega prometa so sledeči:

- velikost paketa: 60 B,
- zakasnitev med paketi: 2 ms (500 paketov na sekundo),
- število paketov: neomejeno (v testno omrežje jih pošiljamo brez prekinitve).

Slednje pomeni obremenitev približno 240 kbit/s, kar ustreza pasovni širini video konference slabše kakovosti. Generiran promet z zgornjimi parametri je bil uporabljen pri vseh testnih scenarijih, razen kjer ni izrecno drugače navedeno. Parametri se znotraj ponovitev istega scenarija ne spreminjajo, morebitne razlike med scenariji pa so navedene pri opisu scenarijev.

Časi iskanja ter prehoda so izmerjeni s pomočjo nadgrajenega gonilnika Intelovega brezžičnega vmesnika, časi prekinitve podatkovnega toka pa s pomočjo vohunskega programa Wireshark, ki vohuni na odjemalcu. Zaradi velikega števila paketov v podatkovnem toku, ki so razporejeni časovno enakomerno, je meritev prekinitve podatkovnega toka natančna do dvakratnika vmesnega časa med posameznima paketoma generiranega prometa (±2 ms).

Vsi rezultati meritev so podani v milisekundah ter zaokroženi na najbližjo celoto, kar je tudi največja natančnost, ki jo lahko pri takem načinu merjenja dobimo. Nadgrajen gonilnik ter Wireshark sicer omogočata beleženje časov do natančnosti μs, vendar je natančnost te informacije zelo vprašljiva. Razlogi za nenatančnost tičijo predvsem v računalniški arhitekturi odjemalca:

- notranja ura ni umerjena ter absolutno natančna,
- neznana je zakasnitev med proženjem in serviranjem prekinitve, prav tako se lahko med delovanjem spreminja (različne prioritete prekinitev itd.),
- v večopravilnem operacijskem sistemu si procesi delijo čas, zato tudi ni povsem točno znan vrstni red izvajanja posameznih programskih sklopov,
- branje ter izpisovanje časa samo po sebi vnaša določeno zakasnitev.

Vohunjenje s programom CommView je v času izvajanja meritev služilo za vpogled v dogajanje na brezžičnem mediju ter kontrolo dogajanja. To se je izkazalo kot zelo koristno pri preverjanju pravilnosti izvajanja meritev ter kasnejšemu vrednotenju in povzemanju dobljenih rezultatov.

Postavitev dostopnih točk ter odjemalca se v testnem omrežju ne spreminja. Fizičen premik odjemalca namreč simuliramo s kasnejšim vklopom odjemalcu bližje dostopne točke. Pri meritvah v omrežju Eduroam pa zaradi fizičnih omejitev pri delovanju dostopnih točk (ne smemo jih poljubno prižigati in ugašati) premikamo odjemalca. Odjemalec se giblje s hitrostjo pešca, kar pa zaradi neagresivnosti algoritmov za iskanje ter menjavo dostopnih točk na odjemalcu na meritve ne vpliva.

Pred vsako ponovitvijo določene meritve v testnem omrežju se obe dostopni točki izklopi iz napajanja ter nato ponovno priklopi samo dostopno točko 1. V času njenega zaganjanja se na odjemalcu izklopi ter ponovno vklopi brezžični vmesnik, kar ima za posledico povrnitev vmesnika v začetno stanje. Po vzpostavitvi asociacije odjemalca z dostopno točko 1 ter vzpostavitvi podatkovnega toka od generatorja prometa do odjemalca, se na napajanje priklopi tudi dostopna točka 2. Nato počakamo, da odjemalec opravi iskanje ter prehod, in meritev zaključimo. V omrežju Eduroam pa se pred vsako ponovitvijo meritve premaknemo nazaj na izhodiščno lokacijo ter izklopimo in ponovno vklopimo brezžični vmesnik. Po vzpostavitvi asociacije z bližnjo dostopno točko se fizično premaknemo na končno lokacijo ter počakamo na odjemalčev prehod, kar pomeni konec meritve.

Vsak testni scenarij je bil ponovljen petnajstkrat, razen če pri posameznem scenariju ni izrecno drugače navedeno.

Statistični povzetek ter komentar dobljenih rezultatov je predstavljen pri posameznem testnem scenariju, točni časi, dobljeni pri testiranjih, pa so podani v prilogi. Za predstavitev dobljenih časov je bila poleg minimuma, maksimuma, povprečja ter standardne deviacije izbrana tudi mediana. Pri večini testnih scenarijev samo eden ali dva rezultata močno odstopata od zelo jasnega povprečja, zato mediana še najbolj realno predstavlja situacijo.

5.2. Prehodi v neobremenjenem omrežju brez šifriranja in generiranega prometa

V okviru testnega scenarija so bili izmerjeni časi prehodov v popolnoma neobremenjenem omrežju in brez uporabe šifriranja (odprt tip avtentifikacije). Prav tako je bil izklopljen generator testnega prometa, zato tudi ni podatka o dolžinah prekinitve podatkovnega toka.

Dobljeni rezultati nam podajajo idealen čas prehoda, ki ga je mogoče doseči, kar nam služi kot primerjalna referenca za vse ostale meritve.

	Dolžina prehoda
Minimum	8,00 ms
Maksimum	196,00 ms
Povprečje	31,29 ms
Standardna deviacija	50,74 ms
Mediana	12,00 ms

Tabela 1: Statistična analiza rezultatov pri prehodih v neobremenjenem omrežju brez šifriranja in generiranega prometa.

Pri 3. ponovitvi scenarija je zaradi neznanega razloga prišlo do izboljšanja signala dostopne točke 1. Slednji se je ves čas izvajanja meritev (približno 4 minute) nahajal nad nivojem, določenim za prehod, zato odjemalec prehoda ni izvedel.

Iz dobljenih rezultatov vidimo, da lahko v povsem neobremenjenem omrežju brez uporabe šifriranja pričakujemo večino časov prehodov med 8 ms in 14 ms, vendar pa ne moremo povsem izključiti tudi občutno daljših period. Tako je izmerjen maksimalni čas prehoda več kot šestnajstkrat večji od mediane.

5.3. Prehodi v neobremenjenem omrežju brez šifriranja

Scenarij je povsem enak kot v 5.2. primeru, vendar pa je bil tokrat generator testnega prometa proti odjemalcu (240 kbit/s) vklopljen, zato so izmerjeni tudi časi prekinitev podatkovnega toka.

	Dolžina prehoda	**Dolžina prekinitve podatkovnega toka**
Minimum	8,00 ms	17,00 ms
Maksimum	647,00 ms	660,00 ms
Povprečje	92,87 ms	103,27 ms
Standardna deviacija	198,20 ms	202,16 ms
Mediana	11,00 ms	18,00 ms

Tabela 2: Statistična analiza rezultatov pri prehodih v neobremenjenem omrežju brez šifriranja.

Pri 8. in 14. ponovitvi scenarija je prišlo do ponovnega iskanja dostopnih točk v času, ko je odjemalec že izvajal prehod. Slednje je tudi razlog za nenavadno dolga časa prehodov, saj so vanj všteti tudi časi iskanj. Lepo je vidna tudi razlika pri iskanju dostopnih točk na pasivnih kanalih, kjer je čas iskanja v teh dveh ponovitvah občutno daljši kot pri ostalih. Daljša iskalna časa sta posledica dejstva, da odjemalec v času izvajanja prehoda ni asociiran in mu ni potrebno skrbeti za pravočasen sprejem svetilnih okvirjev, ki se pošiljajo s periodo 100 ms.

Če v dobljenih rezultatih odmislimo oba ekstremna primera, v katerih je bila prekinitev podatkovnega toka večja od pol sekunde, vidimo, da so dobljeni rezultati prekinitev zelo podobni tistim, izmerjenim v 5.2. testnem scenariju. Torej lahko tudi tu pričakujemo kratke čase prehodov z občasnimi občutno daljšimi izjemami. Dobljeni časi prekinitev podatkovnega toka so v povprečju 10,4 ms daljši od samega časa prehoda, minimalna izmerjena razlika je bila 6ms, maksimalna pa 30 ms. V večini primerov je torej prekinitev podatkovnega toka dovolj kratka, da je pri uporabi VoIP storitev ne zaznamo.

5.4. Prehodi v neobremenjenem omrežju brez šifriranja z dostopno točko na pasivnem kanalu[1]

Scenarij je povsem enak kot v 5.3. primeru, spremenjen je samo kanal dostopne točke 2 (dostopna točka, na katero prehajamo). V tem testnem scenariju se nahaja na kanalu 12 (2,467 GHz) in ne na kanalu 11, kot pri ostalih testnih scenarijih. Na kanalu 12 je namreč prepovedano aktivno iskanje dostopnih točk, tako da so bili v sklopu tega scenarija izmerjeni časi pasivnega iskanja na nepraznem kanalu ter časi prehoda na dostopno točko na pasivnem kanalu.

	Dolžina prehoda	**Dolžina prekinitve podatkovnega toka**
Minimum	205,00 ms	216,00 ms
Maksimum	213,00 ms	891,00 ms
Povprečje	208,57 ms	267,79 ms
Standardna deviacija	2,03 ms	179,42 ms
Mediana	209,00 ms	219,00 ms

Tabela 3: Statistična analiza rezultatov pri prehodih v neobremenjenem omrežju brez šifriranja z dostopno točko na pasivnem kanalu.

Pri 8. ponovitvi scenarija je prišlo do povečanja signala s strani dostopne točke 1, kar je povzročilo, da odjemalec prehoda ni izvedel.

Časi prehodov, ki so posledica uporabe pasivnega kanala, so presenetljivo dolgi ter konstantni, kar je lepo razvidno iz majhne standardne deviacije (2,03 ms). Dolžina prekinitev, ki minimalno znaša 216 ms, pa za VoIP ter druge časovno kritične storitve ni več uporabna.

5.5. Prehodi v neobremenjenem omrežju z WPA šifriranjem

Tudi v tem scenariju je omrežje neobremenjeno, v uporabi pa je WPA šifriranje s skupnim ključem, kar posledično pomeni izmenjavo večjega števila okvirjev med dostopno točko in odjemalcem v času prehoda. Generator testnega prometa proti odjemalcu je vklopljen in predstavlja edini promet v omrežju.

Časi prehodov so približno trikrat daljši od tistih, izmerjenih v enakem omrežju brez uporabe šifriranja (5.3. testni scenarij). Odstopa samo prehod v 1. ponovitvi meritve, kjer gre očitno spet za občasno izjemo.

[1] Kot pasivna kanala smatramo kanala 12 in 13, na katerih je prepovedano aktivno iskanje dostopnih točk.

	Dolžina prehoda	Dolžina prekinitve podatkovnega toka
Minimum	25,00 ms	41,00 ms
Maksimum	1032,00 ms	1046,00 ms
Povprečje	97,67 ms	113,93 ms
Standardna deviacija	258,52 ms	257,90 ms
Mediana	29,00 ms	47,00 ms

Tabela 4: Statistična analiza rezultatov pri prehodih v neobremenjenem omrežju z WPA šifriranjem.

Prav tako se je v tem testnem scenariju podaljšala tudi prekinitev podatkovnega toka, ki je znašala minimalno 41 ms, mediana pa že 47 ms. Slednje je na meji uporabnosti za VoIP storitve, ki lahko tolerirajo prekinitve do 50 ms. Povečanje gre deloma tudi na račun razlike med časom prehoda in časom prekinitve podatkovnega toka, ki sedaj povprečno znaša že 16,27 ms (minimalno 13, maksimalno 24).

5.6. Prehodi v nizko obremenjenem omrežju z WPA šifriranjem

Pri tem testnem scenariju je bil v omrežje dodan še brezžični odjemalec (v nadaljevanju »obremenjevalec«), ki je kanal dostopne točke, na katero prehajamo, obremenil s količino podatkov, ki jo smatramo za nizko obremenitev. Obremenitev je predstavljala 4 GB velika datoteka, ki jo je obremenjevalec v času meritev prenašal po omrežju preko HTTP protokola, hitrost prenosa pa je bila omejena na 200 kB/s. Generator testnega prometa proti odjemalcu je vklopljen, v uporabi je WPA šifriranje s skupnim ključem, dostopna točka 2 pa deluje na kanalu 8.

	Dolžina prehoda	Dolžina prekinitve podatkovnega toka
Minimum	22,00 ms	41,00 ms
Maksimum	2678,00 ms	3251,00 ms
Povprečje	290,33 ms	350,93 ms
Standardna deviacija	710,61 ms	843,81 ms
Mediana	30,00 ms	47,00 ms

Tabela 5: Statistična analiza rezultatov pri prehodih v lahno obremenjenem omrežju z WPA šifriranjem.

Pri 4. in 14. ponovitvi je razlog za občutno daljše čase prehoda zakasnitev pri izmenjavi WPA ključev, ki je v teh dveh primerih trajala nekoliko dlje.

Časi prekinitev so zelo podobni tistim iz IV. testnega scenarija, povečalo pa se je število odstopajočih izjem, kar si lahko razlagamo kot posledico obremenitve omrežja.

5.7. Prehodi v močno obremenjenem omrežju z WPA šifriranjem

Pri tem testnem scenariju je bil v omrežje dodan brezžični odjemalec (v nadaljevanju »obremenjevalec«), ki je kanal dostopne točke, na katero prehajamo, obremenil s količino podatkov, ki jo smatramo za močno obremenitev. Obremenitev je predstavljala 4 GB velika datoteka, ki jo je obremenjevalec v času meritev prenašal po omrežju preko HTTP protokola, hitrost prenosa pa ni bila dodatno omejena. Tako je omejitev hitrosti prenosa predstavljala kar sama hitrost brezžičnega omrežja. Generator testnega prometa proti odjemalcu je vklopljen, v uporabi je WPA šifriranje s skupnim ključem, dostopna točka 2 pa deluje na kanalu 8.

	Dolžina prehoda	Dolžina prekinitve podatkovnega toka
Minimum	256,00 ms	312,00 ms
Maksimum	2678,00 ms	3251,00 ms
Povprečje	985,31 ms	1253,38 ms
Standardna deviacija	665,68 ms	859,46 ms
Mediana	992,00 ms	1089,00 ms

Tabela 6: Statistična analiza rezultatov pri prehodih v močno obremenjenem omrežju z WPA šifriranjem.

6. in 9. ponovitev testnega scenarija žal nista uspeli, saj se obremenjevalec ni uspel pravočasno povezati z želeno dostopno točko ter ustrezno obremeniti omrežja. Tako ga je odjemalec prehitel s prehodom, kar praktično pomeni isto meritev kot pri scenariju 5.5.

Posledice obremenitve omrežja so iz dobljenih rezultatov jasno razvidne. Minimalen čas prehoda se je povzpel na 256 ms, minimalna prekinitev podatkovnega toka pa znaša 312 ms, kar pomeni, da tako omrežje tudi v najboljšem možnem primeru ni več uporabno za storitve, ki zahtevajo minimalne zakasnitve. Poleg povečanja zakasnitev se je spremenila tudi njihova porazdelitev – če smo v predhodnih primerih lahko določili nek osnovni interval, na katerem se je nahajala večina izmerjenih vrednosti (z izjemo določenih ekstremnih primerov), pa sedaj to ni več mogoče. Rezultati so namreč razporejeni po celem intervalu, ki se razteza od minimalne do maksimalne izmerjene vrednosti, med njima pa je razlika za faktor 10.

5.8. Prehodi v neobremenjenem Eduroam omrežju

S tem testnim scenarijem so bili izmerjeni časi prehodov med dostopnimi točkami v neobremenjenem Eduroam omrežju na Fakulteti za računalništvo in informatiko v Ljubljani. Omrežje je bilo zaradi izvajanja meritev v popoldanskem času minimalno obremenjeno. Generator testnega prometa proti odjemalcu je bil vklopljen.

	Dolžina prehoda	Dolžina prekinitve podatkovnega toka
Minimum	121,00 ms	136,00 ms
Maksimum	834,00 ms	31141,00 ms
Povprečje	417,86 ms	2741,07 ms
Standardna deviacija	256,10 ms	8183,39 ms
Mediana	360,00 ms	545,00 ms

Tabela 7: Statistična analiza rezultatov pri prehodih v neobremenjenem Eduroam omrežju.

Razlog za občutno daljšo prekinitev podatkovnega toka pri 10. ponovitvi scenarija je izbira drugačne končne dostopne točke kot pri ostalih ponovitvah. Na to dostopno točko se je odjemalec povezal prvič, kar je zelo verjetno razlog za daljšo prekinitev. Prehod pri 11. izvajanju scenarija ni uspel, saj je odjemalca dostopna točka, na katero je prehajal, zavračala z razlogom neuspele avtentifikacije po standardu IEEE 802.1X. Podobno se je dogajalo tudi pri 12. ponovitvi scenarija, kjer prvi poizkus avtentifikacije ni uspel, zato je odjemalec čakal do izteka časovnika (30 sekund) ter ponovno izvedel postopek avtentifikacije. Ker gre za enako napako pri dveh zaporednih poizkusih, časovno oddaljenih manj kot 2 minuti, lahko sklepamo, da gre za isto napako na strani dostopne točke, ki se po preteku določenega časovnega intervala sanira sama od sebe. Čas prekinitve podatkovnega toka med iskanjem na 13. kanalu pri 13. ponovitvi scenarija je vključen v čas prekinitve podatkovnega toka ob prehodu, saj je odjemalec prehod izvedel takoj po končanem postopku iskanja.

Iz dobljenih rezultatov je jasno vidno, da neobremenjeno Eduroam omrežje ni primerno za časovno kritične storitve. Minimalen čas prekinitve podatkovnega toka, to je posledica uporabe avtentifikacije po standardu IEEE 802.X, je znašal 136 ms, kar je za VoIP že občutno preveč. Problem predstavljajo tudi morebitne težave pri izvajanju avtentifikacije, kot se je pripetilo v 11. in 12. ponovitvi poizkusa, kjer lahko posledično nastanejo tudi več 10 sekund dolge prekinitve podatkovnega toka.

5.9. Prehodi v obremenjenem Eduroam omrežju

Pri tem testnem scenariju pa so bili izmerjeni časi prehodov med dostopnimi točkami v obremenjenem Eduroam omrežju. Obremenitev so predstavljali kar pravi uporabniki brezžičnega omrežja na fakulteti v času njegove največje obremenitve (avla fakultete, odmor ob 12.00 uri). Generator testnega prometa proti odjemalcu je bil vklopljen.

	Dolžina prehoda	**Dolžina prekinitve podatkovnega toka**
Minimum	124,00 ms	171,00 ms
Maksimum	13408,00 ms	69636,00 ms
Povprečje	2045,38 ms	10413,25 ms
Standardna deviacija	3612,11 ms	22655,40 ms
Mediana	683,00 ms	843,00 ms

Tabela 8: Statistična analiza rezultatov pri prehodih v obremenjenem Eduroam omrežju.

Dolgi časi prehodov pri 1. ter 3. ponovitvi scenarija so posledica odjemalčeve izbire alternativnih dostopnih točk. Uspešno se je uspel namreč povezati šele na 3. izbrano dostopno točko. Ker je bil v času zadnjega iskanja dostopnih točk neasociiran, podatki o dolžini prekinitev podatkovnega toka niso bili izmerjeni. Pri 2. ponovitvi se je odjemalec povezal na dostopno točko, na kateri povezava v omrežje ni delovala, saj se podatkovni tok po preteklih 5 minutah od prehoda še vedno ni vzpostavil. Sam prehod ter avtentifikacija po standardu IEEE 802.1X sta bili izvedeni uspešno. Iz neznanega razloga povezava z alternativno dostopno točko ni uspela pri 6. in 13. ponovitvi scenarija. V prvem primeru je bil test prekinjen po dobrih 4 minutah, v drugem pa po 90 sekundah. Čas prekinitve podatkovnega toka med iskanjem na 13. kanalu pri 7. ponovitvi scenarija je vključen v čas prekinitve podatkovnega toka ob prehodu, saj je odjemalec prehod izvedel takoj po končanem postopku iskanja.

Že zaradi dejstva, da neobremenjeno Eduroam omrežje ni primerno za časovno kritične storitve, ne moremo pričakovati, da se obremenjeno Eduroam omrežje obnese kaj bolje. Zaradi obremenjenosti se časi prehodov v povprečju povečajo za več kot sekundo in pol, povprečna dolžina prekinitve podatkovnega toka pa za več kot sedem sekund. Dolžina prekinitev je v nekaterih primerih že tako velika, da izpad opazimo tudi pri časovno nekritičnih storitvah.

5.10. Rezultati meritev časov iskanj

Čase iskanj na posameznih kanalih, izmerjene preko gonilnika, lahko glede na njihovo dolžino ter pogoje, pod katerimi se pojavljajo, razvrstimo v tri skupine.

1. Čase iskanj na praznih aktivnih kanalih, ki trajajo v večini primerov 13 ms. Slednje časovno kritičnim storitvam ne bi smelo predstavljati prevelikih težav.

2. Čase iskanj na zasedenih aktivnih kanalih, ki trajajo v večini primerov 40 ms. Slednje je sicer še v mejah odstopanj, ki jih storitev VoIP tolerira, vendar pa se moramo zavedati, da meja 50 ms ni več tako zelo oddaljena.
3. Čase iskanj na pasivnih kanalih, ki trajajo v večini primerov 90 ms. Dolžina te prekinitve presega toleranco storitev VoIP, tako da lahko posledično pričakujemo ponavljajoče se motnje v delovanju.

Ti časi predstavljajo povprečno vrednost, saj je iz rezultatov meritev razvidno, da so možni tudi drugi časi, ki se pojavljajo bolj izjemoma. Povečanje števila odstopajočih časov iskanj je bilo opaženo predvsem v testnem scenariju 5.7., kjer je bilo brezžično omrežje maksimalno obremenjeno.

Z izjemo časov iskanj na pasivnih kanalih nam ostali časi iskanj ne bi smeli povzročati težav pri delovanju časovno kritičnih storitev, vendar pa je resnica žal drugačna. Trditev velja namreč samo ob doslednem upoštevanju pogoja, da lahko izvajamo iskanje samo na enem kanalu, nato pa se vrnemo nazaj na delujoči kanal ter ponovno vzpostavimo podatkovni tok. Žal pa gonilnik na odjemalcu tega pogoja ne upošteva, kar je lepo razvidno iz rezultatov meritev prekinitev podatkovnega toka. Iskanja po posameznih kanalih namreč združuje, tako da je večina prekinitev podatkovnega toka daljših od kritične meje za VoIP storitve (50 ms). V Eduroam omrežjih tako prekinitev podatkovnega toka med aktivnim iskanjem v povprečju znaša približno 110 ms, v testnih omrežjih pa 60 ms.

6. Ugotovitve in zaključek

V diplomski nalogi so bili izmerjeni časi prekinitev podatkovnih tokov, ki nastanejo kot posledica odjemalčevega prehoda na drugo dostopno točko v brezžičnih omrežjih po standardu IEEE 802.11g. Ugotovljeno je bilo, da prehajanje z brezžičnim vmesnikom WiFi Link 5100 na Linux platformi v nobenem primeru ni primerno za storitve, ki niso odporne na vsaj 100 ms dolge prekinitve podatkovnega toka. Torej je istočasna uporaba prehajanja in storitev VoIP, ki tolerirajo prekinitve do 50 ms, nemogoča. Razlog za tako dolge prekinitve je uporaba pasivnega iskanja dostopnih točk na kanalih 12 in 13, kjer v najboljšem primeru pride do vsaj 94 ms dolge prekinitve podatkovnega toka. Krajši časi samih prehodov nam tu namreč nič ne pomagajo. V bolj obremenjenih omrežjih ali v omrežjih, kjer je v uporabi avtentifikacija po standardu IEEE 802.1X, se časi prehodov opazno povečajo in presežejo čase iskanj na pasivnih kanalih, kar še dodatno oteži situacijo. Tu namreč niti odpornost na 100 ms dolge prekinitve ne zadostuje več.

Seveda lahko kratke čase prehodov in iskanj dosegamo samo z uporabo kvalitetnih brezžičnih vmesnikov ter gonilnikov zanje. Kolikšna je lahko razlika med dobrim in slabim gonilnikom, se je pokazalo med izdelavo diplomske naloge, kjer je bilo potrebno Atherosov brezžični vmesnik nadomestiti z bolj kvalitetnim Intelovim.

6.1. Možne izboljšave

V brezžičnih omrežjih, v katerih vseeno potrebujemo funkcionalnost prehajanja in uporabljamo storitve, ki zahtevajo čim krajše prekinitve podatkovnih tokov, lahko z določenimi kompromisi ter izboljšavami ustvarimo okolje, ki omogoča čim krajše prekinitve. Izboljšave zadevajo tako odjemalce kot dostopne točke, saj samo v tem primeru lahko dosežemo najbolj optimalno delovanje.

1. Odjemalci naj uporabljajo aktivno iskanje dostopnih točk na kanalih od 1 do 11, saj je slednje neprimerno hitrejše od pasivnega iskanja.
2. Ker je ozko grlo iskanje dostopnih točk na pasivnih kanalih, lahko uporabo pasivnih kanalov izklopimo. Slednje mora biti izvedeno v dogovoru med vzdrževalci omrežja, ki dostopne točke ne konfigurirajo na pasivne kanale, ter uporabniki, ki na svojih odjemalcih izklopijo iskanje dostopnih točk na pasivnih kanalih.
3. Omrežje mora biti pravilno dimenzionirano, da ne prihaja do prevelikih obremenitev, ki pogubno vplivajo na čase prehodov. Če ne potrebujemo velikih prenosnih hitrosti, je smiselno omejiti pasovno širino posameznega odjemalca. Tako ne more en sam odjemalec preprečiti pravilnega delovanja storitev ostalim uporabnikom.
4. Preveriti je potrebno delovanje gonilnikov brezžičnih vmesnikov na odjemalcih. V diplomski nalogi so bile ugotovljene kar tri različne težave pri delovanju gonilnikov, ki negativno vplivajo na hitrost prehajanja oziroma iskanja dostopnih točk:
    - gonilnik MadWiFi ne najde dostopnih točk, kadar je sam izvor podatkov v brezžično omrežje,
    - gonilnik MadWiFi brez obremenitve porabi več kot 110ms časa za prehod v testnem scenariju 5.2,
    - gonilnik Intelovega brezžičnega vmesnika pri iskanju preišče več kanalov zapored, kar po nepotrebnem podaljšuje prekinitve podatkovnega toka.

Vse naštete pomanjkljivosti bi bilo treba za izboljšanje delovanja odpraviti.

Nekoliko bolj zahtevna izboljšava pa bi bila uporaba dveh med seboj fizično ločenih brezžičnih vmesnikov na odjemalcu. V tem primeru bi bila njuna naloga sledeča:

1. vmesnik bi skrbel samo za podatkovni prenos s trenutno asociirano dostopno točko. Tako ne bi prihajalo do prekinitev v podatkovnem toku, ki bi bile posledica iskanja dostopnih točk na drugih kanalih.
2. vmesnik pa bi skrbel za iskanje alternativnih dostopnih točk ter prenos asociacije na drugo dostopno točko (v dogovoru s 1. vmesnikom).

Vloga brezžičnih vmesnikov bi se seveda menjavala z vsako menjavo dostopne točke. Tako bi v celoti odpravili prekinitve, ki so posledica iskanja dostopnih točk na drugih kanalih. Najbrž pa bi na tak način tudi zmanjšali čas prekinitve podatkovnega toka v času prehodov, saj bi prvi vmesnik sprejemal podatke dokler drugi vmesnik ne opravi prehoda v celoti (vključno z izmenjavo šifrirnih ključev ali avtentifikacije po standardu IEEE 802.1X) in vzpostavi podatkovnega toka.

Tu predstavljena rešitev pa je primerna res samo za najbolj zahtevna brezžična omrežja, saj ima žal tudi nekaj negativnih lastnosti:

- dva brezžična vmesnika sta dražja od enega samega,
- dva brezžična vmesnika porabita več električne energije, kar pomeni krajši čas avtonomije pri enaki kapaciteti baterij,
- vmesnika ter njune antene se morajo zaradi izogibanja medsebojnih motenj (saturacija sprejemnika itd.) nahajati čim dlje narazen, kar onemogoča uporabo take konfiguracije v manjših napravah, kot so npr. dlančniki ali mobilni telefoni.

Priloge

Tabele z rezultati opravljenih meritev

Prehodi v neobremenjenem omrežju brez šifriranja in generiranega prometa

Vse vrednosti so podane v milisekundah.

Ponovitev	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
1. kanal	40	40		40	40	40	40	40	40	40	40	40	40	40	40
2. kanal	19	40		40	13	12	13	40	40	40	40	40	40	40	40
3. kanal	17	15		13	13	12	13	13	13	12	13	13	13	12	13
4. kanal	13	14		13	13	13	13	13	13	13	13	13	13	12	12
5. kanal	13	13		13	13	12	13	13	13	13	13	14	13	13	13
6. kanal	14	13		13	13	13	13	14	13	13	13	13	13	13	13
7. kanal	13	14		13	14	12	13	14	13	13	13	13	13	13	13
8. kanal	13	13		13	13	12	13	13	12	13	13	13	13	12	13
9. kanal	13	13		14	13	13	13	13	13	12	13	13	13	13	13
10. kanal	13	13		13	14	12	13	12	13	40	13	13	13	13	40
11. kanal	40	40		40	40	40	40	40	40	40	40	40	40	40	41
12. kanal	90	90		90	90	90	90	90	90	90	90	90	90	90	90
13. kanal	90	90		90	90	90	90	90	90	90	90	90	90	90	90

Tabela 9: Časi iskanj v neobremenjenem omrežju brez šifriranja in generiranega prometa merjeni preko gonilnika.

Ponovitev	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Čas prehoda	69	11		13	12	9	14	11	13	51	8	11	196	11	9

Tabela 10: Časi prehodov v neobremenjenem omrežju brez šifriranja in generiranega prometa merjeni preko gonilnika.

Prehodi v neobremenjenem omrežju brez šifriranja

Vse vrednosti so podane v milisekundah.

Ponovitev	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
1. kanal	40	40	40	40	40	40	40	40	40	40	40	40	40	40	40
2. kanal	40	14	13	40	12	40	40	13	40	40	40	40	40	40	40
3. kanal	13	14	13	13	12	12	13	13	15	13	13	13	13	13	13
4. kanal	13	13	12	13	12	13	13	12	13	13	13	13	13	13	13
5. kanal	13	13	13	13	13	13	13	12	12	13	13	13	13	13	13
6. kanal	13	13	13	13	12	13	13	12	15	40	40	27	40	13	20
7. kanal	40	12	40	40	13	13	40	40	40	40	16	13	15	40	40
8. kanal	13	13	13	13	13	13	13	13	13	13	14	13	13	13	12
9. kanal	13	12	13	13	12	13	13	12	13	13	13	13	13	13	13
10. kanal	40	14	40	13	13	13	13	12	14	13	13	14	13	40	12
11. kanal	40	40	40	40	40	40	40	40	40	40	40	40	40	40	40
12. kanal	90	90	90	90	91	90	90	123	90	90	90	90	90	123	90
13. kanal	90	90	90	90	91	90	90	123	90	90	90	90	90	123	90

Tabela 11: Časi iskanj v neobremenjenem omrežju brez šifriranja merjeni preko gonilnika.

Ponovitev	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
1. kanal	44	57	44	43	56	41	44		85	42	43	42	42		44
2. kanal	58		60	54		54	56			55	54	55	55		103
3. kanal		61			58				64						
4. kanal	88			87		60	87			72	74	60	73		94
5. kanal															
6. kanal			59												
7. kanal		59			59				58	58	65	61	63		
8. kanal	72		73	86		88	86								85
9. kanal									73	72					
10. kanal															
11. kanal	44	44	44		44						44	44	44		
12. kanal	94	94	95	95	95	95	95		95	94	94	95	94		95
13. kanal	95	94	95	95	95	95	95		95	94	95	94	95		94

Tabela 12: Dolžina prekinitve podatkovnega toka v neobremenjenem omrežju brez šifriranja v času iskanj.

Ponovitev	1	2	3	4	5	6	7	8
Čas prehoda	10	132	11	10	11	8	10	492
Dolžina prekinitve podatkovnega toka	17	140	18	18	17	18	18	522

Ponovitev	9	10	11	12	13	14	15
Čas prehoda	11	11	10	11	11	647	8
Dolžina prekinitve podatkovnega toka	19	17	29	18	21	660	17

Tabela 13: Časi prehodov v neobremenjenem omrežju brez šifriranja, merjeni preko gonilnika (1. vrstica) ter dolžina prekinitve podatkovnega toka v času prehoda (2. vrstica).

Prehodi v neobremenjenem omrežju brez šifriranja z dostopno točko na pasivnem kanalu

Vse vrednosti so podane v milisekundah.

Ponovitev	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
1. kanal	40	40	40	40	40	40	40		40	40	40	40	40	40	40
2. kanal	40	13	40	40	14	40	14		13	40	13	40	14	12	40
3. kanal	16	13	13	14	14	13	14		16	13	16	13	13	14	13
4. kanal	13	12	12	13	13	13	13		13	13	13	13	13	12	14
5. kanal	13	12	12	13	13	12	13		13	13	13	13	13	12	13
6. kanal	13	13	13	13	13	13	13		12	13	13	13	13	13	13
7. kanal	13	12	12	13	13	14	13		12	13	13	13	13	12	13
8. kanal	13	12	13	13	13	13	13		13	13	13	13	13	13	13
9. kanal	13	13	16	13	13	14	12		13	13	13	13	13	12	13
10. kanal	13	12	13	14	13	13	13		13	13	13	13	14	12	13
11. kanal	13	40	40	40	40	40	40		13	40	40	13	13	40	13
12. kanal	90	90	90	9	90	90	90		90	90	90	90	90	90	90
13. kanal	90	90	90	90	90	90	90		90	90	90	90	91	90	90

Tabela 14: Časi iskanj v neobremenjenem omrežju brez šifriranja z dostopno točko na pasivnem kanalu merjeni preko gonilnika.

Ponovitev	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
1. kanal	82	44	40	42	41	44	60		56	41	56	43	44	55	42
2. kanal		58	58	59	62	58				55		54	62		55
3. kanal	64						60		62		63			59	
4. kanal			58	59		60				61		60			61
5. kanal															
6. kanal		58			60		60		60		60		60	58	
7. kanal	60		89	88		88				87		60			60
8. kanal															
9. kanal		58			58		44		18		44		33	44	
10. kanal															
11. kanal	17														
12. kanal	95	94	95	95	94	94	95		95	95	95	94	95	95	94
13. kanal	95	95	94	95	94	94	95		95	95	94	94	95	95	95

Tabela 15: Dolžina prekinitve podatkovnega toka v neobremenjenem omrežju brez šifriranja z dostopno točko na pasivnem kanalu v času iskanj.

Ponovitev	1	2	3	4	5	6	7	8
Čas prehoda	210	208	209	207	209	206	208	
Dolžina prekinitve podatkovnega toka	891	218	216	217	217	225	220	

Ponovitev	9	10	11	12	13	14	15
Čas prehoda	210	205	207	213	208	210	210
Dolžina prekinitve podatkovnega toka	220	218	217	221	231	217	221

Tabela 16: Časi prehodov v neobremenjenem omrežju brez šifriranja z dostopno točko na pasivnem kanalu merjeni preko gonilnika (1. vrstica) ter dolžina prekinitve podatkovnega toka v času prehoda (2. vrstica).

Prehodi v neobremenjenem omrežju z WPA šifriranjem

Vse vrednosti so podane v milisekundah.

Ponovitev	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
1. kanal	40	40	13	13	40	40	13	40	13	40	13	40	40	40	40
2. kanal	40	40	40	40	40	40	40	40	40	40	40	40	40	40	40
3. kanal	40	40	40	13	40	40	40	13	40	14	13	40	14	40	40
4. kanal	13	13	14	13	13	13	16	13	13	13	20	18	13	14	13
5. kanal	13	13	14	13	13	13	13	13	13	13	13	12	13	13	13
6. kanal	13	13	13	13	13	13	13	13	13	40	13	13	13	13	13
7. kanal	13	13	14	13	13	13	13	13	13	40	12	13	13	13	13
8. kanal	13	13	14	13	13	14	13	40	13	13	13	13	14	13	13
9. kanal	14	13	13	13	13	13	13	40	14	13	13	13	12	13	13
10. kanal	40	13	13	40	40	13	40	13	13	13	12	40	40	40	40
11. kanal	40	40	40	40	40	40	40	16	40	12	40	40	40	40	40
12. kanal	90	90	90	90	90	90	90	90	90	90	90	90	90	90	90
13. kanal	90	90	90	90	90	90	90	90	90	90	90	90	90	90	90

Tabela 17: Časi iskanj v neobremenjenem omrežju z WPA šifriranjem merjeni preko gonilnika.

Ponovitev	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
1. kanal	81	85	17	58	85	80	59	40	58	85	58	82	81	44	85
2. kanal			85					53						83	
3. kanal	59	54		60	59	58	61		59	88	68	59	61		57
4. kanal			61					60						61	
5. kanal	61	60			61	61	60		60			60			61
6. kanal										45	60		87		
7. kanal				87				86						73	
8. kanal			87		59	73	58		73	46		58			59
9. kanal	60	73		44	44		44	35			44	44	44	44	44
10. kanal															
11. kanal	44														
12. kanal	94	95	95	95	94	95	95	94	95	95	94	95	95	94	95
13. kanal	94	95	95	95	95	94	94	94	94	95	94	94	95	103	95

Tabela 18: dolžina prekinitve podatkovnega toka v neobremenjenem omrežju z WPA šifriranjem v času iskanj.

Ponovitev	1	2	3	4	5	6	7	8
Čas prehoda	1032	32	25	33	32	27	29	29
Dolžina prekinitve podatkovnega toka	1046	48	49	49	47	42	46	46

Ponovitev	9	10	11	12	13	14	15
Čas prehoda	28	28	35	38	29	42	26
Dolžina prekinitve podatkovnega toka	42	41	53	54	45	59	42

Tabela 19: Časi prehodov v neobremenjenem omrežju z WPA šifriranjem, merjeni preko gonilnika (1. vrstica) ter dolžina prekinitve podatkovnega toka v času prehoda (2. vrstica).

Prehodi v lahno obremenjenem omrežju z WPA šifriranjem

Vse vrednosti so podane v milisekundah.

Ponovitev	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
1. kanal	40	40	39	40	40	40	38	40	39	40	40	39	40	40	40
2. kanal	40	13	13	40	40	14	40	40	40	40	13	40	40	40	40
3. kanal	13	14	14	16	13	14	16	13	14	14	15	13	13	40	13
4. kanal	13	13	13	13	13	13	13	13	12	13	14	13	13	16	13
5. kanal	13	13	13	14	13	13	13	13	13	13	13	13	13	17	13
6. kanal	13	13	14	13	13	13	13	13	13	40	13	13	13	19	13
7. kanal	15	40	40	40	40	14	12	13	40	40	40	13	13	42	17
8. kanal	40	40	40	40	40	40	40	40	14	13	40	40	40	40	40
9. kanal	40	40	40	40	13	40	40	40	16	13	40	40	1	41	40
10. kanal	15	13	13	14	13	13	14	13	12	13	13	13	14	20	21
11. kanal	17	14	13	13	15	13	13	16	13	12	13	13	26	16	14
12. kanal	90	90	90	90	90	90	90	90	90	90	90	90	90	90	90
13. kanal	90	90	90	90	90	90	90	90	90	90	90	90	90	90	90

Tabela 20: Časi iskanj v nizko obremenjenem omrežju z WPA šifriranjem merjeni preko gonilnika.

Ponovitev	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
1. kanal	41	41	44	87	85	62	83	40	44	85	56	44	55	42	85
2. kanal	57	60	61					53	60			59	61	86	
3. kanal				64	60	62	63			88	64				61
4. kanal	62							60	86			60	60	59	
5. kanal															
6. kanal		64	60												
7. kanal				86	85	59	58			58	85			87	63
8. kanal	86	85	85					86	64			86	86		
9. kanal				60	48	59	60			46	59			67	67
10. kanal	38	33	31					35				32	46		
11. kanal				18		21	17				18			21	18
12. kanal	95	95	95	95	95	95	94	94	95	95	94	94	95	94	95
13. kanal	94	94	94	94	94	94	95	94	95	95	95	94	95	95	94

Tabela 21: Dolžina prekinitve podatkovnega toka v nizko obremenjenem omrežju z WPA šifriranjem v času iskanj.

Ponovitev	1	2	3	4	5	6	7	8
Čas prehoda	28	29	28	1046	226	34	30	29
Dolžina prekinitve podatkovnega toka	45	44	42	1065	248	51	46	46

Ponovitev	9	10	11	12	13	14	15
Čas prehoda	30	28	89	31	27	2678	22
Dolžina prekinitve podatkovnega toka	50	41	105	46	47	3251	137

Tabela 22: Časi prehodov v lahno obremenjenem omrežju z WPA šifriranjem merjeni preko gonilnika (1. vrstica) ter dolžina prekinitve podatkovnega toka v času prehoda (2. vrstica).

Prehodi v močno obremenjenem omrežju z WPA šifriranjem

Vse vrednosti so podane v milisekundah.

Ponovitev	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
1. kanal	40	40	40	40	39		40	40		40	40	40	40	40	40
2. kanal	15	14	14	40	40		40	13		40	13	40	40	40	13
3. kanal	14	40	40	13	40		40	13		16	13	16	40	40	40
4. kanal	14	13	13	13	14		14	15		13	13	14	13	16	14
5. kanal	13	14	19	17	18		19	22		13	22	23	19	17	24
6. kanal	13	25	19	21	25		25	15		13	15	12	15	19	17
7. kanal	13	24	22	30	35		41	33		14	30	36	22	42	28
8. kanal	15	40	40	40	41		40	40		16	42	40	41	40	40
9. kanal	21	42	41	41	40		41	40		18	29	41	42	41	42
10. kanal	29	16	20	19	19		17	17		26	15	15	19	20	20
11. kanal	40	23	18	16	18		18	22		40	16	21	17	16	17
12. kanal	90	90	90	90	90		90	90		91	90	90	90	90	90
13. kanal	90	90	90	90	90		90	90		90	90	90	90	90	90

Tabela 23: Časi iskanj v močno obremenjenem omrežju z WPA šifriranjem merjeni preko gonilnika.

Ponovitev	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
1. kanal	61	58	60	86	83		83	75		83	41	85	86	42	58
2. kanal											70			86	
3. kanal	61	52	54	72	55		54	72		63		54	55	59	55
4. kanal															
5. kanal		69	66		84		91				93	96	62		75
6. kanal															
7. kanal	87	88	87	76	87		87	78		83			88	87	88
8. kanal				65				62			67	62		67	
9. kanal		45	43		43		41						41		43
10. kanal				20				27		45		25		21	
11. kanal	45														
12. kanal	103	94	95	94	95		94	95		95	95	95	95	94	95
13. kanal	95	95	94	94	95		95	94		95	94	94	95	95	95

Tabela 24: Dolžina prekinitve podatkovnega toka v močno obremenjenem omrežju z WPA šifriranjem v času iskanj.

Ponovitev	1	2	3	4	5	6	7	8
Čas prehoda	275	1011	801	256	708		1162	992
Dolžina prekinitve podatkovnega toka	312	1089	1192	345	724		2162	1046

Ponovitev	9	10	11	12	13	14	15
Čas prehoda		312	545	1012	1661	2678	1396
Dolžina prekinitve podatkovnega toka		406	645	1289	1834	3251	1999

Tabela 25: Časi prehodov v močno obremenjenem omrežju z WPA šifriranjem merjeni preko gonilnika (1. vrstica) ter dolžina prekinitve podatkovnega toka v času prehoda (2. vrstica).

Prehodi v neobremenjenem Eduroam omrežju

Vse vrednosti so podane v milisekundah.

Ponovitev	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
1. kanal	40	40	40	40	40	40	40	40	35	40		40	40	40	40
2. kanal	40	40	40	40	40	40	40	40	40	40		40	40	18	40
3. kanal	14	40	40	40	40	41	40	40	13	40		40	40	40	40
4. kanal	40	40	40	40	40	40	40	40	40	40		40	40	40	40
5. kanal	40	40	40	40	40	40	40	40	40	40		40	40	40	40
6. kanal	40	40	40	40	40	40	40	40	40	40		40	40	40	40
7. kanal	40	40	40	17	40	40	40	17	40	40		16	14	40	40
8. kanal	13	14	14	19	16	14	40	17	40	40		14	15	16	15
9. kanal	13	14	13	13	13	14	13	13	13	13		13	13	13	13
10. kanal	14	40	40	40	40	40	13	40	40	14		13	40	40	40
11. kanal	40	13	40	13	40	40	40	40	40	40		13	40	40	15
12. kanal	90	90	90	90	90	90	90	90	90	90		90	90	90	90
13. kanal	90	90	90	92	90	90	90	90	90	90		90	90	90	90

Tabela 26: Časi iskanj v neobremenjenem Eduroam omrežju merjeni preko gonilnika.

Ponovitev	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
1. kanal										41					
2. kanal		126	85					126						105	
3. kanal	169			167	161	168	153		135	127		168	153		151
4. kanal			130					86							
5. kanal		127							86	86				103	
6. kanal	88		88	107	129	127	129					105	104		127
7. kanal								84							
8. kanal									99	88				76	
9. kanal	89	116			77	76	74					64	115		74
10. kanal			115	93				101	88	74				87	
11. kanal		21			136	136	138								111
12. kanal	94	187	101	95				95	95	98		95	95	96	
13. kanal	97		97	98	95	97	96	96	95	95		95	---	94	95

Tabela 27: Dolžina prekinitve podatkovnega toka v neobremenjenem Eduroam omrežju v času iskanj.

Ponovitev	1	2	3	4	5	6	7	8
Čas prehoda	600	121	793	578	215	427	790	229
Dolžina prekinitve podatkovnega toka	615	136	808	597	234	446	807	243

Ponovitev	9	10	11	12	13	14	15
Čas prehoda	204	181		340	379	834	159
Dolžina prekinitve podatkovnega toka	220	1612		31141	493	847	176

Tabela 28: Časi prehodov v neobremenjenem Eduroam omrežju merjeni preko gonilnika (1. vrstica) ter dolžina prekinitve podatkovnega toka v času prehoda (2. vrstica).

Prehodi v obremenjenem Eduroam omrežju

Vse vrednosti so podane v milisekundah.

Ponovitev	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
1. kanal	40	41	40	40	40		40	40	40	40	40	40		40	40
2. kanal	40	40	40	14	15		40	14	40	40	13	40		40	13
3. kanal	16	40	14	40	40		13	40	16	15	40	17		40	40
4. kanal	37	40	40	15	14		18	40	40	40	40	40		40	40
5. kanal	40	40	15	40	40		40	40	41	40	40	40		40	15
6. kanal	40	40	40	40	14		40	40	40	40	40	13		14	40
7. kanal	40	40	41	40	40		40	40	40	40	13	40		40	40
8. kanal	40	40	40	40	40		40	40	40	40	40	40		40	13
9. kanal	15	40	40	14	13		40	15	13	18	15	40		40	40
10. kanal	40	40	42	40	40		40	40	40	40	40	41		40	40
11. kanal	40	40	40	40	40		40	40	40	40	40	40		40	40
12. kanal	124	90	90	90	90		90	90	90	90	90	90		90	90
13. kanal	123	90	90	90	90		90	90	90	90	90	90		90	90

Tabela 29: Časi iskanj v obremenjenem Eduroam omrežju merjeni preko gonilnika.

Ponovitev	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
1. kanal												46			
2. kanal		171		161	117		161	143	188	104	184	113		137	163
3. kanal															
4. kanal										128				87	
5. kanal		74			101			16				100			
6. kanal				88			127	90	89		101			104	
7. kanal		88								88					
8. kanal				101	141			103	101			131			300
9. kanal		136					87			107	114			127	
10. kanal															
11. kanal				137			44	54	50			47			
12. kanal		98			97		95	98	192	101	97	98		97	98
13. kanal		96		95	110		---	97		96	96	96		96	97

Tabela 30: Dolžina prekinitve podatkovnega toka v obremenjenem Eduroam omrežju v času iskanj.

Ponovitev	1	2	3	4	5	6	7	8
Čas prehoda	13408	250	3768	683	414		549	3294
Dolžina prekinitve podatkovnega toka	45608		69636	768	435		694	3339

Ponovitev	9	10	11	12	13	14	15
Čas prehoda	124	180	895	1018		1788	219
Dolžina prekinitve podatkovnega toka	171	222	917	1063		1837	269

Tabela 31: Časi prehodov v obremenjenem Eduroam omrežju merjeni preko gonilnika (1. vrstica) ter dolžina prekinitve podatkovnega toka v času prehoda (2. vrstica).

Seznam tabel

Tabela 1: Statistična analiza rezultatov pri prehodih v neobremenjenem omrežju brez šifriranja in generiranega prometa. 37

Tabela 2: Statistična analiza rezultatov pri prehodih v neobremenjenem omrežju brez šifriranja. 37

Tabela 3: Statistična analiza rezultatov pri prehodih v neobremenjenem omrežju brez šifriranja z dostopno točko na pasivnem kanalu. 38

Tabela 4: Statistična analiza rezultatov pri prehodih v neobremenjenem omrežju z WPA šifriranjem. 39

Tabela 5: Statistična analiza rezultatov pri prehodih v lahno obremenjenem omrežju z WPA šifriranjem. 39

Tabela 6: Statistična analiza rezultatov pri prehodih v močno obremenjenem omrežju z WPA šifriranjem. 40

Tabela 7: Statistična analiza rezultatov pri prehodih v neobremenjenem Eduroam omrežju. 40

Tabela 8: Statistična analiza rezultatov pri prehodih v obremenjenem Eduroam omrežju. 41

Tabela 9: Časi iskanj v neobremenjenem omrežju brez šifriranja in generiranega prometa merjeni preko gonilnika. 45

Tabela 10: Časi prehodov v neobremenjenem omrežju brez šifriranja in generiranega prometa merjeni preko gonilnika. 45

Tabela 11: Časi iskanj v neobremenjenem omrežju brez šifriranja merjeni preko gonilnika. 46

Tabela 12: Dolžina prekinitve podatkovnega toka v neobremenjenem omrežju brez šifriranja v času iskanj. 46

Tabela 13: Časi prehodov v neobremenjenem omrežju brez šifriranja, merjeni preko gonilnika (1. vrstica) ter dolžina prekinitve podatkovnega toka v času prehoda (2. vrstica). 46

Tabela 14: Časi iskanj v neobremenjenem omrežju brez šifriranja z dostopno točko na pasivnem kanalu merjeni preko gonilnika. 47

Tabela 15: Dolžina prekinitve podatkovnega toka v neobremenjenem omrežju brez šifriranja z dostopno točko na pasivnem kanalu v času iskanj. 47

Tabela 16: Časi prehodov v neobremenjenem omrežju brez šifriranja z dostopno točko na pasivnem kanalu merjeni preko gonilnika (1. vrstica) ter dolžina prekinitve podatkovnega toka v času prehoda (2. vrstica). 47

Tabela 17: Časi iskanj v neobremenjenem omrežju z WPA šifriranjem merjeni preko gonilnika. 48

Tabela 18: dolžina prekinitve podatkovnega toka v neobremenjenem omrežju z WPA šifriranjem v času iskanj. 48

Tabela 19: Časi prehodov v neobremenjenem omrežju z WPA šifriranjem, merjeni preko gonilnika (1. vrstica) ter dolžina prekinitve podatkovnega toka v času prehoda (2. vrstica). . 48

Tabela 20: Časi iskanj v nizko obremenjenem omrežju z WPA šifriranjem merjeni preko gonilnika..... 49

Tabela 21: Dolžina prekinitve podatkovnega toka v nizko obremenjenem omrežju z WPA šifriranjem v času iskanj. 49

Tabela 22: Časi prehodov v lahno obremenjenem omrežju z WPA šifriranjem merjeni preko gonilnika (1. vrstica) ter dolžina prekinitve podatkovnega toka v času prehoda (2. vrstica). . 49

Tabela 23: Časi iskanj v močno obremenjenem omrežju z WPA šifriranjem merjeni preko gonilnika..... 50

Tabela 24: Dolžina prekinitve podatkovnega toka v močno obremenjenem omrežju z WPA šifriranjem v času iskanj. 50

Tabela 25: Časi prehodov v močno obremenjenem omrežju z WPA šifriranjem merjeni preko gonilnika (1. vrstica) ter dolžina prekinitve podatkovnega toka v času prehoda (2. vrstica). . 50

Tabela 26: Časi iskanj v neobremenjenem Eduroam omrežju merjeni preko gonilnika. 51

Tabela 27: Dolžina prekinitve podatkovnega toka v neobremenjenem Eduroam omrežju v času iskanj. 51

Tabela 28: Časi prehodov v neobremenjenem Eduroam omrežju merjeni preko gonilnika (1. vrstica) ter dolžina prekinitve podatkovnega toka v času prehoda (2. vrstica). 51

Tabela 29: Časi iskanj v obremenjenem Eduroam omrežju merjeni preko gonilnika. 52

Tabela 30: Dolžina prekinitve podatkovnega toka v obremenjenem Eduroam omrežju v času iskanj. 52

Tabela 31: Časi prehodov v obremenjenem Eduroam omrežju merjeni preko gonilnika (1. vrstica) ter dolžina prekinitve podatkovnega toka v času prehoda (2. vrstica). 52

Seznam slik

Slika 1: ISO/OSI model. 3
Slika 2: Prekrivanje kanalov na 2.4 GHz frekvenčnem področju. 4
Slika 3: Decentralizirano (ad-hoc) omrežje. 5
Slika 4: Centralizirano brezžično omrežje. 5
Slika 5: Primer razširjenega brezžičnega omrežja. 6
Slika 6: Prikaz različnih medokvirskih časov. 10
Slika 7: Prikaz fizične strukture okvirja. 11
Slika 8: Periodično pošiljanje svetilnih okvirjev. 14
Slika 9: Prikaz iskanja z raziskovalnimi zahtevami in odgovori 15
Slika 10: Primer asociacije odjemalca z dostopno točko. 20
Slika 11: Primer prenosa asociacije (reasociacija) na novo dostopno točko. 21
Slika 12: Primer avtentifikacije odjemalca (prosilec) po standardu IEEE 802.1X. 21
Slika 13: Primer prehoda na novo dostopno točko. 23
Slika 14: Topologija testnega omrežja. 26
Slika 15: Skica fizične postavitve testnega omrežja. 27
Slika 16: Shema testnega omrežja z dodanim obremenjevalcem ter spletnim strežnikom. Obremenjene povezave so označene z rdečo barvo. 28
Slika 17: Poenostavljena shema omrežja Eduroam na Fakulteti za računalništvo in informatiko v Ljubljani. 29
Slika 18: Zaslonska slika programa CommView for WiFi. 32
Slika 19: Zaslonska slika programa Wireshark. 33

Seznam uporabljene literature in virov

Knjige:

[1] M. S. Gast, 802.11 Wireless Networks: The Definitive Guide, Second Edition; O'Reilly Media, 2005.

[2] IEEE, IEEE Standard for Information technology - Telecommunications and information exchange between systems - Local and metropolitan area networks - Specific requirements, Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications; New York, 2007.

Spletne strani (dostopne v času pisanja diplomskega dela, oktober 2009 – marec 2010):

[3] (2010) Standard IEEE 802.11
http://en.wikipedia.org/wiki/IEEE_802.11
http://en.wikipedia.org/wiki/IEEE_802.11g-2003
http://en.wikipedia.org/wiki/Wireless_network
http://en.wikipedia.org/wiki/Wireless_ad_hoc_network
http://en.wikipedia.org/wiki/Wireless_LAN

[4] (2010) Standard IEEE 802.11r
http://en.wikipedia.org/wiki/IEEE_802.11r

[5] (2010) Standard IEEE 802.1X
http://en.wikipedia.org/wiki/IEEE_802.1X

[6] (2010) ISM band
http://en.wikipedia.org/wiki/ISM_band

[7] (2006) 802.11 Wireless LAN protocol
http://protocols.netlab.uky.edu/~calvert/classes/571/lectureslides/WiFi.pdf

[8] (2009) D-Scan: Enabling Fast and Smooth Handoffs in AP-dense 802.11 Wireless Networks
http://www.cse.ohio-state.edu/~xuan/papers/09_infocom_mini_txjx.pdf

[9] (2010) Wolf Paulus' Web Journal: La Fonera (FON2100) Hardware Details
http://wolfpaulus.com/journal/embedded/fonera1.html

[10] (2004) pktgen the linux packet generator
ftp://robur.slu.se/pub/Linux/net-development/pktgen-testing/pktgen_paper.pdf