MEDNARODNA PODIPLOMSKA ŠOLA JOŽEFA STEFANA
JOŽEF STEFAN INTERNATIONAL POSTGRADUATE SCHOOL

ROK LIBNIK

PREDAJA ZVEZE V HETEROGENIH OMREŽJIH Z UPORABO SIP PROTOKOLA

DOKTORSKA DISERTACIJA

LJUBLJANA, SEPTEMBER 2010

PREDAJA ZVEZE V HETEROGENIH OMREŽJIH Z UPORABO SIP PROTOKOLA

Doktorska disertacija
Mednarodna podiplomska šola Jožefa Stefana
Ljubljana, Slovenija, september 2010

Mentor: *doc. dr. Aleš Švigelj*

Somentor: *prof. dr. Gorazd Kandus*

Komisija za oceno doktorske disertacije:

doc. dr. Mihael Mohorčič, Odsek za komunikacijske sisteme, Institut "Jožef Stefan", Ljubljana

prof. dr. Marko Jagodič, Omersova 62, Ljubljana

doc. dr. Aleš Švigelj, Odsek za komunikacijske sisteme, Institut "Jožef Stefan", Ljubljana

Rok Libnik

PREDAJA ZVEZE V HETEROGENIH OMREŽJIH Z UPORABO SIP PROTOKOLA

Doktorska disertacija

HANDOVER IN HETEROGENEOUS NETWORKS USING SIP PROTOCOL

Doctoral Dissertation

Mentor: doc. dr. Aleš Švigelj

Somentor: prof. dr. Gorazd Kandus

September 2010

MEDNARODNA PODIPLOMSKA ŠOLA JOŽEFA STEFANA
JOŽEF STEFAN INTERNATIONAL POSTGRADUATE SCHOOL
Ljubljana, Slovenija

Nataliji.

Kazalo

Povzetek

Danes smo priča zelo hitremu razvoju telekomunikacijskih omrežij in storitev. Še posebej je v zadnjih letih zelo napredoval razvoj brezžičnih omrežij. Tako se lahko na različnih tržiščih srečamo z različnimi tehnologijami, ki omogočajo brezžično komuniciranje. Med brezžičnimi omrežji so v zadnjih desetih letih še posebej hitro napredovala mobilna omrežja. Prvi dve generaciji mobilnih omrežij (NMT in GSM) sta bili razviti predvsem za ponujanje govornih storitev, tretja generacija (UMTS) pa že prinaša tudi hitrejše prenose podatkov. Podatke lahko uporabniki prenašajo tudi prek drugih brezžičnih tehnologij, med katerimi sta najbolj razširjena Bluetooth in WLAN, ki običajno uporabljata fiksno omrežje za dostop do hrbteničnega omrežja, kjer nove tehnologije kot sta xDSL in FTTx omogočajo uporabnikom višje hitrosti za dostop do interneta.

Predvsem pri operaterjih, ki ponujajo storitve na fiksnih povezavah, lahko zasledimo pospešeno migracijo hrbteničnih omrežij na IP protokol. Sledijo jim tudi mobilni operaterji. Tako lahko že govorimo tudi o novih heterogenih omrežjih, ki bodo združevala več dostopovnih tehnologij in bodo uporabljala IP hrbtenično omrežje.

Uporabniki imajo na voljo vse več storitev, ki jih bodo želeli uporabljati na kateremkoli omrežju. Danes so že na voljo tehnike, ki omogočajo prehajanje med različnimi segmenti določenega omrežja. V prihodnje pa bodo morali operaterji omogočati tudi prehode med različnimi dostopovnimi omrežji. Tehnike, ki omogočajo uporabnikom prehajanje med različnimi segmenti istega omrežja ali med različnimi omrežji, imenujemo upravljanje z mobilnostjo.

Upravljanje z mobilnostjo v homogenih omrežjih, torej v omrežjih, ki uporabljajo enako tehnologijo, je danes že zelo dobro rešeno in tudi dobro deluje. Heterogena omrežja prihodnosti pa bodo podpirala več različnih tehnologij, zato bo potrebno za izvajanje predaj zvez razviti terminale in storitve, ki bodo sposobni nezaznavno prehajati med posameznimi dostopovnimi omrežji.

Predaja zveze se lahko izvaja na različnih slojih OSI modela, ki smo jih med seboj primerjali. Pri našem delu smo se osredotočali predvsem na rešitve, ki bi jih lahko brez večjih posegov vpeljali v obstoječe omrežje operaterja. Protokol SIP, ki deluje na aplikacijskem sloju, je že vpeljan v večini operaterskih okolij in je bil tudi izbran kot glavni signalizacijski protokol v IMS arhitekturi. Ker uporablja aplikacijski sloj, je SIP neodvisen od dostopovnih tehnologij, kar omogoča uporabo tudi pri gostovanjih v omrežjih operaterja, ki ne ponuja SIP storitev, saj se omrežje, v katerem uporabnik gostuje, uporablja zgolj za dostop do aplikacijskega strežnika v domačem omrežju. Zato smo izbrali SIP protokol za nadaljnje delo in razvoj novih postopkov za upravljanje z mobilnostjo v heterogenih omrežjih.

Z migracijo na popolnoma IP omrežja, se vsi podatkovni tokovi združujejo v enem omrežju, zaradi česar lahko ena storitev vpliva na drugo. To sicer ni problematično za aplikacije, ki nimajo velikih zahtev glede kakovosti storitve (QoS), kot je npr. brskanje po internetu. Lahko pa ima negativen vpliv na časovno kritične aplikacije (npr. govorne in video komunikacije). Takšne aplikacije zahtevajo vpeljavo mehanizmov za zagotavljanje ustreznega nivoja QoS, če hočejo operaterji zagotavljati ustrezen nivo uporabniške izkušnje (QoE). Pri našem delu smo za aplikacijo izbrali IP telefonijo, ki jo lahko uvrstimo med časovno najbolj kritične aplikacije.

Z uvedbo IP telefonije morajo operaterji zaradi zagotavljanja varnostno-regulatornih zahtev v svoja omrežja vpeljati elemente, ki vplivajo na arhitekturo rešitve. Običajno v svoje omrežje implementirajo mejni krmilnik sej (SBC). Vpeljava elementa SBC v omrežje operaterja lahko vpliva na omrežno arhitekturo, tako da ta ni več v skladu z osnovnimi principi SIP arhitekture. SBC, ki podpira SIP protokol, običajno upravlja tako s signalizacijo kot tudi z medijskim (RTP) tokom.

Za aplikacije, ki tečejo v realnem času, kot je IP telefonija, je še posebej pomembno, da uporabljeno omrežje lahko zagotavlja želen nivo QoS. To je še posebej pomembno pri prehajanju med heterogenimi omrežji, kjer najbolj kritičen del procesa predaje zveze predstavlja odločitev, kdaj in če sploh predati zvezo na drugo omrežje. Če bi bila odločitev za predajo zveze odvisna zgolj od razmerja SNR (kar je običajno v homogenih omrežjih), bi uporabniški terminal izvedel predajo na ciljno omrežje vedno, ko bi razmerje SNR preseglo določen prag. Kadar bi se zgodilo, da bi bila dostopovna povezava ciljnega omrežja med postopkom predaje zveze preobremenjena, bi lahko uporabnik zaznal veliko poslabšanje delovanja storitve

ali pa je sploh ne bi mogel več uporabljati. Zato smo razvili nov postopek CAHP, s katerim smo dosegli učinkovitejše izvajanje predaje zvez, saj smo pri odločitvi za predajo upoštevali tudi stopnjo zasedenosti ciljnega omrežja. Postopek deluje med katerima koli dostopovnima omrežjema. Pri našem delu smo zaradi lažje predstavitve delovanja postopka CAHP izbrali omrežji WLAN in HSPA, med katerima smo izvajali predaje zvez. Pri tem smo predpostavili, da se lahko preobremenitve pojavijo zgolj v WLAN omrežju.

Postopek CAHP vsebuje dva algoritma: *Pre-probe* in *Mid-probe* algoritem. Prvi je namenjen testiranju obremenjenosti WLAN dostopovnega omrežja pred predajo zveze in se začne izvajati, ko je izpolnjen osnovni pogoj, t.j. primerno razmerje SNR. Ker se lastnosti WLAN omrežja lahko spremenijo tudi med uporabo tega omrežja, smo definirali drugi algoritem, imenovan *Mid-probe* algoritem, s katerimi preverjamo obremenjenost omrežja tudi po predaji na WLAN omrežje. Postopek CAHP vsebuje več parametrov, med katerimi imata na učinkovitost postopka zelo velik vpliv vrednosti parametrov T_{pre} in T_{mid}, s katerima določamo preiodo pošiljanja sporočil `SIP pre_PROBE` ali `SIP mid_PROBE`, saj neposredno vplivata na hitrost zaznavanja obremenitve omrežja in obremenitev omrežnih elementov. Pri našem postopku smo definirali dva načina za nastavljanje teh dveh parametrov. Pri prvem, imenovanem CAHP-C, parametra nastavljamo na konstantno vrednost. To pomeni, da bosta ves čas simulacije vrednosti parametrov T_{pre} in T_{mid} konstantna in bomo za oba uporabljali isto prednastavljeno vrednost. Pri drugem, imenovanem CAHP-A, pa se parametra adaptivno spreminjata. To pomeni, da vrednosti parametrov T_{pre} in T_{mid} nastavljamo v odvisnosti od trenutne obremenjenosti WLAN omrežja.

Da bi analizirali in ovrednotili delovanje postopka CAHP, smo v simulacijskem orodju OPNET izdelali simulacijski model. OPNET že omogoča simuliranje SIP telefonije, vendar ne podpira predaj zvez z uporabo SIP protokola. Zato smo morali za izdelavo simulacijskega modela, s katerim smo analizirali in ovrednotili postopek CAHP, razviti nekaj dodatnih funkcionalnosti in prilagoditev.

Za ovrednotenje delovanja predlaganega postopka CAHP smo definirali več scenarijev, ki smo jih razdelili v tri simulacijske sklope. V prvem simulacijskem sklopu smo izvedli referenčni scenarij brez uporabe postopka CAHP, s katerim smo pokazali, da lahko pride v obremenjenih omrežjih do velike degradacije kakovosti storitve, če odločitev za predajo temelji zgolj na razmerju SNR. Veliko javnih brezžičnih omrežij, ki so na voljo uporabnikom, omogoča priključitev več uporabnikov, kar lahko ima za posledico občasne preobremenitve omrežja. Uporaba tovrstnih omrežij je največkrat brezplačna in tako zanimiva tudi za uporabo IP telefonije, vendar pa običajno ne uporablja mehanizmov za zagotavljanje kakovosti časovno kritičnim aplikacijam. Iz rezultatov simulacije referenčnega scenarija je razvidno, da se je kakovost storitve ob preobremenitvah zelo zmanjšala. Zakasnitve so narasle tudi nad 1 s, kar je imelo za posledico, da je bila storitev IP telefonije za uporabnika neuporabna. Zato je v bolj obremenjenih omrežjih nujna uporaba mehanizmov za ugotavljanje obremenjenosti ciljnega omrežja. V drugem simulacijskem sklopu smo izvedli ovrednotenje postopka CAHP-C. Ugotovili smo, da lahko s postopkom CAHP-C dosegamo veliko boljše rezultate kot pri referenčnem scenariju. Vendar pa je bilo za doseganje najboljših rezultatov potrebnih zelo veliko dodatnih signalizacijskih sporočil za preverjanje obremenjenosti, kar bi lahko povzročilo težave v operaterskih okoljih, predvsem na elementu SBC. Da bi zmanjšali siganlizacijsko režijo, smo definirali postopek CAHP-A. Učinkovitost postopka CAHP-A smo preverili na več scenarijih, ki jih podajamo v tretjem simulacijskem sklopu. Med scenariji drugega in tretjega simulacijskega sklopa smo poiskali scenarije z optimalnimi parametri na štiri različne načine. Pri vseh se je kot najprimernejši pokazal postopek CAHP-A.

Ker smo v postopku uporabili SIP protokol za pošiljanje sporočil, s katerimi smo preverjali obremenjenost omrežja, je takšen pristop popolnoma neodvisen od nižjih slojev (transportnega, omrežnega, povezavnega in fizičnega). Zaradi neodvisnosti od protokolov, uporabljenih na nižjih slojih, je takšno rešitev, v kolikor operater že ponuja storitev SIP telefonije, enostavno vpeljati v obstoječe operatersko okolje, saj SBC in terminali že podpirajo SIP in jih zato ni potrebno prilagoditi. Ob uvedbi postopka CAHP v omrežjih operaterja bi bilo potrebno zgolj nadgraditi programsko opremo na uporabniških terminalih ter na elementu SBC pri operaterju. Zaradi uporabe SIP protokola lahko v odločitev vključimo tudi druge podatke, ki jih posreduje SIP strežnik (npr. nastavitve uporabnika). Če bi za preverjanje obremenjenosti omrežja uporabili nižje sloje, bi to pomenilo večji poseg v aplikacijo oz. razvoj ločene, povsem nove aplikacije. Izvajanje meritev zakasnitve paketov z drugimi protokoli bi onemogočale tudi varnostne nastavitve na SBC, kjer je običajno dovoljen promet zgolj na vrata, ki jih uporabljata protokola SIP in RTP. Podobne varnostne omejitve veljajo tudi za LAN omrežja pri uporabniku.

Zaključimo lahko, da z upoštevanjem v disertaciji predstavljenih izvirnih prispevkov bistveno izboljšamo nivo QoE med predajami v heterogenih omrežjih in pri tem minimiziramo obremenitev naprav v operaterjevem okolju.

Abstract

Over the last decade we have been witnessing rapid development of telecommunication networks and services, in particular in the filed of new wireless network technologies. On different markets users are able to communicate using different wireless technologies. The first two generation of mobile networks (i.e. NMT and GSM) were developed to provide voice services, while with the third generation (UMTS) the ability for faster data transfer was enabled. Data can be transmitted also over other wireless technologies, among which the most popular are Bluetooth and WLAN that are using fixed line to access to core network. On fixed access with evolving xDSL and FTTx technologies, operators can offer higher and higher data rates.

Operators, that are offering services on fixed lines, are migrating fast to all IP core networks. Mobile operators are following them. As a result of such migration, networks will become more heterogeneous, combining different access technologies connected to IP core network.

The availability of different services is increasing and users will have need to use them using any network. Today there are techniques available that enable movement between different segments of a single network. In the future, operators will need to enable movement also between different access technologies. Techniques that support user movement within and between different networks are defined as mobility management techniques.

Mobility management in homogeneous networks (i.e. networks that are using same technology), is already available today. Heterogeneous networks of the future will support different technologies. Thus, new terminals and services are to be developed in order to provide seamless movement between different access networks.

From the point of view of protocol implementation, handover in heterogeneous network can be performed at different OSI layers and this has been addressed in several studies. In our work we focused on solutions that can be deployed easily in a real operator environment. SIP is used today in many operator environments and has been selected as the primary signalling protocol in IMS (IP Multimedia Subsystem) networks. As it runs on the application layer, SIP is independent of access technologies, which enables roaming in the network of an operator that is not offering SIP services, as the network, in which the user roams, is used just to access the application server in home network. Thus, we choose SIP protocol for development of new procedures for mobility management in heterogeneous networks.

With migration to all-IP networks, all data streams are merged in a single core network, which can lead to situation, where services have effect on each other. This is not problematic for applications that do not have high requirements for quality of service (QoS), such is web browsing. On the other hand it can have major impact on time critical application such as voice and video. Such applications require implementation of mechanisms that provide sufficient level of QoS if operators want to ensure appropriate level of user experience (QoE). In our work we selected IP telephony as the application, which is one of the most time critical applications.

When implementing IP telephony, operators are obliged to provide some additional functionality that can change the architecture of the IP telephony solution, due to regulatory requirements. Usually they add a Session Border Controller (SBC) to their network. By adding SBC to the architecture, some practices can be in conflict with SIP architectural principles. SIP-based SBCs typically handle both signalling and media.

When providing seamless handover in heterogeneous networks, for real-time applications in particular, the ability to provide appropriate QoS in the target network is crucial. The most critical phase of handover process is handover decision. If the decision for handover is made based only on SNR measurement (which is usually the case in homogeneous networks), the user terminal would always handover to another network when the predefined SNR threshold is exceeded. In the case of congestion in the target access network, the service can be significantly degraded or could become unusable. Thus, we developed new procedure named CAHP, which enables to perform handover efficiently, taking into account also the congestion status of the target network. The procedure works with any two networks. In order to present the proposed procedure clearly, we choose WLAN and HSPA network, between which the handovers were made. We assumed that congestion can happen only in WLAN network.

The CAHP procedure consists of two algorithms: *Pre-probe* and *Mid-probe* algorithm. The first is used for testing WLAN network prior handover and it starts when SNR, which stays as prerequisite for handover, exceeds predefined threshold. As network capabilities can change also during its use, we defined the second algorithm, named *Mid-probe*, which is used for congestion testing after handover to WLAN. Among all parameters used in the proposed CAHP procedure the most important are T_{pre} and T_{mid}. Those two parameters need to be set carefully as they affect the level of signalling overhead and speed of detecting potential congestion. We defined two methods of setting those two parameters. In the first, named CAHP-C, the parameters are set on constant value. This means that values of T_{pre} and T_{mid} parameters will stay constant during simulation, equal for both parameters. In the second, named CAHP-A, the parameters are set adaptively, which means that their value changes during the simulation according to current utilisation of WLAN network.

In order to analyze and evaluate the proposed handover procedure, we developed a simulation model of a telecommunication system, which was developed using the simulation tool OPNET Modeler. As we decided for handover on the application layer, which is not supported by OPNET, we customized some pre-defined process models that incorporate SIP procedures.

In order to evaluate the CAHP procedure, we prepared several scenarios, divided in three sets. The first simulation set was used as a reference, where CAHP procedure was not used. With results of that set we showed that in unreliable network significant degradation of service could happen if the decision is made based on SNR ratio only. Such situation can happen in public networks that are usually used by more users, which can lead to congestions in the network. Usage of those networks is mainly free of charge and thus attractive also for IP telephony service. The problem arises as such networks do not support QoS mechanisms for time critical applications. The results of the first set of simulation show, that QoS of IP telephony service was degraded when the target networks became congested and measured delays were above 1 s, which is totally unacceptable for real time applications. Thus, new mechanisms need to be implemented to test congestion status of target networks. In the second simulation set we evaluated CAHP-C procedure and show that the results were much better than in the reference scenario. However for getting the best results a lot of signalization messages for congestion testing was exchanged, which could led to an overload on SBCs. To lower the signalization overhead, we defined CAHP-A procedure. Its evaluation was done in the third simulation set. Among scenarios in the second and third simulation set we were looking for scenario with optimal parameters on four different ways. All showed that the CAHP-A procedure was more appropriate.

In proposed procedure we used SIP protocol for sending messages, by which the congestion status of network was tested. Such approach is completely independent from lower layers (i.e. transport, network, connection and physical). Due to independence from protocols used in lower layers, operators, if they are already offering SIP telephony, easily deploy our procedure to they network as SBCs and IP terminals already support SIP protocol. By implementation of CAHP procedure only software upgrade is needed on SBCs and user terminals. Besides this in our procedure it is also possible to include other parameters (settings of the user) when making the decision for handover. If we would use lower layers for congestion testing, this would lead into bigger changes of the application or even new application development. Congestion testing with other protocols could be limited also with safety settings on SBC, where usually only SIP and RTP traffic is allowed. Similar security limitations can be an issue also in the LAN network in the user's environment.

We can conclude, that by using solutions presented in this dissertation, the QoE can be significantly improved when making handover in heterogeneous networks while the load on operators equipment is minimized.

Seznam kratic

Kratica	Angleški izraz	Slovenski izraz
3G	3rd Generation	tretja generacija
AP	access point	dostopovna točka
BER	bit error rate	delež napačnih bitov
BSSID	base station session ID	identifikator bazne postaje
CAHP	congestion aware handover procedure	postopek za izvajanje predaje zveze z zaznavanjem obremenitev
CDMA	code division multiple access	kodno porazdeljeni sodostop
CH	correspondent host	korespondenčni gostitelj
CN	correspondent node	korespondenčno vozlišče
CSV	comma separated values	vrednosti ločene z vejico
DAR	dynamic alternate routing	dinamično alternativno usmerjanje
DES	discrete event simulation	diskretno orientirane simulacije
DHCP	dynamic host configuration protocol	protokol za dinamično konfiguriranje gostiteljev
DoS	denial of service	ohromitev storitve
FA	foreign agent	tuji agent
FS	fixed server	fiksnim strežnikom
FSM	finite state machine	avtomat končnih stanj
FTP	file transfer protocol	protokol za prenos datotek
FTTx	fiber to the »x«	optično vlakno do "x"
GPRS	general packet radio service	splošna paketna radijska storitev
GPS	global positioning system	sistem za pozicioniranje
GSM	global system for mobile communication	globalni sistem mobilne komunikacije
HA	home agent	domači agent
HIA	hybrid interworking architecture	hibridna arhitektura za medsebojno delovanje
HSPA	high-speed packet access	hitri paketni dostop
HTTP	hypertext transfer protocol	protokol za prenos hiperteksta
IETF	internet engineering task force	delovna skupina za internetno tehniko
IMS	IP multimedia subsystem	IP multimedijski podsistem
IP	internet protocol	internetni protokol
ITU	international telecommunications union	mednarodna telekomunikacijska zveza
LAN	local area network	lokalno omrežje
MH	mobile host	mobilni gostitelj
MIP	mobile IP	mobilni IP

MMUSE	mobility management using sip extensions	upravljanje z mobilnostjo z uporabo razširljivosti sip
MN	mobile node	mobilno vozlišče
mSCTP	mobile SCTP	mobilni SCTP
NAT	network address translation	prevajanje omrežnih naslovov
NB	notebook	prenosni računalnik
nFA	new FA	novi FA
NMT	nordic mobile telephony	nordijska mobilna telefonija
oFA	old FA	stari FA
OSI	open system interconnection	medsebojno povezovanje odprtih sistemov
PC	personal computer	osebni računalnik
QoE	quality of experience	kakovost izkušnje
QoS	quality of service	kakovost storitve
RTP	real-time transport protocol	transportni protokol v realnem času
SBC	session border controller	mejni krmilnik seje
SCTP	stream control transmission protocol	protokol za krmiljenje prenosa pretokov
SDP	session description protocol	protokol za opis seje
SDR	software defined radio	programirljivi radio
SEMCS	sip enhanced mid-call scenario	izboljšan scenarij za mobilnost med klicem
SIP	session initiation protocol	protokol za zagon seje
SNR	signal-to-noise ratio	razmerje signal-šum
TCP	transmission control protocol	protokol za nadzor transporta
TDM	time division multiplexing	časovni multipleks
TTL	time-to-live	življenjska doba
UDP	user data protocol	uporabniški datagramski protokol
UMA	unlicensed mobile access	nelicenčen mobilni dostop
UMTS	universal mobile telecommunications system	univerzalni sistem za mobilno komunikacijo
URI	uniform resource identifier	enotni označevalnik vira
USB	universal serial bus	univerzalno serijsko vodilo
VoIP	voice over IP	govor po IP
WiMAX	worldwide interoperability for microwave access	svetovno združljivo delovanje pri mikrovalovnem dostopu
WLAN	wireless LAN	brezžični LAN
xDSL	digital subscriber line	digitalna naročniška linija

Seznam uporabljenih izrazov

Angleški izraz	Slovenski izraz
access point	dostopovna točka
agent discovery	iskanje agenta
anticipated handover	pričakovana predaja zveze
association	pridružitev
connection path	povezavna pot
downward vertical handover	vertikalna predaja zveze navzdol
dual homing	dvodomnost
dual mode terminal	dvozvrstni terminal
echo	odmev
end to end delay	zakasnitev paketov od konca do konca
error checking and correction	model za preverjanje in odpravljanje napak
error model	model za generiranje napak
hard handover	ostra predaja zveze
horizontal handover	horizontalna predaja
host table	tabela gostiteljev
hot spot	vroča točka
hub	vozlišče
interrupt	prekinitev
jitter	trepetanje zakasnitve paketov
jitter buffer	izravnalniki trepetanja zakasnitev paketov
mid call mobility	mobilnost med klicem
mobility agent	mobilni agent
multi homing	večdomnost
multimode operation	večzvrstna operacija
multimode terminal	večzvrstni terminal
outbound proxy	zunanji posredovalni strežnik
packet loss	izguba paketov
payload	koristna vsebina
point of attachment	povezavna točka
post registration method	metoda poregistracije
pre call mobility	mobilnost pred klicem
pre registration method	metoda predregistracije
proxy server	posredovalni strežnik
reconfigurability	prenastavljanje
redirect server	strežnik za preusmerjanje
registrar	registrator
router/neighbour discovery	odkrivanje sosednjih vozlišč

seed	začetni pogoj
single homing	enodomnost
single point of failure	kritična točka odpovedi
soft handover	mehka predaja zveze
source trigger	izvorno prožilo
spoofing	sleparjenje z naslovi
target network	ciljno omrežje
target trigger	ponorno prožilo
transcoding	prekodiranje
trigger	prožilec
unanticipated handover	nepričakovana predaja zveze
upward vertical handover	vertikalna predaja zveze navzgor
user agent	uporabniški agent
vertical handover	vertikalna predaja zveze
vertical handover agent	agent za vertikalno predajo zveze

Seznam uporabljenih simbolov

Simbol	Opis
T_{pre}	perioda pošiljanja `SIP pre_PROBE` sporočila
T_{mid}	perioda pošiljanja `SIP mid_PROBE` sporočila
D_{e2e}	zakasnitev paketov od konca do konca
T_{com}	čas kompresije
T_{pac}	čas paketizacije
D_{access}	zakasnitev dostopovnega omrežja
D_{core}	zakasnitev hrbteničnega omrežja
T_{depac}	čas depaketizacije
T_{decom}	čas dekompresije
Ro	vpliv razmerja SNR
Is	združuje vplive, ki se pojavijo bolj ali manj hkrati z govornim signalom (npr. kvantizacijski šum)
Id	vpliv zakasnitve in odbojev
Ie	vpliv opreme, ki ga povzročajo kodeki z nizko bitno hitrostjo
S_i	časovni žig RTP paketa i
$D_{i,j}$	čas med paketoma i in j
R_i	čas prihoda paketa i
A	pripravljenost uporabnikov za sprejem slabše kakovosti klica na račun možnosti izvedbe klice
T_i	trepeteanje zakasnitev paketa i
T_{SNR}	prag razmerja SNR
N_{pre}	število `SIP pre_PROBE` sporočil v skupini
T_{inter}	čas med dvema sporočiloma `SIP pre_PROBE` ali `SIP mid_PROBE` v skupini
D_{pre}	povprečno vrednost zakasnitve med terminalom MN in elementom SBC pri uporabi *Pre-probe* algoritma
D_i	izmerjena zakasnitev paketa v odgovoru na i-to `SIP pre_PROBE` sporočilo
T_d	prag zakasnitve
N_{mid}	število `SIP mid_PROBE` sporočil v skupini
D_{mid}	povprečno vrednost zakasnitve med terminalom MN in elementom SBC pri uporabi *Mid-probe* algoritma
D_j	izmerjena zakasnitev paketa v odgovoru na j-to `SIP mid_PROBE` sporočilo
T_{max}	maksimalno možno vrednost za T_{pre} in T_{mid}
D_{min}	minimalno zakasnitev paketov od konca do konca
D_{max}	največjo zakasnitev paketov, ki še ne povzroča degradacije storitve
NSO_i	normirana signalizacijska režija za scenarij i
nSM_i	število signalizacijskih sporočil scenarija i
nSM_{C1}	število signalizacijskih sporočil scenarija C-1
$NSTaT_i$	normiran simulacijski čas, ko je bila zakasnitev paketov nad 200 ms za scenarij i

$STaT_i$	simulacijski čas, ko je bila zakasnitev paketov nad 200 ms za scenarij i
$STaT_{C6}$	simulacijski čas, ko je bila zakasnitev paketov nad 200 ms za scenarij C-6

1 Uvod

Zahteve uporabnikov telekomunikacijskih storitev se iz dneva v dan povečujejo. Uporabniki si želijo dostopati do storitev prek različnih dostopovnih omrežij. Tem zahtevam morajo slediti tudi telekomunikacijski operaterji. Že pred leti je bilo jasno, da morajo operaterji, ki želijo obstati na trgu, čim bolj poenotiti svoja omrežja. Tako danes večina telekomunikacijskih operaterjev teži k enotnemu hrbteničnemu omrežju, ki (bo temeljil) temelji na IP protokolu. Vendar poenotenje tehnologije v hrbteničnem omrežju operaterjem še vedno ne omogoča dovolj velike odzivnosti na trgu, saj v veliki večini še vedno ločujejo storitve po posameznih dostopovnih tehnologijah. Poleg tega so običajno storitve in naročniki še vedno deljeni na mobilni in fiksni svet. Ob upoštevanju dejstva, da se število uporabnikov mobilnih tehnologij zelo hitro povečuje, se v zadnjem času kot ena izmed glavnih smernic na telekomunikacijskem trgu za nadaljnji razvoj kaže fiksno-mobilna konvergenca, ki bo omogočala združevanje storitev tako za mobilne kot fiksne naročnike.

Ker se število omrežij, prek katerih lahko uporabniki komunicirajo, zelo hitro povečuje, bo potrebno v prihodnosti zagotoviti neprekinjeno delovanje storitev pri prehodu med različnimi dostopovnimi tehnologijami. Še posebej pomembno je, da bo takšen prehod za uporabnika nezaznaven. Seveda to pomeni, da morajo imeti uporabniki na voljo terminale z več vmesniki. Proizvajalci terminalske opreme danes že proizvajajo terminale z več vmesniki, ki omogočajo povezovanje v trenutno najbolj razširjena omrežja. V prihodnje lahko pričakujemo, da bo število različnih vmesnikov v terminalih še naraščalo. Sledijo jim tudi operaterji, ki so že začeli s ponujanjem konvergenčnih storitev. British Telecom je bil prvi, ki je v letu 2005 ponudil nezaznaven prehod iz GSM omrežja na WLAN omrežje z uporabo pristopa UMA (*ang. Unlicensed Mobile Access*). Vendar pa bodo uporabniki želeli uporabljati katero koli aplikacijo na kateri koli dostopovni tehnologiji. Pri tem bo zelo pomembno, da se uporabnikova izkušnja med prehajanjem iz enega omrežja na drugega ne bo bistveno spreminjala. To še posebej velja za aplikacije, ki tečejo v realnem času, kot je npr. IP telefonija.

Danes je prehajanje med celicami v mobilnem omrežju že dobro rešeno in za uporabnika nezaznavno, saj gre za prehajanje znotraj enake dostopovne tehnologije. Pri prehajanju med različnimi segmenti današnjih mobilnih omrežij se kot prožilec za predajo zveze uporablja izključno moč signala. Ko moč pade pod določeno mejo, se izvrši predaja zveze na drugo bazno postajo. Odločitev za predajo zgolj na podlagi moči signala je v tem primeru dovolj, saj je omrežje popolnoma pod kontrolo operaterja. S prehodom na IP omrežja pa se po teh pretakajo podatki več aplikacij, ki se lahko med seboj razlikujejo po občutljivosti na prometne obremenitve. Preobremenjeno omrežje lahko močno vpliva na nivo kakovosti storitve, še posebej pri aplikacijah, ki tečejo v realnem času. V primeru, da je na enem dostopovnem omrežju (pre)več uporabnikov, ki uporabljajo različne aplikacije, lahko storitve negativno vplivajo druga na drugo, kar ima za posledico, da odločitev za predajo na podlagi zgolj moči signala ne bo vedno primerna. Potrebno bo ugotoviti, katero izmed omrežij, ki so v odločenem trenutku uporabniku na voljo, bo poleg zadostne moči signala omogočalo tudi zadostno kakovost storitve. Zato je potrebno definirati nove postopke, s katerimi bomo zagotovili nezaznavno prehajanje med različnimi omrežji brez prekinitve delovanja aplikacije.

Namen našega dela je bil izboljšati učinkovitost predaj zvez z uporabo SIP protokola med heterogenimi omrežji, ki uporabljajo IP protokol. Osnovni cilj raziskovanja je bil razvoj novih postopkov za izvajanje predaj zvez, ki bodo omogočali, da se kakovost uporabljene storitve med prehajanjem med različnimi omrežji ne bo zmanjšala, in bodo uporabni tudi za časovno kritične SIP aplikacije, kot sta na primer govor in video. V ta namen smo zgradili simulacijski model telekomunikacijskega omrežja, s pomočjo katerega smo preverili predlagane rešitve.

1.1 Organizacija doktorske disertacije

Pregled problematike heterogenih omrežij podajamo v drugem poglavju, v katerem opisujemo osnovne postopke predajanja zveze ter tudi zahteve za terminale, ki bodo omogočali uporabo storitev v tovrstnih omrežjih.

V tretjem poglavju podrobneje predstavljamo protokole, ki se uporabljajo za upravljanje z mobilnostjo. Osredotočili smo se na omrežni, transportni ter aplikacijski sloj in pri vsakem izbrali najznačilnejšega

predstavnika. Izvedli smo tudi primerjavo med njimi, na podlagi katere smo se odločili za nadaljnjo obravnavo upravljanja z mobilnostjo na aplikacijskem sloju z uporabo SIP protokola.

Med SIP aplikacijami smo pri našem delu izbrali IP telefonijo. Pogoje uporabe SIP telefonije v operaterskem okolju podajamo v četrtem poglavju. Najprej predstavljamo parametre, s katerimi merimo nivoja kakovosti storitve in uporabniške izkušnje. Nato predstavljamo tudi spremembe arhitekture, ki jih morajo operaterji narediti, da zadostijo varnostno-regulatornim zahtevam. Sledijo rezultati praktičnih poizkusov uporabe IP telefonije v različnih dostopovnih omrežjih.

V petem poglavju predstavljamo postopek CAHP, ki smo ga razvili za izboljšanje nivoja uporabnikove izkušnje ob prehajanju med heterogenimi omrežji. Poleg moči signala smo pri odločitvi za predajo zveze uporabili tudi podatek o trenutni obremenjenosti ciljnega omrežja. Obremenjenost preizkušamo z meritvami zakasnitev, ki jih lahko izvajamo na dva različna načina: CAHP-C, kjer smo vrednosti parametrov T_{pre} in T_{mid}, s katerima določamo preiodo pošiljanja sporočil `SIP pre_PROBE` ali `SIP mid_PROBE`, nastavljali na konstantne vrednosti, in CAHP-A, kjer smo vrednosti parametrov T_{pre} in T_{mid} nastavljali adaptivno v odvisnosti od trenutne obremenjenosti dostopovne povezave WLAN omrežja.

Razvoj simulacijskega modela predstavljamo v šestem poglavju, kjer podajamo tudi priporočljive korake pri razvoju novih postopkov. Predstavljamo tudi simulacijsko orodje, ki smo ga izbrali za izvajanje simulacij. Ker izbrano simulacijsko orodje ni podpiralo vseh želenih funkcionalnosti, smo morali nekatere razviti na novo in jih dodati orodju. Nato predstavljamo še arhitekturo in parametre simulacijskega modela ter rezultate verifikacije in ovrednotenja postopka CAHP.

V sedmem poglavju podajamo analizo in ovrednotenje rezultatov. Izvedli smo 52 scenarijev, ki smo jih razdelili v tri simulacijske sklope. V prvem simulacijskem sklopu smo izvedli simulacijo brez postopka CAHP, v drugem simulacijo s postopkom CAHP-C, v tretjem pa rezultate simulacij, kjer smo uporabili postopek CAHP-A. Med rezultati scenarijev drugega in tretjega simulacijskega sklopa smo poiskali scenarije z optimalnimi parametri glede na različne kriterije.

1.2 Prispevki doktorske disertacije

Doktorska disertacija obravnava problematiko nezaznavnega predajanja zvez med različnimi dostopovnimi omrežji. Naš cilj je bil zagotoviti, da se uporabniška izkušnja med prehajanjem med različnimi dostopovnimi omrežji ne poslabša za razliko od referenčnega postopka, ki upošteva le razmerje SNR.

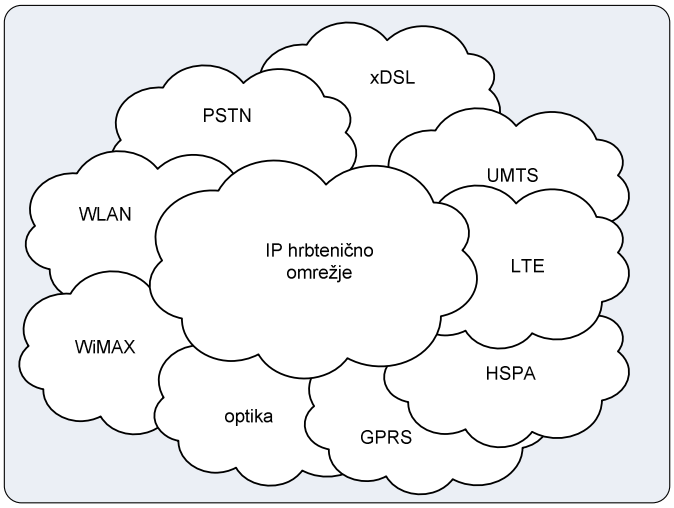
Doktorska disertacija vsebuje naslednje izvirni prispevke:

1. Razvoj izvirnega postopka za učinkovitejše izvajanje predaj zvez pri uporabi SIP aplikacij med heterogenimi omrežji. S pomočjo izboljšanega mehanizma lahko tudi uporabniki časovno kritičnih aplikacij in storitev nezaznavno prehajajo med IP omrežji z različnimi dostopovnimi tehnologijami (poglavje 5).
2. Predlog novih SIP sporočil za preverjanje obremenjenosti dostopovne povezave ciljnega omrežja (poglavje 5).
3. Predlog novega načina izvajanja meritev, s katerim frekvenco meritev obremenitve dostopovne povezave ciljnega omrežja adaptivno prilagajamo trenutni obremenjenosti omrežja (poglavje 5).
4. Razvoj simulacijskega modela na osnovi diskretno orientiranega simulacijskega orodja, ki omogoča: (i) simulacijo predajanja zvez s SIP protokolom, (ii) definicijo obremenjenosti omrežja, (iii) uporabo poljubnih vhodnih podatkov o gibanju moči signala pridobljenih z meritvami v realnem okolju ter (iv) prilagajanje delovanja predlaganega postopka prek vhodnih parametrov (poglavje 6).
5. Ovrednotenje in analiza predlaganega postopka CAHP z definicijo kriterijev za iskanje scenarija z optimalnimi parametri (poglavje 7).

2 Heterogena omrežja

Danes smo priča zelo hitremu razvoju telekomunikacij. V zadnjih letih je zelo napredoval razvoj, predvsem brezžičnih omrežij. Tako se lahko na različnih tržiščih srečamo z različnimi tehnologijami, ki omogočajo brezžično komuniciranje. Večina uporabnikov danes med brezžičnimi omrežji uporablja GSM omrežja, vse bolj se razširjajo tudi UMTS omrežja, ki ju uvrščamo med mobilna brezžična omrežja. Mobilna omrežja so v zadnjih desetletjih izjemno hitro napredovala. Prvi dve generaciji mobilnih omrežij (NMT in GSM) sta bili razviti predvsem za ponujanje govornih storitev, tretja generacija (UMTS) pa že prinaša tudi hitrejše prenose podatkov. Podatke lahko uporabniki prenašajo tudi prek drugih brezžičnih tehnologij, med katerimi sta najbolj razširjena Bluetooth in WLAN, ki običajno uporabljata fiksno omrežje za dostop do hrbteničnega omrežja, kjer nove tehnologije (xDSL in FTTx) omogočajo uporabnikom višje hitrosti za dostop do interneta.

Predvsem pri operaterjih, ki ponujajo storitve na žičnih povezavah, lahko zasledimo pospešeno migracijo hrbteničnih omrežij na IP protokol. Sledijo jim tudi mobilni operaterji. Tako lahko že govorimo tudi o novih heterogenih omrežjih, ki bodo združevala različne dostopovne tehnologije. Slika 1 prikazuje koncept heterogenega omrežja. Takšno omrežje sestavljajo tako žične kot tudi brezžične tehnologije, ki med seboj komunicirajo prek IP hrbteničnega omrežja.

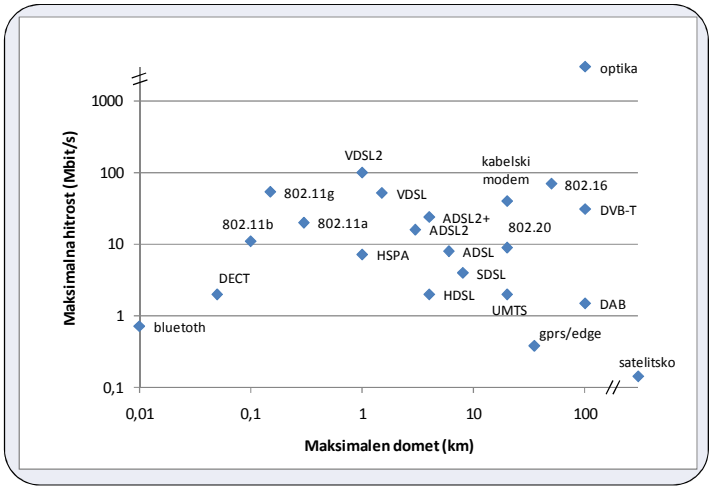


Slika 1: Koncept heterogenega omrežja

Glavne značilnosti heterogenih omrežij prihodnosti so (Siddiqui and Zeadally, 2006):

- dostopnost in uporaba storitev kadarkoli in od koderkoli;
- podpora večpredstavnostnim storitvam z nizkimi stroški transporta;
- združena dostopovna omrežja s skupnim IP hrbteničnim omrežjem;
- uporaba terminalskih naprav, ki bodo podpirale različne dostopovne tehnologije;
- podpora telekomunikacijskih, podatkovnih in večpredstavnostnih storitev;
- podpora storitev, ki si jih bodo lahko uporabniki nastavljali po svojih željah;
- podpora združenih dostopov do storitev, ki jih ponujajo različni ponudniki storitev.

Na sliki 2 je podanih nekaj tehnologij, ki bodo del heterogenih omrežij v prihodnosti, z njihovimi značilnostmi.



Slika 2: Pregled tehnologij z njihovimi glavnimi značilnostmi

Kot je razvidno iz slike 2, je danes na voljo že veliko različnih tehnologij tako za brezžične kot tudi žične komunikacije. Med brezžičnimi tehnologijami največje hitrosti (do 70 Mbit/s) dosegamo pri Wimax omrežjih (802.16). Z razdaljo praviloma hitrosti do uporabnika padajo. Največjo razdalje dosegamo pri satelitskih komunikacijah, vendar pa so hitrosti zelo nizke. Med prizemnimi tehnologijami največje razdalje dosegamo z Wimax in DVB-T tehnologijo. Brezžična omrežja se razlikujejo tudi po ceni. Najcenejše omrežje je WLAN omrežje, saj uporabniki potrebujejo zgolj dostop do interneta in dostopovno točko (*ang. access point*). Najdražja je uporaba satelitskih komunikacij. Z razvojem mobilnih omrežij pa se vse bolj širi tudi prenos podatkov prek teh omrežij. Z novimi tehnologijami, kot sta HSPA ali LTE, bo uporabnikom na voljo velika pasovna širina (do 100 Mbit/s).

Med žičnimi tehnologijami so cene v večini primerov nižje kot pri brezžičnih tehnologijah. Da bi lahko operaterji čim bolj izkoristili obstoječe bakreno omrežje, so se zelo razširile tehnologije xDSL. Zaradi vse večjih potreb po pasovni širini, ki jo zahtevajo nove multimedijske vsebine, kot je predvsem IP TV, pa se razširjajo tudi optična omrežja, ki do uporabnika omogočajo najvišje hitrosti.

Uporabniki imajo na voljo vse več storitev, ki jih bodo želeli uporabljati na kateremkoli omrežju. Danes so že na voljo tehnike, ki omogočajo prehajanje med različnimi segmenti določenega omrežja. V prihodnje pa bodo morali operaterji omogočati tudi prehode med različnimi dostopovnimi omrežji. Tehnike, ki to omogočajo, imenujemo upravljanje z mobilnostjo.

2.1 Upravljanje z mobilnostjo v heterogenih omrežjih

Uporabniki danes uporabljajo različne aplikacije, ki jih lahko razdelimo v dve skupini. V prvi so časovno kritične aplikacije, kot je npr. prenos govora ali videa. V drugi skupini pa so aplikacije, ki časovno niso tako kritične, kot je npr. brskanje po internetu. Pri uporabi slednjih ponovna vzpostavitev povezave ob prehodu v novo omrežje ni problematična s stališča zakasnitev. Na večje težave naletimo pri prvi skupini, kjer že krajša prekinitev zelo poslabša storitev. V prihodnosti bodo uporabniki pričakovali, da bodo lahko brez negativnega vpliva na delovanje uporabljene storitve prehajali med različnimi dostopovnimi tehnologijami, kar imenujemo predaja zveze[1].

Predaja zveze je proces, pri katerem (mobilni) terminal izvede preklop med trenutnim omrežjem in ciljnim omrežjem (*ang. target network*). Predaje zvez lahko razdelimo v dve skupini glede na to, med katerima vrstama omrežja se predaja izvede. V prvi skupini so predaje, ki se zgodijo znotraj omrežja, ki uporablja enotno dostopovno tehnologijo (npr. GSM). Tovrstne predaje imenujemo horizontalne predaje *(ang. horizontal handover)*, ki se zgodijo, ko premikajoči se uporabnik preide iz dometa ene bazne postaje v domet druge bazne postaje. V drugi skupini so predaje, kjer mobilni uporabnik preide iz enega omrežja v drugo omrežje, pri čemer omrežji uporabljata različne dostopovne tehnologije (npr. UMTS, LTE in WLAN). Takšne predaje imenujemo vertikalne predaje zveze (*ang. vertical handover*). Horizontalne predaje so že implementirane v večini danes razširjenih mobilnih omrežjih in so s stališča izvedbe manj

[1] **Čeprav večino v tem delu omenjenih zvez, deluje na IP sloju in bi bil izraz seja bolj primeren, bomo uporabljali izraza zveza in seja kot sinonim, ker gre v večini primerov za telefonske zveze.**

zahtevne. Izvajajo se na nižjih OSI slojih in so za uporabnika popolnoma nezaznavne. Če pa želimo uporabnikom omogočiti prehajanje med omrežji različnih tehnologij in pri tem zagotoviti, da bo trenutna zveza ostala aktivna, lahko zaradi različnih tehnologij naletimo na več tehničnih problemov, kot sta npr. različna pasovna širina, različen frekvenčni spekter. Da bo izvedba vertikalne predaje zveze čim bolj optimalna, je potrebno upoštevati naslednje parametre, ki jih lahko razdelimo na operaterske in uporabniške:

- Na operaterski strani:
    - zmanjšanje signalne režije;
    - učinkovita izraba omrežnih virov;
    - izboljšanje razširljivosti, zanesljivosti in robustnosti.
- Na uporabniški strani:
    - doseganje čim manjše zakasnitve pri procesiranju signalnih sporočil ter vzpostavitvi povezav;
    - čim manjše motenje uporabnikove komunikacije;
    - čim manjši delež neuspelih predaj in čim manj izgubljenih paketov;
    - upoštevati zasedenost ciljnega omrežja.

Na operaterski strani je potrebno zagotoviti čim boljšo izkoriščenost omrežnih virov, na uporabniški pa zagotavljanje ustreznega nivoja uporabniške izkušnje (QoE – *ang. Quality of Experience*) med procesom predaje in po njej.

Zelo pomembno vlogo pri predaji ima tudi terminal uporabnika. Večina terminalov, ki so na voljo danes, ima že vgrajene vmesnike za povezovanje v najbolj razširjena dostopovna omrežja. S širjenjem različnih tehnologij, se bo povečevalo tudi število vmesnikov v terminalih. Poleg vmesnika pa bo moral biti terminal tudi sposoben odločitve, prek katerega omrežja se bo povezal, saj se bo v heterogenih omrežjih večkrat zgodilo, da se bosta dve ali več omrežij popolnoma prekrivali. Podrobneje bo problematika terminalov opisana v poglavju 2.2.

Tabela 1 prikazuje primerjavo strategij za predajo zveze v obstoječih homogenih in bodočih heterogenih omrežjih. V primeru horizontalne predaje odločitev za predajo zveze temelji na kakovosti signala, ki je določena z močjo prejetega signala in ostalih meritev ter razpoložljivosti virov v novi celici. Meritve signala oziroma razmerja SNR (*ang. signal to noise ratio*), ki predstavlja razmerje med signalom in šumom, se izvaja periodično, tako da lahko zaznamo, kdaj je moč signala padla pod neko določeno mejo, kar pomeni, da je izpolnjen osnovni pogoj za izvedbo predaje na drugi radijski signal ali celico. Vendar pa pogojevanje odločitve za predajo zveze zgolj na moč signala onemogoča izvedbo predaje zaradi drugih razlogov, kot je npr. varnost. V primeru horizontalne predaje zveze tudi ni omogočeno, da uporabnik sam izbira omrežja, saj se predpostavlja, da je na voljo samo ena dostopovna tehnologija. Pri predaji v heterogenem okolju je potrebno, poleg zgolj pošiljanja govora/podatkov, kar je v veljavi v homogenih omrežjih, poskrbeti tudi za pošiljanje drugih dodatnih informacij, kot so npr. varnostne informacije, nivo QoS, avtentikacija, uporabnikove nastavitve. Horizontalne predaje so načrtovane za predajo v homogenih omrežjih, ki imajo skupno signalizacijo, tehnike usmerjanja in standarde za upravljanje z mobilnostjo. V heterogenih omrežjih pa morajo mobilni terminali in omrežni usmerjevalniki delovati z različnimi omrežji, njihovimi protokoli in signalizacijami. (Siddiqui and Zeadally, 2006)

Tabela 1: Primerjava strategij za predajo

	Obstoječa homogena omrežja	Bodoča heterogena omrežja
Metrika predaje	Moč signala	Različne: npr. pasovna širina, uporabniške nastavitve, stanje omrežja, varnost, ...
Zahteve na radijski povezavi	Dostava paketov na novo točko povezave	Dostava paketov ter dodatnih informacij (npr.: informacije o varnosti, QoS)
Protokoli	Zanašanje na skupne signalizacijske protokole, usmerjevalne tehnike in standarde za upravljanje z mobilnostjo	Potrebno je medsebojno delovanje mobilnih terminalov ter omrežnih usmerjevalnikov med različnimi omrežji z različnimi protokoli in standardi
Tip omrežja	Predaja se izvrši med celicami/omrežji, ki uporabljajo enako tehnologijo	Predaja se izvrši med celicami/omrežji, ki uporabljajo različne tehnologije
Tip terminala	Terminal ima zgolj en omrežni vmesnik	Večzvrstni terminali (*ang. multimode terminal*) z več različnimi omrežnimi vmesniki

Upravljanje z mobilnostjo v homogenih omrežjih, torej v omrežjih, ki uporabljajo enako tehnologijo, je danes že zelo dobro rešeno in tudi dobro deluje. Horizontalne predaje so tudi precej manj zahtevne, saj obe omrežji uporabljata enake standarde (npr.: protokoli, signalizacija, avtentikacija). Vertikalne predaje pa so precej bolj zahtevne za implementacijo, predvsem zaradi uporabe različnih mehanizmov. V nadaljevanju se bomo posvetili izključno problematiki nezaznavne vertikalne predaje zveze[2].

2.1.1 Vertikalna predaja zveze

Vertikalne predaje zvez se izvajajo med omrežji, ki uporabljajo različne dostopovne tehnologije. Obstaja več možnih delitev, ki jih na kratko opisujemo v nadaljevanju.

Prva delitev je na vertikalne predaje zveze navzgor (*ang. upward-vertical handover*) in na vertikalne predaje zveze navzdol (*ang. downward-vertical handover*). Prva predstavlja predajo zveze iz manjše v večjo celico, ki ima običajno manjšo pasovno širino na enoto površine. V tem primeru se mobilni uporabnik premika iz omrežja, ki omogoča hitrejši dostop na manjšem območju (npr. WLAN), v omrežje, ki omogoča sicer počasnejšo povezavo, je pa na voljo na večjem območju (npr. UMTS). Vertikalna predaja zveze navzdol pa pomeni ravno obratno – torej predajo zveze iz večje celice, ki omogoča nižje hitrosti na enoto površine, v manjšo celico, ki omogoča višje hitrosti prenosa.

Naslednja delitev vertikalnih predaj zvez je na pričakovane (*ang. anticipated*) in nepričakovane (*ang. unanticipated*). Prve pomenijo, da bo mobilni terminal vedno želel izvesti predajo. Običajno so vse vertikalne predaje navzgor pričakovane. Vertikalne predaje navzdol pa so lahko tako pričakovane kot nepričakovane.

Tretja delitev vertikalnih predaj je na ostre (*ang. hard handover*) in mehke (*ang. soft handover*). Prvo pogosto imenujemo tudi »prekini preden narediš«, drugo pa »naredi preden prekineš«. Pri ostri predaji zveze se najprej sprostijo trenutni viri, šele nato se začnejo uporabljati novi viri. Tovrstna predaja pride v poštev, kadar mobilni terminal nima možnosti uporabe več omrežnih vmesnikov hkrati. Pri mehki predaji zveze pa so tako trenutni kot tudi novi viri v uporabi ves čas predajanja zveze, vendar mora biti mobilni terminal sposoben komunicirati prek več omrežnih vmesnikov.

Pri vertikalni predaji zvez je pomembno tudi, kdo sproži proceduro za predajo. Tako lahko predaje razdelimo na tiste, ki jih sproži omrežje, in na tiste, ki jih sproži terminal. Pri slednjih mora terminal sam meriti moč signalov in sam narediti odločitev za predajo.

Postopek vertikalne predaje zveze lahko razdelimo v tri faze:

i. odkrivanje omrežja;
ii. določitev, kdaj se bo predaja izvedla;
iii. izvedba predaje.

---

[2] **Besedno zvezo »nezaznavna vertikalna predaja zveze« bomo v nadaljevanju zamenjevali kar z besedno zvezo »predaja zveze«.**

Odkrivanje omrežja je proces, ko mobilni terminal išče razpoložljiva brezžična omrežja. V tej fazi mora aktivirati radijske vmesnike, da lahko zazna različna brezžična omrežja, ki so v dosegu. Najenostavnejši način za odkrivanje razpoložljivih brezžičnih omrežij je, da ima mobilni terminal ves čas aktivne vse vmesnike. Tabela 2 prikazuje porabo energije v omrežjih 3G in WLAN za tri faze: ko terminal oddaja, sprejema in ko je v mirovanju. Vidimo lahko, da so pri omrežju WLAN razlike med oddajanjem in mirovanjem v primerjavi s 3G omrežji nizke. To pomeni, da bi ves čas aktivirani vsi vmesniki na terminalu zelo obremenili akumulatorje tudi v fazi, ko ni pošiljanja ali sprejemanja paketov. Zato se je potrebno izogibati temu, da bi bili vsi vmesniki ves čas aktivni. Ravno tako je potrebno zagotoviti čim krajši čas odkrivanja novih omrežij, če želimo, da bi uporabniki lahko čim prej začeli uporabljati storitve, ki so na voljo v drugih omrežjih. (Siddiqui and Zeadally, 2006)

Tabela 2: Poraba energije v 3G omrežju in WLAN

Tehnologija	Oddaja (W)	Sprejem (W)	Mirovanje (W)
3G: CDMA 1X brezžični modem NIC	2,8	0,495	0,083
ORINOCO IEEE 802.11b NIC	1,3	0,9	0,74

Poraba energije in čas odkrivanja novega omrežja sta najbolj kritična elementa te faze. Porabo energije lahko zmanjšamo, če določimo periodično preverjanje dosegljivosti novih omrežjih, kar pa ima neposreden vpliv na čas odkrivanja. Če nastavimo visoko frekvenco aktivnosti vmesnikov, bo poraba energije večja. Če pa mobilni terminal redkeje poskuša odkrivati nova omrežja, bomo sicer prihranili energijo, vendar bo čas odkrivanja zato daljši. Zaradi tega je potrebno poiskati kompromis med hranjenjem energije in odkrivanjem novega omrežja. Voung s sodelavci (Voung et. al., 2008) predlaga nov način upravljanja s porabo energije, ki deluje komplementarno z izbiro omrežja z izklapljanjem neprimernih vmesnikov glede na hitrost in trenutno kapaciteto baterije.

Odločitev kdaj se bo predaja izvedla je odvisna od več dejavnikov, ki so odvisni od omrežja, v katerem se uporabnik trenutno nahaja in omrežja, v katerega uporabnik vstopa. Tako na primer odločitev za predajo zveze, ki jo kontrolira mobilni terminal, lahko izvede agent za vertikalno predajo zveze (*ang. vertical handover agent*), ki deluje v mobilnem terminalu, in sicer na podlagi parametrov, kot so pasovna širina omrežja, pokritost, stroški, varnost, nivo QoS ali uporabniške nastavitve. Za določitev točke, ko bo izvedena predaja, je lahko uporabljenih več kriterijev. Metrike se uporabljajo kot pokazatelj, kdaj je potrebno narediti predajo zveze. Pri horizontalni predaji zveze sta bila upoštevana le moč signala in razpoložljivost kanalov, v heterogenih novih omrežjih pa bo potrebno poleg prej omenjenih kriterijev upoštevati tudi metrike, ki lahko vsebujejo več parametrov, kot so (McNair and Zhu, 2004; Kaloxylos et. al., 2006; Wei et. al., 2006 in Nguyen-Vuonga et. al, 2008):

- Moč signala oziroma razmerje SNR: Moč signala ostaja kot predpogoj za predajo zveze.
- Nivo QoS: Za vzdrževanje uporabniške izkušnje na ustreznem nivoju je nujno upoštevati, kakšno kakovost storitev omogoča ciljno omrežje (npr. zakasnitev paketov).
- Stroški: Stroški lahko imajo velik vpliv, saj lahko različni operaterji uporabljajo različne strategije zaračunavanja.
- Omrežje: Z omrežjem povezani parametri, kot so npr. obremenjenost, razpoložljiva pasovna širina, poraba energije ob uporabi določenega omrežja.
- Vrsta storitve: Različne aplikacije lahko imajo različne zahteve po zanesljivosti, zakasnitvah in hitrosti prenosa podatkov.
- Stanje mobilnega terminala: Stanje mobilnega terminala lahko zajema dinamične parametre, kot so hitrost, gibanje in lokacijske informacije. V posameznih primerih je lahko odločujoč faktor pri predaji zveze tudi moč baterije. Tako lahko npr. uporabnik določi, da se ob nizkem stanju akumulatorja izvede predaja zveze na glede porabe energije manj zahtevno omrežje.
- Profil uporabnika: Uporabnik sam z lastnimi nastavitvami vpliva na izbiro novega omrežja. Npr.: uporabnik je naročen na več dostopovnih omrežij ali ima v nastavitvah določeno, da se določene storitve izvajajo preko določene povezave, ali da želi komunicirati zgolj prek omrežij določenega operaterja.
- Profil terminala: Zmogljivosti terminala, kot so npr. podpora Jave, ločljivost ekrana, moč procesorja, velikost pomnilnika.
- Viri v omrežju operaterja: Upravljanje z viri samega operaterja. Npr. operaterji lahko rezervirajo svoje kapacitete samo za njihove najboljše stranke oz. prisilijo določene uporabnike, da se priklopijo v drugo omrežje, ko je opaziti zgoščevanje prometa npr. v UMTS celici.

- Kombinacija zgoraj naštetih.

V tretji fazi se predaja izvede. Izvedba predaje zveze zahteva prenos podatkov na novo brezžično povezavo, tako da preusmerimo povezavno pot (*ang. connection path*) uporabnika na novo povezavno točko (*ang. point of attachment*). Za pravilno usmerjanje paketov potrebujemo omrežje za prenos usmerjevalnih informacij o mobilnem uporabniku novemu dostopovnemu usmerjevalniku. Ker bodo bodoča heterogena omrežja delovala v okoljih z različnimi standardi in omrežji, bo prenos paketov na novo brezžično povezavo vseboval tudi prenos dodatnih informacij. S tem bo omogočeno, da se lahko mobilni terminal premika med različnimi omrežji in pri tem ohrani svoje podatkovne tokove. Želen cilj pri prenosu dodatnih informacij o mobilnem terminalu do novega omrežja je čim bolj zmanjšati zakasnitev ob ponovni vzpostavitvi podatkovnih tokov uporabnika. V primeru, da prenos tovrstnih informacij vnaša tako zakasnitev, kot je čas vzpostavitve nove zveze ali pa če ima občuten vpliv na zakasnitev, so vse prednosti prenašanja izgubljene. Eden ključnih raziskovalnih problemov je, kako zagotoviti ustrezen mehanizem za medoperaterske in medomrežne dogovore za zagotavljanje hitrih predaj med različnimi sistemi in se ob tem izogniti nepotrebnemu signalizacijskem prometu. Razlogi za uporabo dodatnih informacij o mobilnem terminalu med vozlišči v IP dostopovnem omrežju so (Siddiqui and Zeadally, 2006):

- uspeh časovno kritičnih aplikacij, kot sta npr. IP telefonija in video v mobilnem svetu, ki sta močno odvisna od vpliva preusmerjanja prometa za zagotovitev prenosa podatkov na novo točko dostopa;
- med vzpostavljanjem nove posredovalne poti morajo biti vozlišča ob novi poti pripravljena tako, da omogočajo podobno posredovanje IP paketov;
- če želimo replicirati informacije iz enega posredovalnega vozlišča na drugega, je potrebno zagotoviti odprto, standardizirano rešitev za takšne prenose.

Za uspešno izvedbo predaje zveze pa je ključna tudi podpora dodatnih funkcionalnosti v terminalih. Zahteve bomo opisali v nadaljevanju.

2.2 Terminali v bodočih heterogenih omrežjih

Heterogena omrežja prihodnosti bodo podpirala več različnih tehnologij, zato bo potrebno razviti terminale, ki bodo sposobni dostopati do teh tehnologij. Obstoječe terminale, ki imajo več vmesnikov za različna omrežja, lahko razdelimo v dve kategoriji:

- V prvi kategoriji so terminali, ki imajo več različnih omrežnih vmesnikov in primerno programsko opremo za preklapljanje med njimi. Tovrstne terminale imenujemo večzvrstni terminali.
- Druga vrsta terminalov so terminali, ki uporabljajo programske module, ki so sposobni prilagajanja in delujejo kot generična, nastavljiva strojna oprema, ki je sestavljena iz digitalnih signalnih procesorjev (DSP) in mikroprocesorjev, katerih naloga je zagotavljanje radijskih funkcij, kot so tvorjenje oddajanega signala (modulacija) na oddajni strani in prilagajanje/detekcija prejetega signala (demodulacija) na sprejemni strani. Te naprave imenujemo naprave s programirljivim radiem (*ang. software-defined radio*).

Obe kategoriji terminalov sta opisani v nadaljevanju.

2.2.1 Večzvrstni brezžični terminali

Večzvrstni brezžični terminali so naprave, ki podpirajo več radijskih dostopovnih tehnologij ter omogočajo sprejemanje podatkov prek različnih nosilcev z različnimi lastnostmi. Takšna inteligentna naprava mora biti sposobna samostojno določiti primeren omrežni vmesnik za posamezno aplikacijo. Odločitev za zamenjavo vmesnika in predajo aktivne seje na nov vmesnik, je lahko določena tudi z uporabnikovimi nastavitvami. Za izdelavo inteligentne večzvrstne naprave je potrebno izpolniti naslednje zahteve (Siddiqui and Zeadally, 2006):

- terminal mora delovati z minimalnimi posegi uporabnika. S stališča uporabnika je primerneje, da naprave delujejo samodejno, kot pa da vedno, ko je na voljo novo omrežje ali obstoječemu šibi signal, pozovejo uporabnika k odločitvi;
- terminal mora biti sposoben upravljati s predajo zveze na podlagi uporabniških nastavitev;
- radijski vmesnik mora biti izbran na podlagi uporabniških nastavitev, zahtev aplikacije po kakovosti storitve (QoS) ter informaciji o omrežju;
- pred predajo je potrebno pridobiti zahteve trenutno uporabljene aplikacije in se šele nato odločiti

ali se bo uporabniška izkušnja z zamenjavo vmesnika izboljšala ali poslabšala;
- promet se mora med predajo zveze prenašati neprekinjeno in za uporabnika transparentno – torej kolikor se da nezaznavno.

Če želimo zagotoviti nove terminale, ki bodo izpolnjevali vse zgoraj navedene zahteve, je potrebno z razvojem le teh zagotoviti, da bodo sposobni samodejno zaznati razpoložljivost novega omrežja. Kot smo že opisali v poglavju 2.1.1 pri opisu odkrivanja novega omrežja nekatere tehnologije zelo obremenjujejo baterije, če terminali ves čas iščejo nova omrežja. V obstoječih rešitvah je odločitev o začetku iskanja razpoložljive povezave prepuščena uporabniku. Vendar pa bi naj novi terminali potrebovali čim manj uporabnikovih posegov, zato je potrebno te procese narediti samodejne. Poleg tega pa bodo morali novi terminali od omrežja pridobiti določene informacije, na podlagi katerih se nato odločijo za preklop. Na primer, če uporabnik v svojih nastavitvah določi, da želi vedno uporabljati najcenejšo povezavo, mora terminal od omrežja prejeti informacijo o cenovnih modelih operaterja.

2.2.2 Programirljivi radio (SDR)

Programirljivi radio je tehnologija, ki uporablja prilagodljivo programsko ter strojno opremo, ki omogoča kljubovanje problemom, ki nastajajo ob nenehnem razvoju in tehničnih inovacijah brezžične tehnologije. Zaradi teh značilnosti se veliko razvijalcev zanima za to tehnologijo, saj obeta reševanje problemov z implementacijo radijskih funkcionalnosti v obliki programskih modulov, ki tečejo na generični strojni platformi. Radijski sistemi, ki temeljijo zgolj na strojni opremi, so omejeni v funkcionalnostih, saj so parametri vsake funkcionalnosti fiksni. Pri uporabi SDR pa lahko uporabljamo veliko aplikacij, ki za svoje delovanje potrebujejo različne protokole in modulacijske/demodulacijske tehnike. Sistem SDR omogoča prenastavljanje glede na programski modul, ki je trenutno v uporabi. Nove programske module pa lahko uporabniki na svoje terminale naložijo kar s prenosom prek brezžičnih tehnologij. Z uporabo SDR lahko podpremo različne tehnologije, kot so npr. Bluetooth, WLAN, GPS, GPRS.

Komercialni brezžični standardi se ves čas razvijajo iz 2G na 2.5G, 3G proti 4G. Vsaka generacija je prinesla nove standarde, kar je povzročalo težave uporabnikom, mobilnim operaterjem ter proizvajalcem opreme. Uporabniki so prisiljeni kupiti novo terminalsko opremo, če želijo uporabljati nove tehnologije. Operaterji se soočajo s problemi med migracijo na novo generacijo in imajo pri podpiranju več generacij hkrati tudi večje stroške. Proizvajalci opreme morajo zelo hitro na trg poslati nove terminale s podporo novi generaciji. Drugi problem nastane pri gostovanjih. Danes se tehnologije za povezavo na omrežje razlikujejo med geografskimi področji (npr. GSM v Evropi, IS94/CDMA v ZDA). Ta problem onemogoča enostavno gostovanje in prisili uporabnike k uporabi terminalov, ki podpirajo več tehnologij. Operaterji imajo težave pri lansiranju novih storitev, ki bi lahko pri uporabnikih zahtevale veliko nastavitev. Z uporabo SDR pa lahko storitve ponujajo precej enostavneje, saj so posamezne tehnologije podprte v programskih modulih, ki lahko enostavno sobivajo na enotni strojni platformi. Tako lahko operaterji enostavno s pošiljanjem posodobitev nastavijo uporabnikove terminale za potrebe nove storitve. SDR tehnologija lahko tako precej poenostavi prehajanje na nove omrežne tehnologije, vendar pa ima SDR tudi slabosti, saj potrebuje več energije, več procesiranja in višje zagonske stroške. Zato SDR ni primerna za vse oblike brezžičnih naprav. Glavne značilnosti SDR so (Siddiqui and Zeadally, 2006):

- Prenastavljanje (*ang. reconfigurability*): SDR omogoča sobivanje več programskih modulov, ki podpirajo več različnih standardov na enotnem sistemu. Omogočajo dinamično nastavljanje sistema z izbiro najprimernejšega modula. Dinamična konfiguracija se lahko izvaja na terminalih ali na omrežni infrastrukturi. Slednja se lahko npr. nastavi glede na tip uporabniške opreme, uporabniška oprema pa na tip omrežja.
- Večzvrstne operacije (*ang. multimode operation*): SDR omogoča večzvrstne operacije, kar je nujno za brezžične sisteme naslednje generacije. Tako pomaga k zniževanju stroškov operaterjev, saj lahko v primeru, ko imamo eno omrežje, ki je na voljo znotraj nekega prostora, ter drugo omrežje, ki je na voljo zunaj tega področja, z dvozvrstnim terminalom (*ang. dual mode*) brez dodatnih stroškov ponujajo svoje storitve.
- Komunikacija od koderkoli: SDR podpira več omrežnih vmesnikov, ki podpirajo različne standarde na eni platformi. Takšna funkcionalnost omogoča enostavno gostovanje kjerkoli. Na terminal je potrebno zgolj na novo naložiti potreben programski modul za novo omrežje/tehnologijo.
- Medsebojno delovanje: SDR omogoča implementacijo odprtih arhitektur radijskih sistemov. Končni uporabniki lahko brez večjih spreminjanj nastavitev terminala uporabljajo aplikacije tretjih proizvajalcev na njihovih terminalih podobno kot na današnjih računalniških sistemih.

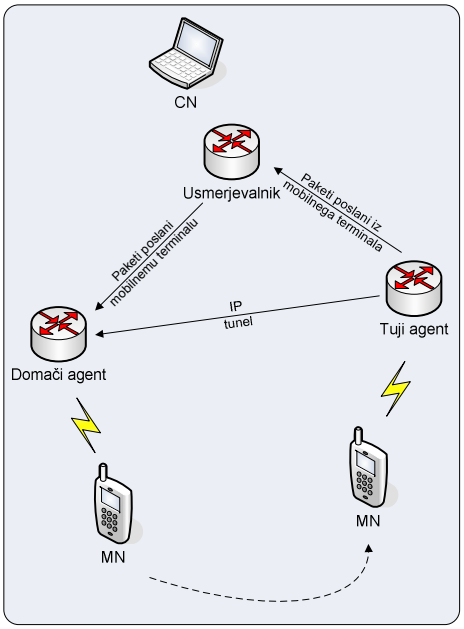
3 Protokoli za upravljanje z mobilnostjo

V tem poglavju bomo predstavili, kako lahko upravljamo z mobilnostjo s pomočjo že uveljavljenih in standardiziranih protokolov. Predaja zveze se lahko izvaja na različnih OSI slojih. Osredotočili se bomo na protokole omrežnega, transportnega ter aplikacijskega sloja, ki so najprimernejši za vertikalno predajo zveze, in za vsak sloj predstavili najbolj značilnega predstavnika. Pri izvajanju predaj zvez sodelujejo tudi protokoli na nižjih slojih, saj mora biti terminal sposoben zaznati, katera omrežja so na voljo. Potem, ko je želeno omrežje izbrano, se terminal poveže z novim omrežjem. S tem je zagotovljena zgolj povezava z novim omrežjem, medtem ko aplikacija še vedno uporablja prejšnje omrežje. Pri našem delu smo predpostavili, da so te rešitve za zagotavljanje osnovne povezljivosti vključene. Postopku povezovanja sledi predaja aplikacije preko novega omrežja.

Pri vsakem od treh izbranih slojev smo izbrali protokol, ki je največkrat uporabljen za predajo zveze. Za omrežni sloj je to protokol MIP (*ang. Mobile IP*), za transportni sloj protokol SCTP (*ang. Stream Control Transmission Protocol*), za aplikacijski sloj pa SIP (*ang. Session Initiation Protocol*). V naslednjih poglavjih bomo predstavnika vsakega sloja kratko opisali.

3.1 Protokol MIP

Na omrežnem (IP) sloju je za predajo zveze najpogosteje predlagan protokol MIP (Akyildiz et. al, 2004; Chang et. al., 2009; Emmelmann et. al, 2007; Rahman and Harmantzis, 2007; Rajavelsamy et. al, 2007; Wang et. al., 2008; Wesley, 2004; Siddiqui and Zeadally, 2006). Namen MIP protokola je zagotavljati, da lahko uporabniki ostanejo povezani ne glede na to, da so med uporabo določene povezave spremenili svojo lokacijo. Čeprav se zdi, da je protokol MIP, glede na svojo arhitekturo, zelo primeren protokol za omogočanje IP mobilnosti v brezžičnih omrežjih, zahteva velike spremembe na omrežni infrastrukturi. Shema delovanja protokola MIP je prikazana na sliki 3 (Perkins, 2002). Protokol MIP vsebuje tri glavne mehanizme, in sicer iskanje agenta (*ang. agent discovery*), registracija in tuneliranje.



Slika 3: Prikaz delovanja protokola MIP

Ko se mobilni uporabnik premika iz enega omrežja v drugega sta v postopek predaje zveze vpletena dva mobilna agenta (*ang. mobility agent*). To sta domači agent (*ang. home agent, HA*) in tuji agent (*ang. foreign agent, FA*). Mobilni agenti oglašujejo svojo prisotnost, tako da jih lahko mobilni terminal zazna. Slika 3 prikazuje primer, ko se terminal MN prestavi v omrežje tujega agenta od katerega dobi začasen IP

naslov. Ta naslov se uporabi kot končna točka tunela, ki terminalu MN omogoča prejem paketov, ki jih pošilja HA. Tuneliranje je metoda, ki je uporabljena za posredovanje sporočil od HA do FA in naprej do MN, z inkapsulacijo originalnega sporočila v nov paket, ki v protokolni glavi uporablja začasni naslov kot naslov cilja. Ko MN prejme začasni naslov, ga registrira pri HA, da bo lahko uporabljal storitve. Vse pakete, ki so poslani na domači naslov terminala MN, HA prestreže in jih prek tunela pošlje na začasni naslov. Ob izhodu iz tunela so paketi nato usmerjeni do terminala MN. Ta postopek imenujemo t.i. trismerno usmerjanje. V obratni smeri, pa so paketi, ki jih pošlje terminal MN običajno poslani z uporabo standardnih IP usmerjevalnih mehanizmov. Tako je terminal MN vselej dosegljiv na svojem domačem IP naslovu.

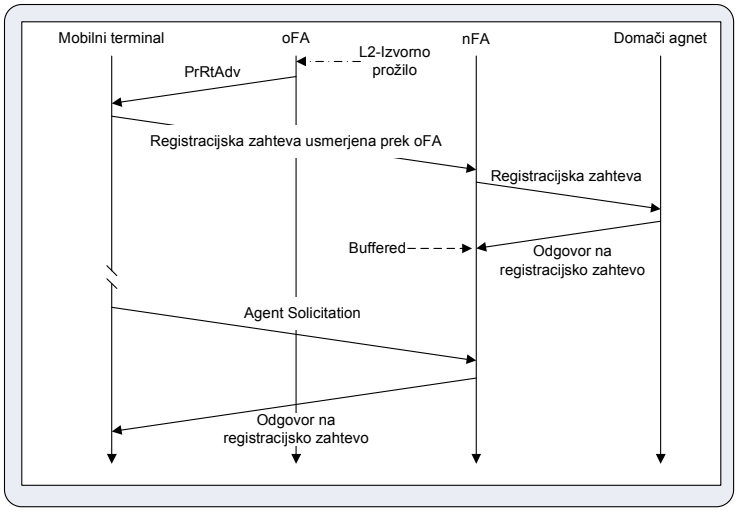
Upravljanje z mobilnostjo pri protokolu MIP lahko vnaša zelo veliko zakasnitev, ki je lahko nad zahtevami za delovanje aplikacij v realnem času. Zakasnitev nastane zato, ker mobilni terminal ne more pošiljati in prejemati paketov v času, ko poteka registracija. To je še posebej očitno pri gibanju terminala MN med podomrežji, kjer ima vsako od podomrežij svojega FA. To pomeni, da bo moral terminal MN med komunikacijo zamenjati začasni naslov. Tako lahko mobilni terminal izvede registracijo šele takrat, ko je že zaključena predaja na 2. sloju na nov tuji agent (nFA). Sam registracijski proces poteka nekaj časa, saj se registracijske zahteve oglašujejo skozi omrežje. V tem času mobilni terminal ne more sprejemati ali oddajati IP paketov. Za odpravo teh dveh problemov je delovna skupina za protokol MIP znotraj IETF predlagala tri metode, s katerimi bi lahko zagotovili manjšo zakasnitev predaje zveze. Te metode so (Malki, 2005):

- metoda predregistracije (*ang. pre-registration*);
- metoda poregistracije (*ang. post-registration*);
- združena metoda.

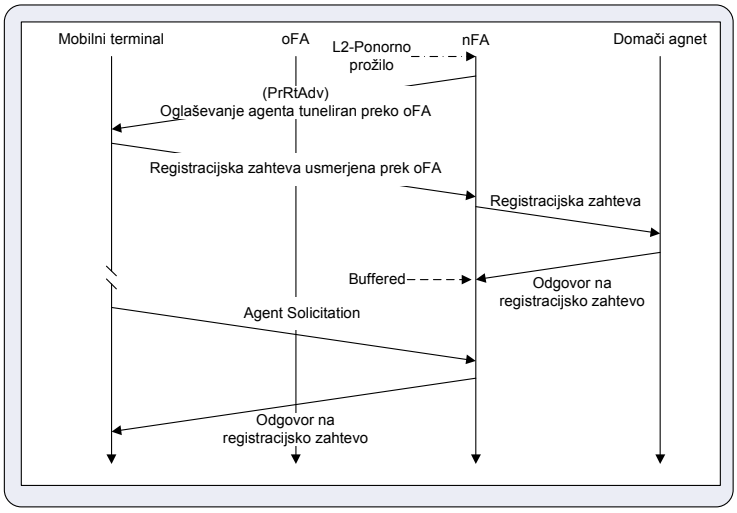
3.1.1 Metoda predregistracije

Ta metoda mobilnemu terminalu omogoča, da je vpleten v predajo zveze. Mobilni terminal s pomočjo omrežja izvede predajo zveze na tretjem sloju, še preden se izvede predaja na drugem sloju. Predaja na tretjem sloju je lahko sprožena s strani omrežja ali pa s strani mobilnega terminala:

- Predaja sprožena s strani omrežja: V tem primeru lahko pride do sprožitve predaje zveze z metodo predregistracije v starem tujem agentu (*ang. old Foreign Agent - oFA*), kjer predajo sproži izvorno prožilo (*ang. source trigger*), ali pa v novem tujem agentu (*ang. new Foreign Agent – nFA*), kjer predajo sproži ponorno prožilo (*ang. target trigger*). Predaja zveze z izvornim prožilom se zgodi, ko oFA sprejme L2 prožilo, ki sporoči, da se je mobilni terminal prestavil iz oFA v nFA. L2 prožilo vsebuje informacije o identifikaciji mobilnega terminala (IPv4 naslov ali pa identifikator, iz katerega lahko dobimo IPv4 naslov) in identifikacijo nFA. Identifikator je lahko IP naslov verzije 4 ali drug identifikator, ki je lasten omrežju (npr. bazna postaja ali identifikacija dostopovne točke). Predaja zveze s ponornim prožilom pa se sproži, ko nFA sprejme L2 prožilo, s katerim mu sporoči, da določen mobilni terminal prihaja iz območja oFA. Sliki 5 in 4 prikazujeta izmenjavo sporočil, ko je predaja sprožena s strani omrežja.

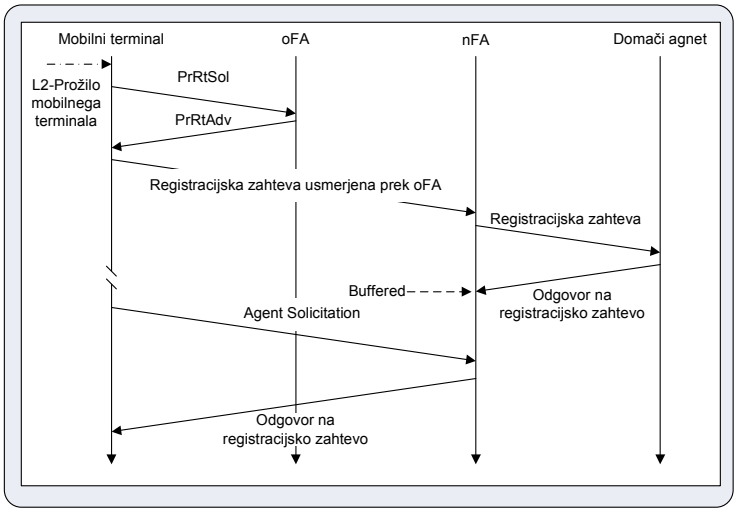


Slika 4: Metoda predregistracije (sprožena iz omrežja, izvorno prožilo)



Slika 5: Metoda predregistracije (sprožena iz omrežja, ponorno prožilo)

- Predaja sprožena s strani mobilnega terminala: Tovrstna predaja zveze se zgodi, ko mobilni terminal prejme L2 prožilo, s katerim je obveščen, da se bo v kratkem prestavil v območje nFA. L2 prožilo vsebuje informacije o identifikaciji nFA (IPv4 naslov ali pa identifikator, iz katerega lahko dobimo IPv4 naslov). Na primer v primeru WLAN omrežja lahko mobilni terminal izvede iskanje za pridobitev BSSID (*ang. base station session ID*) dostopovne točke, ki je potencialna naslednja točka pri predaji (če npr. signal te točke postaja močnejši). Na sliki 6 je prikazana izmenjava sporočil, ko je predaja sprožena s strani mobilnega terminala.



Slika 6: Metoda predregistracije sprožena s strani mobilnega terminala

3.1.2 Metoda poregistracije

Ta metoda prinaša razširitev protokola MIP tako, da lahko oFA in nFA z L2 prožilci vzpostavita dvosmerni tunel med sabo. Mobilni terminal lahko tako še vedno uporablja oFA v podomrežju nFA. To omogoča zelo hitro povezavo na novo povezavno točko, kar zmanjša vpliv na časovno kritične aplikacije. Predaja se odvija po naslednjem scenariju:

1. oFA ali nFA sprejmeta L2 prožilo, ki ju obvesti, da se bo določen mobilni terminal premaknil iz območja oFA v območje nFA. Izvorno prožilo je lahko izvorni pri oFA in ponorni pri nFA. Prožilo vsebuje informacije, kot so L2 naslov mobilnega terminala in identifikacijo nFA oz. oFA (IPv4 naslov ali pa identifikator, iz katerega lahko dobimo IPv4 naslov).
2. Ko FA prejme prožilo, pošlje *HRqst (ang. Handoff Request)* drugemu FA.
   V primeru, da je pošiljatelj oFA, *HRqst* vsebuje:
   - IPv4 domači naslov mobilnega terminala;

- HA naslov mobilnega terminala;
- opcijo LLA z L2 naslovom mobilnega terminala:
- časovni interval, ki določa, koliko časa je oFA pripravljen vzpostavljen tunel vzdrževati.

Če pa je pošiljatelj nFA, pa *HRqst* vsebuje:

- LLA opcijo z L2 naslovom mobilnega terminala;
- časovni interval, s katerim nFA določi, kako dolgo naj bo tunel vzpostavljen.

Domači IPv4 naslov mobilnega terminala ter naslov domačega agenta pa v tem primeru nista poslana.

3. Ko tuji agent sprejme *HRqst* pošlje *HRply (ang. Handoff Replay)* drugemu tujemu agentu.
4. Točka med L2 predajo zveze, v kateri mobilni terminal ni več povezan na podano povezavo, je signalizirana z L2-LD prožilom pri oFA in mobilnem terminalu. Zaključek predaje je signaliziran z L2-LU prožilom pri nFA in mobilnem terminalu.
5. oFA postane aFA, če se mobilni terminal premakne v območje tretjega tujega agenta, preden se izvede MIP registracija z nFA.
6. V primeru, da pride do napake v četrtem koraku zaradi težav na L2 sloju in nastane t.i. ping-pong situacija, je oFA sposoben to napako zaznati.

3.1.3 Združena metoda

Ta metoda združuje prejšnji dve. Katera izmed metod se bo uporabila, je odvisno od trenutnih razmer. Če se lahko izvede predregistracija pred predajo na drugem sloju, bo izbrana metoda predregistracije. Če pa predaja predregistracije ni zaključena v določenem časovnem intervalu, začne oFA pošiljati promet namenjen mobilnemu terminalu na nFA, tako kot je to določeno z metodo poregistracije. Ta metoda je primerna predvsem takrat, ko se predaja po metodi predregistracije ne izvede pred zaključkom predaje na drugem sloju.

3.1.4 Pregled literature - protokol MIP

Ezzouhairi s sodelavci (Ezzouhairi et. al, 2010) je na podlagi protokola MIP predlagal novo arhitekturo HIA (*ang. Hybrid Interworking Architecture*), ki omogoča predajo zvez v mestnih okoljih. Fathi s sodelavci (Fathi et. al., 2005) je predstavil analizo uporabe MIP protokola. Pokazali so, da lahko z metodo predregistracije in metodo poregistracije med predajo dosegamo prekinitve, ki omogočajo tudi uporabo aplikacij v realnem času. Poleg osnovne različice MIP protokola lahko v literaturi najdemo tudi nekaj razširitev, kot so FMIP (Koodli, 2005), ki zmanjšuje izgubo paketov, HMIP (Soliman et. al, 2008), ki zmanjšuje signalizacijo ter PMIP (Gundavelli et. al, 2008), ki omogoča MIP funkcionalnosti v omrežju klientom, ki ne podpirajo protokola MIP. Fathi in sodelavci (Fathi et. al., 2007) so primerjali učinkovitost izvajanja predajanja zvez različnih razširitev protokola MIP. Ugotovili so, da lahko z razširitvama FMIP in HMIP dosegamo precej nižje zakasnitve pri predaji zveze. Kwon s sodelavci (Kwon et. al., 2008) je predlagal izboljšavo FMIP protokola, s katerim lahko dosežemo še manjšo izgubo paketov.
Kljub prednostim protokola MIP, pa ima ta tudi nekaj slabosti (Wesley, 2004; Schulzrinne and Wedlund, 2000):

- Med gostitelji je potrebno vzpostaviti trismerno pot. Paketi, ki jih pošilja mobilni terminal do oddaljenega gostitelja, potujejo direktno med njima, medtem ko paketi, poslani od oddaljenega gostitelja do mobilnega terminala, potujejo prek domačega agenta, ki je v domačem omrežju in je lahko geografsko precej oddaljen od trenutne lokacije uporabnika.
- Domači agent in domače omrežje predstavljata kritično točko odpovedi (*ang. single point of failure*) za povezovanje mobilnega terminala, tudi če je trenutno priklopljen na drugo omrežje. Takšen način delovanja pa povzroča dodatno obremenjenost procesorske moči v domačem omrežju.
- Mobilni terminal v IP paketih vedno uporablja statičen domači naslov kot izvorni naslov. Ko je mobilni terminal zunaj svojega domačega omrežja, bi lahko usmerjevalniki in požarni zidovi predvidevali, da želi uporabnik slepariti z naslovi (*ang. spoofing*) in zato blokirali njegov promet. Rešitev tega problema je, da vzpostavimo tunel tudi v smeri od mobilnega terminala do oddaljenega gostitelja, kar pomeni uporabo manj zanesljive poti in povečanje procesorske obremenitve v domačem omrežju.
- Vmesniki med IP in omrežnimi protokoli niso tako dobro definirani, da bi bili zgornji sloji obveščeni, ko se uporabnik premika med omrežji. Dobra rešitev tega problema bi bila, da bi

transportni sloj poskrbel za zadržanje pošiljanja podatkov za čas predaje zveze in s tem zmanjšal potencialno izgubo paketov.

- Veliko korakov pri izvajanju predaje zveze z MIP protokolom. Mobilni terminal mora zaznati premikanje uporabnika, poiskati novo možnost povezave in posodobiti svojo lokacijo v domačem agentu. Ko se izvajajo te posodobitve, je lahko mobilni terminal brez povezave in paketi, namenjeni mobilnemu terminalu, bodo izgubljeni. Obstajajo sicer metode za izboljšanje takšnih situacij, vendar v večini primerov zahtevajo prenastavljanje usmerjevalnikov v omrežju.
- Uporabniki ne morejo uporabljati storitev v omrežjih, kjer podpora MIP protokola ni mogoča.
- MIP ima za časovno kritične aplikacije nekaj pomanjkljivosti, kot so že omenjene trismerno usmerjanje, trismerna registracija, režija zaradi enkapsulacije in potreba po domačem naslovu.

3.2 Protokol SCTP

Na transportnem sloju je najpogosteje uporabljen protokol SCTP (Launois and Bagnulo, 2006; Siddiqui and Zeadally, 2006; Wesley, 2004; Wang et. al., 2008a; Ezzouhairi et. al, 2010). Protokol SCTP omogoča, da terminali vzdržujejo dve IP povezavi in med njimi preklapljajo, ko začne moč signala enega od omrežij padati. Deluje na istem osi sloju kot TCP in UDP protokola in ga lahko označimo kot zmogljivejšo verzijo TCP protokola. S pomočjo SCTP protokola lahko aplikacije vzdržujejo dva zanesljiva hkratna toka podatkov, brez da bi se ti podatki medsebojno motili. Takšna povezava se v SCTP imenuje pridružitev (*ang. association*). Lahko tudi meša zanesljive tokove podatkov s t.i. »best effort« tokovi podatkov. Omogoča tudi, da se lahko ena naprava poveže z drugo, ki ima dva IP naslova. Prva naprava bo med obema naslovoma izbrala enega kot primarni naslov. V primeru napake na primarnem naslovu bo SCTP sloj samodejno preklopil na alternativni IP naslov. Preklop je neodvisen od aplikacije, ki se trenutno uporablja. Takšen način delovanja lahko zelo poveča zanesljivost, še posebej, če sta IP naslova v različnih omrežjih. Vendar pa lahko takšen preklop traja tudi več sekund, tako da je veliko predolg za časovno kritične aplikacije, kot sta govor in video (Dorenbosh et. al, 2004).

Če želimo zagotavljati predajo sej na transportnem sloju, je potrebno zaznati in prenastaviti mobilni terminal, ko se premika iz enega omrežja v drugega. To zajema zaznavo novega omrežja ter alokacijo novega IP naslova. To običajno izvedemo s pomočjo DHCP ali pa s pomočjo metod za odkrivanje sosednjih vozlišč (*ang. Router/Neighbour Discovery*).

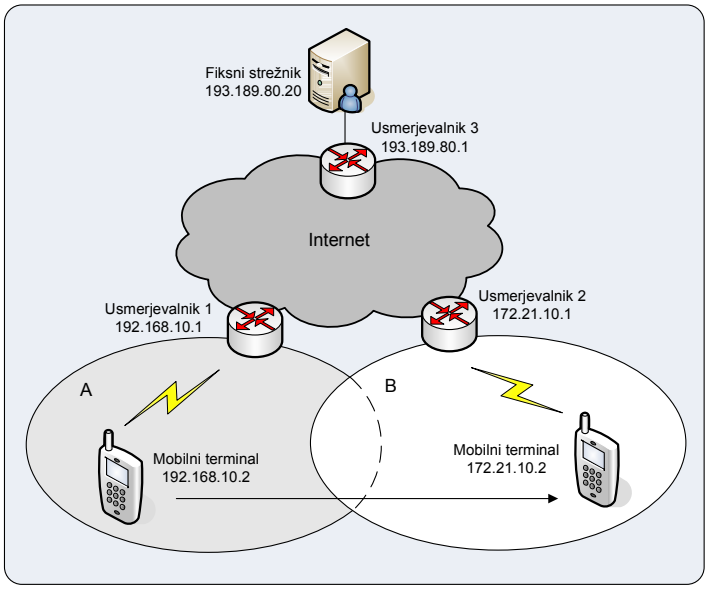
Protokol za predajo zveze na transportnem sloju mora omogočati dinamični preklop IP naslova povezave. Najprej se mora vzpostaviti prva povezava. Ko je na voljo drugo omrežje, se vzpostavi druga povezava. Prva povezava ostane aktivna in po njej se podatki prenašajo brez prekinitev. Nato se zaradi npr. zmanjšanja moči signala prvega omrežja ali cenejše povezave drugega omrežja zgodi preklop med prvo in drugo povezavo brez prekinitve in drugih vplivov na delovanje aplikacije, ki se SCTP sloja sploh »ne zaveda«. Tako lahko zagotovimo nezaznaven preklop med omrežjema. Omrežja so lahko različna, npr. LAN, WLAN, UMTS, Bluetooth (Dorenbosh et. al, 2004).

3.2.1 Protokol SCTP in mobilni uporabniki

Glavna lastnost SCTP protokola je, da lahko vzdržuje več IP povezav hkrati. Vendar mora biti ena določena kot primarna. S takšnim načinom delovanja bi lahko zelo izboljšali uporabo aplikacij z nezanesljivimi povezavami. Vendar pa je potrebno, ob uporabi osnovne različice SCTP, vse IP naslove izmenjati pred začetkom SCTP seje. To pa pomeni, da takšna oblika SCTP protokola ni primerna za mobilne uporabnike, saj mobilni terminali nimajo fiksnega in v naprej znanega IP naslova. Zato so osnovnemu SCTP protokolu dodali funkcionalnost DAR (*ang. Dynamic Alternate Routing*), ki omogoča končnim točkam dodajanje, brisanje ali spreminjanje IP naslovov med aktivno SCTP sejo z uporabo ASCONF sporočil. Razširitev protokola SCTP za mobilne uporabnike imenujemo mSCTP (*ang. mobile SCTP*). Dobra lastnost pri implementaciji mSCTP protokola je, da ni potrebno ničesar spreminjati v omrežju, kar naredi arhitekturo omrežja precej enostavnejšo od tiste, v kateri se uporabljajo rešitve, ki delujejo na omrežnem sloju.

Slika 7 prikazuje primer delovanja protokola mSCTP. Uporabljen je model klient–strežnik, kjer mobilni terminal (klient) komunicira s fiksnim strežnikom (FS) z uporabo protokola mSCTP. Na sliki lahko vidimo, da mobilni terminal uporablja IP naslov 192.168.10.2 na lokaciji A. Promet med mobilnim terminalom in fiksnim strežnikom je usmerjen preko usmerjevalnika 1. Ko se mobilni terminal prestavi iz lokacije A na lokacijo B, zazna dosegljivost usmerjevalnika 2 in prejme nov IP naslov 172.21.10.2. Nov IP naslov mobilni terminal doda v pridružitev tako, da fiksnemu strežniku pošlje sporočilo ASCONF (*Add IP Address, 172.21.10.2*). V tej fazi je promet še vedno usmerjan preko usmerjevalnika 1, ki je določen kot

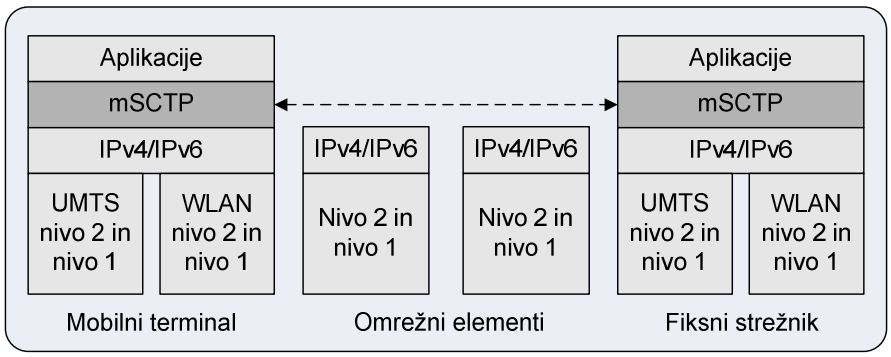
primarna izbira. Ko postane signal usmerjevalnika 2 dovolj močan, pošlje mobilni terminal fiksnemu strežniku sporočilo ASCONF (*Set Primary Address, 172.21.10.2*). Tako postane primarni usmerjevalnik usmerjevalnik 2. V mobilnem terminalu ter fiksnem strežniku se izvrši ustrezna zamenjava usmerjevalnih tabel. Ko postane signal usmerjevalnika 1 tako šibek, da ni več mogoče vzdrževati povezave, mobilni terminal zbriše IP naslov 192.168.10.2 s pošiljanjem sporočila ASCONF (*Delete IP Address, 192.168.10.2*) fiksnemu strežniku.



Slika 7: Predaja zveze s pomočjo protokola mSCTP

Primer uporabe mSCTP protokola: predaja zveze med UMTS in WLAN

Ma s sodelavci (Ma et. al., 2004) podaja primer uporabe mSCTP protokola za predajo zveze med UMTS in WLAN. V povezani UMTS/WLAN arhitekturi mobilni terminal nima fiksnega in v naprej znanega IP naslova. Zato je v tem primeru smiselno izbrati razširitev mSCTP, ki omogoča končnim točkam dodajanje, brisanje in spreminjanje IP naslovov med aktivno SCTP povezavo (pridružitvijo). Vertikalne predaje zvez s protokolom SCTP uporabljajo funkcionalnost večdomnosti (*ang. multi-homing*) med predajo. Tako lahko ima mobilni terminal dva IP naslova – enega za UMTS drugega pa za WLAN omrežje. Na sliki 8 je prikazana arhitektura protokola mSCTP.



Slika 8: Arhitektura protokola mSCTP

Slika 8 prikazuje poenostavljeno arhitekturo protokola. Ker morata tako mobilni klient kot tudi strežnik, na katerega se mobilni klient povezuje, podpirati mSCTP, lahko naletimo na težave, saj večina današnjih strežnikov, priklopljenih v Internet, uporablja protokol TCP in ne mSCTP. Mobilni terminal mora imeti tudi ustrezne vmesnike za podporo obeh omrežij. Na ostalih omrežnih elementih pa spremembe niso potrebne. Za zagotovitev dostopa do katerega koli fiksnega strežnika lahko strežnik s podporo mSCTP deluje kot posredovalni strežnik (*ang. proxy server*), na katerega se mobilni klient priklaplja preko protokola mSCTP, posredovalni strežnik pa z drugimi strežniki preko TCP. Postopek predaje zveze z mSCTP ima naslednje korake:

- dodajanje IP naslova;

- izvedba vertikalne predaje;
- izbris IP naslova.

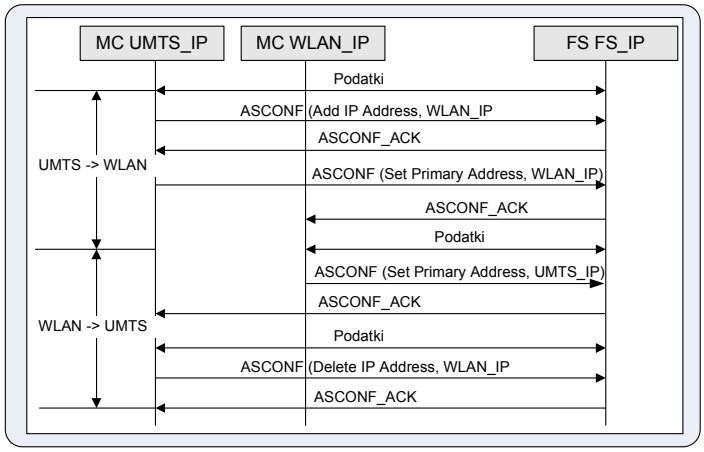
Fiksni strežnik je lahko nastavljen na dva načina:

- Podprta funkcionalnost enodomnosti (*ang. Single-homing*): zagotavlja samo en IP naslov za podporo predaje zveze;
- Podprta funkcionalnost dvodomnosti (*ang. Dual-homing*): zagotavlja več (običajno dva) IP naslovov za podporo predaje zveze.

Večina današnjih strežnikov v Internetu ima določen en IP naslov. Zato je spreminjanje strežnikov za podporo dveh IP naslovov precej zahtevna naloga. V nadaljevanju podajamo opis poteka izmenjave sporočil pri različnih konfiguracijah fiksnega strežnika.

Podprta funkcionalnost enodomnosti

Fiksni strežnik ima IP naslov FS_IP. Mobilni terminal ima ravno tako IP naslov, UMTS_IP za UMTS omrežje, s katerim s fiksnim strežnikom komunicira z uporabo protokola mSCTP. Ko se mobilni terminal premakne v doseg WLAN omrežja, ki je ravno tako v dosegu UMTS celice, pridobi nov IP naslov, WLAN_IP ter začne z dodajanjem WLAN_IP naslova. Mobilni terminal obvesti fiksni strežnik o novem IP naslovu s pošiljanjem ASCONF sporočila, ki vsebuje parameter *add IP address* in WLAN_IP. V primeru UMTS->WLAN predaje zveze, mobilni terminal sproži predajo, ko pošlje ASCONF sporočilo s parametri *set primary address* in WLAN_IP. Ko mobilni terminal od fiksnega strežnika sprejme potrditev ACK, postane WLAN omrežje primarna izbira in promet med mobilnim terminalom in fiksnim strežnikom poteka prek WLAN omrežja. V primeru WLAN->UMTS predaje mobilni terminal sproži predajo zveze s pošiljanjem sporočila ASCONF, ki vsebuje parametre *set primary address* in UMTS_IP. Ko mobilni terminal od fiksnega strežnika sprejme potrditev ACK, postane UMTS omrežje primarna izbira in promet med mobilnim terminalom in fiksnim strežnikom poteka prek UMTS omrežja. Če mobilni terminal izgubi signal WLAN dostopovne točke, začne proceduro za brisanje IP naslova. To stori tako, da pošlje ASCONF sporočilo s parametri *delete IP address* in WLAN_IP in s tem fiksnemu strežniku sporoči, da naj sprosti naslov WLAN_IP s svoje tabele gostiteljev (*ang. host table*). Ko mobilni terminal od fiksnega strežnika sprejme potrditev ACK, zbriše WLAN_IP s svoje liste naslovov in WLAN_IP je sproščen iz pridružitve. Izmenjavo sporočil prikazuje slika 9.



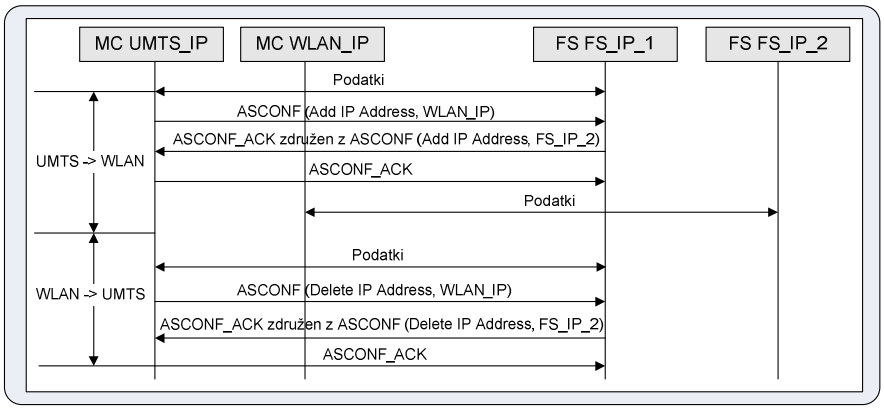
Slika 9: Vertikalna predaja zveze – protokol mSCTP (FS podpira funkcionalnost enodomnosti)

Podprta funkcionalnost dvodomnosti

V takšni konfiguraciji ima fiksni strežnik dva IP naslova; FS_IP_1 in FS_IP_2. Na začetku procesa sta UMTS_IP in FS_IP_1 nastavljena kot primarna naslova. Obstajata dve razliki med pristopom enodomnosti in dvodomnosti. Prva razlika je v procesu dodajanja in brisanja IP naslova iz pridružitve. Ko fiksni strežnik podpira funkcionalnost enodomnosti odgovori zahtevi mobilnega terminala po dodajanju ali brisanju IP naslova s potrditvijo ACK, ki jo združi z ASCOF zahtevo mobilnemu terminalu, da naj doda/izbriše drugi IP naslov fiksnega strežnika. Mobilni terminal nato s pošiljanjem sporočila ACK potrdi zaključek procesa dodajanja/brisanja IP naslova. Druga razlika pa je v proženju procesa predaje. Ker tako mobilni terminal

kot tudi fiksni strežnik podpirata funkcionalnost dvodomnosti, lahko mobilni terminal neposredno nastavi sekundarni naslov fiksnega strežnika kot primaren naslov v svoji usmerjevalni tabeli in začne pošiljati podatke na novo povezavo. Ker v primeru, ko je podprta funkcionalnost dvodomnosti, ni procesa izmenjave naslovov, je zakasnitev predaje manjša kot v primeru, ko je podprta funkcionalnost enodomnosti. Izmenjavo sporočil prikazuje slika 10.

Simulacijski poizkusi so pokazali, da pri uporabi enega naslova strežnika traja preklop okoli 0,5 sekunde (Ma et. al., 2004). Ta čas pa lahko z uporabo dveh naslovov zmanjšamo za približno polovico.



Slika 10: Vertikalna predaja zveze – protokol mSCTP (FS podpira funkcionalnost dvodomnosti)

3.2.2 Pregled literature – protokol SCTP

Budzisz s sodelavci (Budzisz et. al., 2008) predstavlja scenarije, s katerimi ocenjujejo delovanje mSCTP. Ugotovili so, da lahko uporaba mSCTP za izvajanje nezaznavnih predaj zvez za aplikacije, ki tečejo v realnem času, povzroča velike zakasnitve ob predaji. Fitzpatrick in sodelavci (Fitzpatrick et. al., 2009) uporabljajo SCTP za predajo zveze z uporabo metrike, ki določa nivo uporabniške izkušnje med predajo. Hasswa s sodelavci (Hasswa et. al, 2007) predlaga nov pristop za izvajanje predaj zvez, ki uporablja mSCTP imenovan Tramcar (*ang. Transport and Application Layer Architecture for vertical Mobility with Contextawareness*), ki omogoča izvajanje predaj zvez, kjer odločitev za predajo ni odvisna zgolj od lastnosti omrežja. Poleg osnovne različice SCTP/mSCTP protokola lahko v literaturi najdemo tudi nekaj predlaganih izboljšav, kot je PR-SCTP (*ang. Stream Control Transmission Protocol Partial Reliability Extension*) (Stewart et. al, 2004), ki odpravlja problem napačnega vrstnega reda pri sprejemu SCTP sporočil. Uporabnikom omogoča, da nastavijo TTL (*ang. time-to-live*) za posamezna SCTP sporočila, s katerim določajo dolžino časa, v katerem bo pošiljatelj poskušal poslati sporočilo. Če ta čas poteče pred potrditvijo prejema sporočila, se tega sporočila ne pošilja več. Wang in sodelavci (Wang et. al., 2008) predlagajo cmpSCTP (*ang. concurrent multi-path Stream Control Transmission Protocol*), ki k standardnemu SCTP za potrebe nezaznavne predaje zveze dodaja hkratno pošiljanje prek več poti in dinamično upravljanje več poti.

3.3 Protokol SIP

Protokol SIP je večinoma izbran kot glavni protokol na aplikacijskem sloju za izvajanje predaj zvez (Wesley, 2004; Hsieh et. al., 2007, Rajavelsamy et. al, 2007, Siddiqui and Zeadally, 2006). Protokol SIP je predlagala IETF kot splošni večpredstavnostni signalizacijski protokol, ki končnim točkam omogoča vzpostavitev medsebojnih govornih ali pa večpredstavnostnih sej. SIP ogrodje sestavljajo naslednji omrežni elementi (Rosenberg et.al, 2002):

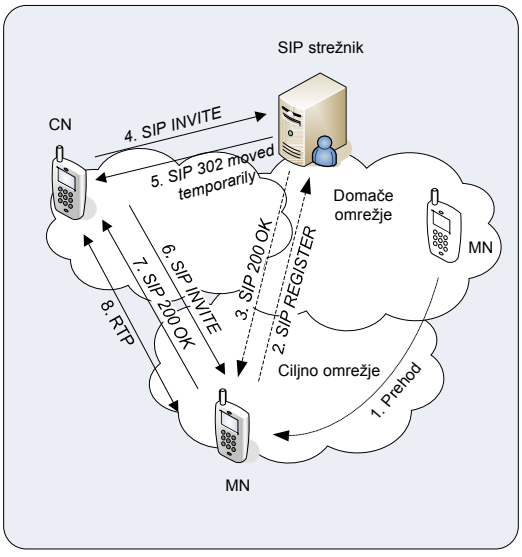
- uporabniški agent (*ang. User Agent*) – končna naprava;
- posredovalni strežnik (*ang. Proxy Server*) – vmesna naprava, ki lahko deluje tako kot strežnik in tudi kot odjemalec z namenom proženja zahtev za uporabniškega agenta;
- strežnik za preusmerjanje (*ang. Redirect Server*) – strežnik, ki sprejema SIP zahteve. Glede na SIP naslov poišče klicanega in preusmeri zahteve;
- registrator (*ang. Registrar*) – strežnik, ki sprejema zahteve za potrebe posodabljanja lokacijske baze s podatki, ki so določeni v zahtevi;
- korespondenčno vozlišče (*ang. Correspondent Node*) – končni del uporabniškega agenta.

Vsak SIP uporabnik ima unikatno identifikacijo v obliki URI (*ang. Universal Resource Indicator*), ki se uporablja za iskanje uporabnika, s katerim želi drugi uporabnik vzpostaviti sejo. IP naslov pa je uporabniku dodeljen za potrebe usmerjanja SIP signalizacije od SIP registratorja do uporabniškega agenta. SIP uporabnik z registracijo pri SIP registratorju naznani svojo prisotnost v omrežju in pripravljenost sprejemanja zahteve za vzpostavitev seje drugih uporabnikov. Običajno se seja začne s pošiljanjem `SIP INVITE` sporočila preko SIP posredovalnih strežnikov. Ko prejemnik sprejme zahtevo in je pošiljatelj o tem obveščen, se začne prenos podatkov med obema uporabnikoma, ki običajno poteka po drugi poti kot signalizacijski tok.

Protokol SIP omogoča različne tipe mobilnosti: mobilnost seje, osebna mobilnost in mobilnost terminala. *Mobilnost seje* uporabnikom omogoča vzdrževanje seje med premikanjem iz enega terminala na drugega. *Osebna mobilnost* omogoča uporabnikom, da so ves čas dosegljivi z enim logičnim naslovom, tudi če uporabnik uporablja različne terminale. *Mobilnost terminala* omogoča napravi, da se premika med podomrežji in medtem ohranja dosegljivost ter trenutno aktivne seje med premikanjem. Pri našem delu smo se osredotočili predvsem na to vrsto mobilnosti. Mobilnost terminala zahteva, da protokol SIP vzpostavi novo povezavo ob prehodu v drugo omrežje. To lahko naredi na začetku nove seje, ko se je terminal že premaknil v novo omrežje ali pa med sejo. Za zadostitev teh funkcionalnosti, sta bili definirani dve metodi. Prva se imenuje mobilnost pred klicem (*ang. pre-call mobility*), druga pa mobilnost med klicem (*ang. mid-call mobility*). V nadaljevanju podajamo podrobnejši opis vsakega načina posebej.

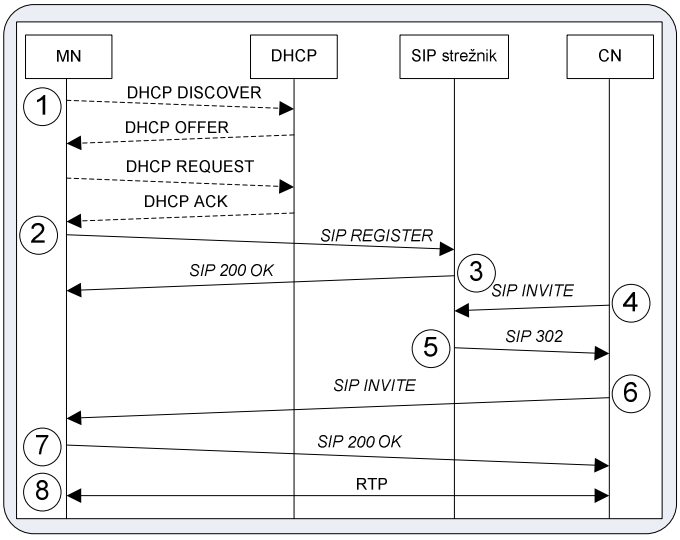
3.3.1 Mobilnost pred klicem

Scenarij mobilnosti pred klicem je prikazan na sliki 11, izmenjava sporočil pa na sliki 12. Ob prehodu v ciljno omrežje (korak 1) se mobilni terminal ponovno registrira pri SIP strežniku v domačem omrežju in mu ob tem sporoči nov IP naslov, ki ga je dobil v ciljnem omrežju (korak 2 in korak 3). Ko terminal CN pokliče terminal MN, pošlje `SIP INVITE` sporočilo SIP strežniku (korak 4), ta mu v odgovoru pošlje nov naslov terminala MN (korak 5). Terminal CN nato pošlje `SIP INVITE` terminalu MN (korak 6) po potrditvi (korak 7), se vzpostavi RTP seja (korak 8). Tovrsten način predstavlja enostavnejši del upravljanja z mobilnostjo z uporabo SIP protokola. Mobilni terminal pridobi nov IP naslov preden začne ali prejme klic. V tem primeru mobilni terminal izvede samo ponovno registracijo s svojim registratorjem in vsakokrat pridobi nov IP naslov. Edini zahtevnejši del tega procesa predstavlja zaznava na aplikacijskem sloju, da je prišlo do spremembe IP naslova. To lahko rešujemo na več načinov, med katerimi je najenostavnejši ta, da odjemalec vsakih nekaj sekund izvede ponovno registracijo.



Slika 11: Mobilnost pred klicem

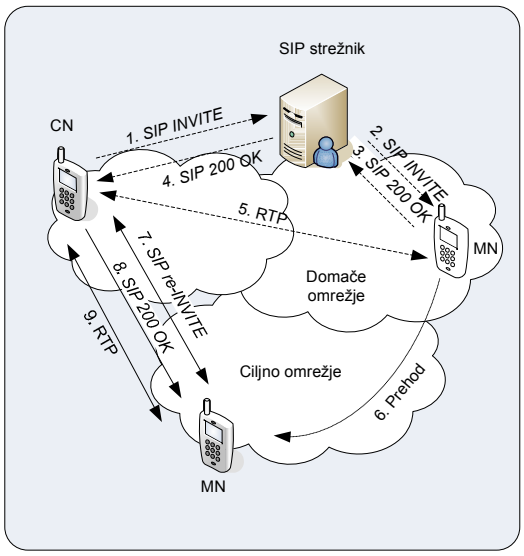
Glavnino zakasnitve pri predaji zveze prispevata odkrivanje novega omrežja ter pridobitev naslova s pomočjo DHCP. Vendar lahko ta del zakasnitve zmanjšamo z uporabo mehanizmov drugega OSI sloja. Ko to storimo nam glavnino zakasnitve prinaša enosmerna zakasnitev pošiljanja `SIP INVITE` sporočila od mobilnega terminala do korespondenčnega gostitelja.



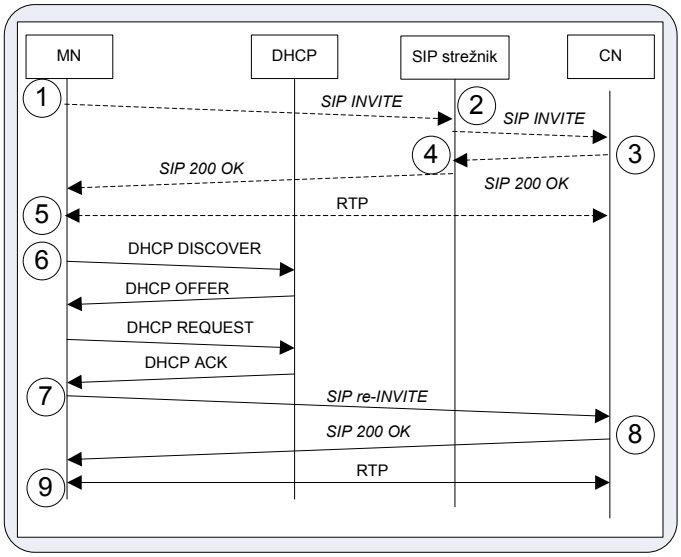
Slika 12: Izmenjava sporočil za mobilnost pred klicem

3.3.2 Mobilnost med klicem

Scenarij mobilnosti med klicem je prikazan na sliki 13 izmenjava sporočil pa na sliki 14. Terminal CN najprej vzpostavi zvezo s terminalom MN preko SIP strežnika (koraki 1-5). Ko se terminal MN prestavi v ciljno omrežje (korak 6), pošlje `SIP re-INVITE` sporočilo neposredno terminalu CN in ga obvesti o spremembi IP naslova (korak 7). Sporočilo vsebuje posodobljen opis seje, ki vsebuje tudi nov IP naslov. Posodabljanje lokacije vnaša enosmerno zakasnitev po tem, ko aplikacija, ki jo uporablja mobilni terminal, odkrije, da je prejela nov IP naslov. Za širokopasovne komunikacije je ta zakasnitev približno enaka zakasnitvi širjenja signala z dodatkom nekaj milisekund, pri ozkopasovnih komunikacijah pa lahko to pomeni zakasnitve reda več 10 milisekund. Po potrditvi (korak 8) se vzpostavi RTP seja (korak 9).



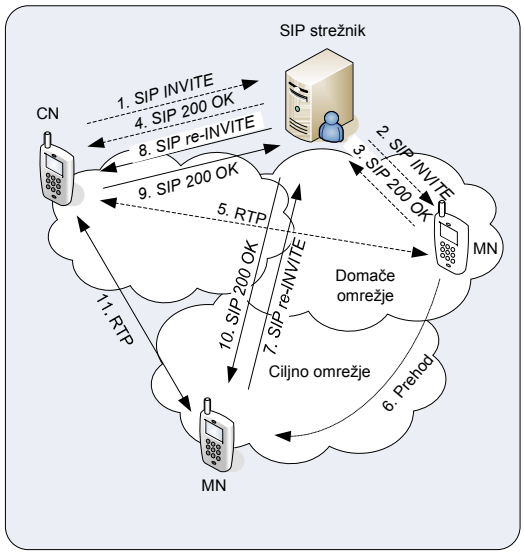
Slika 13: Mobilnost med klicem



Slika 14: Izmenjava sporočil za mobilnost med klicem

3.3.3 Izboljšan scenarij za mobilnost med klicem SEMCS

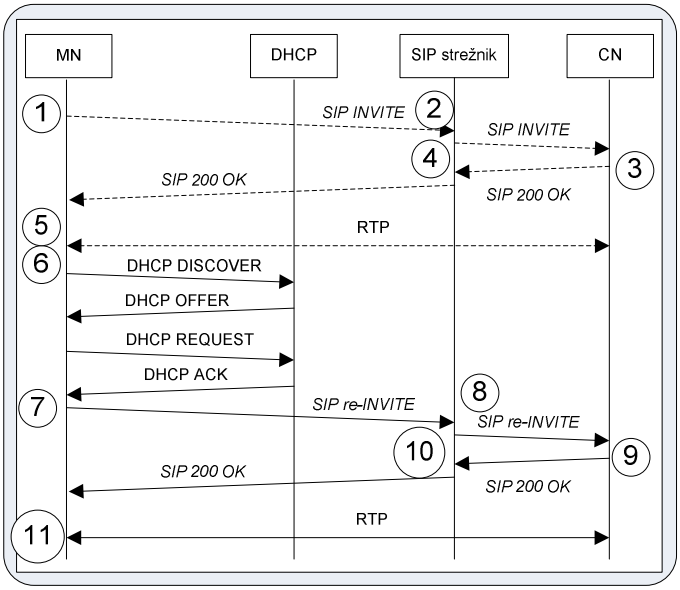
Pri naših raziskavah smo se osredotočili na scenarij mobilnosti med klicem. V prejšnjem poglavju smo kot pomanjkljivost tega scenarija izpostavili povečanje časa predaje zaradi pridobivanja novega IP naslova in obveščanja terminala CN o novem IP naslovu. Poleg tega ima ta pristop še eno pomanjkljivost. Ker se `SIP re-INVITE` sporočilo pošlje direktno terminalu CN, SIP strežnik ni obveščen o spremembi lokacije mobilnega terminala. V literaturi lahko najdemo rešitve, kjer mobilni terminal obvesti SIP strežnik po izvedeni predaji zveze (Rajavelsamy et. al, 2007), vendar je potrebno v realnih omrežjih operaterja SIP strežnik obvestiti, preden se predaja zgodi, ker le na takšen način zagotovimo npr. pravilno zaračunavanje, saj je lahko cena klica v različnih omrežjih različna. Zato smo predlagali izboljšan scenarij za mobilnost med klicem SEMCS (*ang. SIP enhanced mid-call scenario*), ki je prikazan na sliki 15, izmenjava sporočil pa na sliki 16 (Libnik et. al, 2008, Libnik et. al, 2008a).



Slika 15: Scenarij SEMCS

Prvih pet korakov je enakih kot pri scenariju mobilnosti med klicem. Ko se mobilni terminal premakne v drugo omrežje (korak 6) pošlje `SIP re-INVITE` sporočilo SIP strežniku (korak 7) in ga obvesti o spremembi lokacije. SIP strežnik nato pošlje `SIP re-INVITE` sporočilo terminalu CN (korak 8). Po potrditvah (koraka 9 in 10) se vzpostavi nova RTP seja (korak 11).

Tako kot pri obeh v prejšnjem poglavju že predstavljenih scenarijih za mobilnost, mobilni terminal dobi nov IP naslov, ko se premakne v drugo omrežje.



Slika 16: Izmenjava sporočil za scenarij SEMCS

3.3.4 Pregled literature – protokol SIP

Banerjee s sodelavci (Banerjee et. al., 2004), Wu s sodelavci (Wu et. al., 2005) in Salsano s sodelavci (Salsano et. al, 2007) so predstavili rezultate analize predaje zveze med omrežjema UMTS/GPRS in WLAN s SIP protokolom. Ugotovili so, da je zakasnitev predaje na UMTS/GPRS omrežje zelo visoka, medtem ko je zakasnitev predaje zveze na WLAN omrežje dovolj nizka za predajo zveze tudi za aplikacije v realnem času. Zakasnitev je odvisna predvsem od zakasnitev v dostopovnih omrežjih. Banerjee in sodelavci (Banerjee et. al., 2006) predlagajo nov mehanizem izvajanja predaje zvez, s katerim zmanjšujejo zakasnitev ter izgubo paketov. Z novimi načini upravljanja z mobilnostjo za protokol SIP lahko izboljšamo učinkovitost predajanja zvez (zmanjšujejo zakasnitev in hitrost degradacije storitve). Tako Salsano s sodelavci (Salsano et. al., 2008) predlaga nov način imenovan MMUSE (*ang. mobility management using sip extensions*), Yee s sodelavci (Yee et. al., 2008) način PAHO (*ang. Proactive and Adaptive Handover*), Tantra s sodelavci (Tantra et. al., 2008) pa način VMMS (*ang. vertical mobility management scheme*).

3.4 Primerjava protokolov za predajo zveze

Iz opisa protokolov v prejšnjih poglavjih lahko sklenemo, da ima vsak predstavljen protokol svoje prednosti in pomanjkljivosti. V literaturi lahko najdemo tudi predloge sodelovanja med različnimi protokoli ter primerjave delovanja. Chen s sodelavci (Chen et. al., 2007) ter Leu (Leu, 2009) predlagata sodelovanje SCTP in SIP ter tako izboljševanje izvajanja nezaznavnih zvez. Lee s sodelavci (Lee et. al., 2005) in Wang s sodelavci (Wang et. al., 2004) predlagata sodelovanje protokolov SIP in MIP, za izvajanje predaj zvez, ko je uporabljena večpredstavnostna storitev. Kwon in sodelavci (Kwon et. al, 2002) in Polidoro in sodelavci (Polidoro et. al., 2008) so primerjali delovanje protokolov MIP in SIP ter ugotovili, da je čas prekinitve med predajo močno povezan z zakasnitvijo med obema mobilnima terminaloma. Ko so zakasnitve majhne, daje protokol SIP boljše rezultate, ko pa so zakasnitve večje, je bolj smiselna uporaba protokola MIP. Mohanty in Akyildiz (Mohanty and Akyildiz, 2007) sta ugotovila, da je protokol SIP bolj primeren za aplikacije v realnem času, ki uporabljajo protokol UDP, protokol MIP pa za aplikacije, ki ne tečejo v realnem času in uporabljajo protokol UDP.

Da bi lahko primerjali različne pristope (MIP, mSCTP in SIP) smo definirali štiri kriterije (Libnik et. al, 2008a):

- Vpliv na omrežje: ob implementaciji podpore za upravljanje z mobilnostjo bodo lahko v operaterskih omrežjih potrebne spremembe, kot sta npr. dodajanje novih omrežnih elementov ali dodatnih funkcionalnosti.
- Vpliv na aplikacijo: podpora predaje zveze lahko ima za posledico spremembe v uporabniški aplikaciji.
- Uporaba omrežnih virov: za izvedbo predaje zvez je potrebno rezervirati določene omrežne vire na

omrežnih elementih pri operaterju. Ta parameter opisuje vpliv izvajanja predaj zvez na zasedbo omrežnih virov.

- Uporaba v operaterskih okoljih: za podporo mobilnosti morajo operaterji implementirati nove protokole, če ti že ne obstajajo. Takšni posegi so lahko kompleksni in dragi. Ta parameter opisuje pogostost uporabe določenega protokola v obstoječih operaterskih okoljih.

Opisani pristopi so primerjani v tabeli 3.

Tabela 3: Primerjava uporabe različnih protokolov za upravljanje z mobilnostjo

Sloj (protokol)	Vpliv na omrežje	Vpliv na aplikacijo	Uporaba omrežnih virov	Uporaba v operaterskih okoljih
Omrežni sloj (MIP)	Velik (zahteva uvedbo domačih in tujih gostiteljev)	Brez vpliva	Velika	Majhna
Transportni sloj (mSCTP)	Majhen oz. brez vpliva (terminal MN mora podpirati mSCTP)	Velik (aplikacija mora delovati prek SCTP)	Majhna (samo terminal MN)	Majhna oz. ni uporabljen
Aplikacijski sloj (SIP)	Majhen oz. brez vpliva (zahtevan je SIP posredovalni strežnik)	Velik	Srednja (samo posredovalni strežnik)	Velika

Pri uporabi MIP protokola za upravljanje z mobilnostjo je potrebno v omrežje vpeljati domače in tuje gostitelje. Ker je MIP protokol omrežnega sloja, ki se uporablja zgolj za transport, uporabniške aplikacije ni potrebno spreminjati, saj ne sodeluje pri izvajanju predaje zveze. Uporaba omrežnih virov je v tem primeru velika, ker se predaja zveze izvaja v samem omrežju. Uporabnost protokola MIP je omejena tudi z majhno pogostostjo uporabe tega protokola v današnjih operaterskih omrežjih.

Izvajanje predaje zveze na transportnem sloju ima majhen vpliv na omrežje. Če terminal MN podpira mSCTP, operaterjem ni potrebno spreminjati ničesar v njihovem omrežju. Vendar mora aplikacija uporabljati SCTP za transportni protokol za razliko od večine današnjih aplikacij, ki uporabljajo TCP ali UDP. Največja slabost uporabe protokola mSCTP pa je, da ga zelo malo operaterjev uporablja v trenutnih omrežjih.

Prednost uporabe SIP protokola za izvajanje predaje zveze je, da je protokol SIP aplikacijskega sloja in tako nima velikega vpliva na omrežje. Vendar pa je potrebno za podporo predajanja zvez uporabniško aplikacijo prilagoditi oz. izboljšati. Neodvisnost od transportnega sloja pomeni tudi, da ne zaseda veliko omrežnih virov. Največja prednost uporabe protokola SIP pa je, da je zelo pogosto uporabljen v obstoječih operaterskih omrežjih, saj je ta protokol vpeljala večina operaterjev, ki ponujajo storitev IP telefonije, kjer se SIP uporablja za signalizacijo.

Pri našem delu smo se osredotočali predvsem na rešitve, ki bi jih lahko brez večjih posegov vpeljali v obstoječe omrežje operaterja. Protokol SIP je že vpeljan v večini operaterskih okolij in je bil tudi izbran kot glavni signalizacijski protokol v IMS arhitekturi. Ker uporablja aplikacijski sloj, je SIP neodvisen od dostopovnih tehnologij, kar omogoča uporabo tudi pri gostovanjih v omrežjih operaterja, ki ne ponuja SIP storitev, saj se omrežje, v katerem uporabnik gostuje, uporablja zgolj za dostop do aplikacijskega strežnika v domačem omrežju. Zato smo izbrali SIP za nadaljnje delo in razvoj novih postopkov za upravljanje z mobilnostjo.

4 SIP telefonija v operaterskem okolju

Z vpeljavo IP protokola v hrbtenična omrežja so operaterji začeli ponujati nove storitve, ki so jim omogočale konsolidacijo obstoječih omrežij. Z migracijo na popolnoma IP omrežja, se vsi podatkovni tokovi združujejo v enem omrežju, zaradi česar lahko ena storitev vpliva na drugo. To sicer ni problematično za aplikacije, ki nimajo velikih zahtev glede kakovosti storitve (QoS), kot je npr. brskanje po internetu. Vendar pa je lahko zelo kritično za aplikacije, ki potekajo v realnem času (npr. govorne in video komunikacije) in zahtevajo vpeljavo mehanizmov za zagotavljanje ustreznega nivoja QoS, če hočejo operaterji zagotavljati ustrezen nivo uporabniške izkušnje (QoE). Na nivo QoE multimedijskih storitev v glavnem vplivajo izvorna kakovost multimedijske storitve in kakovost dostave (prenosa) vsebine skozi omrežje. Prvi faktor je neproblematičen, saj so avdio ali video vsebine kodirane z določeno bitno hitrostjo, ki ima neposreden vpliv na nivo QoE. Višja bitna hitrost se bo odražala v višjem nivoju QoE in obratno. V nadaljevanju se bomo osredotočali predvsem na drugi faktor – to je kakovost prenosa vsebine skozi omrežje, v katerem se lahko kakovost vsebine zmanjša.

SIP protokol podpira več tipov multimedijskih aplikacij. Pri našem delu smo se osredotočili na predajo zveze med heterogenimi omrežji, pri čemer smo kot aplikacijo izbrali IP telefonijo, ki je ena izmed najbolj uporabljenih SIP aplikacij. V tem poglavju bomo podrobneje obdelali:

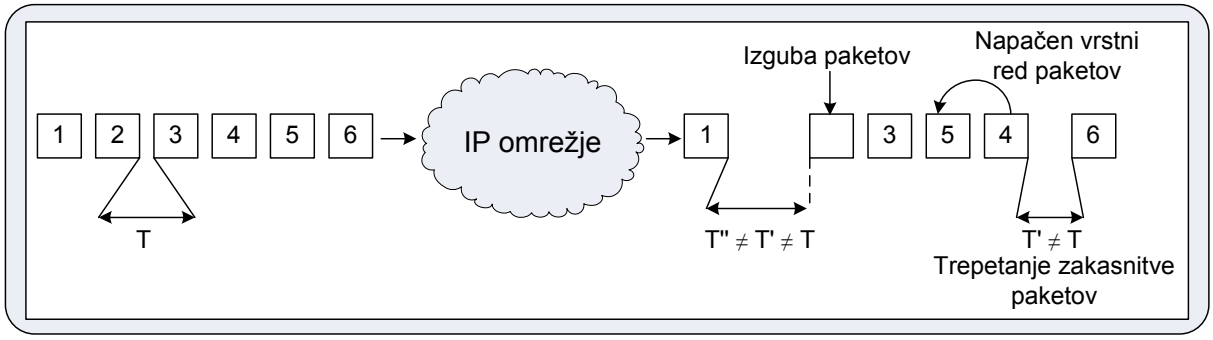
- zagotavljanje kakovosti storitev, kjer bomo predstavili parametre, s katerimi ocenjujemo kakovost storitve IP telefonije;
- spremembe arhitekture omrežja, ki so potrebne za zagotavljanje določenih funkcionalnosti ob ponujanju IP telefonije;
- problematiko, ki se pojavlja v dostopovnih omrežjih, kjer bomo predstavili rezultate praktičnih preizkusov meritev uporabe IP telefonije v WLAN in HSPA omrežjih.

4.1 Parametri za kakovost storitev IP telefonije

Aplikacije, ki tečejo v realnem času, kot so video in govorne storitve, so zelo občutljive na QoS parametre. ITU v standardih izpostavlja štiri parametre, ki lahko vplivajo na kakovost storitve IP telefonije (ITU-D, 2003):

- zakasnitev paketov od konca do konca (*ang. end-to-end delay*);
- trepetanje zakasnitve paketov (*ang. jitter*);
- izguba paketov (*ang. packet loss*);
- odmev (*ang. echo*).

Zakasnitev paketov od konca do konca pomeni čas, ki je potreben, da paket prepotuje pot od oddajnika do sprejemnika. Trepetanje zakasnitve paketov nastane zaradi spremenljivega časa prenosa paketa skozi omrežje. Izguba paketov pomeni izgubo informacije pri prenosu skozi omrežje. Z odmevom pa označujemo čas, ki preteče med prenosom signala in prejemom istega signala v obliki odboja, ki je posledica elektronskih komponent analognega dela sistema, ki del signala vračajo. V nadaljevanju smo se osredotočili na prve tri QoS parametre, ki so predstavljene na sliki 17, medtem ko problematike odmeva ne bomo več obravnavali. Natančnejše opise izbranih parametrov bomo podali v naslednjih poglavjih.



Slika 17: Glavni parametri, ki vplivajo na QoS

4.1.1 Zakasnitev paketov od konca do konca

Zakasnitev paketov od konca do konca (D_{e2e}) je definirana kot čas, ki je potreben, da govorni signal prepotuje pot od oddajnika do sprejemnika:

$$D_{e2e} = T_{com} + T_{pac} + D_{access\_1} + D_{core} + D_{access\_2} + T_{depac} + T_{decom} \quad (1)$$

Kot je podano v enačbi (1) je zakasnitev paketov D_{e2e} sestavljena iz več parametrov. Čas T_{com} je definiran kot čas kompresije, kar pomeni seštevek zakasnitev okvirja, zakasnitev kodiranja in zakasnitev procesiranja. Parameter T_{pac} določa čas paketizacije, torej čas, ki ga aplikacija potrebuje, da ustvari paket. Oba do sedaj opisana parametra predstavljata zakasnitev na strani klicatelja, torej na oddajni strani. Nato se paket pošlje prek različnih omrežij, kar vnaša dodatne zakasnitve. Najprej gre paket čez prvo dostopovno omrežje, v katerem je klicatelj in ima zakasnitev D_{access_1}. To dostopovno omrežje je povezano v hrbtenično omrežje, ki tudi vnaša svojo zakasnitev določeno z D_{core}. Nato paket vstopi v dostopovno omrežje, v katerem je klicani (sprejemnik). V kolikor to omrežje ni isto kot omrežje, v katerem je klicatelj, vnaša drugačno zakasnitev označeno z D_{access_2}. Tako je paket pripotoval do sprejemnika. Na sprejemni strani se najprej zgodi depaketizacija (inverzni postopek paketizacije), katere trajanje opisujemo s parametrom T_{depac}. Temu sledi dekompresija (inverzni postopek kompresije), katere trajanje označujemo s parametrom T_{decom}. Vsi opisani parametri razen D_{access_1}, D_{access_2} ter D_{core} so odvisni od naprav oziroma nastavitev aplikacije in se običajno med komunikacijo ne spreminjajo. Zakasnitev dostopovnih in hrbteničnih omrežij pa se lahko spreminja in vpliva na nivo QoS storitve IP telefonije. Zakasnitev, ki jo vnaša IP omrežje, je lahko precej večja kot zakasnitev v klasičnih TDM omrežjih. Hkrati jo je zelo težko predvideti z visoko stopnjo zanesljivosti, saj je odvisna od velikega števila običajno neznanih parametrov, kot so npr. velikost usmerjevalnih tabel, zgostitve v omrežju kot posledica preobremenjenosti, izpadi linij in čakalne vrste. Zakasnitev D_{core} je običajno manj kritična, saj operaterji hrbtenična omrežja dobro kontrolirajo, upravljajo in prilagajajo arhitekturo tako, da so visoko prepustna. Več težav se pojavi v dostopovnih omrežjih, ki so deljena med več uporabniki in običajno predstavljajo ozko grlo zaradi omejene prepustnosti. To je še posebej pomembno pri javnih brezžičnih omrežjih, kot je npr. WLAN, kjer lahko več uporabnikov povzroča preobremenjenost dostopovnih povezav, kar pomeni, da lahko v tem primeru zakasnitev D_{access} zelo naraste. Natančnejša analiza dostopovnih omrežij je podana v poglavju 4.3.

4.1.2 Trepetanje zakasnitve paketov

Trepetanje zakasnitve paketov je naslednji parameter, ki lahko vpliva na nivo QoS in nastane zaradi spremenljivega časa prenosa paketa skozi omrežje. Protokol UDP, ki se uporablja pri storitvah IP telefonije za prenos govora (za signalizacijo je uporabljen protokol TCP), deluje v nepovezavnem načinu, v katerem paketi ne potujejo nujno po istih poteh. Posledica tega je lahko nihanje časa potrebnega za transport paketa skozi omrežje, kot je prikazano na sliki 17. Za zmanjševanje vpliva na nivo QoS zaradi trepetanja zakasnitev paketov na strani sprejemnika se lahko uporabijo izravnalniki trepetanja zakasnitev paketov (*ang. jitter buffer*), ki omogočajo ponovno sinhronizacijo prihoda paketov z različnimi zakasnitvami. Vendar pa vpeljava takšnega elementa v omrežje še povečuje čas prenosa. ITU priporoča, da mora biti trepetanje zakasnitve paketov manjše od 100 ms, če želimo zagotavljati sprejemljiv nivo kakovosti storitve IP telefonije (ITU-D, 2003).

4.1.3 Izguba paketov

Izguba paketov se kaže kot manjkajoča informacija ob sprejemu avdio signala. Glede na število izgubljenih paketov je lahko kakovost zvoka pri sprejemniku poslabšana. Izguba paketov je integralni del splošnega koncepta IP omrežij, saj morajo usmerjevalniki, z algoritmi za zgodnje odkrivanje, v omrežju odmetavati pakete, da preprečujejo zgostitve. Poznamo štiri glavne vzroke, ki imajo za posledico izgubo paketov (ITU-D, 2003):

- pretečena življenjska doba paketa (TTL=0);
- zakasnitev paketov pri sprejemniku je večja od velikosti izravnalnika trepetanja;
- odmetavanje paketa v modulu, ki je namenjen preprečevanju preobremenitev v omrežju;
- nepravilen format paketa zaradi napak pri prenosu.

Nivo izgube paketov je odvisen od kakovosti povezav uporabljenih za komunikacijo in od dimenzioniranja omrežja. Za sprejemljivo kakovost storitve IP telefonije, mora biti izguba paketov manjša od 20 procentov (ITU-D, 2003).

Izgubo paketov lahko tudi zmanjšujemo. Ena izmed možnih rešitev je vpeljava sistemov za odpravo napak, ki uporabljajo prilagodljive kodeke. To pomeni, da se kodeki spreminjajo glede na nivo izgube paketov, ki je v določenem obdobju statistično spremljana v omrežju. Z uporabo tovrstnih sistemov, je mogoče doseči zelo visok nivo kakovosti zvoka tudi pri prenosu preko interneta.

4.1.4 E-model

Za aplikacije, kot je IP telefonija, je s stališča uporabnika najpomembnejše merilo nivo QoE, s katerim določamo nivo uporabniške izkušnje. Za merjenje nivoja QoE je ITU definiral E-model, ki na podlagi različnih parametrov omogoča izračun subjektivne zaznave kakovosti storitve IP telefonije. Določen je v (ITU-T, 2005). Izhod iz E-modela je faktor *R* (*ang. transsmition rating factor*) izračunan, kot je podano enačbi (2).

$$R = Ro - Is - Id - Ie + A \tag{2}$$

Kjer parameter *Ro* predstavlja vpliv razmerja SNR, ki zajema šum linije in šum okolice, parameter *Is* združuje vplive, ki se pojavijo bolj ali manj hkrati z govornim signalom (npr. kvantizacijski šum), parameter *Id* predstavlja vpliv zakasnitve in odbojev, parameter *Ie* predstavlja vpliv opreme, ki ga povzročajo kodeki z nizko bitno hitrostjo. Parameter *A* predstavlja pripravljenost uporabnikov za sprejem slabše kakovosti klica na račun možnosti izvedbe klice. Na primer uporabniki v mobilnih omrežjih običajno klic enake kakovosti ocenjujejo višje kot v fiksni telefoniji. Tako je vrednost *A* nič za fiksno telefonijo, pet za uporabo mobilne telefonije znotraj stavb, deset za uporabo mobilne telefonije na prostem in dvajset za uporabo satelitskih povezav.

E-model je bil prvotno zasnovan kot orodje za načrtovanje omrežij, danes pa je uporabljen tudi za ugotavljanje kakovosti govora v realnem času. Veliko orodij za testiranje IP telefonije uporablja E-model za izračunavanje nivoja QoE v realnem času. Da bi lahko uporabili E-model v realnem času, je potrebno nekatere vrednosti parametrov, ki jih ne moremo pasivno izmeriti, v enačbi (2) predpostaviti. Parametra *Ro* in *Is* sta povezana s signalom in nanju ne vpliva prenos skozi omrežje. Edina parametra, ki vplivata na spreminjanje faktorja *R* in se spreminjata s prenosom skozi omrežje, sta *Id* in *Ie*. V literaturi lahko najdemo priporočila za poenostavljen način izračunavanja faktorja *R*. Cole s sodelavci (Cole et. al, 2001) podaja izračun faktorja *R* kot $R = 94{,}2 - Id - Ie$, ITU (ITU-T, 2005) kot $R = 93{,}2 - Id - Ie$, Psytechnics (Psytechnics, 2002) pa kot $R = 93{,}34 - Id - Ie$.

Izračunana ali izmerjena vrednost faktorja *R* nam določa nivo QoE storitve. Tabela 4 (ITU-T, 2005) podaja definicijo nivoja kakovosti prenosa govora v odvisnosti od faktorja *R*, tabela 5 pa odvisnost faktorja *R* od zakasnitve paketov za kodek G.711, ki smo ga uporabili pri našem delu (ITU-T, 1999).

Tabela 4: Definicija kakovosti prenosa govora v odvisnosti od faktorja *R*

Vrednosti faktorja *R*	**Nivo kakovosti prenosa govora**	**Zadovoljstvo uporabnikov (QoE)**
$90 \leq R < 100$	Najvišji nivo	Zelo zadovoljni
$80 \leq R < 90$	Visok nivo	Zadovoljni
$70 \leq R < 80$	Srednji nivo	Nekateri uporabniki nezadovoljni
$60 \leq R < 70$	Nizek nivo	Veliko uporabnikov nezadovoljnih
$50 \leq R < 60$	Slab nivo	Skoraj vsi uporabniki nezadovoljni

Tabela 5: Odvisnost faktorja *R* od zakasnitve paketov

Srednja vrednost zakasnitve paketov od konca do konca v eno smer (ms)	~0	50	100	150	200	250	300	350	400	450
Faktor *R*	94	93	92	90	87	80	74	68	63	59

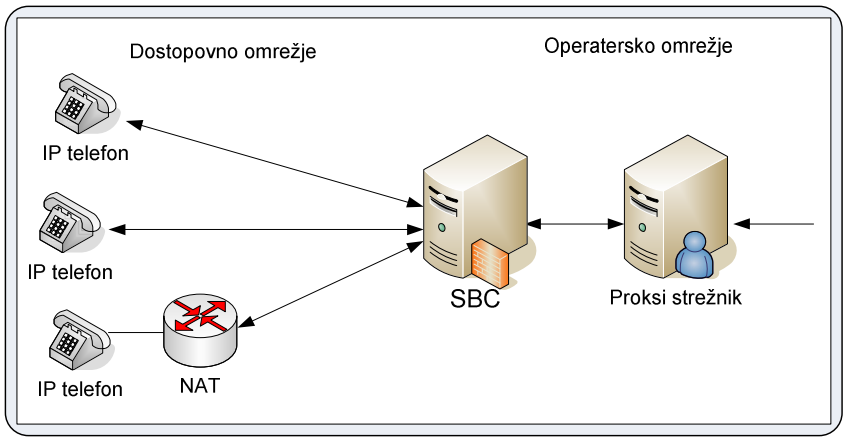
Predstavljene tabele kažejo, da bi morala biti vrednost faktorja *R* nad 90, če hočemo doseči najboljšo kakovost in najvišje zadovoljstvo uporabnikov. To pomeni, da mora biti zakasnitev paketov od konca do konca v eno smer manjša od 150 ms. Vendar pa so izkušnje iz prakse pokazale, da je za uporabnika še vedno sprejemljiva tudi nekoliko višja zakasnitev, zato je splošno sprejeta zakasnitev paketov za ustrezno kakovost govorne komunikacije 200 ms v eno smer (Cisco, 2010).

4.2 Arhitektura operaterskega omrežja za IP telefonijo

Z uvedbo IP telefonije v omrežje morajo operaterji zaradi zagotavljanja varnostno-regulatornih zahtev v svoja omrežja vpeljati elemente, ki vplivajo na arhitekturo rešitve. Običajno v svoje omrežje implementirajo mejni krmilnik sej (SBC), ki omogoča več funkcionalnosti, med katerimi so tudi (Hautakorpi et. al, 2008):

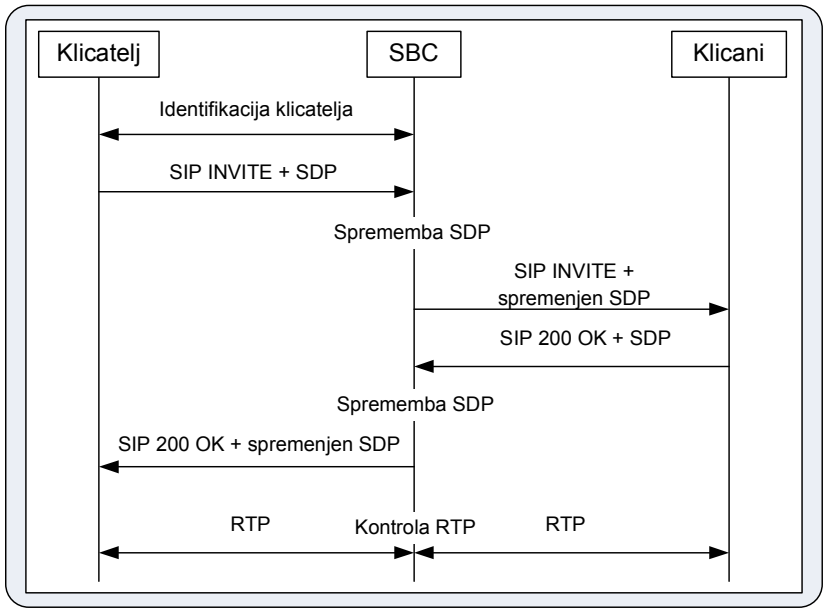
- zaščita elementov, ki vsebuje nadzor dostopa, skrivanje topologije omrežja ter zaznavanje in preprečitev napadov (npr. DoS);
- funkcionalnosti, ki niso na voljo na končnih terminalih, kot sta prečkanje z uporabo NAT (*ang. NAT travesal*) ter medsebojno delovanje različnih protokolov oziroma prekodiranje (*ang. transcoding*);
- upravljanje s prometom (kontrola medijskega toka in nivoja QoS).

Vpeljava elementa SBC v omrežje operaterja lahko ima za posledico, da omrežna arhitektura ni več v skladu z osnovnimi principi SIP arhitekture. Element SBC, ki podpira SIP protokol, običajno upravlja tako s signalizacijo kot tudi z medijskim (RTP) tokom. Koncept uporabe elementa SBC v dostopovnem omrežju operaterja je predstavljen na sliki 18. Element SBC je postavljen na mejo med dostopovnim omrežjem in omrežjem operaterja ter s tem nadzira dostop do operaterjevega omrežja. Zagotavlja zaščito elementom, kot so medijski strežnik, aplikacijski strežnik in medijski prehod, pred neavtorizirano uporabo in pred DoS napadi ter nadzira signalni in RTP promet. Element SBC omogoča tudi nadzor dostopa, s katerim operaterji preprečujejo preveliko število registracij in preobremenjenost dostopovnih povezav. Končne točke (IP terminali) imajo v nastavitvah vpisan naslov elementa SBC kot njihov zunanji posredovalni strežnik (*ang. outbound proxy*).



Slika 18: Koncept uporabe SBC v dostopovnem omrežju operaterja

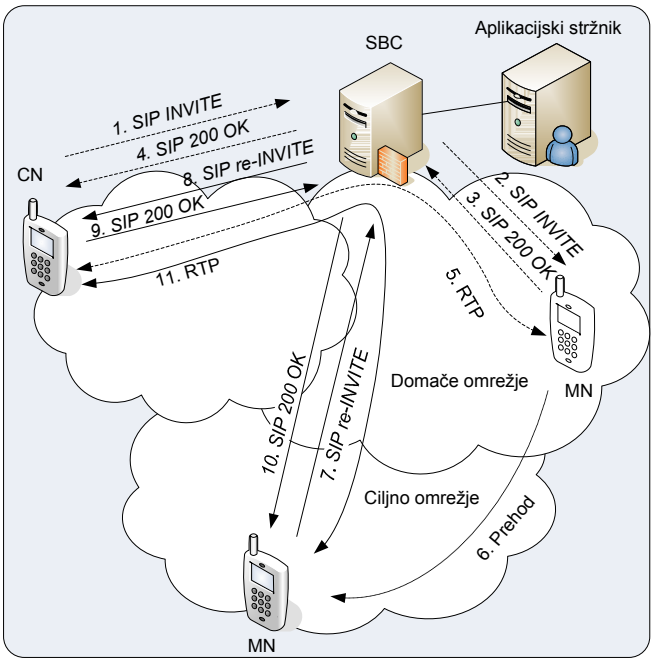
S postavitvijo SBC elementa v omrežje se spremenijo tudi poti, po katerih se prenaša signalni (SIP) in medijski (RTP) promet tako, da je tudi ves medijski promet usmerjan prek SBC, kot je prikazano na sliki 19. Tako govorna komunikacija ne poteka več neposredno med terminali ampak čez SBC.



Slika 19: Primer poteka klica

Ob vzpostavitvi klica element SBC najprej identificira klicatelja. To lahko stori npr. z uporabo informacij, ki jih je sprejel med registracijo. Nekateri krmilniki sej delujejo tako, da prepustijo avtentikacijo uporabniškega agenta, ki vzpostavlja klic, posredovalnemu strežniku. Uporabniki brez avtorizacije so zavrnjeni. Po identifikaciji se v elementu SBC spremni opis seje v sporočilu `SIP INVITE` in `SIP 200 OK`, tako da bo medijski tok usmerjen prek tega elementa. Ko začne medijski tok teči, lahko element SBC preveri, ali je uporabljen pravilen kodek, ki sta si ga na začetku izbrala klicani in klicatelj.

Z opisanimi funkcionalnostmi se spremenijo tudi poti medijskih tokov v scenariju SEMCS. Spremembe so prikazane na sliki 20 in so narejeno tako, da tudi RTP promet teče prek elementa SBC.



Slika 20: Spremenjena pot medijskega toka v SEMCS zaradi uporabe SBC

4.3 Dostopovno omrežje in uporaba IP telefonije

Dostopovno omrežje običajno ni pod nadzorom operaterja. Kot smo predstavili v poglavju 4.1.1 ima lahko poslabšanje razmer v dostopovnem omrežju zelo velik vpliv na kakovost storitve IP telefonije. Problematična so predvsem omrežja, ki so javno dostopna in brezplačna. Veliko število uporabnikov lahko z različnimi aplikacijami (npr. branje elektronske pošte, FTP) popolnoma obremeni dostopovne povezave, kar lahko onemogoča uporabo storitev v realnem času. V tem poglavju bomo predstavili vpliv dostopovnega omrežja na kakovost storitve IP telefonije. Izvedli smo več meritev v realnem okolju. V nadaljevanju bomo najprej predstavili programsko opremo, ki smo jo uporabljali za meritve, nato pa še rezultate praktičnih poizkusov.

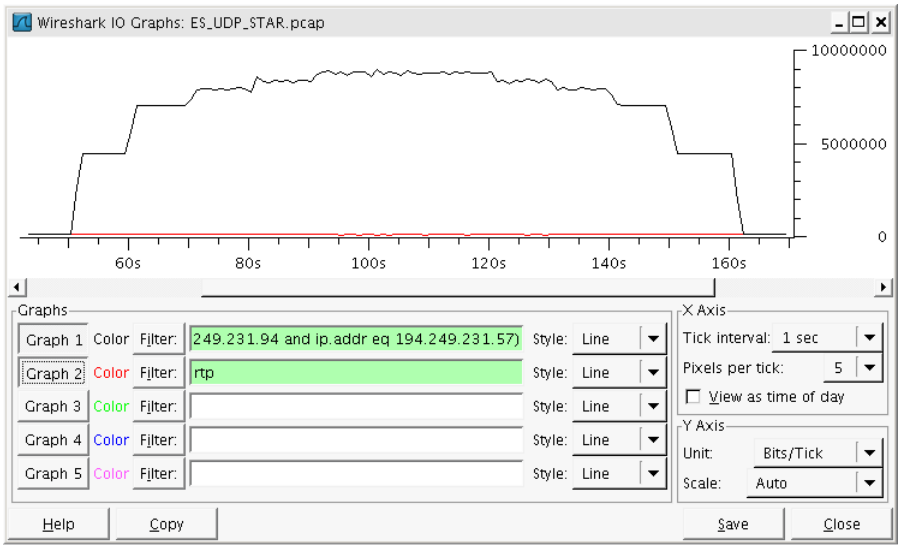
4.3.1 Predstavitev uporabljenih aplikacij

Pri meritvah smo uporabljali tri različne aplikacije, ki jih bomo v nadaljevanju na kratko opisali, in sicer:

- Analizator Wireshark (Wireshark, 2010): namenjen za analizo prejetega prometa, izračun zakasnitve paketov ter izračun trepetanja zakasnitev paketov;
- Orodje NetStumbler (Netstumbler, 2010).: namenjen za meritve razmerja SNR signala WLAN omrežja;
- Orodje D-ITG (D-ITG, 2010): namenjen za generiranje dodatnih UDP paketov.

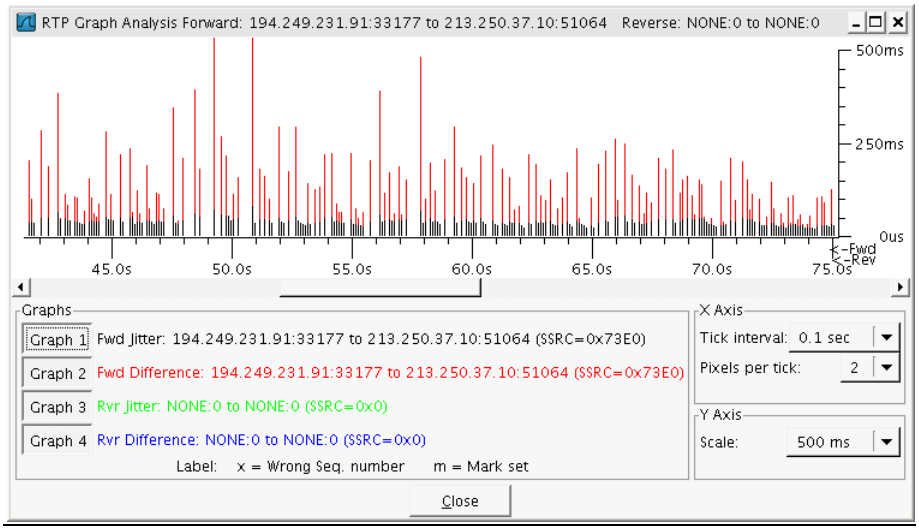
Analizator Wireshark

Analizator Wireshark analizira vsebino vseh paketov, ki se prenašajo po omrežju. Za potrebe analize posameznega tipa prometa lahko uporabimo različne filtre, ki nam omogočajo prikaz želenega prometa, npr. promet med določenima IP naslovoma, promet, ki je nastal z uporabo določenega protokola. Na sliki 21 je prikazan del analize prenesenega prometa. Na takšen način smo lahko natančno analizirali strukturo prometa in ugotavljali tudi delež RTP prometa glede na celoten promet.



Slika 21: Prikaz filtriranja omrežja v analizatorju Wireshark

Poleg osnovne analize prometa analizator Wireshark omogoča tudi ločeno analizo storitve IP telefonije, ki omogoča spremljanje parametrov RTP prometa, kot so trepetanje zakasnitve paketov in zakasnitve paketov, kot je to prikazano na sliki 22.



Slika 22: Uporabniški vmesnik za analizo RTP prometa v analizatorju Wireshark

Zakasnitev paketov od konca do konca podaja informacijo, koliko je posamezen paket zakasnjen, glede na čas prihoda. Analizator Wireshark iz pridobljenih paketov izračuna diferenco zakasnitve in trepetanje zakasnitve paketov po standardu RFC 3550 (Schulzrinne et. al, 2003). Izračun diference zakasnitve paketov je podan v enačbi (3).

$$D_{i,j} = (R_j - R_i) - (S_j - S_i) = (R_j - S_j) - (R_i - S_i) \tag{3}$$

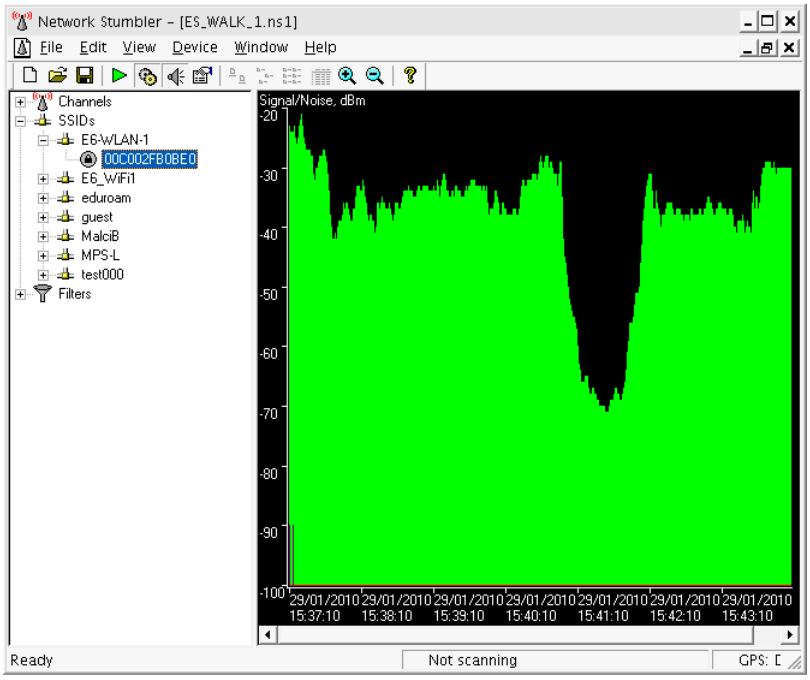
kjer je S_i časovni žig RTP paketa i, R_i je čas prihoda paketa i.

RTP časovni žig temelji na frekvenci vzorčenja posameznega kodeka, ki je 8000 Hz za večino avdio kodekov in 90000 Hz za večino video kodekov. Ker mora biti frekvenca vzorčenja znana za pravilen izračun spremembe zakasnitve paketov, je težko natančno izračunati trepetanje zakasnitev za dolžine koristne vsebine (*ang. payload*), ki se dinamično spreminjajo, saj morata biti znana kodek in frekvenca vzorčenja. Trepetanje zakasnitve paketov je v analizatorju Wireshark izračunana iz pridobljenih diferenc v prihodu po enačbi (4).

$$T_i = T_{i-1} + \frac{(|D_{i-1,i}|) - T_{i-1}}{16} \quad (4)$$

Orodje NetStumbler

Meritve razmerja SNR vrednosti smo izvajali z orodjem NetStumbler. Na sliki 23 je prikazan uporabniški vmesnik.



Slika 23: Uporabniški vmesnik orodja NetStumbler

Orodje NetStumbler omogoča meritve razmerja SNR določenega WLAN omrežja, ki ga izberemo prek ponujenih identifikatorjev BSSID ali z izbiro določenega kanala. Meritve se izvajajo v realnem času. Po končani meritvi omogoča tudi izvoz izmerjenih podatkov v izhodno datoteko.

Orodje D-ITG

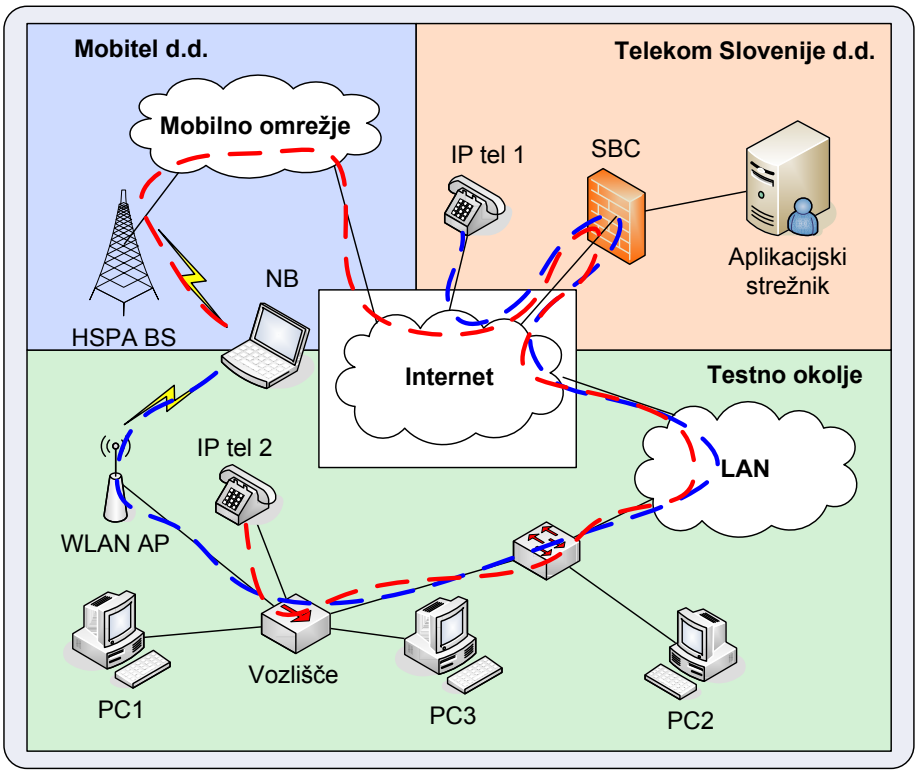
Orodje D-ITG omogoča prek enostavnih ukazov generiranje UDP prometa med dvema IP naslovoma. Na strani oddaje (generatorja) UDP paketov nastavimo:

- sprejemna vrata;
- oddajna vrata;
- velikost UDP paketov;
- število paketov na sekundo;
- trajanje pošiljanja.

Na sprejemni strani pa orodje D-ITG deluje le kot ponor za UDP pakete, ki mu jih pošilja oddajna stran.

4.3.2 Rezultati praktičnih poizkusov

Za potrebe analize dostopovnih omrežij smo vzpostavili testno okolje v operaterskem omrežju. Arhitekturo testiranega omrežja prikazuje slika 24.



Slika 24: Omrežna arhitektura testne postavitve

Cilj poizkusov je bil preučiti uporabnost IP telefonije v realnih HSPA in WLAN omrežjih. WLAN omrežje je bilo priključeno v LAN omrežje. Pri meritvah HSPA omrežja smo uporabili omrežje družbe Mobitel d.d. Moč signala HSPA omrežja je bila v demonstracijskem okolju zelo visoka (antena na sosednji zgradbi), zato smo lahko dosegali zelo dobre rezultate. LAN in HSPA omrežji sta bili preko interneta povezani z javnim IP vmesnikom elementa SBC. Uporabili smo dva tipa SIP terminalov – programskega in namiznega. Programski SIP klient, ki je bil nameščen na prenosnem računalniku NB, je bil preko WLAN vmesnika povezan z WLAN dostopovno točko AP. Prenosni računalnik smo uporabili, da smo lahko merili vpliv gibanja uporabnika na QoS parametre. Na računalniku NB smo uporabili orodje NetStumbler, ki nam je omogočilo meritve signala in šuma WLAN dostopovne točke. NB je bil s HSPA USB modemom povezan tudi na mobilno podatkovno omrežje. Dostopovna točka AP je bila povezana na vozlišče (*ang. hub*), na katero so bili povezani tudi osebni računalnik PC1, IP terminal IP tel 2 ter osebni računalnik PC3. Vozlišče je bilo povezano s stikalom, ki je bilo priključeno na LAN omrežje in na osebni računalnik PC2. Namen uporabe vozlišča je bil dvojen:

i. nadzor dostopovne povezave med PC1 in PC2 ter s tem nadzor nivoja QoS storitve IP telefonije, saj vozlišče deluje tako, da pomnoži ves promet na vsa vrata vozlišča. Tako smo lahko nadzor vsega prometa izvajali na PC3, na katerem smo uporabili analizator Wireshark.
ii. znižati prepustnost povezave na 10 Mbit/s in s tem ustvariti ozko grlo v dostopovnemu omrežju.

Uporabili smo še en IP terminal IP tel 1, ki je bil povezan preko interneta. Za izvajanje meritev smo vzpostavili klic med SIP klientom na NB in IP tel 1 ali IP tel 2. SIP klient in oba IP telefona sta bila registrirana na storitev IP telefonije Telekoma Slovenije.

Izvedli smo štiri poizkuse:

1. ES_BASIC_HSPA: S tem poizkusom smo ovrednotili sposobnosti mobilnega omrežja. Vzpostavili smo klic med SIP klientom na NB in IP tel 2. Klic je bil vzpostavljen prek HSPA USB modema, ki je bil priključen na NB. Prenosnega računalnika nismo premikali. RTP podatkovni tok tega scenarija je prikazan z rdečo črtkano črto.
2. ES_BASIC_WLAN: S tem poskusom smo ovrednotili sposobnosti WLAN omrežja. Vzpostavili smo klic med SIP klientom na NB in IP tel 1. Klic je bil vzpostavljen prek WLAN vmesnika na NB. Razen klica ni bilo na tem dostopovnem omrežju nobenega drugega prometa. Ker računalnika NB nismo premikali in smo bili blizu AP, nam je to omogočalo zelo dober signal. RTP podatkovni tok tega scenarija je prikazan z modro črtkano črto.
3. ES_TRAFFIC: V tem poizkusu smo analizirali vpliv preobremenjenosti na nivo QoE. Najprej smo vzpostavili klic med SIP klientom na NB in IP tel 1 prek AP. Prenosnega računalnika NB med

poizkusom nismo premikali, tako da je bil signal WLAN omrežja ves čas ustrezno visok in ni vplival na kakovost storitve IP telefonije. Med klicem smo začeli generirati dodaten promet med računalnikoma PC1 in PC2, kar je povzročilo zgostitve na dostopovni povezavi. RTP podatkovni tok je prikazan z modro črtkano črto.

4. ES_WALK: V tem poizkusu smo analizirali vpliv razmerja SNR na nivo QoE. Najprej smo vzpostavili klic med SIP klientom na NB in IP tel 1 prek AP. Med klicem smo se s prenosnim računalnikom NB začeli premikati od AP in nazaj k AP. V tem scenariju nismo generirali nobenega drugega prometa. RTP podatkovni tok tega scenarija je prikazan z modro črtkano črto.

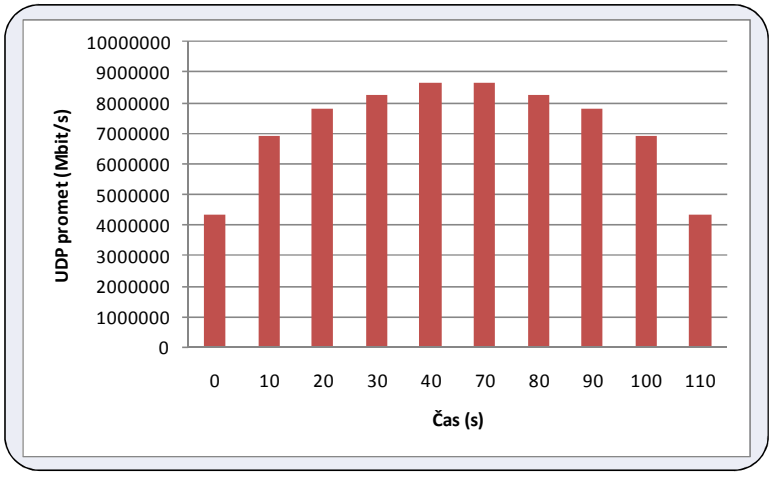
Izvedli smo 10 meritev; najbolj tipične so predstavljene v nadaljevanju. Ker smo želeli dobiti čim bolj primerljive rezultate različnih scenarijev, smo uporabili posnet govor, ki smo ga predvajali na NB med klicem. Tako je pri vsakem klicu govor generiral zgolj SIP klient na NB.

V poizkusih ES_BASIC_HSPA in ES_BASIC_WLAN smo merili zakasnitev paketov od konca do konca ter trepetanje zakasnitve paketov z analizatorjem Wireshark na PC3. Rezultati so statistično povprečje 10-minutnega klica in so predstavljeni v tabeli 6. Kot lahko vidimo, smo v obeh omrežjih izmerili zelo dobre vrednosti zakasnitve in trepetanje zakasnitve paketov.

Tabela 6: Rezultati poizkusov ES_BASIC_HSPA in ES_BASIC_WLAN

Dostopovna tehnologija	Zakasnitev paketov		Trepetanje zakasnitve paketov	
	Srednja vrednost	Standardna deviacija (σ)	Srednja vrednost	Standardna deviacija (σ)
HSPA	29.9 ms	15.7 ms	22.4 ms	182.2 ms
WLAN	29.9 ms	11.6 ms	17.6 ms	183.4 ms

V poizkusu ES_TRAFFIC smo generirali dodaten promet. To smo naredili z orodjem D-ITG. Programska oprema je bila uporabljena na PC1, na katerem smo promet generirali, in PC2, na katerega smo promet pošiljali. UDP promet smo povečevali postopoma, kot je prikazano na sliki 25. Pakete smo definirali tako, da so imeli konstantno koristno vsebino v velikosti 500 bajtov. Skupaj s protokolnimi glavami je bila dolžina enega paketa 542 bajtov.

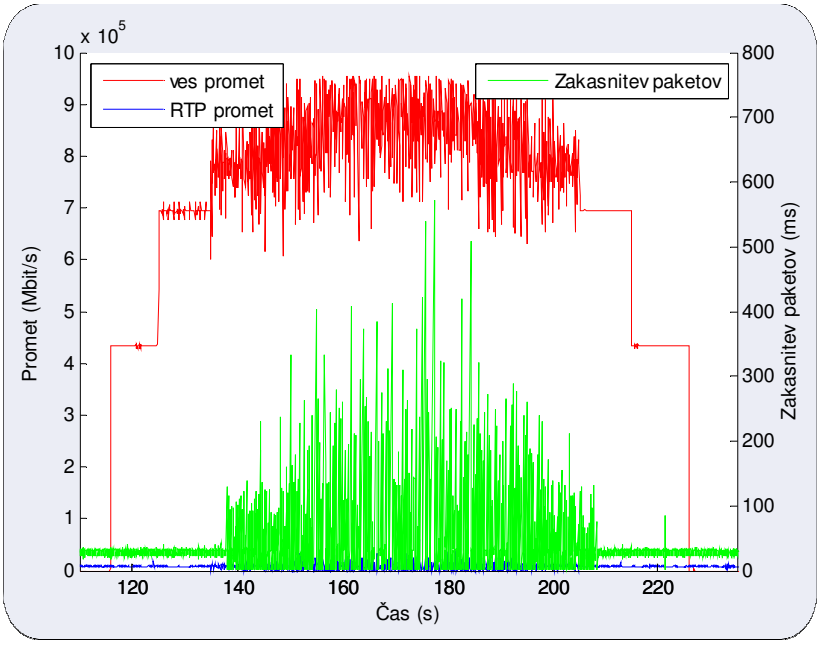


Slika 25: Intenziteta prometa UDP generatorja

Rezultati poizkusa ES_TRAFFIC so predstavljeni na sliki 26. Rdeča črta prikazuje obremenjenost dostopovne povezave med AP in LAN omrežjem. Kot je razvidno iz rezultatov, je bila ob najvišji obremenitvi (med 150. in 190. sekundo scenarija) dostopovna povezava najbolj obremenjena. Modra črta prikazuje zasedenost povezave, ki jo je povzročil RTP promet (glasovni klic), in predstavlja okrog 1,5% celotne zasedenosti povezave. Z zeleno črto prikazujemo zakasnitev paketov od konca do konca za storitev IP telefonije. Vsi trije parametri so bili izmerjeni z analizatorjem Wireshark na PC3.

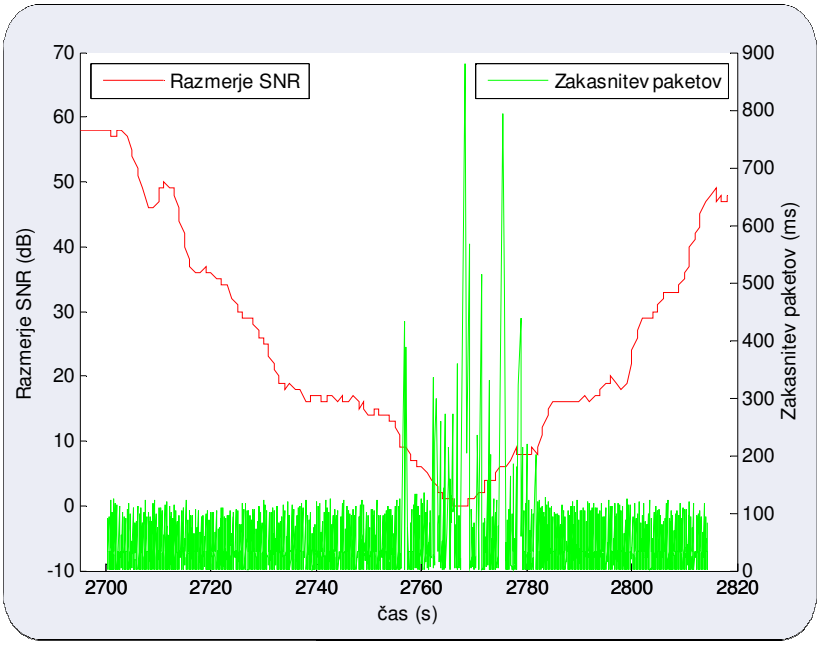
Iz rezultatov lahko vidimo, da se zakasnitev paketov od konca do konca povečuje, ko se obremenjenost dostopovne povezave bliža 100%. Ker prenosnega računalnika (NB) ves čas poizkusa nismo premikali in ker je bil blizu AP, je bilo razmerje SNR WLAN omrežja konstantno okrog 50 dB. Med popolno

obremenjenostjo dostopovne povezave je bila kakovost storitve IP telefonije zelo zmanjšana, saj so se na prejemnikovi strani izgubljale cele besede. V takšnem omrežju ni mogoče uporabljati IP telefonije. Pri tem je potrebno poudariti, da na AP WLAN omrežja razen terminala MN ni bila priključena nobena druga naprava in da je bila hitrost na povezavi ves čas 52 Mbit/s.



Slika 26: Rezultati poizkusa ES_TRAFFIC

Rezultati poizkusa ES_WALK so predstavljeni na sliki 27. Rdeča črta prikazuje razmerje SNR WLAN omrežja, izmerjenega z orodjem NetStumbler na NB. Zelena črta prikazuje zakasnitev paketov od konca do konca storitve IP telefonije, ki je bila izmerjena z analizatorjem Wireshark na PC3. Degradacija storitve, ki se kaže v povečani vrednosti zakasnitve paketov, postane zelo očitna, ko razmerje SNR pade pod 10 dB.



Slika 27: Rezultati poizkusa ES_WALK

Iz predstavljenih rezultatov eksperimentalnih poizkusov lahko zaključimo, da današnja paketna mobilna omrežja nove generacije (HSPA) že omogočajo uporabo storitev IP telefonije z zadovoljivim nivojem kakovosti storitve, kot je razvidno iz rezultatov poizkusa ES_BASIC_HSPA. Poleg tega nam rezultati poizkusa ES_TRAFFIC in ES_WALK v WLAN omrežju pokažejo, da preobremenjenost dostopovne povezave in SNR razmerje manjše od 10 dB, zelo vplivata na storitve IP telefonije.

Sklenemo lahko, da na kakovost storitve IP telefonije ne vpliva zgolj razmerje SNR, ampak tudi razmere na dostopovni povezavi oziroma razmere v dostopovnem omrežju, ki so še posebej problematične, saj niso predvidljive. Poleg tega aplikacije za IP telefonijo še ne omogočajo testiranja omrežja. Vse to moramo upoštevati, ko izvajamo nezaznavno predajo zveze v heterogenih omrežjih. Poleg prikaza delovanja današnjih brezžičnih omrežij so bila ta testiranja izvedena tudi zato, da bomo lahko zasnovali simulacijsko okolje, ki bo čim bolj podobno realnemu omrežju, ki nam bo nato omogočalo ovrednotenje predlaganih naprednih mehanizmov za predajo zveze.

5 Razvoj postopka CAHP za izvajanje predaje zveze z zaznavanjem obremenitev

Pri našem delu smo se osredotočili na nezaznavno predajo zveze v heterogenih omrežjih z uporabo IP telefonije. Kot je razvidno iz predhodnih poglavij predstavlja v procesu predaje najbolj kritičen del odločitev kdaj se bo predaja izvedla. V homogenih omrežjih je odločitev za izvedbo predaje zveze v največji meri odvisna od kakovosti signala ciljnega omrežja. Takšen način v tovrstnih omrežjih zadostuje, saj je celotno omrežje pod nazorom in upravljanjem enega operaterja, ki storitev omogoča. Kadar pa uporabnik izvaja predajo zveze v heterogenih omrežjih se velikokrat zgodi, da ciljno omrežje sploh ni operatersko omrežje (npr. hoteli, domača omrežja). V tovrstnih situacijah, je potrebno pri odločitvi o predaji zveze upoštevati tudi druge parametre, da bo izvajanje predaje za uporabnika čim bolj nezaznavno.

Sprejemna moč signala seveda ostaja predpogoj za izvedbo predaje, saj le-te ni mogoče izvesti, če je moč signala ciljnega omrežja nizka ali signala sploh ni. V nekaterih primerih pa se lahko zgodi, da je razmerje SNR ciljnega omrežja nad želeno mejo, vendar v tistem trenutku ciljno omrežje ni sposobno zagotavljati želenega nivoja QoE, saj nekateri QoS parametri niso zadovoljivi. To se lahko zgodi, če je dostopovna povezava ciljnega omrežja preobremenjena, kar se pogosto dogaja v omrežjih, ki so na voljo več uporabnikom (npr. javno omrežje v kongresnem centru) in so brez dodeljevanja prioritet za časovno kritične storitve ter ne omejujejo števila uporabnikov, ki sočasno uporabljajo omrežje. Iz eksperimentalnih rezultatov predstavljenih v poglavju 4.3 je razvidno, da je lahko nivo QoE uporabnika zelo zmanjšan, če je obremenjenost dostopovne povezave previsoka, kljub visoki vrednosti razmerja SNR in visoki hitrosti prenosa od terminala MN do AP WLAN omrežja. Zato je potrebno razviti nove mehanizme, ki bodo učinkoviteje izvajali predajo zvez in pri tem upoštevali tudi stopnjo zasedenosti ciljnega omrežja.

Za naše delo smo izbrali dve skupini omrežij z različnimi lastnostmi. V prvi skupini so omrežja, ki so zanesljiva in običajno cenovno manj ugodna (npr. UMTS, HSPA in LTE), v drugi pa so omrežja, ki so v večini primerov cenovno ugodnejša ali celo brezplačna, a mnogokrat nezanesljiva (npr. WLAN). Iz vsake skupine smo izbrali tipičnega predstavnika. Iz prve skupine smo izbrali HSPA omrežje, kot predstavnika druge skupine pa WLAN omrežje. Naš postopek deluje med poljubnima omrežjema, vendar pa bosta ti dve omrežji uporabljeni v nadaljevanju, za lažjo predstavitev predlaganega postopka za predajo zveze. Predpostavili smo, da lahko pride do prevelike obremenjenosti dostopovnega omrežja, kar pomeni zmanjšanje nivoja QoE, samo v WLAN omrežju. Zato bo to omrežje tisto, ki ga bomo testirali pred in po predaji zveze.

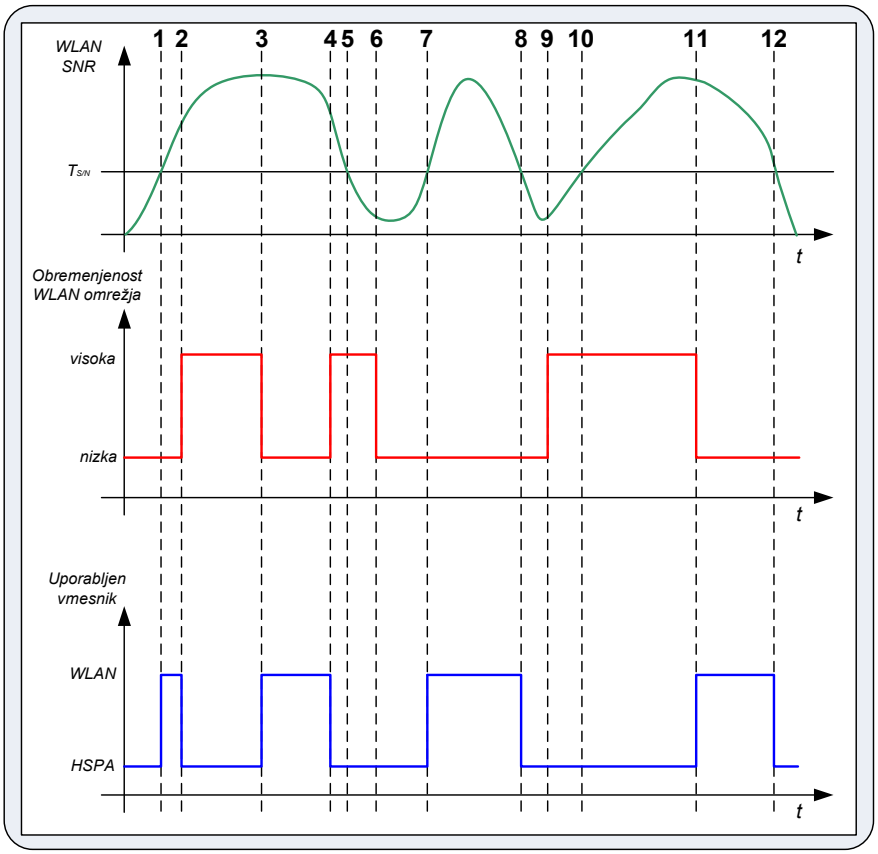
Pred razvojem naprednega postopka za predajo zveze smo si zadali nekaj ciljev, ki jih želimo z novim postopkom doseči:

- Proces predaje se sproži zgolj takrat, ko vrednost razmerja SNR WLAN omrežja preseže določen prag.
- Potrebno je razviti način, ki bo omogočal preverjanje obremenjenosti dostopovne povezave WLAN omrežja, preden se predaja na to omrežje dejansko izvede. Če je obremenjenost (ob izpolnitvi osnovnega pogoja – t.j. ustrezno razmerje SNR) pred predajo previsoka, mora biti proces predajanja zveze zaustavljen oziroma zakasnjen.
- Potrebno je razviti način, ki bo omogočal preverjanje obremenjenosti dostopovne povezave WLAN omrežja tudi med komunikacijo po njem. Če postane obremenjenost po predaji prevelika, moramo sprožiti predajo nazaj na omrežje HSPA.
- Če ob uporabi omrežja WLAN razmerje SNR WLAN omrežja pade pod določen prag, se brezpogojno izvede predaja na HSPA omrežje.
- Ko je razmerje SNR omrežja WLAN pod pragom, se ne preverja obremenjenosti.

Na sliki 28 je prikazano želeno delovanje postopka za različne kombinacije gibanja razmerja SNR in obremenitev dostopovne povezave WLAN omrežja. V zgornjem delu slike je prikazano spreminjanje razmerja SNR sprejetega signala WLAN omrežja. S horizontalno črto je prikazan prag T_{SNR}, ki predstavlja predpogoj za predajo zveze. V srednjem delu je podana obremenjenost dostopovne povezave od dostopovne točke WLAN omrežja do hrbteničnega omrežja operaterja, ki predstavlja ozko grlo. Kot lahko

vidimo, je omrežje v treh intervalih preobremenjeno. V spodnjem delu je prikazano, kateri vmesnik je uporabljen na mobilnem terminalu.

Za bolj nazoren prikaz smo izpostavili 12 časovnih točk, ki prikazujejo želeno delovanje postopka. Ob časovni točki 1 se prvič zgodi, da razmerje SNR omrežja WLAN preseže prag T_{SNR}. Zadostno razmerje SNR kot predpogoj sproži postopek predaje zveze. Nov algoritem mora sedaj pred dokončno izvedbo predaje preveriti, ali je WLAN omrežje sposobno zagotavljati ustrezen nivo QoE. Ker v tem trenutku dostopovna povezava WLAN omrežja ni preobremenjena, se izvede predaja zveze iz omrežja HSPA na omrežje WLAN. Po predaji moramo še vedno spremljati stopnjo obremenjenosti dostopovne povezave WLAN omrežja, ki se ob časovni točki 2 poveča, zato algoritem sproži predajo nazaj na omrežje HSPA. Ker je osnovni pogoj (razmerje SNR nad pragom) še vedno izpolnjen, z algoritmom ves čas preverjamo obremenjenost dostopovne povezave WLAN omrežja. Ko ta v točki 3 pade, se izvede ponoven prehod na WLAN omrežje. V točki 4 se obremenjenost WLAN omrežja zopet poveča, kar ponovno sproži predajo zveze nazaj na HSPA omrežje. Do točke 5, ko je razmerje SNR še vedno nad pragom, z algoritmom spremljamo obremenjenost WLAN omrežja. Ker obremenjenost ni padla, v točki 5 prenehamo s testiranjem, saj se je razmerje SNR zmanjšalo pod prag. V točki 6 sicer obremenjenost WLAN omrežja pade, vendar to ne vpliva na delovanje postopka, ki tega ne zazna, saj ni izpolnjen osnovni pogoj (razmerje SNR). V točki 7 razmerje SNR WLAN omrežja naraste nad prag in ker omrežje ni obremenjeno, zvezo predamo na WLAN omrežje ter začnemo s spremljanjem obremenjenosti. Obremenjenost je ves čas nizka, zato se naslednja predaja zgodi šele v točki 8, ko razmerje SNR pade pod prag. V točki 9 se obremenjenost WLAN omrežja poveča, vendar algoritem tega ne zazna, saj zaradi prenizkega razmerja SNR preverjanje ne poteka. V točki 10 razmerje SNR zraste nad prag, zato začnemo s preverjanjem dostopovne povezave. Algoritem ugotovi preveliko obremenjenost omrežja, zato se izvajanje predaje ustavi in nadaljujemo s preverjanjem povezave. Ko v točki 11 obremenjenost pade, se zaradi še vedno dovolj visokega razmerja SNR izvede predaja na WLAN omrežje. S padcem razmerja SNR pod prag v točki 12 se sproži predaja nazaj na HSPA omrežje.



Slika 28: Prikaz delovanja novega postopka

Na podlagi opisanih zahtev in želenega delovanja smo razvili postopek, ki bi takšne funkcionalnosti podpiral (Libnik et. al, 2010a, Libnik et. al, 2009, Libnik et. al, 2010). Poimenovali smo ga CAHP (*ang. congestion aware handover procedure*). Kot smo opisali v poglavju 4.1 običajno merimo več QoS parametrov pri uporabi storitve IP telefonije. Izmed treh glavnih parametrov lahko dva izmed njih z

določenimi ukrepi zmanjšamo. Trepetanje zakasnitve paketov in izguba paketov se lahko zmanjša z uporabo izravnalnikov trepetanja in s pravilnim načrtovanjem omrežja. Večja težava je zakasnitev paketov od konca do konca, ki jo zelo težko izničimo, še posebej, če do zakasnitev prihaja zaradi preobremenjenosti dostopovnega omrežja. Zato smo se pri našem delu osredotočili na zakasnitev paketov od konca do konca, ki smo jo uporabili kot merilo za nivo zasedenosti ciljnega omrežja. Pri tem za previsoko obremenitev omrežja štejemo stanje, ko omrežje ni sposobno zagotavljati zakasnitev paketov, manjših od v naprej določenega praga. Ker je predlagan postopek namenjen uporabi v operaterskih okoljih, merimo zakasnitev paketov od konca do konca med terminalom in elementom SBC. Kadar je zakasnitev paketov previsoka, je potrebno izbrati drug vmesnik. Tako bomo z izbiro ustreznejšega dostopovnega omrežja, ki ima manjšo zakasnitev paketov, zmanjševali zakasnitev paketov IP telefonije in s tem izboljševali nivo QoE.

Predlagan postopek CAHP za izvajanje predaje zvez je podan na sliki 29, izmenjava sporočil pa na sliki 30. Za zaznavo obremenitve dostopovne povezave WLAN omrežja smo razvili postopek preverjanja obremenjenosti. Postopek CAHP vsebuje dva algoritma: *Pre-probe* in *Mid-probe* algoritem. Prvi je namenjen testiranju obremenjenosti WLAN dostopovnega omrežja pred predajo zveze. Zaženemo ga, ko je izpolnjen osnovni pogoj, t.j. primerno razmerje SNR. Da smo lahko preverjali nivo obremenjenosti ciljnega omrežja, smo definirali novo SIP sporočilo `SIP pre_PROBE`, ki ga pošljemo pred `SIP re-INVITE` sporočilom. V predlaganem algoritmu terminal MN pošlje `SIP pre_PROBE` sporočilo elementu SBC vedno, ko razmerje SNR preseže določen prag T_{SNR}. Element SBC nato odgovori s standardnim `SIP 200 OK` sporočilom. Tu se nova zveza seveda ne vzpostavi, saj gre le za testiranje obremenjenosti ciljnega dostopovnega omrežja. Ker je zakasnitev paketov med terminalom MN in elementom SBC zelo odvisna od trenutnega stanja omrežja, smo se odločili, da pošljemo skupino več (N_{pre}) `SIP pre_PROBE` sporočil in tako dobimo boljše razumevanje stanja WLAN dostopovnega omrežja. Sporočila v skupini bi lahko poslali enega neposredno za drugim, vendar pa smo se odločili, da čas med dvema sporočiloma `SIP pre_PROBE` nastavimo s parametrom T_{inter}. Po prejetju odgovorov na poslana sporočila terminal MN izračuna povprečno vrednost zakasnitve D_{pre} med terminalom MN in elementom SBC, kot je prikazano v enačbi (5).

$$D_{pre} = \frac{\sum_{i=1}^{N_{pre}} D_i}{N_{pre}} \tag{5}$$

kjer je N_{pre} število poslanih sporočil `SIP pre_PROBE` in D_i izmerjena zakasnitev paketa v odgovoru na i-to `SIP pre_PROBE` sporočilo.

Če je D_{pre} nad v naprej definiranim pragom T_d, kar pomeni, da je dostopovno omrežje WLAN preobremenjeno, se predaja ne izvede in `SIP re-INVITE` sporočilo ni poslano. S parametrom T_{pre} določimo čas po katerem ponovno pošljemo `SIP pre_PROBE` sporočila in zopet počakamo na odgovore. To ponavljamo toliko časa, dokler zakasnitev D_{pre} ne pade pod T_d. Ko se to zgodi, terminal MN pošlje `SIP re-INVITE` sporočilo in predaja na omrežje WLAN se izvede.

Lastnosti WLAN omrežja se lahko spremenijo tudi med uporabo tega omrežja. Zato smo definirali drugi algoritem, imenovan *Mid-probe* algoritem. Da bi lahko zaznali spremembo razmer na WLAN omrežju smo definirali novo SIP sporočilo `SIP mid_PROBE`. To sporočilo uporabimo, da lahko preverjamo morebitno preobremenjenost dostopovne povezave WLAN omrežja. Algoritem začne delovati, ko se vzpostavi povezava prek WLAN omrežja. Elementu SBC pošljemo več (N_{mid}) `SIP mid_PROBE` sporočil s časom T_{inter} med dvema sporočiloma v skupini. Tako kot na `SIP pre_PROBE` sporočilo, element SBC na `SIP mid_PROBE` sporočilo odgovori s standardnim `SIP 200 OK` sporočilom. Tudi zdaj se ne vzpostavi nova seja. Po prejetju odgovora na poslana sporočila terminal MN izračuna povprečno vrednost zakasnitve D_{mid} med terminalom MN in elementom SBC, kot je prikazano v enačbi (6).

$$D_{mid} = \frac{\sum_{j=1}^{N_{mid}} D_j}{N_{mid}} \tag{6}$$

kjer je N_{mid} število poslanih sporočil `SIP mid_PROBE` in D_j izmerjena zakasnitev paketa v odgovoru na j-to `SIP mid_PROBE` sporočilo.

Če je D_{mid} pod v naprej definiranim pragom T_d, kar pomeni, da dostopovno omrežje WLAN ni preobremenjeno, določimo parameter T_{mid}, ki nam definira, kdaj ponovno pošljemo `SIP mid_PROBE`

sporočila. Po prejetju odgovorov izračunamo zakasnitev paketov med terminalom MN ter elementom SBC. To ponavljamo toliko časa, dokler D_{mid} ne zraste nad T_d, kar pomeni, da je WLAN omrežje postalo preobremenjeno. Če in ko se to zgodi, terminal MN pošlje `SIP re-INVITE` sporočilo, s katerim se izvede predaja nazaj na HSPA omrežje.

V primeru, da razmerje SNR pade pod prag T_{SNR} med pošiljanjem `SIP pre_PROBE` ali `SIP mid_PROBE` sporočil ali med čakanjem na odgovor, postopek izvajanja predaje zveze prekinemo. V primeru, da se katero od poslanih `SIP pre_PROBE` ali `SIP mid_PROBE` sporočil iz skupine izgubi po izteku določenega časovnika vrednosti parametrov T_{pre} ali T_{mid} nastavimo na privzeto vrednost.

Sporočila `SIP pre_PROBE` in `SIP mid_PROBE` predstavljata dodaten promet v omrežju, ki jih lahko označimo kot signalizacijsko režijo. Ker je velikost paketov majhna, uporaba teh sporočil nima velikega vpliva na promet v hrbteničnem omrežju operaterja. Vendar pa lahko takšna povečava signalizacije dodatno obremenjuje SBC, ki mora vsa ta sporočila procesirati.

Na novo definirana algoritma smo dodali scenariju SEMCS za mobilnost med klicem. Tako so sporočila `SIP pre_PROBE` in `SIP mid_PROBE` poslana do elementa SBC, preko katerega je speljan tudi RTP podatkovni tok.

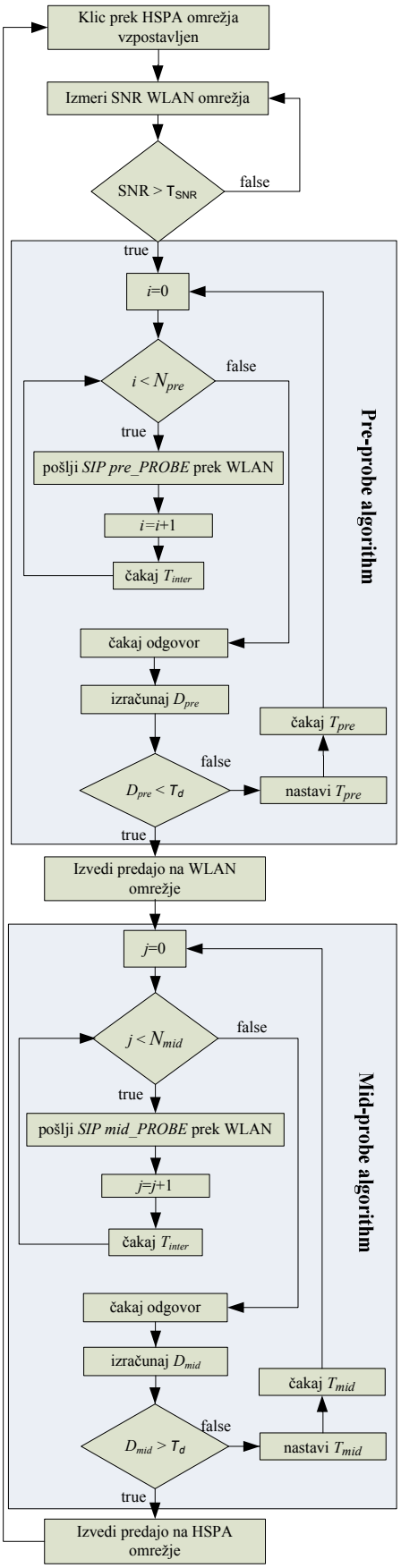
V primeru, da v operaterskem okolju ne bi bilo elementa SBC, bi bilo potrebno implementirati nov omrežni element z naslednjimi funkcionalnostmi:

- Ves RTP podatkovni tok mora teči skozi to napravo.
- Naprava bi morala reševati problematiko NAT in požarnih zidov pri uporabniku.
- Naprava mora biti pod nadzorom operaterja.

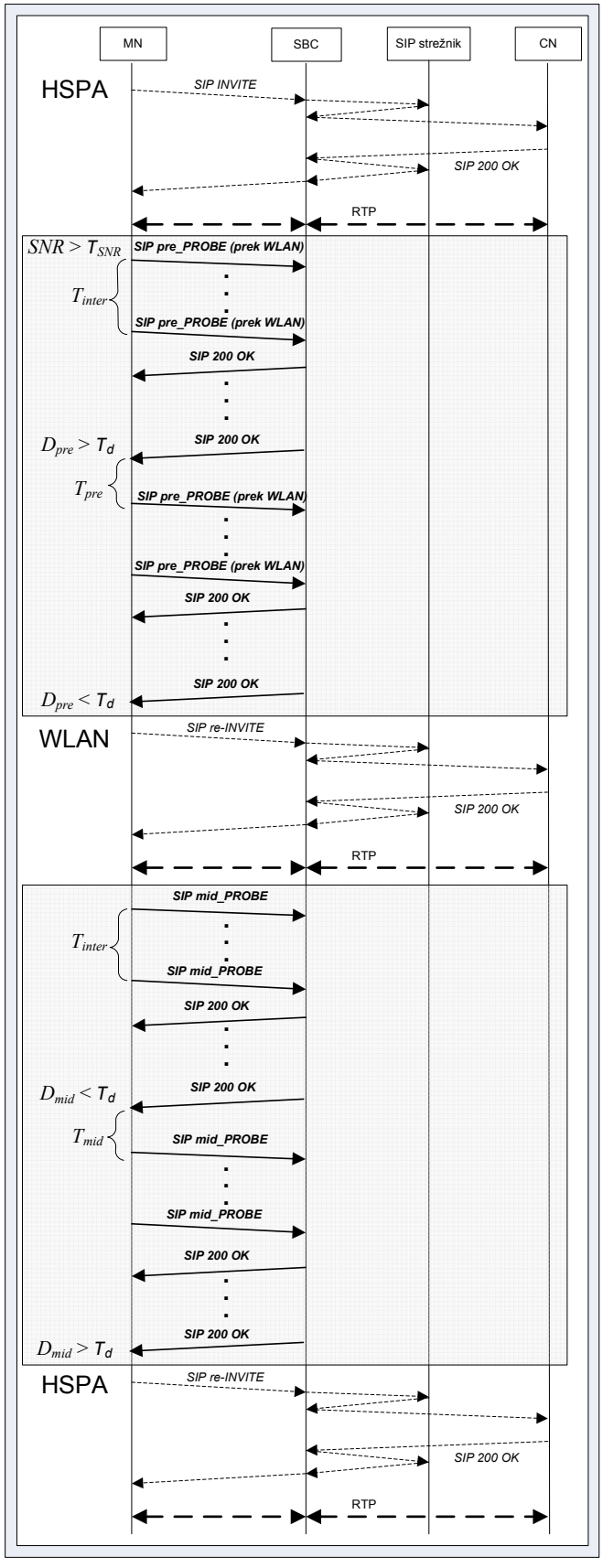
Ker SBC že zadošča vsem zgoraj omenjenim funkcionalnostim, smo postopek implementirali z elementom SBC.

Pri predlaganem postopku smo upoštevali naslednje lastnosti:

- Postopek se začne, ko je terminal MN že povezan na obe omrežji (trenutno in ciljno) hkrati.
- Terminal MN lahko pošilja testna SIP sporočila prek WLAN vmesnika, medtem ko je za RTP še vedno uporabljen HSPA vmesnik (in obratno).
- WLAN omrežje ima prioriteto pri uporabniku, kar pomeni, da bomo poskušali narediti predajo zveze na to omrežje vedno, ko bo izpolnjen osnovni pogoj (SNR > T_{SNR}).



Slika 29: Diagram poteka postopka CAHP



Slika 30 : Izmenjava sporočil postopka CAHP

Med vsemi parametri, ki se uporabljajo v predlaganem postopku, imata na učinkovitost postopka bistven vrednosti parametrov T_{pre} in T_{mid}, saj neposredno vplivata na hitrost zaznavanja obremenitve omrežja.

Pri našem postopku smo definirali dva načina za nastavljanje parametrov T_{pre} in T_{mid}.

- CAHP-C: Parametra nastavljamo na konstantno vrednost. To pomeni, da bosta ves čas simulacije vrednost parametrov T_{pre} in T_{mid} konstantna in bomo za oba uporabljali enako prednastavljeno vrednost (Libnik et. al, 2010a).
- CAHP-A: Parametra se adaptivno spreminjata. To pomeni, da bomo vrednosti parametrov T_{pre} in T_{mid} nastavljali v odvisnosti od trenutne obremenjenosti WLAN omrežja (Libnik et. al, 2009, Libnik et. al, 2010).

V prvem načinu določanja sta vrednosti parametrov T_{pre} in T_{mid} ves čas konstantni. V praksi se velikokrat dogaja, da lahko omrežje postane preobremenjeno zgolj za določen čas. Preostanek časa pa lahko zagotavlja ustrezen nivo QoE. V takšnem primeru bi pri neobremenjenem omrežju in konstantni vrednosti parametrov T_{pre} in T_{mid} omrežje testirali v enakih intervalih in s tem povzročali nepotrebno dodatno signalizacijo. Zato smo razvili adaptivno določanje parametrov T_{pre} in T_{mid}. Cilj takšnega načina določanja je bil, da bi se pogostost testiranja obremenjenosti WLAN omrežja povečevala, tem bolj bi se izmerjene vrednosti D_{pre} in D_{mid} približevale določenemu pragu, saj je verjetnost, da bo zakasnitev paketov narasla nad določen prag večja, ko so izmerjene vrednosti blizu pragu, in manjša, ko so izmerjene vrednosti bolj oddaljene od praga. Tako smo lahko bolj učinkovito zaznavali potencialne preobremenitve v dostopovnem omrežju brez nepotrebne signalizacije. Pri izračunu parametrov T_{pre} in T_{mid} po načinu CAHP-A smo za osnovo uporabili normirano funkcijo. Rezultat smo pomnožili s T_{max} in tako dobili vrednosti obeh parametrov med 0 in T_{max}. Matematična izpeljava normiranih funkcij je prikazana v prilogi B. Definirali smo dve funkciji. Prva, ki je podana v enačbi (7), kaže način izračunavanja T_{pre}, druga, podana v enačbi (8), pa način izračunavanja T_{mid}. Za osnovo smo uporabili normirano funkcijo. Rezultat smo pomnožili s T_{max} in tako dobili vrednosti obeh parametrov med 0 in T_{max}.

$$T_{pre} = \begin{cases} \text{N/A}; & D_{pre} \leq D_{max} \\ T_{max} \cdot \left(\frac{D_{pre} - D_{min}}{D_{max} - D_{min}} - 1\right)^{\alpha}; & D_{max} < D_{pre} < 2 \cdot D_{max} - D_{min} \\ T_{max}; & D_{pre} \geq 2 \cdot D_{max} - D_{min} \end{cases}$$

$$pri\ čemer\ velja\ \alpha > 0 \tag{7}$$

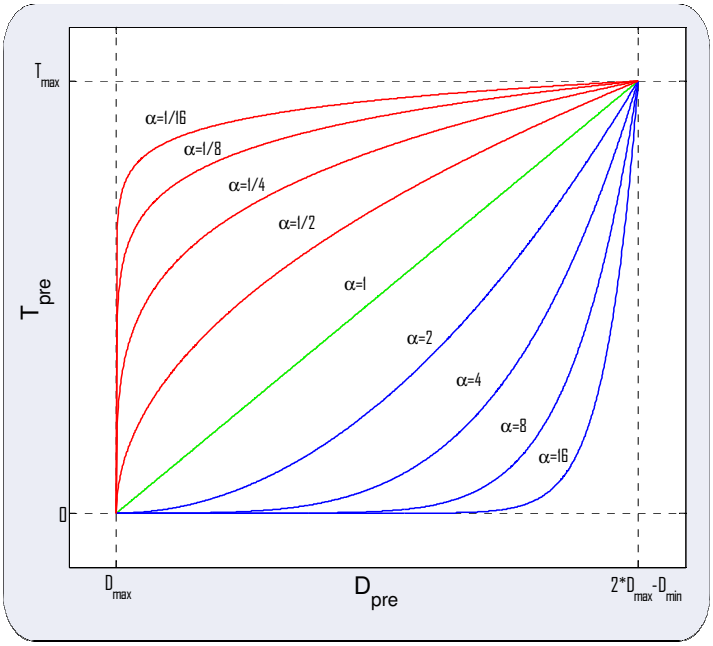
$$T_{mid} = \begin{cases} T_{max}; & D_{mid} \leq D_{min} \\ T_{max} \cdot \left(1 - \frac{D_{mid} - D_{min}}{D_{max} - D_{min}}\right)^{\alpha}; & D_{min} < D_{mid} < D_{max} \\ \text{N/A}; & D_{mid} \geq D_{max} \end{cases}$$

$$pri\ čemer\ velja\ \alpha > 0 \tag{8}$$

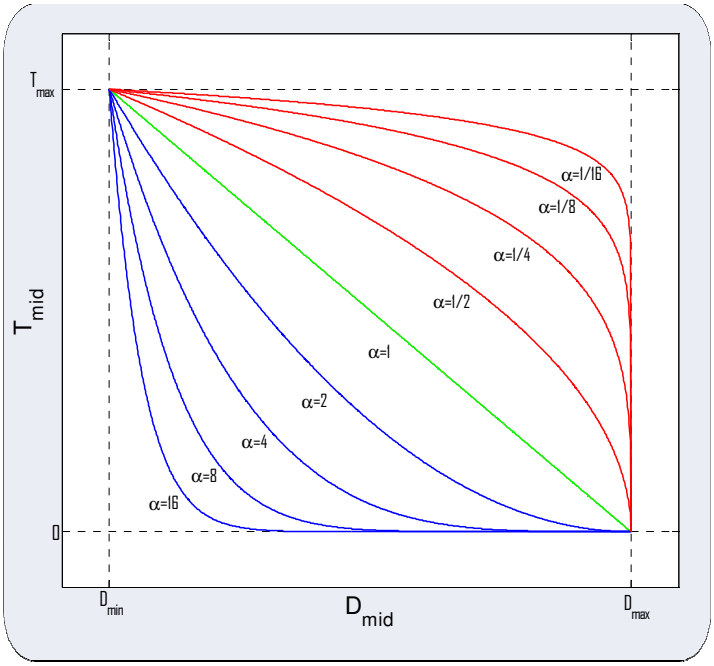
kjer T_{max} predstavlja maksimalno možno vrednost za T_{pre} in T_{mid}, D_{min} minimalno zakasnitev paketov od konca do konca – t.j. zakasnitev paketov neobremenjenega omrežja, D_{max} pa največjo zakasnitev paketov, ki še ne povzroča degradacije storitve – nima vpliva na nivo QoE.

Pri T_{pre} smo ta parameter izračunavali samo za vrednosti D_{pre}, ki so v odprtem intervalu med D_{max} in $2 \cdot D_{max} - D_{min}$. Interval smo izbrali tako, da je njegova dolžina $D_{max} - D_{min}$. Če je izmerjena vrednost D_{pre} večja od zgornje meje intervala, čas T_{pre} postavimo na T_{max}. Če je izmerjena vrednost D_{pre} pod spodnjo mejo intervala, se izvede predaja zveze, zato vrednosti T_{pre} ne nastavljamo, ker se izvede predaja. Enako dolžino odprtega intervala smo uporabili tudi za računanje T_{mid}. Kot pri T_{pre} izven mej intervala vrednosti nastavljamo brez izračunavanja. Če je D_{mid} pod D_{min}, nastavimo T_{mid} na T_{max}. Če pa je D_{mid} nad D_{max}, potem se izvede predaja in zato vrednosti T_{mid} ne nastavljamo. Pri obeh smo uporabili α kot eksponent, ki je vedno večji od 0.

Z izbiro različnih vrednosti α lahko definiramo različne krivulje za T_{pre} in T_{mid}. Nekatere možnosti za izbrana intervala so predstavljene na slikah 31 in 32.



Slika 31: Odvisnost T_{pre} od parametrov D_{pre} in α



Slika 32: Odvisnost T_{mid} od parametrov D_{mid} in α

Kot je razvidno iz enačb (7) in (8) sta T_{pre} in T_{mid} v definiranem odprtem intervalu funkciji parametra α in izmerjene D_{pre} oziroma D_{mid}. Minimalna vrednost parametra α je 0, maksimalna navzgor ni omejena. V izračunih spodaj bomo pokazali, kaj se z vrednostmi T_{pre} in T_{mid} dogaja ob mejnih vrednostih parametra α.

Najprej izračunamo mejne vrednosti za T_{pre}, ko gre α proti ∞, kot je prikazano v enačbi (9).

$$\_\_\_\_\_ \qquad (9)$$

DOKAZ: Vrednosti D_{pre} se gibljejo po odprtem intervalu med D_{max} in $2 \cdot D_{max} - D_{min}$. Ker zgornja in spodnja meja nista vključeni, velja naslednje:

$$1 < \left(\frac{D_{pre}-D_{min}}{D_{max}-D_{min}}\right) < 2 \tag{10}$$

torej velja tudi

$$0 < \left(\frac{D_{pre}-D_{min}}{D_{max}-D_{min}} - 1\right) < 1 \tag{11}$$

Če potenciramo število manjše od 1 in večje od 0 z vrednostmi, ki gredo proti ∞, potem se rezultat približuje vrednosti 0, kar pomeni, da je enačba (9) enaka 0.

Izračun mejne vrednosti za T_{pre}, ko gre α proti 0, je podan v enačbi (12).

$$\lim_{\alpha\to 0}\left(T_{max}\cdot\left(\frac{D_{pre}-D_{min}}{D_{max}-D_{min}} - 1\right)^{\alpha}\right) = T_{max} \tag{12}$$

DOKAZ: Katerakoli vrednost, potencirana z eksponentom, ki gre proti 0, se približuje vrednosti 1, kar pomeni, da je enačba (12) enaka T_{max}.

Izračun znotraj določenega intervala za T_{mid}, ko se vrednost α približuje ∞, prikazuje enačba (13).

$$\lim_{\alpha\to\infty}\left(T_{max}\cdot\left(1-\frac{D_{mid}-D_{min}}{D_{max}-D_{min}}\right)^{\alpha}\right) = 0 \tag{13}$$

DOKAZ: Vrednosti D_{mid} se gibljejo po odprtem intervalu med D_{min} in D_{max}. Ker zgornja in spodnja meja nista vključeni, velja naslednje:

$$1 > \left(\frac{D_{mid}-D_{min}}{D_{max}-D_{min}}\right) > 0 \tag{14}$$

torej velja tudi

$$0 < \left(1-\frac{D_{mid}-D_{min}}{D_{max}-D_{min}}\right) < 1 \tag{15}$$

Če potenciramo število manjše od 1 in večje od 0 z vednostmi, ki gredo proti ∞, potem se rezultat približuje vrednosti 0, kar pomeni, da je enačba (13) enaka 0.

Izračun mejne vrednosti za T_{mid}, ko gre α proti 0, je podan v enačbi (16).

$$\lim_{\alpha\to\infty}\left(T_{max}\cdot\left(1-\frac{D_{mid}-D_{min}}{D_{max}-D_{min}}\right)^{\alpha}\right) = T_{max} \tag{16}$$

DOKAZ: Katerakoli vrednost, potencirana z eksponentom, ki gre proti 0, se približuje vrednosti 1, kar pomeni, da je enačba (16) enaka T_{max}.

Vidimo lahko, da ko se α približuje vrednosti 0, se vrednosti T_{pre} in T_{mid} približujeta T_{max}. To pomeni, da bo preverjanje WLAN omrežja manj pogosto, kar lahko ima za posledico nepravočasno zaznavanje preobremenitve dostopovne povezave WLAN omrežja in zmanjšanje nivoja QoE. Ko pa se α približuje neskončnosti, se vrednosti T_{pre} in T_{mid} bližata 0. To pomeni, da je pogostost pošiljanja skupine SIP sporočil, s katerimi preverjamo obremenjenost dostopovne povezave WLAN omrežja, velika in bomo lahko potencialno preobremenjenost zaznali zelo hitro. S takšnim načinom lahko zadržimo QoE na ustreznem

nivoju. Iz tega sledi, da se postopek CAHP-A v limitah obnaša kot postopek CAHP-C za vrednosti 0 s oziroma T_{max}.

SIP sporočila, s katerimi preverjamo obremenitev dostopovne povezave WLAN omrežja, predstavljajo signalizacijsko režijo. Pri adaptivnem načinu določanja parametrov T_{pre} in T_{mid} se ta režija povečuje z večanjem vrednosti α in zmanjšuje z manjšanjem parametra α. Zato lahko parameter α označimo tudi kot parameter, ki določa signalizacijsko režijo (večji kot je α, večja je režija).

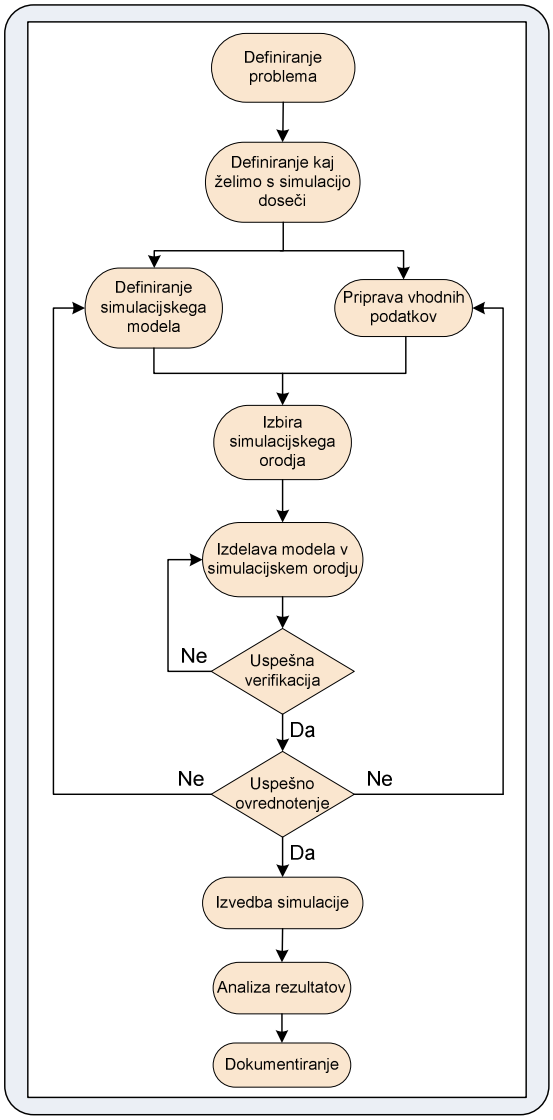
Ker smo v postopku uporabili SIP protokol za pošiljanje sporočil, s katerimi smo preverjali obremenjenost dostopovne povezave WLAN omrežja, je takšen pristop popolnoma neodvisen od nižjih slojev (transportnega, omrežnega, povezavnega in fizičnega). Zaradi neodvisnosti od protokolov uporabljenih na nižjih slojih, je takšno rešitev, v kolikor operater že ponuja storitev SIP IP telefonije, enostavno vpeljati v obstoječe operatersko okolje, saj SBC in terminali že podpirajo SIP in jih zato ni potrebno prilagoditi. Ob uvedbi postopka CAHP v omrežjih operaterja, bi bilo potrebno zgolj nadgraditi programsko opremo na uporabniških terminalih ter na elementu SBC pri operaterju. Če bi za preverjanje obremenjenosti omrežja uporabili nižje sloje, bi to pomenilo večji poseg v aplikacijo oz. razvoj ločene povsem nove aplikacije. Zaradi uporabe SIP protokola lahko v odločitev vključimo tudi druge podatke, ki jih posreduje SIP strežnik (npr. nastavitve uporabnika). Izvajanje meritev zakasnitve paketov z drugimi protokoli bi onemogočale tudi varnostne nastavitve na SBC, kjer je običajno dovoljen promet zgolj na vrata, ki jih uporabljata protokola SIP in RTP. Podobne varnostne omejitve veljajo tudi za LAN omrežja pri uporabniku.

Da bi postopek CAHP uporabili v polni funkcionalnosti, morajo vsi elementi MN in SBC podpirati predlagan postopek. V fazi uvajanja storitve, ko bodo samo nekateri elementi MN in SBC podpirali postopek CAHP, bi element SBC element MN obvestil, da ne podpira postopka CAHP in tako preprečil nepotrebno obremenjevanje elementa SBC. Na prvo *SIP pre_PROBE* sporočilo bi SBC odgovoril s standardnim SIP sporočilom 501 Not Implemented, ki bi ustavil izvajanje procedure CAHP. Uporabnik bi lahko v tem primeru še vedno naredil predajo zveze, vendar pa QoE ne bi bil več zagotovljen.

6 Razvoj simulacijskega modela

Dosegljivost namenskih simulacijskih orodij in zelo velike procesne sposobnosti današnjih računalnikov z znižanjem cene na operacijo je omogočilo, da simulacije postanejo najbolj uporabljano orodje pri raziskovanju in sistemskih analizah. Simulacija lahko zelo izboljša proces razvoja novih storitev, saj omogoča predhodno testiranje v simulacijskem okolju, kjer lahko preizkušamo tudi najslabše možne scenarije, ki se lahko zgodijo v realnem okolju. Telekomunikacijski operaterji lahko s pomočjo simulacij preizkušajo nove arhitekture omrežja za analizo in ovrednotenje novih protokolov in storitev. To je še posebej pomembno v današnjem zelo konkurenčnem okolju, kjer je ponujanje storitev, ki omogočajo ustrezen nivo QoE uporabnikov, zelo pomembno.

Če želimo izvesti simulacijo za potrebe ovrednotenja novega postopka, moramo slediti določenim korakom. Na sliki 33 so prikazani osnovni koraki simulacijske analize, ki zajemajo vse korake od predpriprave do dokumentiranja in bodo na kratko opisane v nadaljevanju.



Slika 33: Koraki simulacijske analize

V prvem koraku fazi je potrebno definirati problem skupaj z osnovnimi predpostavkami. Kljub izbranim predpostavkam se lahko zgodi, da se bo problem kasneje spremenil.

V naslednjem koraku je potrebno definirati vprašanja, na katera želimo dobiti odgovore s simulacijo. V tej fazi se je potrebno tudi odločiti, ali je simulacija sploh primerna metoda za rešitev izbranega problema.

Sledita dve koraka, ki tečeta vzporedno. Prvi je definiranje simulacijskega modela, kjer poskušamo na abstrakten način prikazati ključne značilnosti problema. Priporočljivo je, da začnemo z enostavnim modelom, ki ga nato nadgrajujemo. V tem koraku tudi izberemo in po potrebi spremenimo osnovne predpostavke, ki določajo/označujejo problem. Določiti je potrebno tudi, kaj so glavni simulacijski rezultati (npr.: ovrednotenje novih postopkov, protokolov ali izdelava študije zmogljivosti sistema). Simulacijski model ni nujno popolna kopija realnega sistema – zajemati mora samo bistvene značilnosti.

Drugi vzporedni korak zajema pripravo vhodnih podatkov. Obstaja stalna povezava med izgradnjo modela in zbiranjem potrebnih vhodnih podatkov. S spreminjanjem kompleksnosti modela se lahko spremenijo tudi zahteve glede vhodnih podatkov. Vhodni podatki so zelo pomembni za dobre rezultate in jih je zato potrebno pripraviti z veliko mero previdnosti. Običajno je potrebno vhodne podatke začeti pripravljati že v najzgodnejših fazah izdelave modela.

Ko je simulacijski model definiran in so vhodni podatki zbrani, je potrebno izbrati simulacijsko orodje. Danes je na voljo veliko simulacijskih orodij, ki jih lahko razdelimo na komercialna (npr. OPNET, SPW, MATLAB, SIMULINK, OMNES) in akademska (npr. NS2/3, LEONART, LeoSim, GaliLEO, OMNET). Delitev orodij lahko izvedemo tudi na podlagi lastnosti/možnosti posameznih orodij. Ena od možnosti je razdelitev orodij glede na uporabljen programski jezik (npr. C/C++, C#, Java, Fortran). Simulacijska orodja se razlikujejo tudi po tem, ali podpirajo OSI sloje. Tako npr. ns-2 ne podpira OSI slojev in obravnava posamezne pakete kot sporočila, OPNET in OMNeT++ pa podpirata OSI sloje. Nekatera našteta simulacijska orodja podpirajo tudi zelo kompleksne modele terminalskih naprav (npr. OPNET), druge pa podpirajo zgolj zelo enostavne modele terminalskih naprav (npr. ns-2). Odločitev, katero simulacijsko orodje bomo izbrali, je odvisna predvsem od potreb, ki jih imamo glede izvedbe simulacije in tudi glede na razpoložljiva sredstva.

Po izbiri ustreznega simulacijskega orodja sledi v naslednjem koraku izdelava simulacijskega modela, kar pomeni prevod modela v programsko kodo. Lahko se tudi zgodi, da ni potrebe po programiranju celotnega simulacijskega modela, saj nekatera orodja že podpirajo določene funkcionalnosti.

Po izdelavi modela v simulacijskem orodju sledi verifikacija in ovrednotenje. Najprej izvedemo verifikacijo, katere cilj je ugotoviti, ali program deluje ustrezno oziroma ali model deluje pravilno s testnimi podatki. Če simulacijski model ne deluje pravilno, je potrebno ustrezno popraviti programsko kodo. Po uspešni verifikaciji sledi še ovrednotenje. Namen ovrednotenja je ugotoviti, ali je model sploh uporaben za ovrednotenje sistema, za katerega je bil narejen. V tej fazi lahko izvedemo tudi primerjave simulacijskega modela z realnim sistemom in po potrebi izvedemo kalibracijo modela, s katerim ga še izboljšamo.

Po uspešni verifikaciji in ovrednotenju izvedemo želeno simulacijo. Pri tem je potrebno paziti, da sistem ni kaotičen, kar pomeni, da majhna sprememba na vhodu zelo vpliva na rezultate simulacije. Predvsem pri testiranju omrežnih protokolov je potrebno včasih določiti zagonski čas, ki omogoča popolni zagon (da se omrežje ustali) in morebitno samodejno konfiguracijo modela. Rezultate, pridobljene v zagonskem času zanemarimo in se ne upoštevajo pri rezultatih simulacije.

Po izvedeni želeni simulaciji sledi statistična analiza rezultatov in njihova predstavitev. V zadnji fazi simulacijske analize izvedemo dokumentiranje ustvarjenega simulacijskega modela.

Pri našem delu smo sledili opisanim korakom. Tako smo prva dva koraka opisali v uvodnih poglavjih, pridobitev vhodnih podatkov je bila izvedena na podlagi meritev v realnem okolju, predstavljenih v poglavju 4.3. Simulacijski model smo definirali v poglavju 5. Izbrano simulacijsko orodje bo predstavljeno v poglavju 6.1. V poglavjih 6.2 in 6.3 bomo predstavili potrebne prilagoditve že vgrajenih procesov, ki so nam omogočile implementacijo predlaganega postopka v simulacijskem modelu. Verifikacija in ovrednotenje bosta predstavljeni v poglavju 6.5. Opis glavne simulacije, analiza ter ovrednotenje rezultatov bo podano v poglavju 7. Model je dokumentiran v prilogi D.

6.1 Simulacijsko orodje OPNET Modeler

Simulacijsko orodje OPNET Modeler (OPNET, 2010) je vodilno orodje za modeliranje telekomunikacijskih omrežij in za izvajanje simulacij. Uporabljajo ga tako raziskovalci kot inženirji, ki se ukvarjajo z načrtovanjem komunikacijskih omrežij, produktov, tehnologij in protokolov, saj omogoča veliko prilagodljivost in razširljivost.

Orodje Modeler pospešuje raziskave in razvoj na področju omrežij in skrajšuje čas od razvoja produkta do lansiraja le-tega na trg. Z uporabo simulacij lahko inženirji, ki se ukvarjajo z omrežji, zmanjšajo stroške, povezane z raziskavami in razvojem ter zagotavljajo maksimalno kakovost produktov. Orodje Modeler omogoča inovacije in uporabnikom nudi:

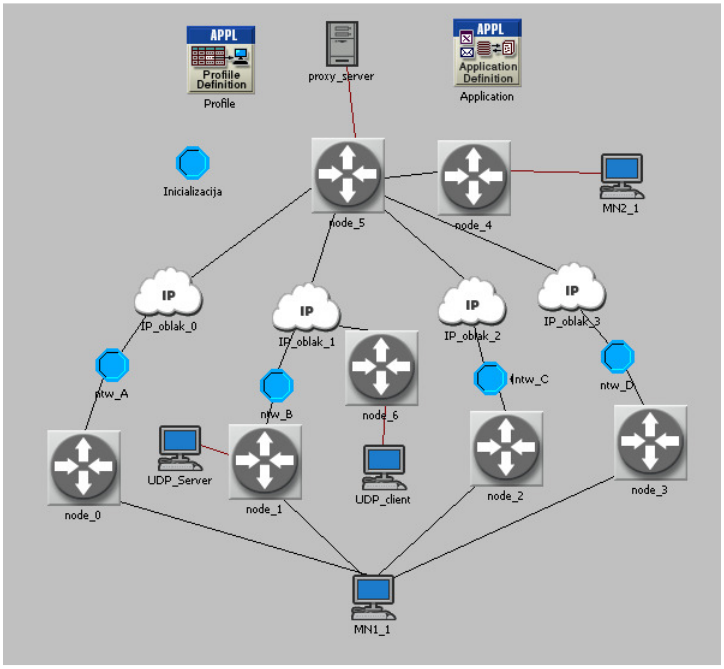
- spreminjanje obstoječih protokolov in tehnologij;
- razvoj novih protokolov in tehnologij;
- testiranja in demonstracije načrtov realnih scenarijev pred produkcijo;
- optimizacijo protokolov in aplikacij;
- načrtovanje mobilnih omrežij z upoštevanjem vplivov terena in širjenja brezžičnega signala.

Orodje Modeler, ki je bilo najprej razvito na inštitutu MIT, so predstavili leta 1987, kot prvi komercialni simulator omrežij. Glavne značilnosti orodja Modeler so:

- najhitrejše DES (*ang. discrete event simulation*) okolje med vodilnimi industrijskimi rešitvami;
- več žičnih in brezžičnih protokolov ter odprto kodo za modele naprav različnih vodilnih proizvajalcev;
- objektno orientirano modeliranje;
- brezžične simulacije, ki vključujejo lastnosti terena in mobilnosti;
- 32-bitni in 64-bitni grafični vmesnik;
- prilagodljivo modeliranje brezžičnih tehnologij;
- diskretne, hibridne in analitične simulacije;
- podpora GRID tehnologiji za distribuirane simulacije;
- vgrajena razhroščevalnik in izvajanje nekaterih analiz;
- odprti vmesniki za vključevanje zunanjih objektov, knjižnic ali drugih simulacij.

Arhitekturno je simulacijsko orodje Modeler sestavljeno iz serije hierarhičnih nivojev, ki skupaj tvorijo strukturo realnih omrežij, naprav in protokolov.

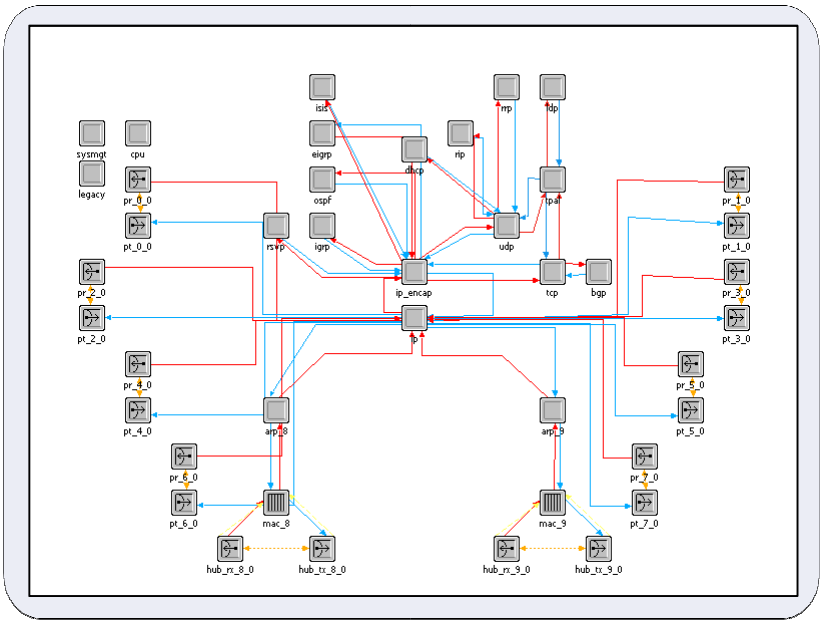
Prvi hierarhični nivo, prikazan na sliki 34, je nivo omrežja, ki določa topologijo komunikacijskega omrežja. Uporabnik ustvarja objekte vozlišč in povezav, ki predstavljajo elemente omrežnih tehnologij ter omogoča enostavno nastavljanje posameznih elementov prek pojavnih oken. Projekti lahko vključujejo več scenarijev, kar omogoča primerjavo različnih možnosti med sabo.



Slika 34: Nivo omrežja v orodju OPNET

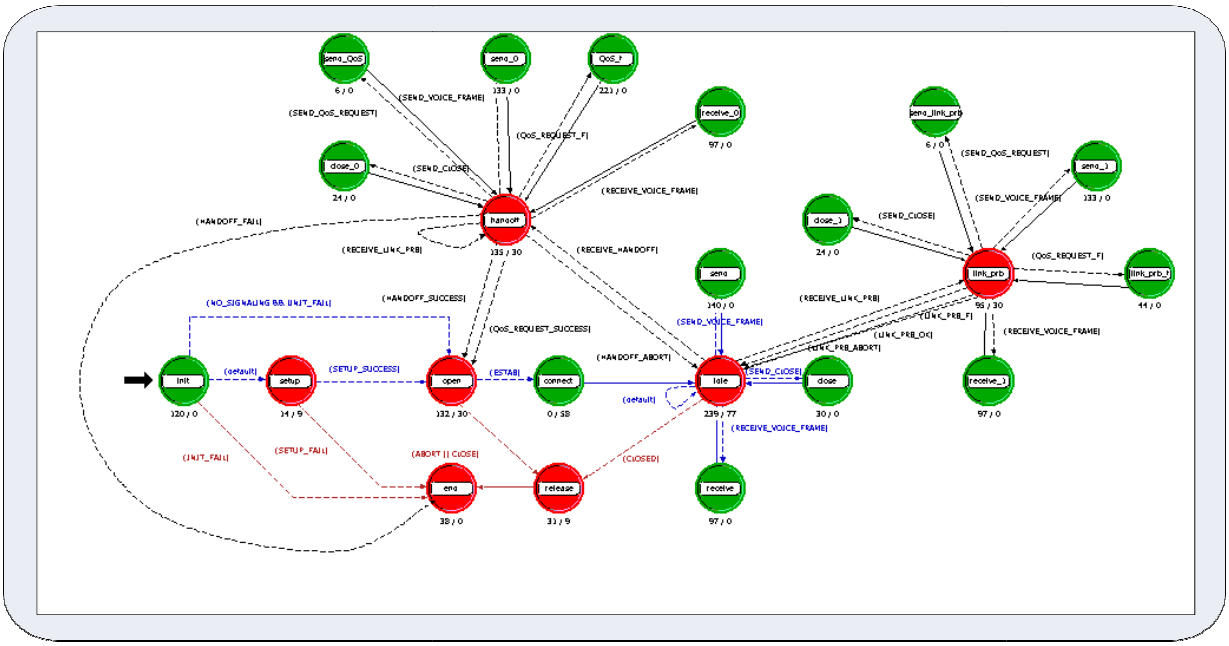
Drugi hierarhični nivo, prikazan na sliki 35, predstavlja nivo vozlišč, ki zajema arhitekturo omrežne naprave ali sistema z opisom toka podatkov med funkcionalnimi elementi, ki jih imenujemo moduli. Moduli običajno predstavljajo omrežne protokole ali algoritme. Modulom so dodeljeni modeli procesov, ki

jih razvijemo v urejevalniku procesov (tretji nivo), da dosežemo želeno obnašanje modula.



Slika 35: Nivo vozlišč v orodju OPNET

Nivo procesov uporablja zmogljiv FSM (*ang. Finite State Machine*) pristop za podporo natančnih zahtev protokolov, virov, aplikacij, algoritmov in mehanizmov čakalnih vrst in je prikazan na sliki 36. Avtomati končnih stanj so dinamični in jih lahko ustvarimo med simulacijo kot odgovor na določen dogodek. Vsako stanje procesa je opisano s C/C++ kodo, ki jo lahko prilagajmo lastnim potrebam. Jedrne funkcije orodja OPNET pospešujejo razvoj in podporo skupnih komunikacijskih mehanizmov, kot so npr. paketi, čakalne vrste in promet.



Slika 36: Nivo procesov v orodju OPNET

Obsežna knjižnica simulacijskega orodja Modeler vsebuje več kot 400 protokolov, modelov naprav proizvajalcev, kar zelo pospešuje načrtovanje procesov. Med najbolj razširjenimi podprtimi modeli protokolov, ki jih orodje Modeler podpira so BGP, HAIPE, IPv6, MANET (AODV, DSR, GRP, OLSR, OSPFv3, TORA), MPLS, RIPng, satelitske tehnologije, SIP, TCP, UMTS, VLAN, VOIP, VPN, WIMAX (802.16e), WLAN (802.11a, b, e, g) ter ZigBee (802.15.4). Modeli omrežne opreme zajemajo modele vodilnih proizvajalcev, kot so Alcatel-Lucent, Cisco Systems, Extreme, Foundry, HP, IBM, Juniper in Nortel. Vsi standardni modeli so na voljo z odprto kodo, kar omogoča prilagajanje.

DES jedro orodja Modeler, jedro simulacijskega okolja, so v zadnjih 20 letih nenehno izboljševali, da bi

omogočal hitrejše simulacije. Poleg osnovnih zmogljivosti orodje Modeler omogoča tudi več načinov za hitrejše izvajanje zahtevnejših simulacij, vključno s 64-bitnim jedrom, vzporednimi simulacijami in podporo GRID tehnologije.

Vzporedne DES simulacije orodja Modeler omogočajo večjedrnim procesorjem ali večprocesorskim napravam pohitritev simulacijskih tekov. Uporabniki lahko izberejo, kateri modeli procesov se bodo izvršili paralelno za dosego optimalne uporabe. Zaradi podpore GRID tehnologiji lahko orodje Modeler distribuira serijo simulacij na več naprav.

Orodje Modeler omogoča več vgrajenih statistik za hitre simulacijske analize. Uporabniki lahko prilagodijo obstoječo statistiko ali ustvarijo svojo. Rezultati simulacij so predstavljeni neposredno v orodju Modeler. Grafikoni in druge oblike prikazovanja rezultatov so ustvarjeni avtomatsko iz izbranih meritev, tako da ni potrebe po kasnejšem procesiranju. Predstavitev rezultatov simulacij je enostavno spreminjati z uporabo številnih filtrov, ki vključujejo matematične operacije.

Na podlagi opisanih lastnosti smo za naše delo izbrali simulacijsko orodje OPNET, ki z orodjem Modeler ponuja odprto kodo najbolj uporabljenih protokolov, kar je zelo primerno za ovrednotenje izvajanja novih ali izboljšanih tehnik za upravljanje z mobilnostjo (Chan et. al, 2002). OPNET že omogoča simuliranje SIP telefonije, vendar ne podpira predaj zvez z uporabo SIP protokola. Zato smo morali za izdelavo simulacijskega modela postopka CAHP implementirati nekaj dodatnih funkcionalnosti. Izvedli smo veliko manjših prilagoditev, ki so nam omogočale uvoz vhodnih podatkov ter izvoz rezultatov. Določili smo tudi element, kjer smo definirali vse vhodne parametre simulacije. Implementacijo predlaganega postopka CAHP v simulacijskem modelu smo naredili na obstoječem modelu za SIP telefonijo, povezavah in terminalih ter bo opisana v nadaljevanju.

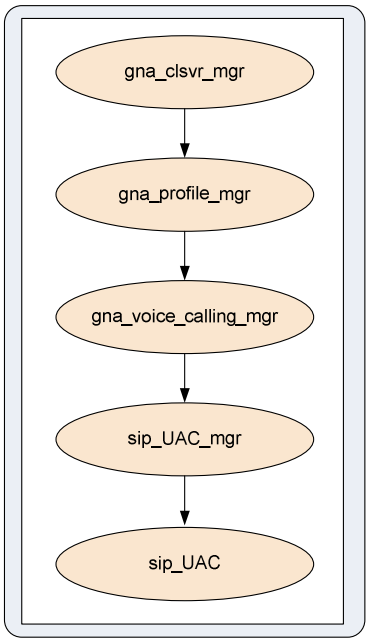
6.2 Razvoj novih funkcionalnosti modela za SIP IP telefonijo

SIP protokol uporablja za komunikacijo aplikacijski sloj. Tako je tudi v orodju OPNET podprt na aplikacijskem sloju. OPNET omogoča, da lahko uporabimo več različnih že vgrajenih aplikacij, med katerimi je tudi IP telefonija, ki za signalizacijo uporablja SIP protokol. Aplikacijo izberemo s posebnim elementom za definicijo aplikacij, ki ga vstavimo v urejevalnik projektov. Vsakemu elementu, ki bo uporabljal določeno aplikacijo, priredimo določen profil, s katerim določimo, kako bo element deloval. To storimo v dodatnem elementu za definicijo profilov, ki ga ravno tako vstavimo v projekt. Za vsak projekt lahko določimo več različnih profilov, ki jih nato dodeljujemo različnim elementom. Tako lahko na primer pri govornih zvezah določimo, kakšno je razmerje med govorom in tišino, kakšna je intenziteta govora itd.

V orodju OPNET podpora govornih aplikacij vključuje več različnih procesov:

- *gna_clsvr_mgr*: krovni aplikacijski model, ki se zažene ob začetku simulacije na vsakem elementu, ki odpira aplikacijski sloj. Uporablja se za upravljanje z aplikacijami, ki so definirane v elementu za definicijo aplikacij. Ta proces na določenem omrežnem elementu zažene aplikacijo, ki smo jo predhodno izbrali.
- *gna_profile_mgr*: procesni model, ki ga ustvari *gna_clsvr_mgr* za upravljanje s profili posameznega odjemalca.
- *gna_voice_calling_mgr*: procesni model, ki je namenjen izključno govornim aplikacijam. Ustvari ga *gna_profile_mgr* za podporo govornim aplikacijam, ki jih zažene *gna_clsvr_mgr*.
- *sip_UAC_mgr*: procesni model, ki ga ustvari *gna_voice_calling_mgr*, ko želi vzpostaviti govorno sejo. Model *sip_UAC_mgr* običajno nadzoruje več procesnih modelov *sip_UAC* in statusov klicev, ki se odvijajo na posameznem *sip_UAC* procesnem modelu.
- *sip_UAC*: procesni model, ki ga ustvari *sip_UAC_mgr* za vzpostavitev seje med odjemalcem in strežnikom.

Iz zgoraj zapisnega lahko povzamemo, da obstaja hierarhična povezava med različnimi procesi. Grafično so razmerja prikazana na sliki 37. Procesni model *gna_voice_calling_mgr* je tisti, ki začne neposredno komunicirati s SIP procesnim modelom. Ko se pojavi potreba po vzpostavitvi govorne seje z oddaljenim gostiteljem, kliče funkcijo *sip_request_invite()* in poskuša odpreti ter vzdrževati aktivno povezavo z oddaljeno stranjo. Govor se po vzpostavitvi signalizacijske poti prenaša z uporabo RTP protokola.



Slika 37: Hierarhična povezava procesov na aplikacijskem sloju

Za implementacijo predlaganega postopka v simulacijskem okolju smo morali v orodju OPNET nekatere funkcionalnosti obstoječih procesov, ki so uporabljeni pri simulacijah IP telefonije, razviti na novo. Dodaten razvoj je bil potreben, da bi lahko izvedli ovrednotenje predlaganega postopka CAHP, opisanega v poglavju 5. Tako je bil glavni proces v orodju OPNET, ki sodeluje pri simulacijah IP telefonije (*gna_voice_calling_mgr*) dopolnjen s podporo opisanih funkcionalnosti v novih stanjih. Potrebno je bilo dodatno definirati tudi prekinitve (*ang. interrupt*), s katerimi smo nadzorovali potek simulacije. Ravno tako smo definirali novi SIP sporočili za preverjanje stopnje obremenjenosti dostopovne povezave WLAN omrežja.

Kot smo že opisali, OPNET uporablja FSM za implementacijo obnašanja posameznega protokola ali modula. FSM uporablja stanja in prehode med njimi za ugotavljanje, katere akcije naj modul izvede kot odgovor na določen dogodek. Sestavljen je iz dveh tipov stanj, ki so med seboj povezani s povezavami. V vsakem od njih definiramo vhodne in izhodne akcije. Rdeče stanje je tisto stanje, ki vrača kontrolo simulacije glavnemu simulacijskemu jedru po končani izvedbi predpisanih akcij za to stanje. Proces nato v tem stanju čaka na ustrezno prožilo (*ang. trigger*), ki sproži premik v naslednje stanje. Zeleno stanje je stanje, ki ne vrne kontrole, ampak takoj izvede predpisane akcije. Proces se po izvedbi akcij takoj prek povezave premakne v naslednje stanje.

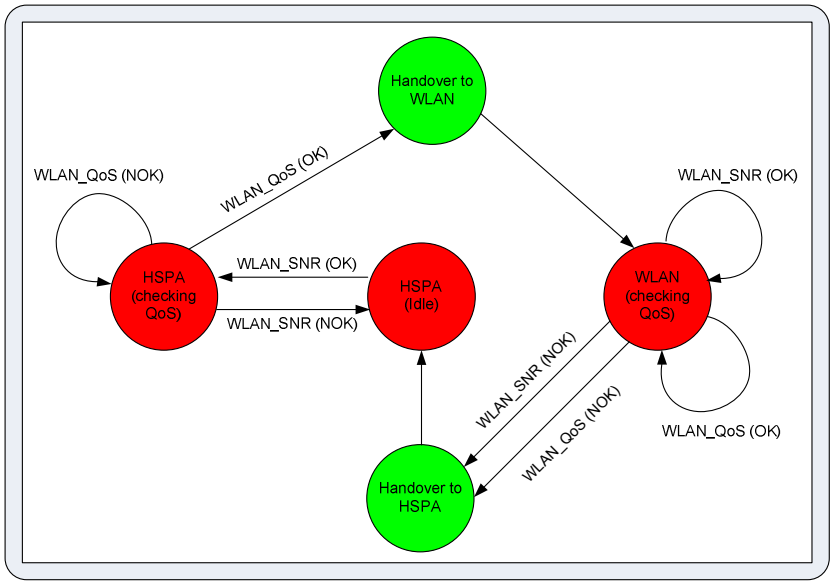
V simulacijskem scenariju smo izvajali predajo zveze med WLAN in HSPA omrežjem. Predpostavili smo, da je HSPA omrežje vedno na voljo in ima dobre QoS lastnosti, medtem ko ima WLAN omrežje omejen doseg in je nezanesljivo, saj je večkrat preobremenjeno. Na podlagi uporabniških nastavitev ima WLAN omrežje prioriteto, kar pomeni, da bo SIP aplikacija poskušala narediti predajo zveze vedno, ko bo razmerje SNR nad določenim pragom.

Shematičen prikaz FSM predlaganega postopka je predstavljen na sliki 38. Prvi klic je bil narejen prek HSPA omrežja. Ko se zveza vzpostavi, je proces v stanju *HSPA (idle)*, kjer ves čas merimo razmerje SNR WLAN omrežja. Ko razmerje SNR preseže določen prag, prekinitev *WLAN_SNR (OK)* sproži premik procesa v stanje *HSPA (checking QoS)*, v katerem se začne testiranje dostopovne povezave WLAN omrežja. Za testiranje obremenjenosti WLAN omrežja smo uporabili `SIP pre_PROBE` sporočila. Ko so `SIP pre_PROBE` sporočila poslana, proces počaka na odgovore. Ob prejetju odgovorov izračunamo povprečno zakasnitev paketov med terminalom MN in elementom SBC. Če povprečna zakasnitev paketov pokaže, da dostopovno omrežje WLAN v tem trenutku ni preobremenjeno, se proces s prekinitvijo *WLAN_QoS (OK)* premakne v stanje *Handover to WLAN*, kjer se izvede predaja iz WLAN na HSPA omrežje. Ko se vzpostavi nova seja, se proces takoj pomakne v stanje *WLAN (checking QoS)*. Če pa izračunana zakasnitev paketov med terminalom MN in elementom SBC v stanju *HSPA (checking QoS)* pokaže, da je WLAN omrežje preobremenjeno in tako ni sposobno zagotavljati ustreznega nivoja QoE, s prekinitvijo *WLAN_QoS (NOK)* sprožimo določitev T_{pre}, ki predstavlja čas ponovnega pošiljanja `SIP pre_PROBE` sporočil. Če razmerje SNR WLAN omrežja pade pod določen prag, medtem ko pošiljamo sporočila ali čakamo na odgovore, se proces vrne v stanje *HSPA (Idle)* s prekinitvijo *WLAN_SNR (NOK)*.

Ko je klic predan na WLAN omrežje, je ob vzpostavitvi povezave proces v stanju *WLAN (checking*

QoS). Za preprečitev degradacije nivoja QoE, to omrežje več čas preizkušamo s `SIP mid_PROBE` sporočili. Na podlagi odgovorov izračunamo zakasnitev paketov med terminalom MN in elementom SBC. Če izračun pokaže, da WLAN omrežje trenutno ni preobremenjeno, proces ostane v stanju *WLAN (checking QoS)*. S prožilcem *WLAN_QoS (OK)* sprožimo določitev časa T_{mid}, ki določa tisti čas, ko ponovno pošljemo `SIP mid_PROBE` sporočila. Če pa zaznamo, da WLAN omrežje ni sposobno zagotavljati ustreznega nivoja QoE, se proces s prekinitvijo *WLAN_QoS (NOK)* premakne v stanje *Handover to HSPA*. Ko je nova seja vzpostavljena, se proces vrne v stanje *HSPA (Idle)*. Poleg zakasnitve paketov med terminalom MN in elementom SBC v stanju *WLAN (checking QoS)* ves čas merimo tudi razmerje SNR WLAN omrežja. Če ta pade pod prag, se s prekinitvijo *WLAN_SNR (NOK)* proces premakne v stanje *Handover to HSPA*, kjer se izvede predaja zveze nazaj na HSPA omrežje.

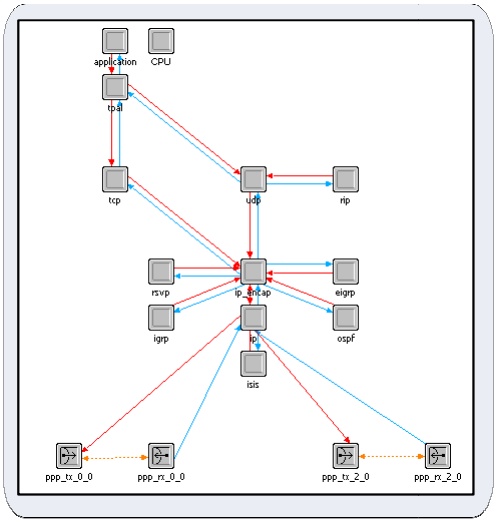
V stanjih *HSPA (idle)*, *HSPA (checking QoS)* in *WLAN (checking QoS)* sprejemamo in pošiljamo tudi RTP pakete. Stanja za prejemanje/pošiljanje RTP paketov so za boljšo preglednost iz slike odstranjena.



Slika 38: FSM postopka CAHP

6.3 Opis uporabljenih povezav in terminalov

Pri implementaciji postopka CAHP v simulacijskem orodju smo potrebovali večzvrstni terminal. V obstoječih modelih OPNET ne podpira večzvrstnih terminalov, vendar pa ponuja orodje, s katerim je takšen terminal mogoče definirati. Tako smo definirali terminal z dvema IP povezavama v omrežje. Ker se celotna predaja zveze izvaja na nivojih od tretjega OSI sloja navzgor, smo izbrali dva IP vmesnika. Tako smo dobili popolno neodvisnost od dostopovne tehnologije. Zgradba terminala, ki smo ga uporabljali pri simulaciji, je prikazana na sliki 39.



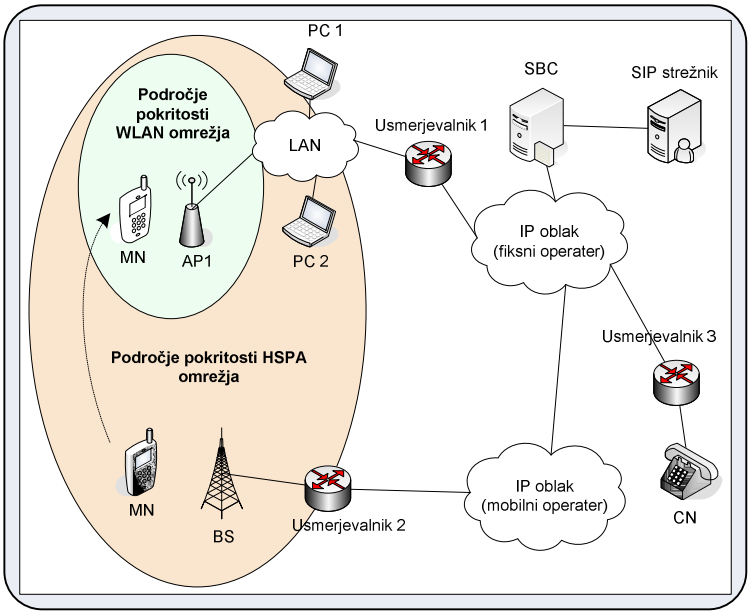
Slika 39: Zgradba dvozvrstnega terminala

Glavni namen našega dela je bil simulirati predajo zveze v heterogenih omrežjih. V orodju OPNET je veliko brezžičnih tehnologij že podprtih (npr. UMTS, WLAN, Wimax). Vendar pa smo naleteli na omejitve pri modeliranju realnega okolja, saj OPNET v osnovi predstavlja idealne pogoje. Želeli smo razviti takšen simulacijski model, ki nam bo omogočal uporabo meritev signala iz realnega okolja, s čimer bi lahko modelirali gibanje uporabnika in njegovo obnašanje, kot sta npr. gibanje uporabnika po stavbi, vstop uporabnika v dvigalo. Zato smo definirali različne povezave za različne dostopovne tehnologije. Na teh povezavah smo definirali modele za preverjanje in odpravljanje napak (*ang. error checking and correction*) in modele za generiranje napak (*ang. error model*), s katerimi smo določili lastnosti posameznega dostopovnega omrežja. Tako smo lahko simulirali kakršno koli dostopovno tehnologijo in tudi uporabili meritve razmerja SNR iz realnega okolja. Kot smo predstavili v poglavju 4.3, smo razmerje SNR v realnem okolju merili z orodjem NetStumbler, ki omogoča izvoz izmerjenih vrednosti v CSV (*ang. Comma Seperatet Values*) datoteki. Ti podatki so bili nato dodatno obdelani, tako da so ustrezali obliki, ki smo jo definirali za uporabo v orodju OPNET.

6.4 Arhitektura in parametri simulacijskega okolja

V orodju OPNET smo za analizo in ovrednotenje razvitega postopka zasnovali simulacijski model, ki je sestavljen iz dveh omrežij, WLAN in HSPA. Definirali smo tudi dva terminala, MN in CN, ki uporabljata storitev IP telefonije, pri kateri smo uporabili kodek G.711. Izničevanje tišine ni bilo uporabljeno, kar je imelo za posledico konstanten RTP podatkovni tok s 100 paketi na sekundo. Terminal MN je dvozvrstni terminal z možnostjo povezav v WLAN omrežje (lahko predstavlja fiksnega operaterja) in v HSPA omrežje (lahko predstavlja mobilnega operaterja). Terminal CN je običajen IP terminal, ki je z IP povezavo povezan v omrežje, preko katerega je povezan na SBC, na katerega je povezan SIP strežnik.

Omrežna arhitektura simulacijskega okolja je predstavljena na sliki 40.



Slika 40: Omrežna arhitektura simulacijskega okolja

Pri simulaciji smo upoštevali naslednje pogoje:

- HSPA omrežje je vedno na voljo in je zanesljivo.
- WLAN omrežje ima omejen doseg pokritosti (npr. kongresni center), a je na voljo več uporabnikom in zato velikokrat preobremenjeno.
- WLAN omrežje ima pri uporabniku prioriteto, kar pomeni da bo terminal MN poskušal narediti predajo vedno, ko bo razmerje SNR WLAN omrežja nad določenim pragom.
- Terminal MN je dvozvrstni terminal, ki ima sposobnost pošiljanja RTP paketov in SIP signalizacijskih sporočil ob istem času prek različnih vmesnikov.

Ker smo želeli, da bi bil simulacijski model čim bolj podoben okolju operaterja, smo kot vhodne parametre za simulacije omrežij uporabili rezultate, ki so bili predstavljeni v poglavju 4.3. Zakasnitve v IP oblakih so bile nastavljene na enake vrednosti, kot smo jih predstavili v tabeli 6. Za povečanje prometa na dostopovni povezavi WLAN omrežja smo dodali dodatne kliente (predstavljeni s prenosnima računalnikoma na sliki 40), ki so generirali dodaten UDP promet.

Določili smo tudi vrednosti pragov in drugih prametrov, ki jih uporabljamo v predlaganem postopku. Zakasnitve paketov od konca do konca manjše od 200 ms ne vplivajo na zmanjšanje nivoja QoE, zato smo to vrednost izbrali za prag T_d. Na modelu WLAN povezave smo izbrali modulacijo cck-11, ki se uporablja pri WLAN standardu 802.11b, za hitrosti 11 Mbit/s. Vsaka modulacija ima svojo krivuljo, ki določa BER. Vrednosti BER za izbrano modulacijo pri različnih vrednostih razmerja SNR so prikazani v tabeli 7. Kot je razvidno iz tabele, se za modulacijo cck-11 ob vrednostih razmerja SNR, ki je manjša od 10 dB, zelo poveča možnost izgube paketov, kar potrjuje rezultate eksperimentov, zato smo prag T_{SNR} nastavili na 10 dB.

Tabela 7: BER modulacijska tabela za cck-11

S/N	(+0dB)	(+0.25dB)	(+0.50dB)
+ 5.00	0.0081	0.005	0.003
+ 5.75	0.0021	0.0014	0.00078
+ 6.50	0.00044	0.00025	0.00014
+ 7.25	0.000081	0.000044	0.000022
+ 8.00	0.00001	0.0000048	0.0000021
+ 8.75	0.00000081	0.00000037	0.00000016
+ 9.50	0.000000061	0.0000000016	0.0000000056

V skupini testnih `SIP pre-PROBE` in `SIP mid-PROBE` smo pošiljali 3 sporočila ($N_{pre} = N_{mid} = 3$). Čas T_{inter} med njimi smo nastavili na 10 ms, kar je običajna vrednost paketizacije za IP telefonijo. Tako smo se

s poizkusnimi sporočili približali simulaciji govornega toka (RTP prometa). Za določitev, kdaj se bo predaja zveze zgodila, smo uporabili postopek CAHP, ki je bil predstavljen v poglavju 5. Tako se predaja zveze na WLAN omrežje (ob izpolnjenem osnovnem pogoju SNR > T_{SNR}) izvede le, če je dostopovno omrežje WLAN sposobno zagotavljati ustrezen nivo QoE in je predana nazaj na HSPA omrežje, če postane WLAN omrežje preobremenjeno med klicem ali SNR razmerje pade pod T_{SNR}.

Pred začetkom izvajanja glavne simulacije smo izvedli verifikacijo delovanja uporabe predlaganega postopka in ovrednotenje simulacijskega modela.

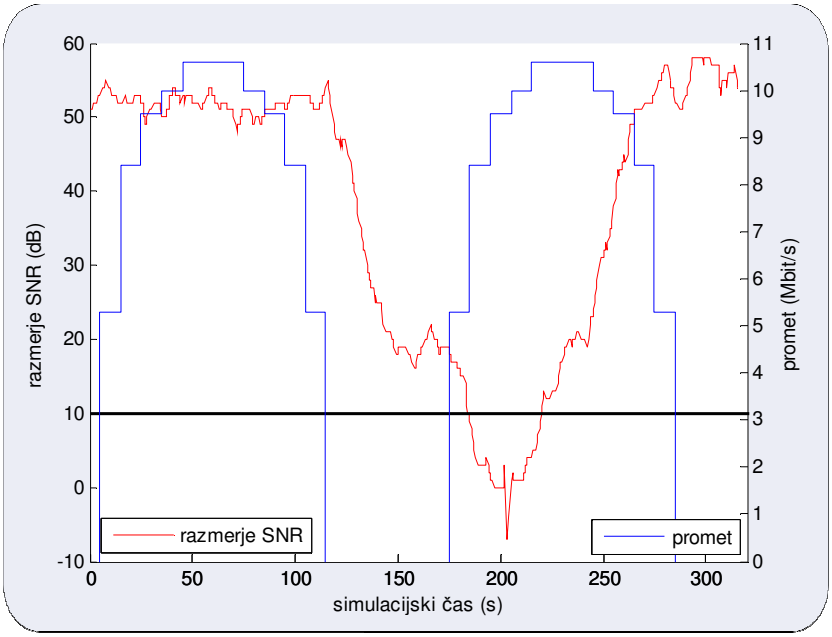
6.5 Verifikacija in ovrednotenje postopka CAHP

Namen verifikacije je bil analizirati, ali predlagani postopek implementiran v simulacijskem orodju OPNET deluje v skladu s predlaganim algoritmom predstavljenim na sliki 28. Poleg verifikacije smo izvedli tudi ovrednotenje postopka CAHP. V ta namen smo definirali krajši scenarij, v katerem bo uporabnik najprej vzpostavil klic v WLAN omrežju, ki je nezanesljivo, saj lahko postane preobremenjeno. Med klicem se bo uporabnik začel premikati izven območja pokritosti WLAN omrežja in se nato (še vedno v trajanju istega klica) začel premikati nazaj proti WLAN omrežju. Ker to omrežje uporabljajo tudi drugi uporabniki, je ob začetku procesa predajanje zveze dostopovno omrežje WLAN preobremenjeno.

Uporaba predlaganega postopka bo na različne načine vplivala na predajanje zveze med WLAN in HSPA omrežjem. Razdelimo jih lahko v dve skupini:

- Vpliv razmerja SNR WLAN omrežja:
  - Če bo ob premikanju terminala izven WLAN omrežja razmerje SNR padlo pod T_{SNR}, bo to sprožilo predajo zveze na HSPA omrežje.
  - Če bo ob premikanju terminala nazaj proti WLAN omrežju, razmerje SNR zraslo nad T_{SNR}, bo to sprožilo postopek predaje zveze na WLAN omrežje.
- Vpliv obremenjenosti dostopovne povezave WLAN omrežja:
  - Če bo razmerje SNR WLAN omrežja zrastlo nad prag in bo to v istem trenutku preobremenjeno, bo to povzročilo zadržanje predaje zveze.
  - Če bo ob uporabi WLAN omrežja to postalo preobremenjeno kljub zadostnemu razmerju SNR, bo to sprožilo predajo zveze na HSPA omrežje.

Kot vhodni podatki za verifikacijo so bili za potek razmerja SNR uporabljeni rezultati meritev ES_WALK predstavljeni v poglavju 4.3, kot prikazuje slika 41. Na sliko smo dodali horizontalno črto, ki prikazuje vrednost 10 dB razmerja SNR, ki je bila uporabljena kot prag.



Slika 41: Vhodni parametri simulacijskega scenarija za WLAN omrežje

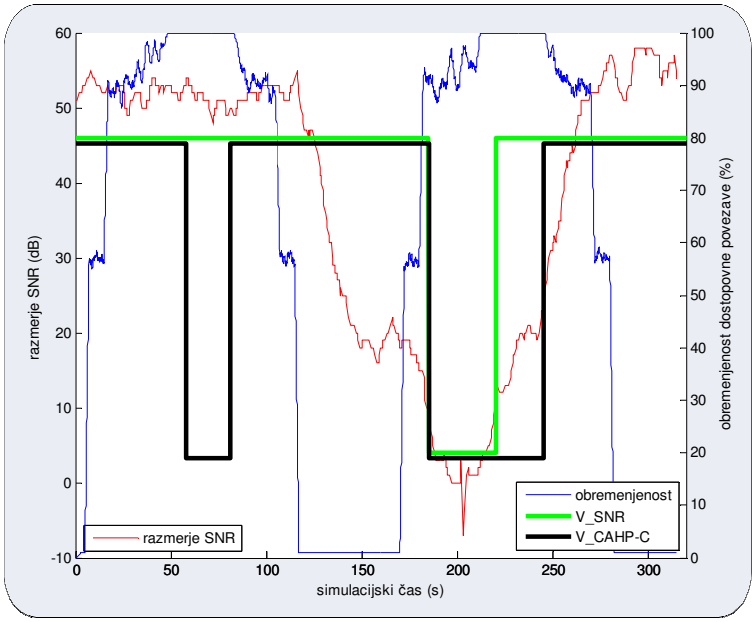
Razporeditev obremenitev je enaka kot v ES_TRAFFIC in je prikazana z modro črto na sliki 41. Za definiran scenarij smo izvedli dva simulacijska teka:

1. V simulacijskem teku V_SNR smo predaje izvajali zgolj na podlagi merjenja razmerja SNR,

brez uporabe *Pre-porbe* ter *Mid-probe* algoritma, torej brez merjenja obremenjenosti dostopovne povezave WLAN omrežja.

2. V simulacijskem teku V_CAHP-C smo uporabili celoten postopek CAHP. Parametra T_{pre} in T_{mid} smo nastavili na konstantno vrednost 1 s.

Rezultati simulacije so predstavljeni na sliki 42.



Slika 42: Simulacijski rezultati

Rdeča črta prikazuje vrednosti razmerja SNR, ki smo jih dobili z meritvami v ES_WALK in so bile uporabljene v orodju OPNET. Modra črta predstavlja obremenjenost povezave med AP in LAN omrežjem izmerjena v orodju OPNET. Obremenitev povezave je posledica uporabe dodatnih klientov, ki so generirali UDP promet. Črna in zelena črta prikazujeta, katero omrežje je bilo uporabljeno za oba simulacijska teka.

V simulacijskem teku V_SNR, se je predaja (zgolj na podlagi meritev razmerja SNR) izvedla dvakrat. Prvič iz omrežja WLAN na omrežje HSPA ob simulacijskem času 185,4 sekunde, ko je razmerje SNR padlo pod 10 dB. Druga predaja zveze pa iz omrežja HSPA na WLAN omrežje ob simulacijskem času 220,6 sekunde, ko je razmerje SNR zraslo nad prag. Pri obeh predajah se je izvedla osnovna predaja zveze zgolj zaradi spremembe moči signala.

V simulacijskem teku V_CAHP-C se je predaja izvedla štirikrat. Prva se je izvršila, ker smo z algoritmom *Mid-probe* zaznali preveliko obremenitev dostopovne povezave WLAN omrežja med uporabo tega omrežja ob simulacijskem času 58,0 s. Ker je bilo razmerje SNR še vedno nad pragom, je terminal MN s *Pre-probe* algoritmom začel meriti obremenitve in testiranje izvajal tako dolgo, dokler ni obremenjenost WLAN omrežja padla tako nizko, da to ni imelo več bistvenega vpliva na zakasnitev paketov IP telefonije, kar je sprožilo drugo predajo ob simulacijskem času 81,4 s. Tretja predaja je enaka kot pri simulacijskem teku V_SNR in se je zgodila zaradi padca razmerja SNR WLAN omrežja ob simulacijskem času 185,4 s. Četrta predaja je bila sprožena zaradi dviga razmerja SNR ob istem času kot pri V_SNR. Vendar smo s *Pre-probe* algoritmom v tem trenutku zaznali preobremenjenost WLAN omrežja in postopek predaje prekinili. Testiranje s `SIP pre-PROBE` sporočili se je nadaljevalo in ko je obremenjenost padla, se je zgodila predaja na WLAN omrežje ob simulacijskem času 245,4 s. Uporaba *Pre-probe* algoritma je imela za posledico, da je bila izvedba predaje v simulacijskem teku V_CAHP-C zakasnjena glede na simulacijski tek V_SNR.

Pri obeh simulacijskih tekih smo merili povprečno in maksimalno zakasnitev paketov. Ker ta dva podatka ne dajeta popolne informacije o vplivu na storitev IP telefonije (npr. maksimalna zakasnitev paketov se lahko pojavi zgolj enkrat in je lahko za uporabnika nemoteča), smo merili tudi delež časa glede na celoten simulacijski čas, ko je bila zakasnitev paketov višja od 200ms. Povzetek rezultatov za oba scenarija je prikazan v tabeli 8.

Tabela 8: Povzetek rezultatov

	V_SNR	V_CAHP-C
Parameter		
Povprečna zakasnitev paketov	158 ms	95 ms
Največja zakasnitev paketov	624 ms	289 ms
Skupen čas z zakasnitvami nad 200 ms	20%	2%
Št. Predaj zvez	2	4
Simulacijski čas, ko je bila izvedena predaja	185,4 s (iz WLAN na HSPA) 220,6 (iz HSPA na WLAN)	58,0 s (iz WLAN na HSPA) 81,4 s (iz HSPA na WLAN) 185,4 s (iz WLAN na HSPA) 245,4 (iz HSPA na WLAN)

Iz rezultatov je razvidno, da predlagan postopek deluje pričakovano in pravilno ter da lahko z uporabo predlaganega postopka pričakujemo izboljšanje nivoja QoE za uporabnika med gibanjem po heterogenih omrežjih, saj se je močno zmanjšal čas komunikacije, ko je bila zakasnitev paketov od konca do konca nad 200 milisekund (iz 20 % na 2 %). Podrobna analiza in ovrednotenje predlaganega postopka CAHP je podana v poglavju 7.

7 Analiza in ovrednotenje predlaganega postopka CAHP

V tem poglavju bomo predstavili natančnejšo analizo in ovrednotenje predlaganega postopka CAHP. Za analizo smo uporabili simulacijski model, predstavljen v poglavju 6.4. Definirali smo več simulacijskih scenarijev. Ker smo želeli med seboj primerjati rezultate različnih scenarijev, smo definirali osnovne pogoje, ki so skupni vsem scenarijem:

- Uporabnik se ne premika in je ves čas v območju pokritosti WLAN omrežja, kar pomeni, da je razmerje SNR ves čas simulacije nad določenim pragom T_{SNR}.
- Simulacijski čas je 8 ur, kar znaša 28800 sekund.
- Preobremenitve dostopovne povezave WLAN omrežja se dogajajo naključno, njihovo pojavljanje in trajanje je porazdeljeno po eksponentni funkciji.

Spreminjanje razmerja SNR ima na vse scenarije enak vpliv, saj pomeni brezpogojno predajo zveze na omrežje HSPA. Zato smo definirali prvi pogoj, kar nam je omogočilo, da smo dobili rezultate, ki so odvisni samo od zaznavanja obremenjenosti, in ne tudi od spreminjanja razmerja SNR. Prikaz delovanja postopka CAHP na podlagi nihanja razmerja SNR je prikazan v poglavju 6.5. Drugi pogoj (dolžina simulacije) nam je omogočil dovolj reprezentativne rezultate, saj se je postopek izvajal velikokrat. V času simulacije je bil vzpostavljen le en klic, vendar lahko rezultate razširimo tudi na scenarij, kjer bi več uporabnikov vzpostavljalo več zaporednih klicev, katerih skupna dolžina bi bila 8 ur. S tretjim pogojem smo definirali preobremenitve dostopovnega omrežja. Ker smo predpostavili, da se lahko preobremenitev zgodi le v dostopovnem omrežju, na katerega je priključena AP omrežja WLAN, smo v omrežje dodali dodaten UDP promet na dostopovni povezavi. Dodaten promet je povzročal zgostitve prometa na omrežju. Trajanje posamezne zgostitve zaradi UDP prometa je bila distribuirana po eksponentni funkciji, kot je podano v enačbi (17).

$$f_x(x_0) = \begin{cases} a \cdot e^{-a \cdot x_0}; & x_0 > 0 \\ 0; & drugače \end{cases} \tag{17}$$

kjer vedno velja $a > 0$. Srednja vrednost je enaka $E(x) = a^{-1}$, varianca pa $\sigma_x^2 = a^{-2}$.

Eksponentno funkcijo smo izbrali, ker je matematično dobro obvladljiva in se zato pogosto uporablja v simulacijskih okoljih. Za srednjo vrednost eksponentne funkcije trajanja posamezne zgostitve smo izbrali 20 sekund. Čas med dvema zgostitvama je bil ravno tako naključno porazdeljen po eksponentni funkciji s srednjo vrednostjo 10 sekund. Tako smo dobili popolnoma naključne preobremenitve WLAN omrežja, kar nam je omogočilo, da smo predlagan postopek lahko preizkusili večkrat. OPNET omogoča, da se pri vsakem zagonu simulacije psevdo-naključne vrednosti razporedijo enako glede na začetne pogoje (*ang. seed*). To nam je omogočilo, da smo lahko ob vsakem zagonu simulacije z enakimi začetnimi pogoji dosegli enako razporeditev naključnih vrednosti in tako primerjali rezultate različnih izvedenih scenarijev.

Izvedli smo tri simulacijske sklope:

1. V prvem smo izvedli scenarij, kjer ni bil uporabljen postopek CAHP. V tem primeru bo uporabnik ves čas uporabljal WLAN omrežje (razmerje SNR je vedno nad pragom T_{SNR}). Izvedena ne bo nobena predaja. Rezultati tega simulacijskega sklopa nam dajo osnovno sliko obnašanja WLAN omrežja pri simulaciji in vpliv naključnih preobremenitev na zakasnitev paketov storitve IP telefonije.
2. V drugem simulacijskem sklopu smo izvajali več scenarijev, pri katerih smo za parametra T_{pre} in T_{mid} uporabljali konstante vrednosti z uporabo postopka CAHP-C. Izbrali smo več različnih vrednosti za T_{pre} in T_{mid} in naredili medsebojno primerjavo vpliva spreminjanja teh vrednosti na rezultate.
3. V tretjem simulacijskem sklopu smo vrednosti T_{pre} in T_{mid} nastavljali adaptivno s postopkom CAHP-A. Da bi preučili vpliv različnih vrednosti α in T_{max} na rezultate, smo izvedli več scenarijev pri različnih vrednostih α in T_{max}.

Vsi simulacijski scenariji za vse tri simulacijske sklope so predstavljeni v tabeli 9. Pri izvajanju simulacije smo zbirali več tipov podatkov, ki jih bomo prikazali v rezultatih. Rezultate lahko v splošnem razdelimo v dve skupini:

- Rezultati pomembni za uporabnika:
  - nivo QoE uporabe storitve IP telefonije
  - cena komunikacije
- Rezultati pomembni za operaterja:
  - povečanje signalizacijske režije

Med rezultati, ki so pomembni za uporabnika, merimo nivo QoE in ceno komunikacije. Naše merilo za nivo QoE je bila zakasnitev RTP paketov med terminalom MN in elementom SBC. Tako smo v vseh simulacijskih scenarijih merili zakasnitev vseh poslanih RTP paketov. V rezultatih bomo prikazali izmerjene vrednosti, ki smo jih dobili neposredno iz orodja OPNET. Ker orodje OPNET omogoča meritve zakasnitev vsakega paketa, smo tako dobili zelo natančne vrednosti zakasnitev paketov za celotno simulacijo. Za lažjo primerjavo in preglednost smo izmerjene vrednosti razporedili v razrede širine 50 ms in ugotovili frekvenco pojavljanja paketov znotraj posameznega razreda. Pri simulaciji IP telefonije smo uporabili čas paketizacije 10 ms. Ker smo želeli dobiti skupen simulacijski čas, ko je bila zakasnitev paketov v določenem intervalu, smo to storili tako, da smo število paketov z zakasnitvijo znotraj posameznega razreda pomnožili s časom paketizacije. Drugi pomemben podatek s stališča uporabnika je cena komunikacije, ki smo jo ocenili s skupnim časom, ko je uporabnik uporabljal HSPA omrežje, saj smo predpostavili, da je WLAN omrežje brezplačno.

Iz stališča operaterja je najbolj pomemben podatek, kako se bo povečala signalizacijska režija. V postopku CAHP smo testirali dostopovno omrežje WLAN z na novo definiranimi SIP sporočili. Pri vsakem testiranju zakasnitve WLAN omrežja pošljemo skupino treh SIP sporočil, ki povzročajo signalizacijsko režijo in večjo obremenitev elementa SBC. V rezultatih bomo predstavili število dodatnih sporočil, ki so bila poslana za preverjanje obremenjenosti WLAN omrežja.

Zaradi velike količine podatkov v rezultatih podajamo zgolj najpomembnejše vrednosti. Rezultati so v celoti predstavljeni v prilogi C.

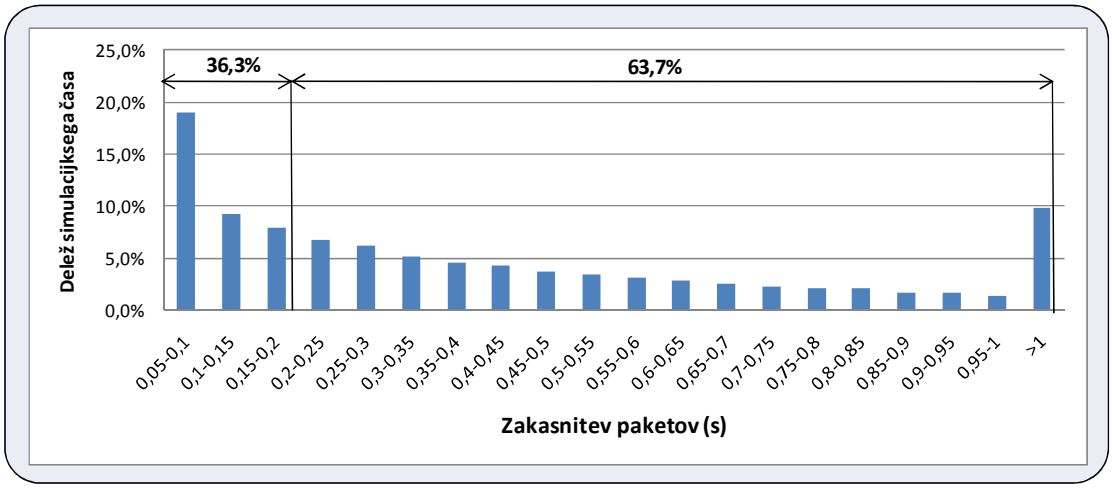
Tabela 9: Simulacijski scenariji za ovrednotenje predlaganega postopka

Sim. sklop	Št. scenarija	Ime scenarija	T_{pre}	T_{mid}	α	T_{max}
1	1	R-1	N/A	N/A	N/A	N/A
2	1	C-1	0 s	0 s	N/A	N/A
	2	C-2	1 s	1 s	N/A	N/A
	3	C-3	2 s	2 s	N/A	N/A
	4	C-4	4 s	4 s	N/A	N/A
	5	C-5	8 s	8 s	N/A	N/A
	6	C-6	16 s	16 s	N/A	N/A
3	1	A-1	adaptiven	adaptiven	1/16	1 s
	2	A-2	adaptiven	adaptiven	1/8	1 s
	3	A-3	adaptiven	adaptiven	1/4	1 s
	4	A-4	adaptiven	adaptiven	1/2	1 s
	5	A-5	adaptiven	adaptiven	1	1 s
	6	A-6	adaptiven	adaptiven	2	1 s
	7	A-7	adaptiven	adaptiven	4	1 s
	8	A-8	adaptiven	adaptiven	8	1 s
	9	A-9	adaptiven	adaptiven	16	1 s
	10	A-10	adaptiven	adaptiven	1/16	2 s
	11	A-11	adaptiven	adaptiven	1/8	2 s
	12	A-12	adaptiven	adaptiven	1/4	2 s
	13	A-13	adaptiven	adaptiven	1/2	2 s
	14	A-14	adaptiven	adaptiven	1	2 s
	15	A-15	adaptiven	adaptiven	2	2 s
	16	A-16	adaptiven	adaptiven	4	2 s
	17	A-17	adaptiven	adaptiven	8	2 s
	18	A-18	adaptiven	adaptiven	16	2 s
	19	A-19	adaptiven	adaptiven	1/16	4 s
	20	A-20	adaptiven	adaptiven	1/8	4 s
	21	A-21	adaptiven	adaptiven	1/4	4 s
	22	A-22	adaptiven	adaptiven	1/2	4 s
	23	A-23	adaptiven	adaptiven	1	4 s
	24	A-24	adaptiven	adaptiven	2	4 s
	25	A-25	adaptiven	adaptiven	4	4 s
	26	A-26	adaptiven	adaptiven	8	4 s
	27	A-27	adaptiven	adaptiven	16	4 s
	28	A-28	adaptiven	adaptiven	1/16	8 s
	29	A-29	adaptiven	adaptiven	1/8	8 s
	30	A-30	adaptiven	adaptiven	1/4	8 s
	31	A-31	adaptiven	adaptiven	1/2	8 s
	32	A-32	adaptiven	adaptiven	1	8 s
	33	A-33	adaptiven	adaptiven	2	8 s
	34	A-34	adaptiven	adaptiven	4	8 s
	35	A-35	adaptiven	adaptiven	8	8 s
	36	A-36	adaptiven	adaptiven	16	8 s
	37	A-37	adaptiven	adaptiven	1/16	16 s
	38	A-38	adaptiven	adaptiven	1/8	16 s
	39	A-39	adaptiven	adaptiven	1/4	16 s
	40	A-40	adaptiven	adaptiven	1/2	16 s
	41	A-41	adaptiven	adaptiven	1	16 s
	42	A-42	adaptiven	adaptiven	2	16 s
	43	A-43	adaptiven	adaptiven	4	16 s
	44	A-44	adaptiven	adaptiven	8	16 s
	45	A-45	adaptiven	adaptiven	16	16 s

7.1 Rezultati prvega simulacijskega sklopa (brez postopka CAHP)

V prvem simulacijskem sklopu smo želeli pridobiti zgolj referenčne rezultate in nismo uporabili postopka CAHP. Tako ni bilo poslanih nobenih SIP sporočil za preverjanje obremenjenosti WLAN omrežja, kar je pomenilo, da se med klicem ni zgodila nobena predaja zveze. Uporabnik je ves čas uporabljal WLAN omrežje, katerega dostopovna povezava je bila občasno preobremenjena.

Na sliki 43 prikazujemo razporeditev zakasnitev paketov, izmerjeno v orodju OPNET. Nad histogrami podajamo tudi delež časa v odvisnosti od celotnega časa simulacije (8 ur), ko je bila izmerjena zakasnitev paketov pod oziroma nad 200 ms.

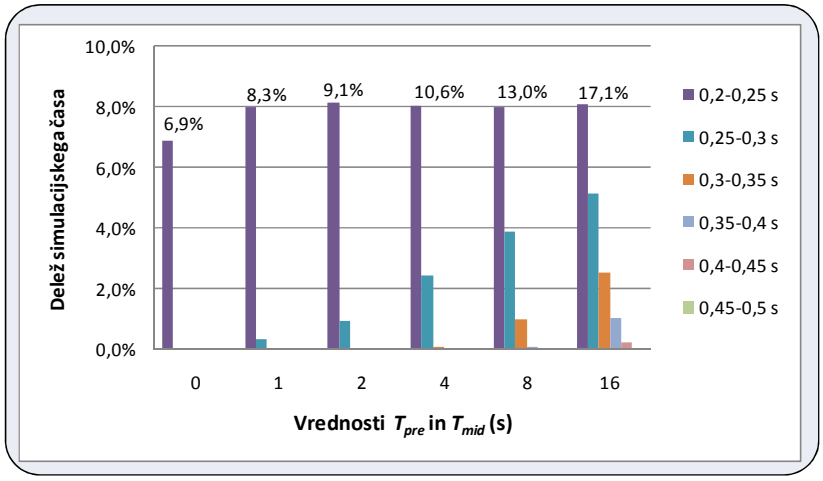


Slika 43: Razporeditev zakasnitev paketov (prvi simulacijski sklop, brez postopka CAHP)

Iz rezultatov je razvidno, da je bila kar 63,7% simulacijskega časa zakasnitev paketov nad 200 ms, kar je pričakovan rezultat, saj je bilo razmerje časa med posameznimi obremenitvami in trajanjem ene obremenitve 1:2. Do 2,9 odstotnih točk razlike (66,6%-63,7%) pride, ker je bil potreben določen čas, da je število dodatnih UDP paketov povzročilo preobremenitev. Opazimo lahko tudi, da je skoraj 10% simulacijskega časa zakasnitev paketov nad 1 s. To pomeni, da je nivo uporabniške izkušnje v takšnem primeru zelo nizek. V praksi na takšnem omrežju sploh ne bi bilo mogoče komunicirati.

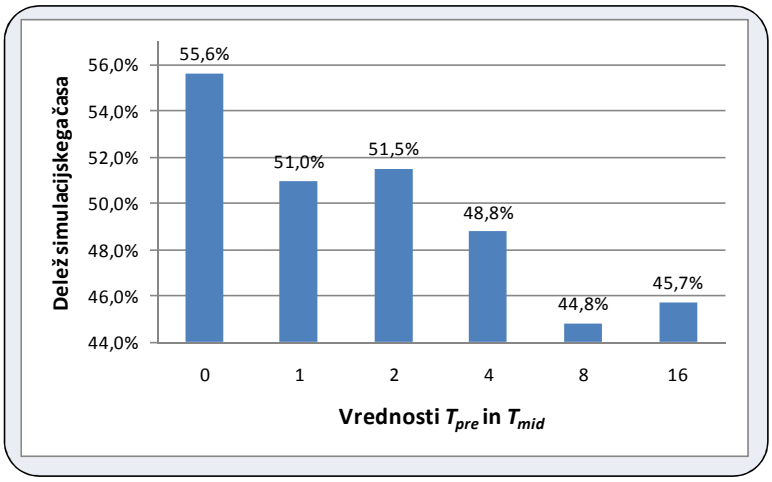
7.2 Rezultati drugega simulacijskega sklopa (postopek CAHP-C)

V tem simulacijskem sklopu smo vrednosti parametrov T_{pre} in T_{mid} nastavljali po načinu CAHP-C. Definirali smo šest simulacijskih scenarijev, kjer smo za vrednosti parametrov T_{pre} in T_{mid} izbrali vrednosti 0 s, 1 s, 2 s, 4 s, 8 s in 16 s. Razporeditev v orodju OPNET izmerjenih zakasnitev paketov za vse scenarije je prikazana na sliki 44. Zaradi bolj preglednega prikaza smo izbrali zgolj razrede, večje od 200 ms, ki lahko negativno vplivajo na nivo QoE. Za vsak scenarij je nad histogrami prikazan tudi delež skupnega simulacijskega časa, ko je zakasnitev presegala 200 ms. Vidimo lahko, da se delež simulacijskega časa z zakasnitvami paketov nad 200 ms veča, čim večji sta vrednosti parametrov T_{pre} in T_{mid}. To je posledica manjše pogostosti preverjanja obremenitev pri višjih vrednostih parametrov T_{pre} in T_{mid}, kar lahko ima za posledico, da obremenitev ni pravočasno zaznana. Najboljši rezultat po pričakovanjih dosegamo, ko smo parametra T_{pre} in T_{mid} postavili na 0 sekund, kar pomeni, da je bilo omrežje ves čas testirano in smo lahko preobremenitev zaznali skoraj takoj, ko se je pojavila.



Slika 44: Razporeditev zakasnitev paketov (drugi simulacijski sklop, postopek CAHP-C)

Čas, ko je bil uporabljen HSPA vmesnik, je prikazan na sliki 45.



Slika 45: Delež simulacijskega časa na HSPA omrežju (drugi simulacijski sklop, postopek CAHP-C)

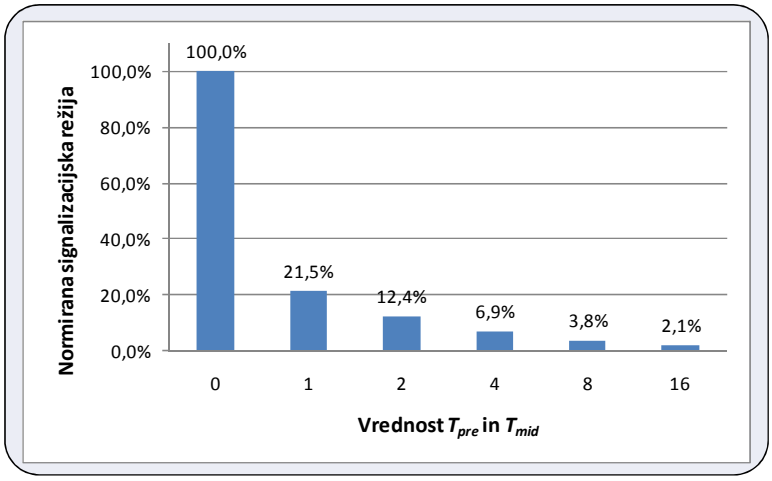
Opazimo lahko, da se delež uporabe HSPA omrežja manjša z večanjem vrednosti parametrov T_{pre} in T_{mid}. Vendar pa razlika ni tako velika, saj je med 0 s in 16 s razlike 9,9 odstotnih točk. Za uporabnika je najcenejša komunikacija, ko sta parametra T_{pre} in T_{mid} nastavljena na 8 s. Iz rezultatov lahko sklenemo, da z uporabo CAHP-C postopka ne vplivamo občutno na povečevanje uporabe HSPA vmesnika in s tem na ceno komunikacije.

Po pričakovanjih je največ signalizacijske režije v scenariju C-1, kjer sta bila parametra T_{pre} in T_{mid} nastavljena na 0 sekund. V tem scenariju je bilo poslanih 304.221 sporočil. Zato smo ta scenarij ($T_{pre} = T_{mid} = 0$) vzeli za referenco s katerim smo normirali ostale, kot je to prikazano v enačbi (18):

$$NSO_i = \frac{nSM_i}{nSM_{C1}} \cdot 100\% \tag{18}$$

kjer je NSO_i normirana signalizacijska režija (*ang. normalized signalling overhead*) za scenarij i, nSM_i število signalizacijskih sporočil (*ang. number of signalling messages*) scenarija i, nSM_{C1} število signalizacijskih sporočil scenarija C-1.

Na sliki 46 je prikazana normirana signalizacijska režija za vseh šest scenarijev.



Slika 46: Signalizacijska režija (drugi simulacijski sklop, postopek CAHP-C)

Vidimo lahko, da se delež signalizacije zelo zmanjša že v drugem scenariju (na 21,5%). Najnižjo vrednost signalizacije dosežemo pri šestem scenariju, kjer je število SIP sporočil zmanjšano za 97,9 odstotnih točk.

7.3 Rezultati tretjega simulacijskega sklopa (postopek CAHP-A)

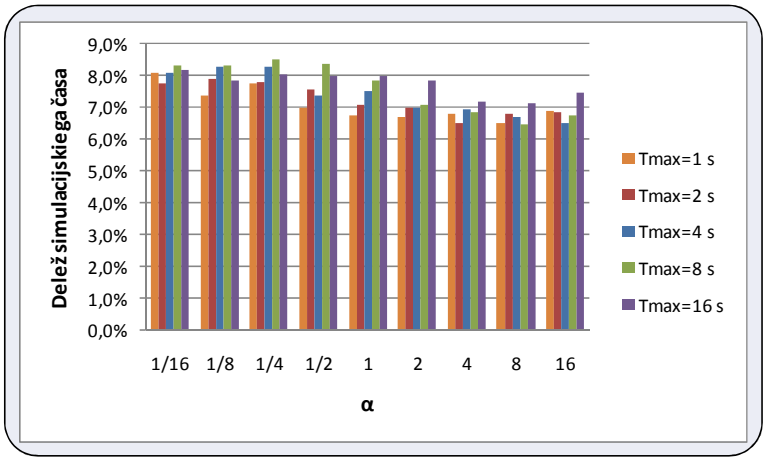
V tretjem simulacijskem sklopu smo za nastavljanje parametrov T_{pre} in T_{mid} uporabili adaptivni način CAHP-A, pri katerem se vrednosti teh dveh parametrov spreminjata v odvisnosti od trenutne obremenjenosti omrežja. Pri izračunu parametrov smo uporabili dve spremenljivki, in sicer α in T_{max}. Da bi lahko ocenili vpliv različnih vrednosti teh spremenljivk na nivo QoE med predajanjem zveze, smo definirali 45 scenarijev, v katerih smo vrednosti α izbirali med 1/16, 1/8, 1/4, 1/2, 1, 2, 4, 8 in 16. Te vrednosti smo uporabili pri različnih vrednostih T_{max}, za katerega smo izbirali med vrednostmi 1 s, 2 s, 4 s, 8 s in 16 s.

V nadaljevanju bomo podali rezultate za različne vrednosti α ob različnih vrednostih spremenljivke T_{max} za vse tri tipe rezultatov, ki smo jih spremljali.

7.3.1 Analiza izmerjenih zakasnitev paketov

V tem poglavju bomo predstavili rezultate izmerjenih zakasnitev paketov. Zaradi boljše preglednosti bomo ločeno prikazali posamezne razrede izmerjenih zakasnitev paketov nad 200 ms. Pri vseh podajamo delež simulacijskega časa v odvisnosti od celotnega simulacijskega časa, ko je bila zakasnitev v posameznem razredu.

Na sliki 47 in v tabeli 10 je prikazana razporeditev izmerjenih zakasnitev paketov med 200 ms in 250 ms za različne vrednosti spremenljivk α in T_{max}.



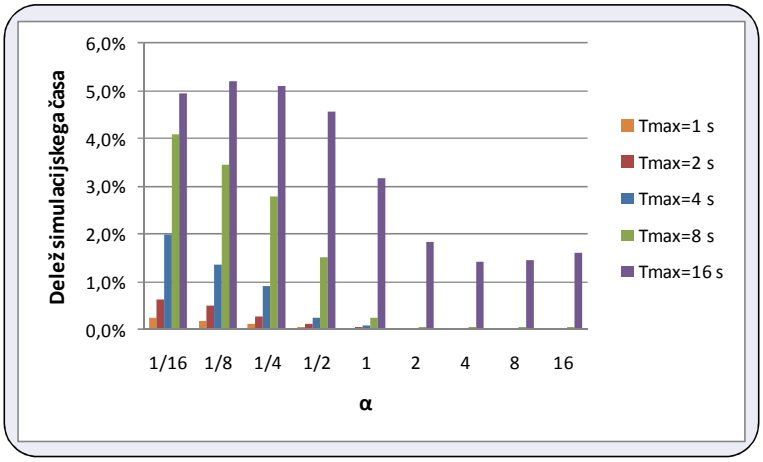
Slika 47: Delež simulacijskega časa z zakasnitvami paketov med 200 in 250 ms (tretji simulacijski sklop, postopek CAHP-A)

Tabela 10: Simulacijski čas z zakasnitvami paketov med 200 in 250 ms (tretji simulacijski sklop)

T_{max} \ α	1/16	1/8	1/4	1/2	1	2	4	8	16
1 s	2330,9 s	2120,7 s	2233,0 s	2010,2 s	1949,5 s	1935,2 s	1952,9 s	1878,3 s	1987,6 s
2 s	2232,5 s	2279,7 s	2245,2 s	2173,1 s	2036,7 s	2006,4 s	1881,1 s	1962,9 s	1974,4 s
4 s	2335,4 s	2380,2 s	2379,7 s	2125,9 s	2162,8 s	2006,9 s	1993,8 s	1926,3 s	1878,4 s
8 s	2398,0 s	2396,6 s	2458,6 s	2413,6 s	2262,1 s	2041,0 s	1972,0 s	1864,9 s	1949,3 s
16 s	2353,1 s	2260,9 s	2311,5 s	2301,4 s	2296,9 s	2259,6 s	2073,3 s	2059,3 s	2149,4 s

Iz slike 47 je razvidno, da se pri vseh scenarijih pojavljajo zakasnitve paketov med 200 in 250 ms. Opazen je majhen trend padanja deleža simulacijskega časa z večanjem parametra α in trend naraščanja tega deleža z večanjem T_{max} za zakasnitve paketov v opazovanem območju.

Na sliki 48 in tabeli 11 je prikazana razporeditev izmerjenih zakasnitev paketov med 250 ms in 300 ms za različne vrednosti spremenljivk α in T_{max}.



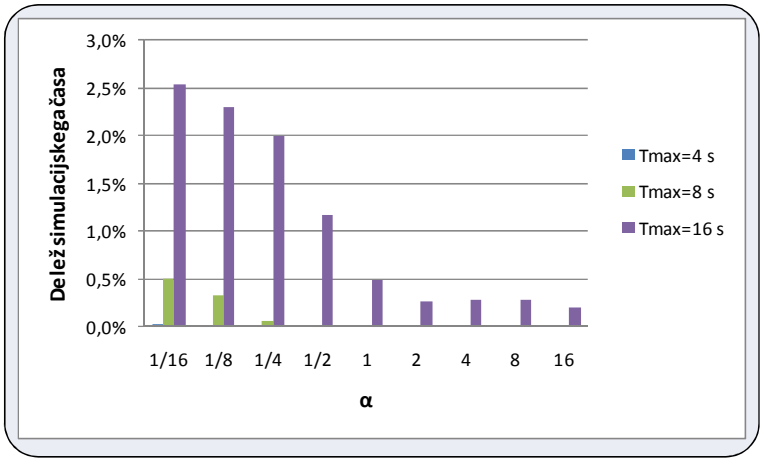
Slika 48: Delež simulacijskega časa z zakasnitvami paketov med 250 in 300 ms (tretji simulacijski sklop, postopek CAHP-A)

Tabela 11: Simulacijski čas z zakasnitvami paketov med 250 in 300 ms (tretji simulacijski sklop, postopek CAHP-A)

T_{max} \ α	1/16	1/8	1/4	1/2	1	2	4	8	16
1 s	74,2 s	51,6 s	36,2 s	20,5 s	10,8 s	8,4 s	7,9 s	9,4 s	11,1 s
2 s	184,9 s	142,1 s	82,5 s	32,2 s	12,0 s	9,5 s	11,4 s	10,0 s	9,7 s
4 s	571,2 s	393,2 s	263,3 s	74,2 s	21,6 s	9,6 s	10,3 s	10,8 s	11,0 s
8 s	1176,9 s	992,8 s	804,7 s	436,5 s	72,3 s	19,3 s	14,2 s	12,6 s	14,6 s
16 s	1427,2 s	1500,7 s	1468,5 s	1311,7 s	912,3 s	529,5 s	409,4 s	416,5 s	466,7 s

Iz slike 48 je razvidno, da se pri vseh scenarijih pojavljajo zakasnitve paketov med 250 in 300 ms. Opazimo lahko izrazitejši trend padanja deleža simulacijskega časa z večanjem parametra α in trend naraščanja deleža simulacijskega časa z večanjem T_{max} za zakasnitve paketov v opazovanem območju. Iz tabele 11 je razvidno, da pri nekaterih scenarijih dosegamo že zelo nizke vrednosti (pod 10 s) skupnega simulacijskega časa, ko so bile izmerjene zakasnitve paketov v intervalu med 250 in 300 ms. To so scenariji A-6, A-7, A-8, A-15, A-18 in A-24.

Na sliki 49 in tabeli 12 je prikazana razporeditev izmerjenih zakasnitev paketov med 300 ms in 350 ms za različne vrednosti spremenljivk α in T_{max}



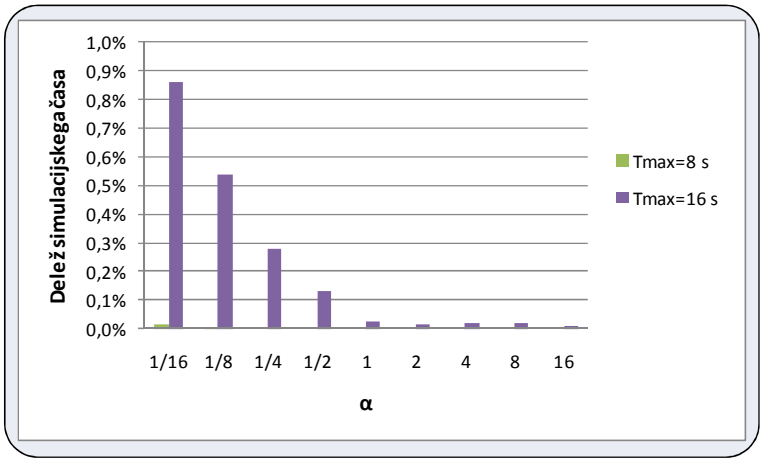
Slika 49: Delež simulacijskega časa z zakasnitvami paketov med 300 in 350 ms (tretji simulacijski sklop, postopek CAHP-A)

Tabela 12: Simulacijski čas z zakasnitvami paketov med 300 in 350 ms (tretji simulacijski sklop, postopek CAHP-A)

T_{max} \ α	1/16	1/8	1/4	1/2	1	2	4	8	16
1 s	0,0 s	0,0 s	0,0 s	0,0 s	0,0 s	0,0 s	0,0 s	0,0 s	0,0 s
2 s	0,0 s	0,0 s	0,0 s	0,0 s	0,0 s	0,0 s	0,0 s	0,0 s	0,0 s
4 s	9,1 s	2,5 s	0,0 s	0,0 s	0,0 s	0,0 s	0,0 s	0,0 s	0,0 s
8 s	146,8 s	93,8 s	19,2 s	1,4 s	0,0 s	0,0 s	0,0 s	0,0 s	0,0 s
16 s	729,7 s	659,9 s	577 s	338,2 s	142,4 s	76,2 s	80,6 s	81,5 s	59,0 s

Iz tabele 12 je razvidno, da se zakasnitve paketov v intervalu med 300 in 350 ms pojavljajo samo pri nekaterih scenarijih. Ker pri scenarijih od A-1 do A-18 nismo izmerili zakasnitev paketov v tem intervalu, smo histograme za vrednosti T_{max} = 1 s ter T_{max} = 2 s iz slike 49 izločili. Trend padanja deleža simulacijskega časa z večanjem parametra α in trend naraščanja deleža simulacijskega časa z večanjem T_{max} ostaja. Iz tabele 12 je razvidno, da se večji deleži simulacijskega časa, ko je bila izmerjena zakasnitev paketov med 300 in 350 ms, pojavijo pri scenarijih A-28, A-29, A-30, kjer je T_{max} = 8 s, ter pri scenarijih od A-37 do A-45, kjer je bila vrednost T_{max} nastavljena na 16 s. Pri vseh ostalih so vrednosti nizke (pod 10 s).

Na sliki 50 in tabeli 13 je prikazana razporeditev izmerjenih zakasnitev paketov med 350 ms in 400 ms za različne vrednosti spremenljivk α in $T_{max.}$



Slika 50: Delež simulacijskega časa z zakasnitvami paketov med 350 in 400 ms (tretji simulacijski sklop, postopek CAHP-A)

Tabela 13: Simulacijski čas z zakasnitvami paketov med 350 in 400 ms (tretji simulacijski sklop, postopek CAHP-A)

T_{max} \ α	1/16	1/8	1/4	1/2	1	2	4	8	16
1 s	0,0 s	0,0 s	0,0 s	0,0 s	0,0 s	0,0 s	0,0 s	0,0 s	0,0 s
2 s	0,0 s	0,0 s	0,0 s	0,0 s	0,0 s	0,0 s	0,0 s	0,0 s	0,0 s
4 s	0,0 s	0,0 s	0,0 s	0,0 s	0,0 s	0,0 s	0,0 s	0,0 s	0,0 s
8 s	4,7 s	0,8 s	0,0 s	0,0 s	0,0 s	0,0 s	0,0 s	0,0 s	0,0 s
16 s	248,2 s	154,9 s	79,7 s	37,9 s	7,1 s	4,7 s	6,0 s	5,5 s	2,9 s

Iz tabele 13 je razvidno, da se izmerjene zakasnitve paketov v intervalu med 350 in 400 ms pojavljajo samo pri scenarijih A-28, A-29 ter pri scenarijih od A-37 do A-45. Ostale smo iz slike 50 izločili. Trend padanja deleža simulacijskega časa z večanjem parametra α in trend naraščanja deleža simulacijskega časa z večanjem T_{max} ostaja. Iz tabele 13 je razvidno, da se večji deleži simulacijskega časa, ko je bila izmerjena zakasnitev paketov med 350 in 400 ms, pojavijo zgolj pri scenarijih od A-37 do A-40, kjer je bila vrednost T_{max} nastavljena na 16 s. Pri vseh ostalih simulacijski čas z zakasnitvami paketov med 350 in 400 ms majhen (pod 10 s).

Zakasnitve paketov iz naslednjega intervala (med 400 in 450 ms) smo izmerili zgolj pri scenarijih od scenarija A-37 do scenarija A-40 ter pri A-43, vendar pa delež simulacijskega časa z zakasnitvami v tem intervalu majhen, kot je razvidno iz tabele 14. Zakasnitve paketov med 450 in 500 ms pa smo izmerili zgolj pri 14 paketih scenarija A-37.

Tabela 14: Delež simulacijskega časa z zakasnitvami paketov med 400 in 450 ms (tretji simulacijski sklop, postopek CAHP-A)

T_{max} \ α	1/16	1/8	1/4	1/2	1	2	4	8	16
1 s	0,0 s	0,0 s	0,0 s	0,0 s	0,0 s	0,0 s	0,0 s	0,0 s	0,0 s
2 s	0,0 s	0,0 s	0,0 s	0,0 s	0,0 s	0,0 s	0,0 s	0,0 s	0,0 s
4 s	0,0 s	0,0 s	0,0 s	0,0 s	0,0 s	0,0 s	0,0 s	0,0 s	0,0 s
8 s	0,0 s	0,0 s	0,0 s	0,0 s	0,0 s	0,0 s	0,0 s	0,0 s	0,0 s
16 s	41,5 s	12,1 s	3,6 s	3,2 s	0,0 s	0,0 s	0,3 s	0,0 s	0,0 s

Za uporabnika je najbolj pomemben podatek, kako velike so zakasnitve paketov in koliko je bil skupen čas komunikacije, ko je bila izmerjena zakasnitev paketov nad 200 ms. Ta podatek prikazujemo v tabeli 15, kjer podajamo deleže časa, ko je bila zakasnitev paketov nad 200 ms.

Tabela 15: Skupen simulacijski čas nad 200 ms za različne vrednosti parametrov T_{max} in α (tretji simulacijski sklop, postopek CAHP-A)

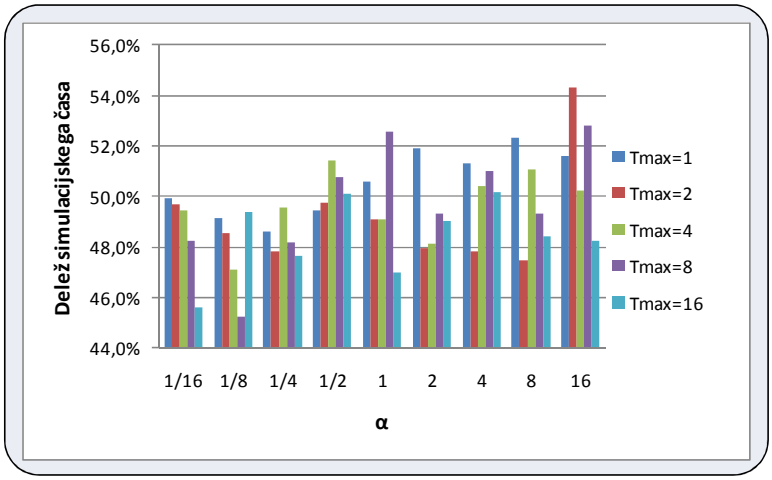
T_{max} \ α	1/16	1/8	1/4	1/2	1	2	4	8	16
1 s	8,4%	7,5%	7,9%	7,1%	6,8%	6,7%	***6,8%***	6,6%	6,9%
2 s	8,4%	8,4%	8,1%	7,7%	7,1%	7,0%	6,6%	6,9%	6,9%
4 s	10,1%	9,6%	9,2%	7,6%	7,6%	7,0%	7,0%	6,7%	6,6%
8 s	12,9%	12,1%	11,4%	9,9%	8,1%	7,2%	6,9%	**6,5%**	6,8%
16 s	16,7%	15,9%	15,4%	13,9%	11,7%	10,0%	8,9%	8,9%	9,3%

Iz predstavljenih rezultatov lahko ugotovimo, da lahko z določanjem različnih vrednosti za α ter T_{max} občutno vplivamo na zakasnitve paketov v komunikaciji. S stališča velikosti zakasnitev paketov je najbolj primeren scenarij A-7 (označen odebeljeno in napisano poševno v tabeli 15), kjer smo izmerili najnižji delež (0,02%) skupnega simulacijskega časa, ko je bila zakasnitev paketov med 250 in 300 ms; zakasnitev paketov nad 300 ms v tem scenariju nismo izmerili. Scenarij z najmanjšim skupnim časom simulacije, ko je bila zakasnitev paketov nad 200 ms, pa je A-35 (označen odebeljeno in podčrtano v tabeli 15). V tem scenariju je bil čas komunikacije nad 200 ms 1877,5 s, kar znaša 6,52% celotnega simulacijskega časa.

7.3.2 Čas uporabe HSPA vmesnika

V tem poglavju bomo prikazali rezultate uporabe HSPA vmesnika. Na sliki 51 prikazujemo delež

simulacijskega časa, ko je bil uporabljen HSPA vmesnik za različne vrednosti parametra α ter T_{max}.



Slika 51: Delež simulacijskega časa na HSPA (tretji simulacijski sklop, postopek CAHP-A)

Pri različnih vrednostih T_{max} delež uporabe s povečanjem T_{max} niha. Maksimumi in minimumi časa uporabe vmesnika HSPA so prikazani v tabeli 16. Za uporabnika je najcenejša komunikacija pri scenariju A-29.

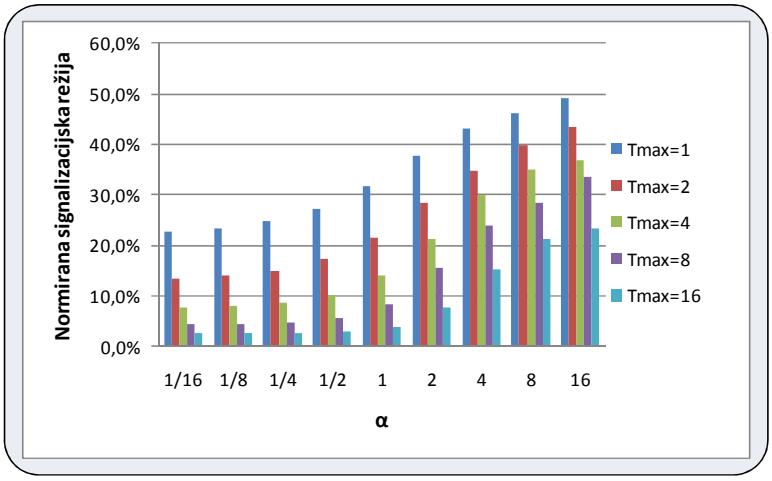
Tabela 16: Minimumi in maksimumi uporabe HSPA vmesnika za različne vrednosti T_{max} (tretji simulacijski sklop, postopek CAHP-A)

Vrednost T_{max}	**Minimum**	**Maksimum**
1 s	48,6%, scenarij A-3	52,3%, scenarij A-8
2 s	47,8%, scenarij A-12	54,3%, scenarij A-18
4 s	47,1%, scenarij A-20	51,4%, scenarij A-22
8 s	45,3%, scenarij A-29	52,8%, scenarij A-36
16 s	45,6%, scenarij A-37	50,2%, scenarij A-43

Vidimo lahko, da se majhen trend povečevanja deleža simulacijskega časa, ko je bil uporabljen HSPA vmesnik, kaže s povečevanjem parametra α. Vendar je dinamika majhna. Najnižjo vrednost dosegamo v scenariju A-29, najvišjo pa v scenariju A-18. Razlika med njima je zgolj 9 odstotnih točk. Iz rezultatov lahko sklenemo, da z uporabo CAHP-A postopka ne vplivamo občutno na povečevanje uporabe HSPA vmesnika in s tem na ceno komunikacije.

7.3.3 Signalizacijska režija

V tem poglavju bomo predstavili rezultate meritev signalizacijske režije, ki jo povzročajo na novo definirana SIP sporočila za preverjanje obremenjenosti WLAN omrežja. Največjo signalizacijsko režijo dosegamo v scenariju C-1 v drugem simulacijskem sklopu. Število signalizacijskih sporočil v tem scenariju smo vzeli za referenco in s to vrednostjo normirali izmerjene vrednosti scenarijev tretjega simulacijskega sklopa, kot je prikazano v enačbi (18). Na sliki 52 je tako prikazan odstotek števila na novo definiranih signalizacijskih sporočil `SIP pre-PROBE` in `SIP mid-PROBE`, ki smo jih uporabili za preizkušanje obremenjenosti dostopovne povezave WLAN omrežja v odvisnosti od števila signalizacijskih sporočil scenarija C-1.



Slika 52: Signalizacijska režija (tretji simulacijski sklop, postopek CAHP-A)

Iz slike 52 je pri vseh scenarijih tretjega simulacijskega sklopa viden trend naraščanja signalizacijske režije z naraščanje vrednosti α, ter padanja števila dodatnih signalizacijskih sporočil z naraščanjem vrednosti T_{max}. Tabela 17 prikazuje minimalne in maksimalne deleže števila dodatnih signalizacijskih sporočil za različne vrednosti T_{max} v odvisnosti od izmerjenih vrednosti v scenariju C-1.

Tabela 17: Minimalni in maksimalni delež števila dodatnih signalizacijskih sporočil za različne vrednosti T_{max} (tretji simulacijski sklop, postopek CAHP-A)

Vrednost T_{max}	**Minimum**	**Maksimum**
1 s	22,7%, scenarij A-1	49,2%, scenarij A-9
2 s	13,4%, scenarij A-10	43,3%, scenarij A-18
4 s	7,7%, scenarij A-19	36,7%, scenarij A-27
8 s	4,4%, scenarij A-28	33,6%, scenarij A-36
16 s	2,5%, scenarij A-37	23,3%, scenarij A-45

Opazimo lahko veliko dinamiko, saj je razlika med najmanjšim deležem signalizacijskih sporočil v odvisnosti od izmerjenih vrednosti v scenariju C-1, ki ga dosegamo v scenariju A-37, in največjim deležem, ki ga dosegamo v scenariju A-9, 46,7 odstotnih točk. S stališča signalizacijske režije je najbolj primeren scenarij A-37, kjer pošljemo zgolj 7590 signalizacijskih sporočil, kar pomeni 1 dodatno sporočilo na vsakih 3,8 s simulacijskega časa.

7.4 Analiza in ovrednotenje rezultatov

Rezultate drugega in tretjega simulacijskega sklopa bomo uporabili za iskanje scenarija z optimalnimi parametri. Predstavljene rezultate lahko obravnavamo iz uporabniškega ali operaterskega vidika. Iz nadaljnje obravnave bomo izločili rezultate, ki kažejo delež uporabe HSPA omrežja, saj je dinamika spreminjanja deleža med različnimi scenariji drugega in tretjega simulacijskega sklopa majhna (med 44,8% in 55,6%). V praksi takšna dinamika pomeni, da bi cena komunikacije nihala za 10,6 odstotnih točk. Večji vpliv spreminjanja vhodnih podatkov na rezultate opazimo pri meritvah nivoja QoE, ki smo ga merili z zakasnitvami paketov nad 200 ms, ter pri signalizacijski režiji, ki nam jo določa število na novo definiranih SIP sporočil, s katerimi preverjamo obremenjenost dostopovne povezave WLAN omrežja.

Uporabniki želijo uporabljati omrežje z dobro kakovostjo. Kakovost storitve IP telefonije smo merili z zakasnitvami paketov nad 200 milisekund – slike 44, 47, 48, 49 ter slika 50. S stališča operaterja je zelo pomembno povečanje signalizacijske režije (sliki 46 ter 52). Na podlagi rezultatov lahko sklenemo, da bo potreben določen kompromis med zagotavljanjem ustreznega nivoja QoE in signalizacijsko režijo, saj se medsebojno izključujeta.

Če bi se operater osredotočil zgolj na čim nižjo signalizacijsko režijo, bi bil izmed vseh scenarijev drugega in tretjega simulacijskega sklopa najbolj primeren scenarij C-6, kjer smo T_{pre} in T_{mid} nastavili na 16 s po načinu CAHP-C. V tem scenariju predstavlja delež dodatnih na novo definiranih SIP sporočil zgolj 2,1% števila dodatnih sporočil, ki smo jih izmerili v scenariju C-1.

Če bi se operater osredotočil zgolj na zagotavljanje čim boljšega nivoja QoE (čim nižji skupen simulacijski čas nad 200 ms), bi bil optimalen scenarij A-35, kjer smo T_{pre} in T_{mid} nastavljali po načinu

CAHP-A s T_{max} = 8 s ter parametrom α = 8. V tem primeru zmanjšamo čas nad 200 ms na 6,5%.

Scenarij z optimalnimi parametri bomo poiskali med scenariji drugega in tretjega simulacijskega sklopa. Pred tem bomo določili še maksimalne vrednosti, ki jih bomo uporabili za referenco. Največjo signalizacijsko režijo smo dosegli pri scenariju C-1, kjer smo vrednosti parametrov T_{pre} in T_{mid} nastavili na fiksno vrednost 0 s.

S stališča uporabnika želimo, da je pri uporabi storitve IP telefonije čas, ko je zakasnitev paketov nad 200 ms, čim krajši. Najvišji delež simulacijskega časa, ko je zakasnitev paketov nad 200 ms, dosežemo pri scenariju C-6, kjer sta bila T_{pre} in T_{mid} nastavljena po CAHP-C na 16 s. V tem primeru je kar 17,1% skupnega simulacijskega časa zakasnitev paketov nad sprejemljivo mejo.

Scenarija C-1 in C-6 bomo zato vzeli za referenco in ugotavljali relativno razliko rezultatov drugih scenarijev. Normirane vrednosti za signalizacijsko režijo smo izračunali po enačbi (18), normirane vrednoti simulacijskega časa, ko je bila zakasnitev paketov nad 200 ms, pa po enačbi (19):

$$NSTa\mathrm{T}_i = \frac{STa\mathrm{T}_i}{STa\mathrm{T}_{C6}} \cdot 100\% \tag{19}$$

kjer je $NSTa\mathrm{T}_i$ normiran simulacijski čas, ko je bila zakasnitev paketov nad 200 ms (*ang. normalized simulation time above threshold*) za scenarij *i*, $STa\mathrm{T}_i$ simulacijski čas, ko je bila zakasnitev paketov nad 200 ms (*ang. simulation time above threshold*) za scenarij *i*, $STa\mathrm{T}_{C6}$ simulacijski čas, ko je bila zakasnitev paketov nad 200 ms za scenarij C-6.

Da bi lahko poiskali scenarij z optimalnimi parametri, smo definirali pogoje, ki jim mora takšen scenarij ustrezati:

- Pogoj POG-Z: Pri vseh scenarijih se pojavljajo paketi, ki so zakasnjeni med 250 in 300 ms. V nekaterih se pojavljajo tudi paketi z višjimi zakasnitvami. V scenariju z optimalnimi parametri se ne smejo pojaviti paketi z zakasnitvijo večjo od 300 ms.
- Pogoj POG-S1: Signalizacijska režija mora biti zmanjšana vsaj za 70% glede na scenarij C-1.
- Pogoj POG-S2: Signalizacijska režija mora biti zmanjšana vsaj za 80% glede na scenarij C-1.
- Pogoj POG-S3: Signalizacijska režija mora biti zmanjšana vsaj za 90% glede na scenarij C-1.

Scenarij z optimalnimi parametri bomo poiskali na več načinov:

- Optimum OPT-A: Naredili bomo ožji izbor scenarijev, ki ustrezajo pogoju POG-Z. Med izbranimi bomo izbrali tistega z najnižjo signalizacijsko režijo.
- Optimum OPT-B1: Naredili bomo ožji izbor scenarijev, ki ustrezajo pogoju POG-S1. Med izbranimi bomo izbrali tistega z najnižjim deležem simulacijskega časa, ko je bila izmerjena zakasnitev paketov nad 200 ms.
- Optimum OPT-B2: Naredili bomo ožji izbor scenarijev, ki ustrezajo pogoju POG-S2. Med izbranimi bomo izbrali tistega z najnižjim deležem simulacijskega časa, ko je bila izmerjena zakasnitev paketov nad 200 ms.
- Optimum OPT-B3: Naredili bomo ožji izbor scenarijev, ki ustrezajo pogoju POG-S3. Med izbranimi bomo izbrali tistega z najnižjim deležem simulacijskega časa, ko je bila izmerjena zakasnitev paketov nad 200 ms.

7.4.1 Iskanje scenarijev z optimalnimi parametri po optimumu OPT-A

Najprej poiščemo optimum med scenariji drugega simulacijskega sklopa. Med temi scenariji pogoj POG-Z izpolnjujeta scenarija C-1 in C-2, vendar pa ima drugi precej nižjo signalizacijsko režijo, zato smo v drugem simulacijskem sklopu za scenarij z optimalnimi parametri izbrali scenarij C-2 s T_{pre} in T_{mid}, nastavljenima na 1 s po načinu CAHP-C. V tem primeru je signalizacija zmanjšana na 21,5% glede na scenarij C-1, čas nad 200 ms pa na 48,7% glede na scenarij C-6.

V tretjem simulacijskem sklopu smo vrednosti parametrov T_{pre} in T_{mid} nastavljali po načinu CAHP-A v odvisnosti od trenutne obremenitve dostopovne povezave WLAN omrežja. V nadaljevanju bomo za bomo za vsako od vrednosti T_{max} poiskali optimum.

Za T_{max} = 1 s pri nobenem od scenarijev nismo izmerili zakasnitev paketov nad 300 ms, zato vse uvrstimo v ožji izbor. Scenarij z najnižjo signalizacijsko režijo je scenarij A-1, kjer je vrednost α=1/16. V tem scenariju je signalizacijska režija zmanjšana na 22,7% glede na scenarij C-1, čas z zakasnitvami nad

200 ms pa na 48,9% glede na scenarij C-6.

Tudi pri T_{max} = 2 s opazimo, da so vse izmerjene vrednosti zakasnitev paketov pod 300 ms, zato vse uvrstimo v ožji izbor. Med izbranimi ima najnižjo signalizacijsko režijo scenarij A-10 z vrednostjo α=1/16. V tem scenariju je signalizacijska režija zmanjšana na 13,4% glede na scenarij C-1, čas z zakasnitvami nad 200 ms pa na 49,1% glede na scenarij C-6.

Pri T_{max} = 4 s vsi scenariji ustrezajo pogoju POG-Z, razen scenarijev A-19 (α=1/16) ter A-20 (α=1/8). Ostale uvrstimo v ožji izbor. Med izbranimi ima najnižjo signalizacijsko režijo scenarij A-21 z vrednostjo α=1/4. V tem scenariju je signalizacijska režija zmanjšana na 8,6% glede na scenarij C-1, čas z zakasnitvami nad 200 ms pa na 53,7% glede na scenarij C-6.

Pri scenarijih s T_{max} = 8 s zakasnitve paketov ustrezajo pogoju POG-Z zgolj pri scenarijih od A-32 do A-36, kjer je vrednost α med 1 in 16, zato te scenarije tretjega simulacijskega sklopa uvrstimo v ožji izbor. Med izbranimi ima najnižjo signalizacijsko režijo scenarij A-32 z vrednostjo α=1. V tem scenariju je signalizacijska režija zmanjšana na 8,4% glede na scenarij C-1, čas z zakasnitvami paketov nad 200 ms pa na 47,4% glede na scenarij C-6.

Pri T_{max} = 16 s nobeden od scenarijev ne ustreza pogoju POG-Z, zato za T_{max}=16 s ne moremo določiti scenarija z optimalnimi parametri.

V tabeli 18 je prikazan povzetek scenarijev z optimalnimi parametri po optimumu OPT-A.

Tabela 18: Povzetek scenarijev z optimalnimi parametri po optimumu OPT-A

Način določanja T_{pre} in T_{mid}	T_{max}	T_{pre}	T_{mid}	α	Delež signalizacijske režije glede na scenarij C-1	Delež časa nad 200 ms glede na scenarij C-6	Ime scenarija
CAHP-C		1 s	1 s		21,5%	48,7%	C-2
CAHP-A	1 s			1/16	22,7%	48,9%	A-1
CAHP-A	2 s			1/16	13,4%	49,1%	A-10
CAHP-A	4 s			1/8	8,6%	53,7%	A-21
CAHP-A	**8 s**			**1**	**8,4%**	**47,4%**	**A-32**
CAHP-A	16 s			N/A	N/A	N/A	N/A

Med posameznimi scenariji z optimalnimi parametri po OPT-A kot najbolj primernega izberemo tistega z najmanjšim deležem signalizacijske režije. Iz predstavljenih rezultatov lahko sklenemo, da je po optimumu OPT-A scenarij z najbolj primernimi parametri scenarij A-32, kjer smo parametra T_{pre} in T_{mid} nastavljali po načinu CAHP-A z vrednostmi α=1 in T_{max}=8 s (označen odebeljeno v tabeli 18).

7.4.2 Iskanje scenarijev z optimalnimi parametri po optimumu OPT-B1

Najprej poiščemo optimum med scenariji drugega simulacijskega sklopa. Pri vrednostih parametrov T_{pre} in T_{mid}, določenih po načinu CAHP-C, pogoj POG-S1 izpolnjujejo scenariji od C-2 do C-6. Izmed teh ima najnižjo vrednost časa nad 200 ms C-2, ki predstavlja scenarij z optimalnimi parametri po OPT-B1 in načinu CAHP-C določanja vrednosti parametrov T_{pre} in T_{mid}. V scenariju C-2 je čas nad 200 ms glede na scenarij C-6 zmanjšan na 48,7%, signalizacijska režija pa na 21,5 %.

V tretjem simulacijskem sklopu smo vrednosti parametrov T_{pre} in T_{mid} nastavljali po načinu CAHP-A v odvisnosti od trenutne obremenitve dostopovne povezave WLAN omrežja. V nadaljevanju bomo za vsako od vrednosti T_{max} poiskali optimum.

Za T_{max} = 1 s pogoju POG-S1 ustrezajo scenariji od A-1 do A-4 z vrednostmi parametra α 1/16, 1/8, 1/4 in 1/2. Med izbranimi ima najnižji delež časa z zakasnitvami paketov nad 200 ms scenarij A-4 z vrednostjo α=1/2. V tem scenariju je čas nad 200 ms glede na scenarij C-6 zmanjšan na 41,3%, signalizacijska režija pa je glede na scenarij C-1 zmanjšana na 27,2 %.

Pri T_{max} = 2 s pogoju POG-S1 ustrezajo vsi scenariji, razen scenarijev A-16 (α = 4), A-17 (α = 8) ter A-18 (α = 16). Preostale uvrstimo v ožji izbor. Med izbranimi ima najnižji delež časa z zakasnitvami paketov nad 200 ms scenarij A-15 z vrednostjo α=2. V tem scenariju je čas z zakasnitvami paketov nad 200 ms glede na scenarij C-6 zmanjšan na 41,0%, signalizacijska režija pa je glede na scenarij C-1 zmanjšana na 28,4%.

Za T_{max} = 4 s pogoju POG-S1 ustrezajo vsi scenariji, razen scenarijev A-26 (α=8) ter A-27 (α=8). Ustrezne uvrstimo v ožji izbor. Med izbranimi ima najnižji delež časa z zakasnitvami paketov nad 200 ms scenarij A-25 z vrednostjo α=4. V tem scenariju je čas z zakasnitvami paketov nad 200 ms glede na

scenarij C-6 zmanjšan na 40,4%, signalizacijska režija pa je glede na scenarij C-1 zmanjšana na 29,4%.

Pri T_{max} = 8 s pogoju POG-S1 ustrezajo vsi scenariji, razen scenarija A-36 (α=16). Preostale uvrstimo v ožji izbor. Med izbranimi ima najnižji delež časa z zakasnitvami paketov nad 200 ms scenarij A-34 z vrednostjo parametra α=4. V tem scenariju je čas z zakasnitvami paketov nad 200 ms glede na scenarij C-6 zmanjšan na 40,7%, signalizacijska režija pa je glede na scenarij C-1 zmanjšana na 29,9%.

Ko je T_{max} = 16 s pogoju POG-S1 ustrezajo vsi scenariji, ki jih tako uvrstimo v ožji izbor. Med izbranimi ima najnižji delež časa z zakasnitvami paketov nad 200 ms scenarij A-44 z vrednostjo parametra α=8. V tem scenariju je čas z zakasnitvami paketov nad 200 ms glede na scenarij C-6 zmanjšan na 52,1%, signalizacijska režija pa je glede na scenarij C-1 zmanjšana na 21,3%.

V tabeli 19 je prikazan povzetek scenarijev z optimalnimi parametri po OPT-B1.

Tabela 19: Povzetek scenarijev z optimalnimi parametri po optimumu OPT-B1

Način določanja T_{pre} in T_{mid}	T_{max}	T_{pre}	T_{mid}	α	Delež signalizacijske režije glede na scenarij C-1	Delež časa nad 200 ms glede na scenarij C-6	Ime scenarija
CAHP-C		1 s	1 s		21,5%	48,7%	C-2
CAHP-A	1 s			1/2	27,2%	41,3%	A-4
CAHP-A	2 s			2	28,4%	41,0%	A-15
CAHP-A	**4 s**			**4**	**29,4%**	**40,4%**	**A-25**
CAHP-A	8 s			4	29,9%	40,7%	A-34
CAHP-A	16 s			8	21,3%	52,1%	A-44

Med posameznimi scenariji z optimalnimi parametri po OPT-B1 kot najbolj primernega izberemo tistega z najnižjim deležem simulacijskega časa nad 200 ms. Iz predstavljenih rezultatov lahko sklenemo, da je po optimumu OPT-B1 scenarij z najbolj primernimi parametri scenarij A-25, kjer smo parametra T_{pre} in T_{mid} nastavljali po načinu CAHP-A z vrednostmi α=4 in T_{max}=4 s (označen odebeljeno v tabeli 19).

7.4.3 Iskanje scenarijev z optimalnimi parametri po optimumu OPT-B2

Najprej poiščemo optimum med scenariji drugega simulacijskega sklopa. Pri vrednostih parametrov T_{pre} in T_{mid}, določenih po načinu CAHP-C, pogoj POG-S2 izpolnjujejo scenariji od C-3 do C-6. Izmed teh ima najnižjo vrednost časa nad 200 ms scenarij C-3, ki predstavlja scenarij z optimalnimi parametri po OPT-B1 in načinu CAHP-C določanja vrednosti parametrov T_{pre} in T_{mid}. V scenariju C-3 je čas nad 200 ms glede na scenarij C-6 zmanjšan na 53,1%, signalizacijska režija pa je glede na scenarij C-1 zmanjšana na 12,4 %.

V tretjem simulacijskem sklopu smo vrednosti parametrov T_{pre} in T_{mid} nastavljali po načinu CAHP-A v odvisnosti od trenutne obremenitve dostopovne povezave WLAN omrežja. V nadaljevanju bomo za bomo za vsako od vrednosti T_{max} poiskali optimum.

Za T_{max} = 1 s nobeden od scenarijev ne ustreza pogoju POG-S2, zato ne moremo določiti optimuma.

Pri T_{max} = 2 s pogoju POG-S2 ustrezajo scenariji od A-10 do A-13 z vrednostmi parametra α med 1/16 in 1/2, ki jih uvrstimo v ožji izbor. Med izbranimi ima najnižji delež časa z zakasnitvami paketov nad 200 ms scenarij A-13 z vrednostjo α=1/2. V tem scenariju je čas z zakasnitvami paketov nad 200 ms glede na scenarij C-6 zmanjšan na 44,8%, signalizacijska režija pa je glede na scenarij C-1 zmanjšana na 11,2%.

Za T_{max} = 4 s pogoju POG-S2 ustrezajo vsi scenariji, razen scenarijev od A-24 do A-27, kjer je vrednost parametra α 2, 4, 8 in 16. Ustrezne uvrstimo v ožji izbor. Med izbranimi ima najnižji delež časa z zakasnitvami paketov nad 200 ms scenarij A-23 z vrednostjo α=1. V tem scenariju je čas z zakasnitvami paketov nad 200 ms glede na scenarij C-6 zmanjšan na 44,4%, signalizacijska režija pa je glede na scenarij C-1 zmanjšana na 14,1%.

Pri T_{max} = 8 s pogoju POG-S2 ustrezajo vsi scenariji, razen scenarijev A-34, A-35 ter A-36 z vrednostmi α 4,8 in 16. Preostale uvrstimo v ožji izbor. Med izbranimi ima najnižji delež časa z zakasnitvami paketov nad 200 ms scenarij A-33 z vrednostjo parametra α=2. V tem scenariju je čas z zakasnitvami paketov nad 200 ms glede na scenarij C-6 zmanjšan na 41,9%, signalizacijska režija pa je glede na scenarij C-1 zmanjšana na 15,5%.

Ko je T_{max} = 16 s pogoju POG-S2 ustrezajo vsi scenariji tretjega simulacijskega sklopa, razen scenarijev A-44 ter A-45 z vrednostmi α 8 in 16. Preostale uvrstimo v ožji izbor. Med izbranimi ima najnižji delež časa z zakasnitvami paketov nad 200 ms scenarij A-43 z vrednostjo parametra α=4. V tem scenariju je čas z zakasnitvami paketov nad 200 ms glede na scenarij C-6 zmanjšan na 52,2%, signalizacijska režija pa je

glede na scenarij C-1 zmanjšana na 15,2%.

V tabeli 20 je prikazan povzetek scenarijev z optimalnimi parametri po optimumu OPT-B2.

Tabela 20: Povzetek scenarijev z optimalnimi parametri po optimumu OPT-B2

Način določanja T_{pre} in T_{mid}	T_{max}	T_{pre}	T_{mid}	α	Delež signalizacijske režije glede na scenarij C-1	Delež časa nad 200 ms glede na scenarij C-6	Ime scenarija
CAHP-C		2 s	2 s		12,4%	53,1%	C-4
CAHP-A	1 s			N/A	N/A	N/A	N/A
CAHP-A	2 s			1/2	11,2%	44,8%	A-13
CAHP-A	4 s			1	14,1%	44,4%	A-23
CAHP-A	**8 s**			**2**	**15,5%**	**41,9%**	**A-33**
CAHP-A	16 s			4	15,2%	52,1%	A-43

Med posameznimi scenariji z optimalnimi parametri po OPT-B2 kot najbolj primernega izberemo tistega z najnižjim deležem simulacijskega časa nad 200 ms. Iz predstavljenih rezultatov lahko sklenemo, da je po optimumu OPT-B2 scenarij z najbolj primernimi parametri scenarij, kjer smo parametra T_{pre} in T_{mid} nastavljali po načinu CAHP-A ter kjer je vrednost α=2 in T_{max}=8 s (označen odebeljeno v tabeli 20).

7.4.4 Iskanje scenarijev z optimalnimi parametri po optimumu OPT-B3

Pri vrednostih parametrov T_{pre} in T_{mid}, določenih po načinu CAHP-C, pogoj POG-S3 izpolnjujejo scenariji od C-4 do C-6. Izmed teh ima najnižjo vrednost časa nad 200 ms C-4, ki predstavlja scenarij z optimalnimi parametri po OPT-B1 in načinu CAHP-C določanja vrednosti parametrov T_{pre} in T_{mid}. V scenariju C-4 je čas nad 200 ms glede na referenco zmanjšan na 61,9%, signalizacijska režija pa na 6,9 %.

V tretjem simulacijskem sklopu smo vrednosti parametrov T_{pre} in T_{mid} nastavljali po načinu CAHP-A v odvisnosti od trenutne obremenitve dostopovne povezave WLAN omrežja. V nadaljevanju bomo za vsako od vrednosti T_{max} poiskali optimum.

Pri T_{max} = 1 s in T_{max} = 2 s nobeden od scenarijev ne ustreza pogoju POG-S3, zato ne moremo določiti optimuma.

Pri T_{max} = 4 s pogoju POG-S3 ustrezajo scenariji A-19 (α=1/16), A-20 (α=1/8) ter A-21 (α=1/4). Med izbranimi ima najnižji delež časa z zakasnitvami paketov nad 200 ms scenarij A-21 z vrednostjo α=1/4. V tem scenariju je čas z zakasnitvami paketov nad 200 ms glede na scenarij C-6 zmanjšan na 53,7%, signalizacijska režija pa je glede na scenarij C-1 zmanjšana na 8,6%.

Pri T_{max} = 8 s pogoju POG-S3 ustrezajo scenariji od A-28 do A-32, z vrednostmi α med 1/16 in 1, ki jih uvrstimo v ožji izbor. Med izbranimi ima najnižji delež časa z zakasnitvami paketov nad 200 ms scenarij A-32 z vrednostjo parametra α=1. V tem scenariju je čas z zakasnitvami paketov nad 200 ms glede na scenarij C-6 zmanjšan na 47,4%, signalizacijska režija pa je glede na scenarij C-1 zmanjšana na 8,4%.

Ko je T_{max} = 16 s pogoju POG-S3 ustrezajo scenariji od A-37 do A-42, z vrednostmi α med 1/16 in 2, ki jih uvrstimo v ožji izbor. Med izbranimi ima najnižji delež časa z zakasnitvami paketov nad 200 ms scenarij A-42 z vrednostjo parametra α=2. V tem scenariju je čas z zakasnitvami paketov nad 200 ms glede na scenarij C-6 zmanjšan na 58,3%, signalizacijska režija pa je glede na scenarij C-1 zmanjšana na 7,8%.

V tabeli 21 je prikazan povzetek scenarijev z optimalnimi parametri po OPT-B3.

Tabela 21: Povzetek scenarijev z optimalnimi parametri po optimumu OPT-B3

Način določanja T_{pre} in T_{mid}	T_{max}	T_{pre}	T_{mid}	α	Delež signalizacijske režije glede na scenarij C-1	Delež časa nad 200 ms glede na scenarij C-6	Ime scenarija
CAHP-C		4 s	4 s		6,9%	61,9%	C-4
CAHP-A	1 s			N/A	N/A	N/A	N/A
CAHP-A	2 s			N/A	N/A	N/A	N/A
CAHP-A	4 s			1/4	8,6%	53,7%	A-21
CAHP-A	**8 s**			**1**	**8,4%**	**47,4%**	**A-32**
CAHP-A	16 s			2	7,8%	58,3%	A-42

Med posameznimi scenariji z optimalnimi parametri po OPT-B3 kot najbolj primernega izberemo tistega z najnižjim deležem simulacijskega časa nad 200 ms. Iz predstavljenih rezultatov lahko sklenemo, da je po optimumu OPT-B3 scenarij z najbolj primernimi parametri scenarij A-32, kjer smo parametra T_{pre} in T_{mid} nastavljali po načinu CAHP-A ter kjer je vrednost α=1 in T_{max}=8 s (označen odebeljeno v tabeli 21).

7.5 Povzetek simulacijskih rezultatov

Za ovrednotenje delovanja postopka CAHP smo definirali več scenarijev, ki smo jih razdelili v tri simulacijske sklope. V prvem simulacijskem sklopu smo izvedli referenčen scenarij R-1 brez uporabe postopka CAHP in pokazali, da lahko pride do velike degradacije kakovosti storitve, če odločitev za predajo temelji zgolj na razmerju SNR. Veliko javnih brezžičnih omrežij, ki so na voljo uporabnikom omogoča priključitev več uporabnikov in običajno ne omogočajo mehanizmov za zagotavljanje kakovosti časovno kritičnim aplikacijam, kar lahko ima za posledico občasne preobremenitve omrežja. Uporaba tovrstnih omrežij je običajno brezplačna in tako zanimiva tudi za uporabo IP telefonije. Iz rezultatov simulacije prvega simulacijskega sklopa je razvidno, da se je kakovost storitve ob preobremenitvah zelo zmanjšala. Zakasnitve so narasle tudi nad 1 s, kar je imelo za posledico, da je bila storitev IP telefonije za uporabnika neuporabna. Zato je v bolj obremenjenih omrežjih nujna uporaba mehanizmov za ugotavljanje obremenjenosti ciljnega omrežja. V drugem simulacijskem sklopu smo izvedli ovrednotenje predlaganega postopka CAHP-C, kjer smo vrednosti parametrov Tpre in Tmid nastavljali na konstantne vrednosti. Ugotovili smo, da lahko s postopkom CAHP-C dosegamo veliko boljše rezultate kot pri referenčnem scenariju R-1. Vendar pa je bilo za doseganje najboljših rezultatov potrebnih zelo veliko dodatnih signalizacijskih sporočil, za preverjanje obremenjenosti, kar bi lahko povzročilo težave v operaterskih okoljih, predvsem na elementu SBC. Zato smo definirali postopek CAHP-A, kjer smo vrednosti parametrov Tpre in Tmid nastavljali v odvisnosti od trenutne obremenjenosti dostopovne povezave WLAN omrežja. Da bi preverili učinkovitost postopka CAHP-A smo definirali več scenarijev, ki jih podajamo v tretjem simulacijskem sklopu. Med scenariji drugega in tretjega simulacijskega sklopa smo poiskali scenarij z optimalnimi parametri na štiri različne načine.

Pri vseh se je kot najbolj primeren pokazal postopek CAHP-A.

8 Zaključki

V doktorski disertaciji obravnavamo problematiko predajanja zvez v heterogenih omrežij s pomočjo SIP protokola. Glavni cilj našega dela je bil razvoj postopkov, ki omogočajo prehajanje med heterogenimi omrežji z minimalnim negativnim vplivom na nivo uporabniške izkušnje in čim manjšim negativnim vplivom na operatersko okolje. Pri analizi meritev poizkusov v operaterskem okolju smo ugotovili, da odločanje o predaji zveze zgolj na podlagi nivoja SNR ni vedno dovolj. To je še posebej pomembno pri predajah med omrežji, ki niso pod nadzorom operaterja in so javno dostopna. V ta namen smo razvili postopek za predajo zvez CAHP, s katerim ob izpolnjenem osnovnem pogoju (zadosten nivo SNR) pred izvedbo predaje preverjamo trenutno obremenjenost ciljnega omrežja.

V nadaljevanju na kratko povzemamo vsebino doktorske disertacije s poudarkom na najpomembnejših ugotovitvah in izvirnih prispevkih. Na koncu podajamo še smernice za nadaljnje delo.

8.1 Pregled vsebine in izvirnih prispevkov

V disertaciji najprej obravnavamo problematiko upravljanja z mobilnostjo pri uporabi različnih protokolov. Na podlagi primerjave smo se odločili za nadaljnje raziskovanje izvajanja predaj zvez s SIP protokolom, ki je še posebej primeren za uporabo v operaterskih okoljih, saj je že vpeljan v večini operaterskih okolij in je bil tudi izbran kot glavni signalizacijski protokol v IMS arhitekturi. Ker uporablja aplikacijski sloj, je SIP protokol neodvisen od dostopovnih tehnologij, kar omogoča uporabo tudi pri gostovanjih v omrežjih operaterja, ki ne ponuja SIP storitev, saj se omrežje, v katerem uporabnik gostuje, uporablja zgolj za dostop do aplikacijskega strežnika v domačem omrežju. Med SIP aplikacijami smo za naše delo izbrali IP telefonijo, ki spada med časovno kritične storitve, saj deluje v realnem času in je še posebej občutljiva na kakovost predaje zveze.

V nadaljevanju smo podali rezultate praktičnih poizkusov, na podlagi katerih smo ugotovili, da lahko kljub zadostnemu nivoju SNR prihaja do poslabšanja kakovosti storitve IP telefonije zaradi prevelike obremenjenosti dostopovne povezave WLAN omrežja. Da bi preprečili uporabo preobremenjenega dostopovna omrežja, smo definirali postopek CAHP (poglavje 5). Postopek je sestavljen iz dveh algoritmov: *Pre-probe* in *Mid-probe*. S prvim, ob izpolnjenem osnovnem pogoju – ustrezen nivo SNR – pred samo izvedbo predaje preverimo trenutno obremenjenost dostopovne povezave ciljnega omrežja z meritvami zakasnitev med terminalom MN in elementom SBC. V kolikor omrežje ni preobremenjeno, izvedemo postopek predaje, sicer pa ne. Ker se lahko razmere v ciljnem omrežju spremenijo tudi med klicem, smo definirali algoritem *Mid-probe*, s katerim preverjamo uporabljeno omrežje po predaji med samo zvezo. V kolikor pride do poslabšanja razmer (omrežje postane preobremenjeno) s postopkom CAHP sprožimo predajo na drugo omrežje.

Obremenitev dostopovne povezave ciljnega omrežja preverjamo z na novo definiranimi SIP sporočili `SIP pre_PROBE` in `SIP mid_PROBE`. Frekvenco preverjanja obremenjenosti dostopovnega omrežja določimo s parametroma T_{pre} in T_{mid}. Vrednost teh dveh parametrov neposredno vpliva na hitrost zaznavanja preobremenitev. Vendar pa višja frekvenca preverjanja povzroča tudi večjo signalizacijsko režijo, ki obremenjuje predvsem element SBC. Definirali smo dva načina določanja časa, s katerim določamo frekvenco pošiljanja na novo definiranih SIP sporočil. V prvem, imenovanem CAHP-C, vrednosti parametrov T_{pre} in T_{mid} nastavljamo na konstantne vrednosti, v drugem, ki smo ga poimenovali CAHP-A, pa se te vrednosti spreminjajo glede na trenutno obremenjenost dostopovne povezave ciljnega omrežja.

Da bi preverili delovanje postopka CAHP, smo definirali simulacijski model (poglavje 6), ki smo ga implementirali v simulacijskem orodju OPNET. Ker orodje OPNET ne podpira upravljanja z mobilnostjo na aplikacijskem sloju, smo te funkcionalnosti dodatno razvili. Na novo je bilo potrebno definirati funkcionalnosti predajanja zveze ter definirati nova SIP sporočila, ki jih uporabljamo za preverjanje obremenjenosti ciljnega dostopovnega omrežja. Simulacijskemu modelu smo dodali tudi možnost uporabe v operaterskem okolju izmerjenih vrednosti razmerja SNR, kar nam je omogočilo simulacije različnih načinov gibanja uporabnika. Model s takšnimi funkcionalnostmi omogoča preverjanje velikega nabora scenarijev, saj lahko obremenitve ciljnega omrežja ter gibanje uporabnika (prek uvažanja izmerjenega

SNR) poljubno nastavljamo. Zato simulacijski model omogoča širšo uporabo in bo lahko uporabljen tudi pri drugih raziskavah s področja upravljanja z mobilnostjo.

Po implementaciji simulacijskega modela v orodju OPNET smo izvedli ovrednotenje delovanja modela in izvedli analizo rezultatov (poglavje 7). Iz rezultatov lahko sklenemo, da lahko s postopkom CAHP ohranimo ustrezen nivo uporabniške izkušnje uporabe SIP aplikacij v realnem času pri prehajanju med nezanesljivimi heterogenimi omrežji. S postopkom CAHP-C smo dosegli veliko boljše rezultate glede na referenčni scenarij (brez uporabe postopka CAHP). Vendar se je močno povečala signalizacijska režija, zato smo definirali drugi način CAHP-A, ki zmanjšuje signalizacijsko režijo. Med izvedenimi scenariji drugega in tretjega simulacijskega sklopa se je za zadržanje nivoja uporabniške izkušnje s čim manjšim vplivom na obremenitve omrežnih elementov operaterskem okolju kot najučinkovitejšo izkazala uporaba postopka CAHP-A.

V postopku CAHP smo uporabili SIP protokol za pošiljanje sporočil, s katerimi smo preverjali obremenjenost omrežja. Zato je takšen pristop popolnoma neodvisen od nižjih slojev (transportnega, omrežnega, povezavnega in fizičnega). Zaradi neodvisnosti od protokolov, uporabljenih na nižjih slojih, je takšno rešitev, v kolikor operater že ponuja storitev SIP IP telefonije, enostavno vpeljati v obstoječe operatersko okolje, saj SBC in terminali že podpirajo SIP protokol in jih zato ni potrebno prilagoditi. Ob uvedbi postopka CAHP v omrežjih operaterja bi bilo potrebno zgolj nadgraditi programsko opremo na uporabniških terminalih ter na elementu SBC pri operaterju. Zaradi uporabe SIP protokola lahko v odločitev vključimo tudi druge podatke, ki jih posreduje SIP strežnik (npr. nastavitve uporabnika). Če bi za preverjanje obremenjenosti omrežja uporabili nižje sloje, bi to pomenilo večji poseg v aplikacijo oz. razvoj ločene povsem nove aplikacije. Izvajanje meritev zakasnitve paketov z drugimi protokoli bi onemogočale tudi varnostne nastavitve na SBC, kjer je običajno dovoljen promet zgolj na vrata, ki jih uporabljata protokola SIP in RTP. Podobne varnostne omejitve veljajo tudi za LAN omrežja pri uporabniku.

Zaključimo lahko, da z upoštevanjem v disertaciji predstavljenih izvirnih prispevkov bistveno izboljšamo nivo QoE med predajami v heterogenih omrežjih in pri tem minimiziramo obremenitev naprav v operaterjevem okolju.

8.2 Smernice za nadaljnje delo

Upravljanje z mobilnostjo postaja vse bolj pomembno tudi v operaterskih okoljih. Raziskave na področju predaje zveze v heterogenih omrežjih, predstavljene v tej disertaciji, nikakor niso izčrpane, ampak predstavljajo temelj za nadaljnje raziskovanje tega področja.

Najbolj kritičen del predaje zveze je odločitev za predajo, ki mora zajemati ustrezne parametre. V nadaljevanju našega dela bi lahko pri odločitvi upoštevali tudi druge parametre, kot so na primer SIP nastavitve uporabnika ali nastavitve operaterja.

Vrednosti parametrov T_{pre} in T_{mid} smo pri postopku CAHP-A, v odvisnosti od obremenjenosti ciljnega omrežja, prilagajali po eksponentni funkciji. Preveriti bi bilo potrebno vpliv uporabe različnih funkcij.

Pri našem delu smo se osredotočili zgolj na prehajanje med dvema dostopovnima omrežjema. Pri nadaljevanju našega dela, bi bilo potrebno preveriti možnost uporabe predlaganega postopka pri izbiri med več ciljnimi omrežji, kjer bi lahko s postopkom CAHP izbrali bolj primerno omrežje. Pri tem bi lahko postopek CAHP nadgradili tudi z inteligentnim sistemom in tako pri prehajanju med omrežji upoštevali predhodne izkušnje z določenim dostopovnim omrežjem.

Nenazadnje bi lahko pri odločitvi za predajo upoštevali tudi smer in hitrost gibanja uporabnika in s sistemom predvidevanja preprečevali predaje, ki bi se zgodile pri zelo hitro premikajočem uporabniku, saj bi uporabnik zaradi velike hitrosti ciljno omrežje uporabljal zelo kratek čas.

9 Zahvale

Pisanje doktorske disertacije je dolga in zavita pot, zato bi se rad zahvalil vsem, ki so mi na tej poti stali ob strani, me spodbujali in mi pomagali k cilju.

Na tej poti sem prečkal mnogo križišč, pred katerimi sem se spraševal kako in kam naprej. Odgovore sem dobival pri mentorju doc. dr. Alešu Šviglju ter somentorju prof. dr. Gorazdu Kandusu, ki se jima zahvaljujem za usmerjanje proti cilju, spodbudo in izčrpne diskusije. Zahvala gre tudi ostalim sodelavcem Odseka za komunikacijske sisteme Instituta "Jožef Stefan" za diskusije o obravnavani problematiki.

Ves čas me je ob poti spremljala in spodbujala tudi Natalija, ki bi se ji rad še posebej zahvalil. Hvala za spodbude in podporo, ki so prišle vedno takrat, ko sem to najbolj potreboval. Hvala tudi za razumevanje ob prikrajšanih vikendih in popoldnevih v preteklih letih, ki jih nisva mogla preživeti skupaj.

Tik pred ciljem je bil čas za pogled na besedilo tudi iz slovnične plati. Tu sta mi s svojimi komentarji in predlogi pomagala Petra Bercko in Vid Libnik, ki se jima zahvaljujem za lektoriranje besedila.

Zahvaljujem se tudi Telekomu Slovenije d.d., v katerem sem zaposlen, za finančno podporo pri študiju. Poleg finančne so mi v podjetju ponudili tudi časovno podporo, brez katere bi se ta pot časovno precej podaljšala.

10 Literatura in viri

Akyildiz, F. I.; Xie, J.; Mohanty S. A survey of mobility management in next-generation all-IP-based wireless systems. *IEEE Wireless Communications* **04**, (2004).

Banerjee, N.; Acharya, A.; Das, S. K. Seamless SIP-Based Mobility for Multimedia Applications. *IEEE Network* **6**, (2006).

Banerjee, N.; Wu, W.; Basu, K.; Das, S. K. Analysis of SIP-based mobility management in 4G wireless networks. *Computer Communications* **27**, (2004).

Budzisz, Ł.; Ferrus, R.; Brunstrom, A.; Grinnemo, K.-J.; Fracchia, R.; Galante, G.; Casadevall, F. Towards transport-layer mobility: Evolution of SCTP multihoming. *Computer Communications* **31**, (2008).

Chan, P.M.L., Wyatt-Millington, R. A., Svigelj, A., Sheriff, R. E., Hu, Y. F., Conforto, P., Tocci, C. Performance analysis of mobility procedures in a hybrid space terrestrial IP environment. *Computer networks* **39**, (2002).

Chang, M.; Lee, H.; Lee, M. A per-application mobility management platform for application-specific handover decision in overlay networks. *Computer Networks* **53**, (2009).

Chen, Y.-S.; Chiu, K.-L.; Hwang, R.-H. SmSCTP: SIP-Based MSCTP Scheme for Session Mobility over WLAN/3G Heterogeneous Networks. *IEEE WCNC*, (2007).

Cisco. Understanding Delay in Packet Voice Networks. http://www.cisco.com/en/US/tech/tk652/tk698/technologies_white_paper09186a00800a8993.shtml (dostop: januar 2010).

Cole, R.G., Rosenbluth, J.H. Voice over IP performance monitoring. *SIGCOMM Comput. Commun.* **2**, (2001).

D-ITG. Distributed Internet Traffic Generator. http://www.grid.unina.it/software/ITG (dostop: februar 2010).

Dorenbosh, J. P.; Bennett, R. L.; Raymer, D. L. Method and apparatus for effecting a seamless handoff between IP connections. *US 6,768,726 B2*, (2004).

Emmelmann, M.; Wiethoelter, S.; Koepsel, A; Kappler, C.; Wolisz, A. Moving toward seamless mobility: state of the art and emerging aspects in standardization bodies. *Wireless Personal Communications* **43**, (2007).

Ezzouhairi, A.; Quintero, A.; Pierre, S. Towards cross layer mobility support in metropolitan networks. *Computer Communications* **33**, (2010).

Fathi, H.; Chakraborty, S.; Prasad, R. Optimization of Mobile IPv6-Based Handovers to Support VoIP Services in Wireless Heterogeneous Networks. *IEEE Transactions On Vehicular Technology* **01**, (2007).

Fathi, H.; Prasad, R.; Chakraborty, S. Mobility management for VoIP in 3G systems: evaluation of Low-latency handoff schemes. *IEEE Wireless Communications* **05**, (2005).

Fitzpatrick, J.; Murphy, S.; Atiquzzaman, M.; Murphy, J. Using cross-layer metrics to improve the performance of end-to-end handover mechanisms. *Computer Communications* **32**, (2009).

Gundavelli S., Leung K., Devarapalli V., Chowdhury K., Patil B. Proxy Mobile IPv6. *IETF RFC 5213*, (2008).

Hasswa, A.; Nasser, N.; Hassanein, H. A seamless context-aware architecture for fourth generation wireless networks. *Wireless Personal Communications* **43**, (2007).

Hautakorpi, J., Camarillo, G., Penfield, R., Hawrylyshen, A., Bhatia, M. Requirements from SIP (Session Initiation Protocol) Session Border Control Deployments. *Internet-Draft*, (2008).

Hsieh, H.-Y.; Li, C.-W.; Liao, S.-W.; Chen, Y.-W.; Tsai, T.-L.; Lin, H.-P. Moving toward end-to-end support for handoffs across heterogeneous telephony systems on dual-mode mobile devices. *Computer Communications* **31**, (2008).

islovar. http://www.islovar.org (dostop: marec 2010).

ITU-D. The Essential Report on IP Telephony. (ITU, 2003).

ITU-T. Recommendation G.107, The E model, A Computational Model for Use in Transmission Planning. (ITU, 2005).

ITU-T. Recommendation G.177. Transmission planning for voiceband services over hybrid Internet/PSTN connections. (ITU, 1999).

Koodli, R. Fast Handovers for Mobile IPv6. *IETF RFC 4068*, (2005).

Kwon, D.-H.; Kim, W.-J.; Suh, Y.-J. An efficient mobile multicast mechanism for fast handovers: A study from design and implementation in experimental networks. *Computer Communications* **31**, (2008).

Kwon, T. T.; Gerla, M.; Das, S.; Das, S. Mobility Management for VoIP Service: Mobile IP vs. SIP. *IEEE Wireless Communications* **02**, (2002).

Launois, D.; Bagnulo, M. The paths toward IPv6 multihoming. *IEEE Communications Surveys & Tutorials* **2**, (2006).

Lee H.; Song, J.-Y.; Lee, S.-H.; Lee, S.; Cho, D.-H. Integrated Mobility Management methods for Mobile IP and SIP in IP based Wireless Data Networks. *Wireless Personal Communications* **35**, (2005).

Leu, F.-L. A novel network mobility handoff scheme using SIP and SCTP for multimedia applications. *Journal of Network and Computer Applications* **32**, (2009).

Libnik, R., Kandus, G., Švigelj, A. Performance evaluation of congestion aware adaptive SIP based handover procedure. *EURASIP Journal on Wireless Communications and Networking*, (2010). V pregledu od avgusta 2010.

Libnik, R., Švigelj, A., Kandus, G. A novel SIP based procedure for congestion aware handover in heterogeneous networks. *Computer Communications*, (2010a). Sprejet v objavo 14.9.2010. DOI: 10.1016/j.comcom.2010.09.007

Libnik, R., Švigelj, A., Kandus, G. Adaptive SIP based procedure for congestion aware handover in heterogeneous networks. IET Communications, (2009). V pregledu od novembra 2009.

Libnik, R., Švigelj, A., Kandus, G. Performance evaluation of SIP based handover in heterogeneous access networks. *WSEAS transactions on communications* **5**, (2008a).

Libnik, R., Švigelj, A., Kandus, G. Simulation environment for performance evaluation of SIP handover. *International Conference on Electronics, Hardware, Wireless and Optical Communications EHAC '08*, (2008).

LTFE IKT slovar. http://slovar.ltfe.org (dostop: marec 2010).

Ma, L.; Yu, F.; Leung, V.C.M.A New method to support UMTS/WLAN vertical handover using SCTP. *IEEE Wireless Communications* **04**, (2004).

Meše, P. *Telekomunikacijske storitve : pojmovnik, angleško-slovenski slovar, slovensko-angleški slovar, kratice*. (Elektrotehniška zveza Slovenije, Ljubljana, 2004).

Mohanty, S.; Akyildiz, I. F. Performance analysis of handoff techniques based on Mobile IP, TCP-Migrate, and SIP. *IEEE transactions on mobile computing* **7**, (2007).

Netstumbler. http://www.netstumbler.com (dostop: februar 2010).

Nguyen-Vuonga, Q.-T. Agoulmine, N., Ghamri-Doudanea, Y. A user-centric and context-aware solution to interface management and access network selection in heterogeneous wireless environments. *Computer Networks* **18**, (2008).

OPNET. http://www.opnet.com (dostop: februar 2010).

Polidoro, A.; Salsano, S.; Niccolini, S. Performance Evaluation of vertical handover mechanisms in IP networks. *IEEE WCNC*, (2008).

Psytechnics. Estimating E Model Id within a VoIP Network. *Technical Report*, (2002).

Rahman, M.; Harmantzis, F. Low-latency handoff inter-WLAN IP mobility with broadband network control. *Computer Communications* **30**, (2007).

Rajavelsamy, R., Anand, S., Song, O., Choi, S. A novel scheme for mobility management in heterogeneous wireless networks. *Wireless Personal Communications* **3**, (2007).

Rosenberg, J., Schulzrinne, H., Camarillo, G., Johnston, A., Peterson, J., Sparks, R., Handley, M., Schooler, E. SIP: Session Initiation Protocol. *IETF RFC 3261*, (2002).

Salsano, S.; Polidoro, A.; Mingardi, C.; Niccolini S.; Veltri, L. SIP-based mobility management in next generation networks. *IEEE Wireless Communications* **08**, (2008).

Salsano, S.; Veltri, L.; Polidoro, A.; Ordine, A. Architecture and testbed implementation of vertical handovers based on SIP session border controllers. *Wireless Personal Communications* **43**, (2007).

Schulzrinne, H., Casner, S., Federick, R., Jacobson, V. RTP: A Transport Protocol for Real-Time Applications. IETF RFC 3550, (2003).

Schulzrinne, H., Wedlund, E. Application-Layer Mobility Using SIP. *ACM SIGMOBILE Mobile Computing and Communications Review* **4**, (2000).

Siddiqui, F.; Zeadally, S. Mobility management across hybrid wireless networks: Trends and challenges. *Computer Communications* **29**, (2006).

Soliman, H., Castelluccia, C., ElMalki, K., Bellier L. Hierarchical Mobile IPv6 (HMIPv6) Mobility Management. *IETF RFC 5380*, (2008).

Stewart, R.; Ramalho, M.; Xie, Q.; Tuexen, M.; Conrad, P. Stream Control Transmission Protocol (SCTP) Partial Reliability Extension. *IETF RFC* **3758**, (2004).

Tantra, J. W.; Son, M. N.; Nguyen, D. D.; Lim, T. M.; Yeo, C. K.; Lee, B.-S. Seamless Mobility Across Heterogeneous Wireless Domains. *IEEE CCNC*, (2008).

Wang Q.; Abu-Rgheff, M. A.; Akram, A. Design and Evaluation of an Integrated Mobile IP and SIP Framework for Advanced Handoff Management. *IEEE Communications Society* **04**, (2004).

Wang, J.; Liao J.; Zhu, X. Latent Handover: A flow-oriented progressive handover mechanism. *Computer Communications* **31**, (2008).

Wang, Q; Atkinson, R; Dunlop, J. Design and evaluation of flow handoff signalling for multihomed mobile nodes in wireless overlay networks. *Computer Networks* **52**, (2008).

Wesley, M. E. At What Layer Does Mobility Belong?. *IEEE Communications Magazine* **04**, (2004).

Wireshark. http://www.wireshark.org (dostop: februar 2010).

Wu, W.; Banerjee, N.; Basu, K.; Das, S. K. SIP-based vertical handoff between WWANs and WLANs. *IEEE Wireless Communications* **5**, (2005).

Yee, Y.C.; Choong, K.N.; Low, A. L. Y.; Tan, S.W. SIP-based proactive and adaptive mobility management framework for heterogeneous networks. *Journal of Network and Computer Applications* **31**, (2008).

Kazalo slik

Kazalo tabel

Priloge

Priloga A: Lastne objave uporabljene v disertaciji

Libnik, R., Kandus, G., Švigelj, A. Performance evaluation of congestion aware adaptive SIP based handover procedure. *EURASIP Journal on Wireless Communications and Networking*, (2010). V pregledu od avgusta 2010.

Libnik, R., Švigelj, A., Kandus, G. A novel SIP based procedure for congestion aware handover in heterogeneous networks. *Computer Communications*, (2010a). Sprejet v objavo 14.9.2010. DOI: 10.1016/j.comcom.2010.09.007

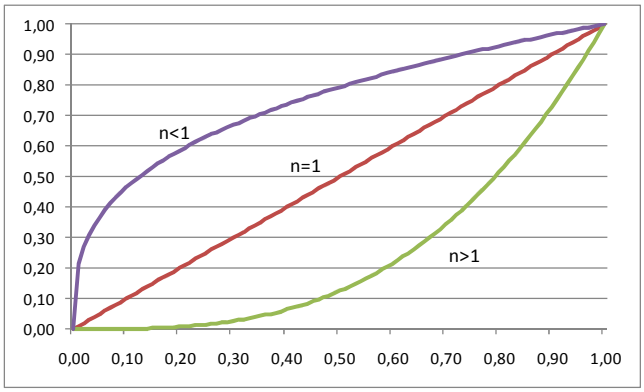
Libnik, R., Švigelj, A., Kandus, G. Adaptive SIP based procedure for congestion aware handover in heterogeneous networks. IET Communications, (2009). V pregledu od novembra 2009.

Libnik, R., Švigelj, A., Kandus, G. Performance evaluation of SIP based handover in heterogeneous access networks. *WSEAS transactions on communications* **5**, (2008a).

Libnik, R., Švigelj, A., Kandus, G. Simulation environment for performance evaluation of SIP handover. *International Conference on Electronics, Hardware, Wireless and Optical Communications EHAC '08*, (2008).

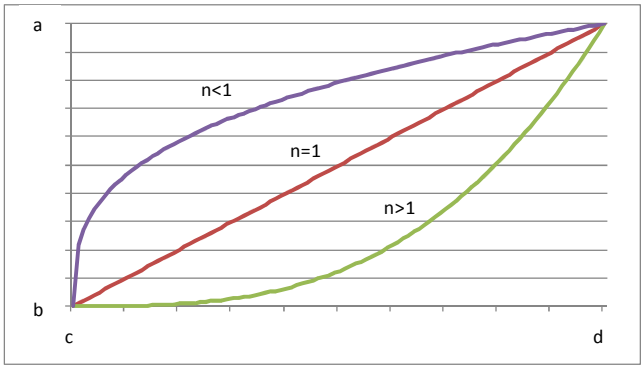
Priloga B: Izpeljava normiranih funkcij

V tej prilogi bomo podali izpeljave normiranih funkcij, ki smo jih uporabili v enačbah (7) in (8) v poglavju 5. Iskali smo univerzalne normirane funkcije, s katerimi bi lahko sestavili kakršno koli obliko želene končne funkcije.



Slika 53: Osnovna normirana funkcija 1

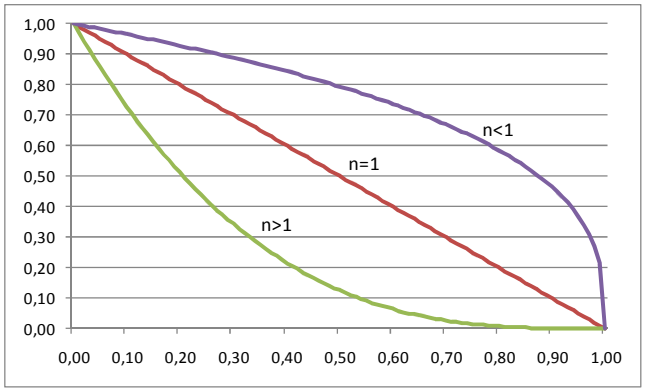
Osnovna funkcija 1 je $y = x^n$. Tako smo dobili normirano funkcijo. Ker pri našem delu uporabljamo različne intervale je potrebno to funkcijo preoblikovati v splošno obliko, ki nam bo omogočala sestavljanje kakršnih koli funkcij. Na sliki 54 je prikazana splošna oblika funkcije 1.



Slika 54: Splošna funkcija 1

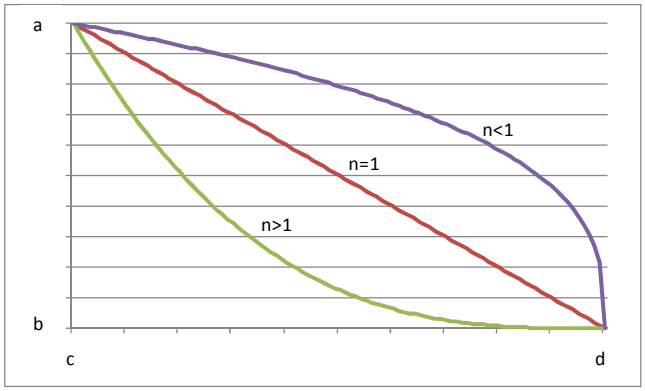
Da bomo še vedno dobili normirano funkcijo je potrebno os y premakniti za a in jo normirati z $a - b$. Os x pa je potrebno premakniti za c in jo normirati z $d - c$.
Izpeljava:

$$\frac{y-b}{a-b} = \left(\frac{x-c}{d-c}\right)^n \rightarrow y = (a-b) \cdot \left(\frac{x-c}{d-c}\right)^n + b \tag{20}$$



Slika 55: Osnovna normirana funkcija 2

Osnovna funkcija 2 je $y = (1 - x)^n$. Tako smo dobili normirano funkcijo. Ker pri našem delu uporabljamo različne intervale je potrebno to funkcijo preoblikovati v splošno obliko, ki nam bo omogočala sestavljanje kakršnih koli funkcij. Na sliki 56 je prikazana splošna oblika funkcije 2.



Slika 56: Splošna funkcija 2

Da bomo še vedno dobili normirano funkcijo je potrebno os y premakniti za a in jo normirati z $a - b$. Os x pa je potrebno premakniti za c in jo normirati z $d - c$.
Izpeljava:

$$\frac{y-b}{a-b} = \left(1 - \frac{x-c}{d-c}\right)^n \rightarrow y = (a-b) \cdot \left(1 - \frac{x-c}{d-c}\right)^n + b \tag{21}$$

Enačbi (20) in (21) omogočata sestavo kakršne koli funkcije.

Priloga C: Rezultati ovrednotenja postopka CAHP

Frekvenca pojavljanja paketov po razredih zakasnitev za prvi in drugi simulacijski tek

Ime scenarija	R-1	C-1	C-2	C-3	C-4	C-5	C-6
Vrednosti za T_{pre} in T_{mid}	brez	0	1	2	4	8	16
0,05-0,1 s	548822	2069704	1963012	1996645	1934873	1872055	1796310
0,1-0,15 s	267244	315858	371854	342771	342119	350119	311030
0,15-0,2 s	229018	294647	304944	278944	298336	284185	280568
0,2-0,25 s	195500	197875	229573	233938	232145	229782	233259
0,25-0,3 s	176599	1026	10048	27252	70138	112061	148661
0,3-0,35 s	150511	0	0	1	2077	29176	73533
0,35-0,4 s	132471	0	0	0	0	2468	29294
0,4-0,45 s	123088	0	0	0	0	44	6869
0,45-0,5 s	107505	0	0	0	0	0	451
0,5-0,55 s	99653	0	0	0	0	0	0
0,55-0,6 s	91483	0	0	0	0	0	0
0,6-0,65 s	82704	0	0	0	0	0	0
0,65-0,7 s	74104	0	0	0	0	0	0
0,7-0,75 s	64683	0	0	0	0	0	0
0,75-0,8 s	59986	0	0	0	0	0	0
0,8-0,85 s	58641	0	0	0	0	0	0
0,85-0,9 s	48903	0	0	0	0	0	0
0,9-0,95 s	46235	0	0	0	0	0	0
0,95-1 s	39062	0	0	0	0	0	0
>1 s	283763	0	0	0	0	0	0
Št. paketov nad 200ms	1834891	198901	239621	261191	304360	373531	492067
Delež št. paketov z zakasnitvami nad 200ms	63,7%	6,9%	8,3%	9,1%	10,6%	13,0%	17,1%

Frekvenca pojavljanja paketov po razredih zakasnitev za tretji simulacijski tek (T_{max}=1 s)

Ime scenarija	A-1	A-2	A-3	A-4	A-5	A-6	A-7	A-8	A-9
Vrednosti parametra α	1/16	1/8	1/4	1/2	1	2	4	8	16
0,05-0,1 s	1944511	1983362	1930571	1986289	2007622	2011210	2003472	2040522	2027130
0,1-0,15 s	378119	380303	386336	375749	366398	364616	371081	352910	359138
0,15-0,2 s	316187	298453	335442	314089	309180	308971	308553	297036	293015
0,2-0,25 s	233091	212072	223301	201021	194951	193521	195294	187831	198762
0,25-0,3 s	7424	5159	3620	2045	1076	836	788	935	1105
0,3-0,35 s	0	0	0	0	0	0	0	0	0
0,35-0,4 s	0	0	0	0	0	0	0	0	0
0,4-0,45 s	0	0	0	0	0	0	0	0	0
0,45-0,5 s	0	0	0	0	0	0	0	0	0
0,5-0,55 s	0	0	0	0	0	0	0	0	0
0,55-0,6 s	0	0	0	0	0	0	0	0	0
0,6-0,65 s	0	0	0	0	0	0	0	0	0
0,65-0,7 s	0	0	0	0	0	0	0	0	0
0,7-0,75 s	0	0	0	0	0	0	0	0	0
0,75-0,8 s	0	0	0	0	0	0	0	0	0
0,8-0,85 s	0	0	0	0	0	0	0	0	0
0,85-0,9 s	0	0	0	0	0	0	0	0	0
0,9-0,95 s	0	0	0	0	0	0	0	0	0
0,95-1 s	0	0	0	0	0	0	0	0	0
>1 s	0	0	0	0	0	0	0	0	0
Št. paketov nad 200 ms	240515	217231	226921	203066	196027	194357	196082	188766	199867
Delež št. paketov z zakasnitvami nad 200 ms	8,4%	7,5%	7,9%	7,1%	6,8%	6,7%	6,8%	6,6%	6,9%

Frekvenca pojavljanja paketov po razredih zakasnitev za tretji simulacijski tek (T_{max}=2 s)

Ime scenarija	A-10	A-11	A-12	A-13	A-14	A-15	A-16	A-17	A-18
Vrednosti parametra α	1/16	1/8	1/4	1/2	1	2	4	8	16
0,05-0,1 s	1997713	1956872	1969518	1967248	1978159	1983319	1994194	1971700	2040367
0,1-0,15 s	354042	375684	377641	379763	382252	382868	381676	398674	347600
0,15-0,2 s	286057	304725	299492	311708	313931	311407	314190	311586	292879
0,2-0,25 s	223250	227966	224516	217305	203669	200642	188106	196289	197438
0,25-0,3 s	18492	14209	8251	3223	1202	950	1141	997	971
0,3-0,35 s	0	0	0	0	0	0	0	0	0
0,35-0,4 s	0	0	0	0	0	0	0	0	0
0,4-0,45 s	0	0	0	0	0	0	0	0	0
0,45-0,5 s	0	0	0	0	0	0	0	0	0
0,5-0,55 s	0	0	0	0	0	0	0	0	0
0,55-0,6 s	0	0	0	0	0	0	0	0	0
0,6-0,65 s	0	0	0	0	0	0	0	0	0
0,65-0,7 s	0	0	0	0	0	0	0	0	0
0,7-0,75 s	0	0	0	0	0	0	0	0	0
0,75-0,8 s	0	0	0	0	0	0	0	0	0
0,8-0,85 s	0	0	0	0	0	0	0	0	0
0,85-0,9 s	0	0	0	0	0	0	0	0	0
0,9-0,95 s	0	0	0	0	0	0	0	0	0
0,95-1 s	0	0	0	0	0	0	0	0	0
>1 s	0	0	0	0	0	0	0	0	0
Št. paketov nad 200 ms	241742	242175	232767	220528	204871	201592	189247	197286	198409
Delež št. paketov z zakasnitvami nad 200 ms	8,4%	8,4%	8,1%	7,7%	7,1%	7,0%	6,6%	6,9%	6,9%

Frekvenca pojavljanja paketov po razredih zakasnitev za tretji simulacijski tek (T_{max}=4 s)

Ime scenarija	A-19	A-20	A-21	A-22	A-23	A-24	A-25	A-26	A-27
Vrednosti parametra α	1/16	1/8	1/4	1/2	1	2	4	8	16
0,05-0,1 s	1950547	1948723	1950802	2033344	1976613	1959735	1976955	2006008	2027173
0,1-0,15 s	340023	356367	370066	345298	381123	396280	375408	378580	374155
0,15-0,2 s	297512	296941	294363	280807	303053	321490	326466	300973	288976
0,2-0,25 s	233541	238016	237970	212586	216280	200692	199380	192628	187843
0,25-0,3 s	57123	39323	26331	7423	2157	960	1034	1078	1096
0,3-0,35 s	912	254	0	0	0	0	0	0	0
0,35-0,4 s	0	0	0	0	0	0	0	0	0
0,4-0,45 s	0	0	0	0	0	0	0	0	0
0,45-0,5 s	0	0	0	0	0	0	0	0	0
0,5-0,55 s	0	0	0	0	0	0	0	0	0
0,55-0,6 s	0	0	0	0	0	0	0	0	0
0,6-0,65 s	0	0	0	0	0	0	0	0	0
0,65-0,7 s	0	0	0	0	0	0	0	0	0
0,7-0,75 s	0	0	0	0	0	0	0	0	0
0,75-0,8 s	0	0	0	0	0	0	0	0	0
0,8-0,85 s	0	0	0	0	0	0	0	0	0
0,85-0,9 s	0	0	0	0	0	0	0	0	0
0,9-0,95 s	0	0	0	0	0	0	0	0	0
0,95-1 s	0	0	0	0	0	0	0	0	0
>1 s	0	0	0	0	0	0	0	0	0
Št. paketov nad 200 ms	291576	277593	264301	220009	218437	201652	200414	193706	188939
Delež št. paketov z zakasnitvami nad 200 ms	10,1%	9,6%	9,2%	7,6%	7,6%	7,0%	7,0%	6,7%	6,6%

Frekvenca pojavljanja paketov po razredih zakasnitev za tretji simulacijski tek (T_{max}=8 s)

Ime scenarija	A-28	A-29	A-30	A-31	A-32	A-33	A-34	A-35	A-36
Vrednosti parametra α	1/16	1/8	1/4	1/2	1	2	4	8	16
0,05-0,1 s	1891593	1851393	1914030	1959725	1992897	1957680	1980234	1990824	2006790
0,1-0,15 s	338551	366061	342064	341095	364503	383368	379537	386712	372310
0,15-0,2 s	277011	313961	295351	293602	288460	332153	320776	314039	303770
0,2-0,25 s	239803	239656	245864	241355	226214	204095	197195	186487	194934
0,25-0,3 s	117692	99283	80474	43648	7233	1931	1424	1263	1461
0,3-0,35 s	14681	9383	1920	139	0	0	0	0	0
0,35-0,4 s	469	75	0	0	0	0	0	0	0
0,4-0,45 s	0	0	0	0	0	0	0	0	0
0,45-0,5 s	0	0	0	0	0	0	0	0	0
0,5-0,55 s	0	0	0	0	0	0	0	0	0
0,55-0,6 s	0	0	0	0	0	0	0	0	0
0,6-0,65 s	0	0	0	0	0	0	0	0	0
0,65-0,7 s	0	0	0	0	0	0	0	0	0
0,7-0,75 s	0	0	0	0	0	0	0	0	0
0,75-0,8 s	0	0	0	0	0	0	0	0	0
0,8-0,85 s	0	0	0	0	0	0	0	0	0
0,85-0,9 s	0	0	0	0	0	0	0	0	0
0,9-0,95 s	0	0	0	0	0	0	0	0	0
0,95-1 s	0	0	0	0	0	0	0	0	0
>1 s	0	0	0	0	0	0	0	0	0
Št. paketov nad 200ms	372645	348397	328258	285142	233447	206026	198619	187750	196395
Delež št. paketov z zakasnitvami nad 200 ms	12,9%	12,1%	11,4%	9,9%	8,1%	7,2%	6,9%	6,5%	6,8%

Frekvenca pojavljanja paketov po razredih zakasnitev za tretji simulacijski tek (T_{max}=16 s)

Ime scenarija	A-37	A-38	A-39	A-40	A-41	A-42	A-43	A-44	A-45
Vrednosti parametra α	1/16	1/8	1/4	1/2	1	2	4	8	16
0,05-0,1 s	1777759	1847408	1845032	1892579	1914150	1941343	1971376	1947166	1939445
0,1-0,15 s	333574	303252	313142	310598	346621	348425	354301	373225	363252
0,15-0,2 s	288648	270457	277762	277464	283119	302776	296822	302795	309018
0,2-0,25 s	235314	226092	231151	230142	229693	225961	207333	205931	214944
0,25-0,3 s	142722	150071	146851	131174	91226	52947	40943	41650	46669
0,3-0,35 s	72971	65985	57696	33816	14240	7621	8055	8150	5904
0,35-0,4 s	24822	15493	7971	3794	708	469	596	550	288
0,4-0,45 s	4146	1205	361	322	0	0	26	0	0
0,45-0,5 s	14	0	0	0	0	0	0	0	0
0,5-0,55 s	0	0	0	0	0	0	0	0	0
0,55-0,6 s	0	0	0	0	0	0	0	0	0
0,6-0,65 s	0	0	0	0	0	0	0	0	0
0,65-0,7 s	0	0	0	0	0	0	0	0	0
0,7-0,75 s	0	0	0	0	0	0	0	0	0
0,75-0,8 s	0	0	0	0	0	0	0	0	0
0,8-0,85 s	0	0	0	0	0	0	0	0	0
0,85-0,9 s	0	0	0	0	0	0	0	0	0
0,9-0,95 s	0	0	0	0	0	0	0	0	0
0,95-1 s	0	0	0	0	0	0	0	0	0
>1 s	0	0	0	0	0	0	0	0	0
Št. paketov nad 200ms	479989	458846	444030	399248	335867	286998	256953	256281	267805
Delež št. paketov z zakasnitvami nad 200 ms	16,7%	15,9%	15,4%	13,9%	11,7%	10,0%	8,9%	8,9%	9,3%

Število sekund na HSPA vmesniku za scenarije prvega in drugega simulacijskega teka

Ime scenarija	Vrednosti za T_{pre} in T_{mid}	Čas na HSPA (s)	Čas na HSPA (%)
R-1	**brez**	0 s	0 %
C-1	**0 s**	16012,8 s	55,6%
C-2	**1 s**	14677,2 s	51,0%
C-3	**2 s**	14835,6 s	51,5%
C-4	**4 s**	14043,6 s	48,8%
C-5	**8 s**	12906 s	44,8%
C-6	**16 s**	13165,2 s	45,7%

Število sekund na HSPA vmesniku za scenarije tretjega simulacijskega teka (T_{max}=1 s)

Ime scenarija	Vrednosti parametra α	Čas na HSPA (s)	Čas na HSPA (%)
A-1	1/16	14378,4 s	49,9%
A-2	1/8	14158,8 s	49,2%
A-3	1/4	14004 s	48,6%
A-4	1/2	14241,6 s	49,5%
A-5	1	14576,4 s	50,6%
A-6	2	14950,8 s	51,9%
A-7	4	14785,2 s	51,3%
A-8	8	15062,4 s	52,3%
A-9	16	14868 s	51,6%

Število sekund na HSPA vmesniku za scenarije tretjega simulacijskega teka (T_{max}=2 s)

Ime scenarija	Vrednosti parametra α	Čas na HSPA (s)	Čas na HSPA (%)
A-10	1/16	14302,8 s	49,7%
A-11	1/8	13975,2 s	48,5%
A-12	1/4	13766,4 s	47,8%
A-13	1/2	14331,6 s	49,8%
A-14	1	14140,8 s	49,1%
A-15	2	13816,8 s	48,0%
A-16	4	13777,2 s	47,8%
A-17	8	13665,6 s	47,5%
A-18	16	15645,6 s	54,3%

Število sekund na HSPA vmesniku za scenarije tretjega simulacijskega teka (T_{max}=4 s)

Ime scenarija	Vrednosti parametra α	Čas na HSPA (s)	Čas na HSPA (%)
A-19	1/16	14238 s	49,4%
A-20	1/8	13561,2 s	47,1%
A-21	1/4	14277,6 s	49,6%
A-22	1/2	14806,8 s	51,4%
A-23	1	14137,2 s	49,1%
A-24	2	13867,2 s	48,1%
A-25	4	14518,8 s	50,4%
A-26	8	14706 s	51,1%
A-27	16	14472 s	50,2%

Število sekund na HSPA vmesniku za scenarije tretjega simulacijskega teka (T_{max}=8 s)

Ime scenarija	Vrednosti parametra α	Čas na HSPA (s)	Čas na HSPA (%)
A-28	1/16	13896 s	48,2%
A-29	1/8	13035,6 s	45,3%
A-30	1/4	13870,8 s	48,2%
A-31	1/2	14623,2 s	50,8%
A-32	1	15141,6 s	52,6%
A-33	2	14198,4 s	49,3%
A-34	4	14688 s	51,0%
A-35	8	14198,4 s	49,3%
A-36	16	15210 s	52,8%

Število sekund na HSPA vmesniku za scenarije tretjega simulacijskega teka (T_{max}=16 s)

Ime scenarija	Vrednosti parametra α	Čas na HSPA (s)	Čas na HSPA (%)
A-37	1/16	13136,4 s	45,6%
A-38	1/8	14227,2 s	49,4%
A-39	1/4	13723,2 s	47,7%
A-40	1/2	14425,2 s	50,1%
A-41	1	13528,8 s	47,0%
A-42	2	14122,8 s	49,0%
A-43	4	14443,2 s	50,2%
A-44	8	13953,6 s	48,5%
A-45	16	13892,4 s	48,2%

Število sporočil `SIP pre_PROBE` in `SIP mid_PROBE` za scenarije prvega in drugega simulacijskega teka

Ime scenarija	Vrednosti za T_{pre} in T_{mid}	Število signalizacijskih sporočil
R-1	**brez**	0
C-1	**0 s**	304221
C-2	**1 s**	65355
C-3	**2 s**	37818
C-4	**4 s**	21096
C-5	**8 s**	11469
C-6	**16 s**	6294

Število sporočil `SIP pre_PROBE` in `SIP mid_PROBE` za scenarije tretjega simulacijskega teka (T_{max}=1 s)

Ime scenarija	Vrednosti parametra α	Število signalizacijskih sporočil
A-1	1/16	69075
A-2	1/8	70956
A-3	1/4	75126
A-4	1/2	82890
A-5	1	96240
A-6	2	114474
A-7	4	131511
A-8	8	140490
A-9	16	149592

Število sporočil `SIP pre_PROBE` in `SIP mid_PROBE` za scenarije tretjega simulacijskega teka (T_{max}=2 s)

Ime scenarija	Vrednosti parametra α	Število signalizacijskih sporočil
A-10	1/16	40743
A-11	1/8	42318
A-12	1/4	45237
A-13	1/2	52308
A-14	1	65250
A-15	2	86247
A-16	4	106020
A-17	8	120789
A-18	16	131748

Število sporočil `SIP pre_PROBE` in `SIP mid_PROBE` za scenarije tretjega simulacijskega teka (T_{max}=4 s)

Ime scenarija	Vrednosti parametra α	Število signalizacijskih sporočil
A-19	1/16	23349
A-20	1/8	24246
A-21	1/4	26055
A-22	1/2	30702
A-23	1	42972
A-24	2	64863
A-25	4	90990
A-26	8	106557
A-27	16	111732

Število sporočil `SIP pre_PROBE` in `SIP mid_PROBE` za scenarije tretjega simulacijskega teka (T_{max}=8 s)

Ime scenarija	Vrednosti parametra α	Število signalizacijskih sporočil
A-28	1/16	13296
A-29	1/8	13581
A-30	1/4	14718
A-31	1/2	17241
A-32	1	25509
A-33	2	47043
A-34	4	72903
A-35	8	86178
A-36	16	102165

Število sporočil `SIP pre_PROBE` in `SIP mid_PROBE` za scenarije tretjega simulacijskega teka (T_{max}=16 s)

Ime scenarija	Vrednosti parametra α	Število signalizacijskih sporočil
A-37	1/16	7590
A-38	1/8	7710
A-39	1/4	8001
A-40	1/2	8853
A-41	1	11325
A-42	2	23742
A-43	4	46284
A-44	8	64941
A-45	16	70830

Priloga D: Opis simulacijskega modela

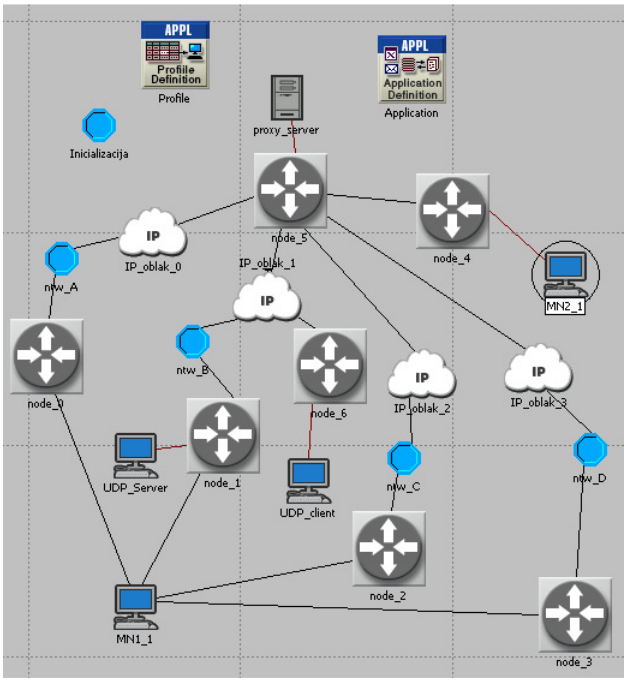
Orodje OPNET v osnovi podpira samo IP telefonijo - torej SIP protokol za signalizacijo in RTP za prenos govornega signala. Za potrebe podpore mobilnosti smo morali prilagoditi in na novo razviti nekatere procese znotraj posameznih elementov. Spremembe lahko razdelimo v šest sklopov:

- prilagoditve za potrebe simulacije
- nove funkcije in parametri;
- prilagoditev in razvoj procesov;
- zamenjava IP naslova;
- vhodni podatki.

Na tem mestu bomo vključevali samo dele spremenjene kode zaradi lažjega razumevanja in boljše preglednosti.

Prilagoditve za potrebe simulacije

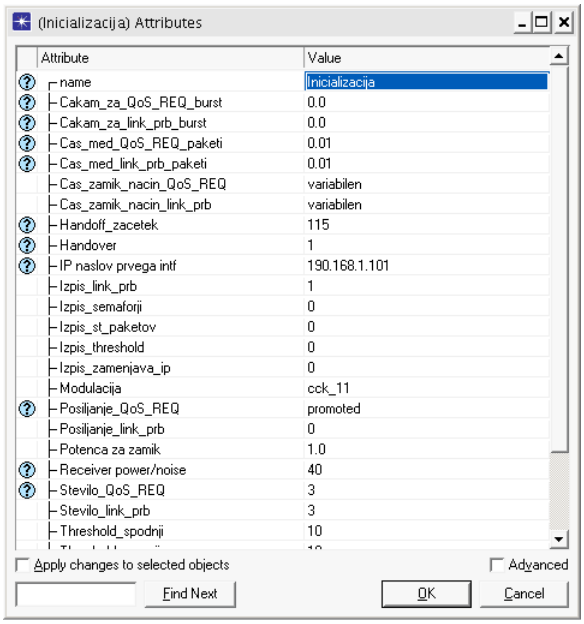
Slika 57 prikazuje shemo omrežja v simulacijskem modelu. Omrežje je sestavljeno iz dveh terminalov MN1_1 in MN2_1. Terminal MN_1 je povezan na štiri usmerjevalnike, ki so povezani na štiri različna IP omrežja. Namen več omrežij je bil, da lahko hkrati simuliramo predaje med štirimi različnimi dostopovnimi tehnologijami.



Slika 57: Shema omrežja v simulacijskem modelu

Za boljšo simulacijsko obdelavo smo v model dodali lasten element, ki smo ga poimenovali Inicializacija. Ta element je inicializacijski element, kjer se določijo začetne vrednosti spremenljivk, ki jih kasneje uporabimo pri simulaciji. Te parametre lahko razdelimo v dve skupini. V prvi skupini so spremenljivke, s katerimi lahko vplivamo na potek simulacije. Te spremenljivke smo definirali kot parametre elementa

Inicializacija in jih lahko enostavno nastavljamo pred zagonom vsake simulacije kot je to prikazano na sliki 58, v tabeli 22 pa so ti parametri opisani.



Slika 58: Parametri elementa Inicializacija

Tabela 22: Opis parametrov z njihovimi funkcionalnostmi

Ime nastavitve	**Parameter**	**Opis funkcionalnosti**
Handover	ex_handover	Ta parameter določa ali se predaja izvede
Zamenjava inet_addr	ex_zamenjava_inet_addr	Ta parameter določa ali se ob predaji na MN2_1 nastavi IP naslov drugega vmesnika MN1_1
Zamenjava routinga	ex_zamenjava_routinga	Ta parameter določa ali se na MN1_1 ob predaji izbere drugi IP naslov
IP naslov prvega intf	ex_MN1_1_intf_naslov1_str	Ta parameter določa naslov prvega vmesnika na MN1_1
Handoff_zacetek	ex_handoff_zacetek	Ta parameter določa simulacijski čas v sekundah, ko se začne predaja, v kolikor je kot prožilo nastavljen čas
Receiver power/noise	ex_rcvd_power_test	Ta parameter določa koliko je razmerje SNR na MN1_1, če te vrednosti niso določene v datoteki
Modulacija	ex_modulacija	Ta parameter določa izbiro modulacije na MN1_1
Trigger	ex_trigger	Ta parameter določa tip prožila ali čas ali pa SNR
Threshold_zgornji	ex_threshold_zgornji	Ta parameter določa prag, kadar je prožilo razmerje SNR in se SNR vrednosti manjšajo
Threshold_spodnji	ex_threshold_spodnji	Ta parameter določa prag, kadar je prožilo razmerje SNR in se SNR vrednosti večajo
Vrsta predaje	ex_predaja_na_intf	Ta parameter določa iz katerega vmesnika na MN1_1 na kateri vmesnik se bo predala zveza ob predaji
Izpis_zamenjava_ip	ex_izpis_zamenjava_ip	Ta parameter določa ali se bo v razhroščevalniku izpisovalo kdaj se je zamenjal IP naslov MN1_1
Izpis_st_paketov	ex_izpis_st_paketov	Ta parameter določa ali se bo v

		razhroščevalniku izpisovalo število paketov
Izpis_semaforji	ex_izpis_semaforji	Ta parameter določa ali se bodo v razhroščevalniku izpisovale vrednosti semaforjev, ki smo jih uporabili
Izpis_threshold	ex_izpis_threshold	Ta parameter določa ali se bo v razhroščevalniku izpisovalo kdaj je bil presežen prag
Izpis_link_prb	ex_izpis_link_prb	Ta parameter določa ali se bo v razhroščevalniku izpisovalo kdaj so bila poslana SIP mid_PROBE sporočila
Posiljanje_QoS_REQ	ex_QoS_REQ	Ta parameter določa ali se pošiljajo SIP pre_PROBE sporočila
Stevilo_QoS_REQ	ex_st_QoS_REQ	Ta parameter določa koliko SIP pre_PROBE sporočil bo poslanih v skupini
Posiljanje_link_prb	ex_link_prb	Ta parameter določa ali se pošiljajo SIP mid_PROBE sporočila
Stevilo_link_prb	ex_st_link_prb	Ta parameter določa koliko SIP mid_PROBE sporočil bo poslanih v skupini
Cakam_za_QoS_REQ_burst	ex_cas_zamik_QoS_REQ	Ta parameter določa koliko časa počakamo preden se ponovno pošlje nova skupina SIP pre_PROBE sporočil, v kolikor je uporabljen CAHP-C postopek
Cakam_za_link_prb_burst	ex_cas_zamik_link_prb	Ta parameter določa koliko časa počakamo preden se ponovno pošlje nova skupina SIP mid_PROBE sporočil, v kolikor je uporabljen CAHP-C postopek
Cas_zamik_nacin_QoS_REQ	ex_cas_zamik_nacin_QoS_REQ	Izbira CAHP-C ali CAHP-A za SIP pre_PROBE sporočila
Cas_zamik_nacin_link_prb	ex_cas_zamik_nacin_link_prb	Izbira CAHP-C ali CAHP-A za SIP pre_PROBE sporočila
Potenca za zamik	ex_exp	Ta parameter določa vrednost parametra α
Cas_med_QoS_REQ_paketi	ex_cas_paketizacije_QoS_REQ	Ta parameter določa čas T_{inter} za sporočila SIP pre_PROBE
Cas_med_link_prb_paketi	ex_cas_paketizacije_link_prb	Ta parameter določa čas T_{inter} za sporočila SIP mid_PROBE

Vse dodatne globalne spremenljivke smo definirali v novi knjižnici *handoff_ext_variables.h*, in sicer na naslednji način:

Definicija:

```
#ifdef  HANDOFF_MAIN_EXTERNAL_VARIABLES
#define GLOBAL
#else
#define GLOBAL extern
#endif
```

in spremenljivke:

```
GLOBAL          double                          ex_cas_1;
```

Definicija *#define HANDOFF_MAIN_EXTERNAL_VARIABLES* se mora pojaviti samo enkrat, zato smo jo dodali le v glavo procesnega modela Inicializacija.

Poleg spremenljivk, ki so uporabljene kot parametri elementa Inicializacija smo definirali tudi spremenljivke, ki jih kasneje uporabljajmo:

- za statistiko;
- za vrednosti, ki morajo biti na voljo več procesom;
- spremenljivke, ki jih uporabimo kot semaforje, s pomočjo katerih kasneje začenjamo oziroma končujemo določene aktivnosti.

Tudi te so definirane v knjižnici *handoff_ext_variables.h*. Glavne spremenljivke te skupine so:

- *ex_rtp_start_MN1_1*: Privzeta vrednost te spremenljivke je 0. Ko začne terminal MN1_1 pošiljati RTP pakete prek drugega vmesnika, jo postavimo na 1.
- *ex_rtp_start_MN2_1*: Privzeta vrednost te spremenljivke je 0. Ko začne terminal MN2_1 pošiljati RTP pakete na drugi vmesnik terminala MN1_1, jo postavimo na 1.
- *ex_rtp_start_MN2_1_nazaj_na_intf0*: Privzeta vrednost te spremenljivke je 0. Ko začne terminal MN2_1 pošiljati RTP pakete nazaj na prvi vmesnik terminala MN1_1, jo postavimo na 1.
- *ex_routing_ok*: Privzeta vrednost te spremenljivke je 0. Ko zamenjamo vmesnik na terminalu MN1_1 jo postavimo na 1.
- *ex_routing_ok_nazaj_na_intf0*: Privzeta vrednost te spremenljivke je 0. Ko zamenjamo vmesnik na terminalu MN1_1 iz drugega nazaj na prvega jo postavimo na 1.
- *ex_handover_traja*: Privzeta vrednost te spremenljivke je 0. Spremenljivka dobi vrednost 1 v času, ko se pošilja signalizacija za predajo zveze iz prvega na drugi vmesnik terminala MN1_1. Ko je zveza vzpostavljena jo nastavimo nazaj na privzeto vrednost.
- *ex_handover_traja_nazaj_na_intf0*: Privzeta vrednost te spremenljivke je 0. Spremenljivka dobi vrednost 1 v času, ko se pošilja signalizacija za predajo zveze iz drugega na prvi vmesnik terminala MN1_1. Ko je zveza vzpostavljena jo nastavimo nazaj na privzeto vrednost.
- *ex_uporabljen_intf*: Spremenljivka določa kateri vmesnik je trenutno uporabljen.
- *ex_cas_QoS_REQ*: V to spremenljivko zapišemo čas, ko je bil poslan SIP pre_PROBE paket
- *ex_st_RTP_sej*: V spremenljivko zapisujemo število vzpostavljenih RTP sej.
- *ex_stevilo_handoverjev*: V spremenljivko zapisujemo, koliko predaj se je zgodilo.

Ostale spremenljivke so razporejene po sklopih, in sicer:

Spremenljivke, ki jih uporabim za izračun krivulje pri CAHP-A:

- *ex_d_min*: Spremenljivka določa D_{min}
- *ex_d_max*: Spremenljivka določa D_{max}
- *ex_zamik_max*: Spremenljivka določa T_{max}
- *ex_exp*: Spremenljivka določa α

Spremenljivke za uspešno predajo zveze:

- *ex_handover_ok*: Privzeta vrednost te spremenljivke je 0. Spremenljivko postavimo na 1, ko se začne predaja iz prvega na drugi vmesnik terminala MN1_1. S tem dosežem tudi, da se funkcija *gna_voice_sip_call_handoff ()* kliče samo enkrat.
- *ex_handover_ok_nazaj_na_intf0*: Privzeta vrednost te spremenljivke je 0. Spremenljivko postavimo na 1, ko se začne predaja iz drugega na prvi vmesnik terminala MN1_1. S tem dosežem tudi, da se funkcija *gna_voice_sip_call_handoff ()* kliče samo enkrat.
- *ex_handover_stream*: Privzeta vrednost te spremenljivke je 0. Spremenljivko postavimo na 1, ko se je vzpostavila RTP zveza pri predaji iz prvega na drugi vmesnik terminala MN1_1, kar pomeni, da lahko začnemo pošiljati RTP pakete po drugi povezavi.
- *ex_handover_stream_nazaj_na_intf0*: Privzeta vrednost te spremenljivke je 0. Spremenljivko postavimo na 1, ko se je vzpostavila RTP zveza pri predaji iz drugega na prvi vmesnik terminala MN1_1, kar pomeni, da lahko začnemo pošiljati RTP pakete po prvi povezavi.

- *ex_handover_abort*: Privzeta vrednost te spremenljivke je 0. Če je njena vrednost 1, potem moramo predajo zveze prekiniti. To pride v poštev, ko je na povezavi na katero želimo narediti predajo razmerje SNR padlo pod prag T_{SNR}.
- *ex_handover_abort_traja*: Privzeta vrednost te spremenljivke je 0. Če je njena vrednost 1, potem smo ravno v fazi prekinjanja predaje.

Spremenljivke za stanja *pipeline*
- *ex_SNR*: enaka funkcija kot OPC_TDA_RA_SNR
- *ex_SNR_CALC_TIME*: enaka funkcija kot OPC_TDA_RA_SNR_CALC_TIME
- *ex_BER*: enaka funkcija kot OPC_TDA_RA_BER

Spremenljivke za pragove:
- *ex_threshold_zgornji_presezen*: Privzeta vrednost te spremenljivke je 0. Na vrednost 1 jo postavimo, ko je presežena vrednost praga T_{SNR} pri padanju vrednosti razmerja SNR.
- *ex_threshold_spodnji_presezen*: Privzeta vrednost te spremenljivke je 0. Na vrednost 1 jo postavimo, ko je presežena vrednost praga T_{SNR} pri rasti vrednosti razmerja SNR.
- *ex_trigger_nastavljen*: Privzeta vrednost te spremenljivke je 0. Na vrednost 1 jo postavimo, ko je presežen prag T_{SNR} in se zaradi tega nastavi prožilo, ki sproži predajo zveze iz prvega na drugi vmesnik terminala MN1_1.
- *ex_trigger_nastavljen_nazaj_na_intf0*: Privzeta vrednost te spremenljivke je 0. Na vrednost 1 jo postavimo, ko je presežen prag T_{SNR} in se zaradi tega nastavi prožilo, ki sproži predajo zveze iz drugega na prvi vmesnik terminala MN1_1.

Spremenljivke za SIP mid_PROBE sporočila:
- *ex_link_prb_ok*: Privzeta vrednost te spremenljivke je 0. Na vrednost 1 jo postavimo, ko je izračunana zakasnitev D_{mid} pod pragom T_d.
- *ex_cas_link_prb*: V to spremenljivko zapišemo čas, ko je bila poslana skupina sporočil `SIP mid_PROBE`
- *ex_link_prb_handover*: Privzeta vrednost te spremenljivke je 0. Na vrednost 1 jo postavimo, ko je se je izvedla predaja zveze, ker je izračunana zakasnitev D_{mid} narasla nad prag T_d.
- *ex_link_prb_abort*: Privzeta vrednost te spremenljivke je 0. Če je njena vrednost 1, potem moramo predajo zveze prekiniti. To pride v poštev, ko je na povezavi na katero želimo narediti predajo razmerje SNR padlo pod prag T_{SNR}.

Nove funkcije in parametri

Predajo zveze sprožimo s SIP re-INVITE sporočilom. Da bi ločili standardno SIP INVITE in SIP re-INVITE sporočilo smo definirali posebno sporočilo imenovano SIP HANDOFF, ki je po funkciji enako INVITE sporočilu. Poleg tega je bilo potrebno definirati tudi novi sporočili SIP pre_PROBE in SIP mid_PROBE, ki je ravno tako podobno INVITE sporočilu. Za podporo novim sporočilom smo morali definirati tudi nove konstante. V knjižnici *sip_api.h* smo to storili na naslednji način:

```
#define     SIPC_CALL_HANDOFF            110
#define     SIPC_CALL_HANDOFF_SUCCESS    210
#define     SIPC_CALL_HANDOFF_FAIL       410
#define     SIPC_HANDOFF_ABORT           500
#define     SIPC_LINK_PRB_OK             501
#define     SIPC_LINK_PRB_F              502
#define     SIPC_LINK_PRB_ABORT          503
#define     SIPC_QoS_REQUEST             120
#define     SIPC_SEND_QoS_REQUEST        130
#define     SIPC_QoS_REQUEST_SUCCESS     220
#define     SIPC_QoS_REQUEST_F           420
```

Na podoben način smo v knjižnici *sip_support.h* definirali tudi nov tip zahteve ter nov status klica:

```
typedef enum
      {
      SIPC_Request_Type_Invite,
      SIPC_Request_Type_Bye,
      SIPC_Request_Type_Handoff,
      SIPC_Request_Type_QoS_Request
}
SIPT_Request_Type;

typedef enum
      {
      SIPC_Call_Uninitiated,
      SIPC_Call_Initiated,
      SIPC_Call_Being_Connected,
      SIPC_Call_Connected,
      SIPC_Call_Disconnected,
      SIPC_Call_Dropped,
      SIPC_Call_Handoffed
}SIPT_Call_Status;
```

Po vzpostavitvi zveze se govor prenaša po RTP protokolu, kar pomeni, da mora ta poleg običajnih parametrov, kot so vzpostavitev in prekinitev zveze, zaznati tudi, ko gre za predajo zveze in kadar se pošiljata SIP pre_PROBE ali SIP mid_PROBE sporočili. Tako smo v knjižnici *Rtp_api.h* definirali novo stanje, ki detektiva predajo zveze:

```
#define     RTPC_HANDOFF            2004
#define     RTPC_QOS_REQUEST        2005
#define     RTPC_LINK_PRB           2006
```

Poleg tega je bilo potrebno na novo definirati več funkcij, ki sodelujejo v pošiljanju HANDOFF in SIP QoS_TEST sporočila.
Te funkcije so:

- V procesnem modelu *gna_voice_calling_mgr:*
  - *gna_voice_sip_call_handoff*
  - *gna_voice_sip_QoS_request*
- V *sip_support.ex.c:*
  - *sip_request_handoff*
  - *sip_request_QoS*
- V *SIP_UAC:*
  - *sip_UAC_process_request_handoff*
  - *sip_UAC_send_handoff_to_UAS*
  - *sip_UAC_call_handoff*
  - *sip_UAC_call_handoff_accept*
  - *sip_UAC_call_handoff_reject*
  - *sip_UAC_handoff_success*
  - *sip_UAC_handoff_fail*
  - *sip_UAC_process_request_QoS*
  - *sip_UAC_send_QoS_request_to_UAS*
  - *sip_UAC_QoS_request*
  - *sip_UAC_QoS_request_accept*
  - *sip_UAC_QoS_request_reject*
  - *sip_UAC_QoS_request_success*
  - *sip_UAC_QoS_request_f*

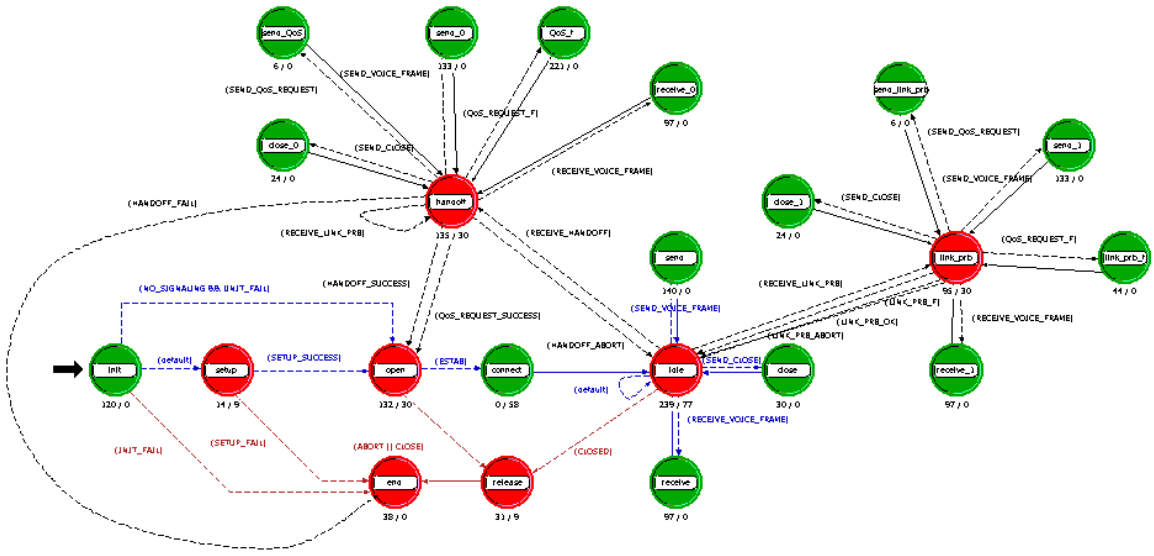
- V *SIP_UAS:*
  - *sip_UAS_handoff_success*
  - *sip_UAS_handoff_fail*
  - *sip_UAS_handoff_req_process*
  - *sip_UAS_QoS_request_success*
  - *sip_UAS_QoS_request_f*
  - *sip_UAS_QoS_request_req_process*

Prilagoditev in razvoj procesov

Pri analizi poteka vzpostavitve in trajanja govornega klica smo ugotovili, da je najprimernejši proces v katerem bi izvedli predajo zveze *gna_voice_calling_mgr*. Ta proces je namreč aktiven ves čas trajanja klica in predstavlja hierarhično najvišji proces za podporo govornim aplikacijam. Ko se izvaja aplikacija IP telefonije, se v procesu nahajamo v stanju *idle*. V času trajanja klica ves čas merimo razmerje SNR. Ko razmerje preseže v naprej določeno vrednost se nastavi samodejna prekinitev s kodo 2004, ki pomeni predajo zveze.

```
op_intrpt_schedule_self (ex_handoff_zacetek, 2004);
```

Na sliki 59 lahko vidimo spremenjen model. Stanja *send_0*, *receive_0*, *close_0, send_1*, *receive_1* in *close_1* so identični stanjem *send*, *receive* in *close* in smo jih dodali za omogočanje pošiljanja in sprejemanja paketov tudi v stanju *handoff* ter stanju *link_prb*, ki sta glavna dodatna element. Dodana so tudi popolnoma nova stanja kot sta *send_QoS* in *QoS_f* ter *send_link_prb* in *link_prb_f*, ki omogočajo pošiljanje in obdelavo `SIP pre_PROBE` in `SIP mid_PROBE` sporočil.



Slika 59: Prilagoditve procesnega modela *gna_voice_calling_mgr*

Iz stanja *handoff* smo z drugimi stanji naredili več transakcij. V času trajanja pogovora, ko tudi pričakujemo predajo zveze, se element v tem procesu nahaja v stanju *idle* in se ob sprejemu ali oddaji paketov premika v stanji *send* in *receive*. Ko signal preseže v naprej predpisano vrednost, se začne procedura izvajanja predaja zveze. Iz stanja *idle* se s kodo 2004, ki pomeni RTPC_HANDOFF, pomaknemo v stanje *handoff*, kjer se začnejo izvajati vse nadaljnje procedure. Za čas trajanja vzpostavitve nove zveze se preko transakcij s stanji *send_0*, *receive_0* in *close_0* izvaja pošiljanje in prejemanje paketov po obstoječi povezavi. V stanju *handoff* se začnejo pošiljati `SIP pre_PROBE` sporočila, in sicer z ukazom:

```
for (RL_k=0; RL_k<ex_st_QoS_REQ; RL_k++)
{
```

```
op_intrpt_schedule_self (op_sim_time()+(RL_k*ex_cas_paketizacije_QoS_REQ), 130);
}
```

Z zgornjim postopkom nastavimo samodejno prekinitev s kodo 130, ki pomeni SIPC_SEND_QoS_REQUEST in prehod v stanje *send*_QoS, kjer se pošiljanje tudi izvede. Ob trenutku pošiljanja si zapišemo tudi čas poslanih `SIP pre_PROBE` sporočil. Ko klicani dobi to sporočilo, nanj odgovori s sporočilom SIP_REQUEST_F. Ko kličoči dobi odgovor, se premakne v stanje *QoS_f*, kjer se izračuna povprečna vrednost zakasnitve D_{pre}. Če je zakasnitev D_{pre} večja od praga T_d, se zopet pošljejo `SIP pre_PROBE` sporočila. V procesu se pomaknemo nazaj v stanje *handoff*. To se dogaja tako dolgo dokler zakasnitev ne pade pod prag T_d oz. če se v tem času razmerje SNR pade pod prag T_{SNR}. V tem primeru se procedura predaje zveze prekine s kodo HANDOFF_ABORT, s katero se prestavimo nazaj v stanje *idle*, kjer čakamo, da razmerje SNR zopet preseže prag T_{SNR}.

V primeru, da je v stanju QoS_f izračunana vrednost zakasnitve pod določenim pragom, se vrnemo v stanje handoff, od koder se s kodo HANDOFF_SUCCESS sproži procedura vzpostavljanja nove zveze. Iz stanja handoff se lahko ob neuspešni vzpostavitvi povezave prestavimo v stanje end. V primeru, da je vzpostavitev povezave in s tem predaje zveze uspešna, pa se prestavimo v stanje open. Ker se pri drugem klicu RTP povezava ne sme vzpostaviti, v kolikor je že aktiven en RTP podatkovni tok, nastavimo zgolj prenos signalizacije:

```
if (ex_st_RTP_sej>1)
    {
          simulation_mode = GNAC_CONTROL_ONLY;
    }
```

Enako je potrebno narediti tudi v procesu *gna_voice_calling_mgr* v stanju *connect*. Po uspešni vzpostavitvi te povezave, element zopet preide v stanje *idle*, kjer prejema in oddaja pakete po novi povezavi.

Ko je nova povezava vzpostavljena se s kodo RTPC_LINK_PRB prestavimo v stanje link_prb, v katerem pošljemo SIP mid_PROBE sporočila z ukazom:

```
for (RL_c=0; RL_c<ex_st_link_prb; RL_c++)
{
  op_intrpt_schedule_self     (op_sim_time()+(RL_c*ex_cas_paketizacije_link_prb),
130);
}
```

Po prejetju odgovorov na enak način kot pri `SIP pre_PROBE` sporočilih izračunamo zakasnitev D_{mid}. Če je zakasnitev D_{mid} manjša od praga T_d, se zopet pošljejo `SIP mid_PROBE` sporočila. To se dogaja tako dolgo, dokler zakasnitev ne zraste nad prag T_d oz. če se v tem času razmerje SNR pade pod prag T_{SNR}. V tem primeru se procedura predaje zveze prekine s kodo LINK_PRB_ABORT, s katero se prestavimo nazaj v stanje *idle*, kjer čakamo, da razmerje SNR zopet preseže prag T_{SNR}.

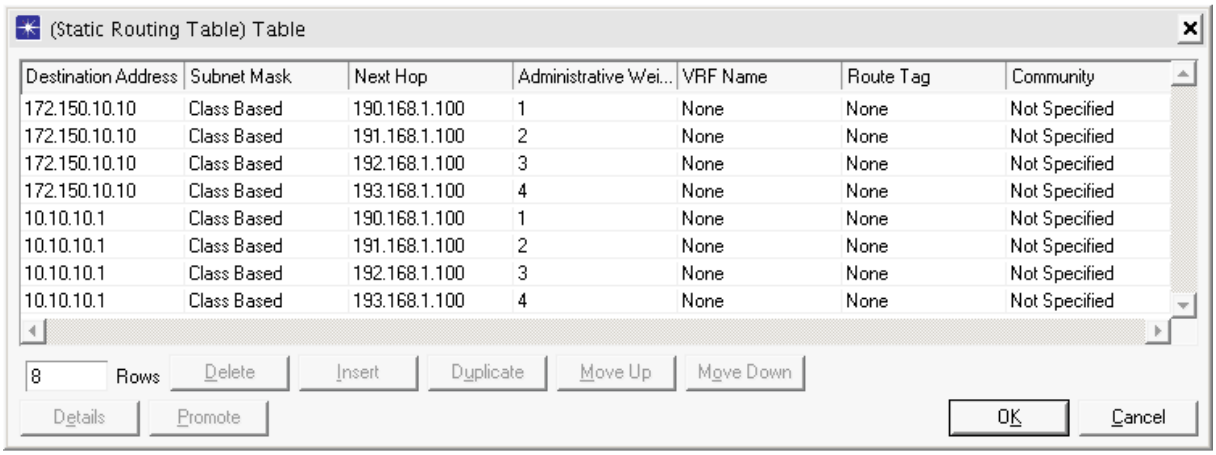
Zamenjava IP naslova

Ob uspešni izvedbi predaje zveze morata začeti terminala MN1_1 in MN2_1 pošiljati in prejemati pakete po novi povezavi. Usmerjevanje IP datagramov se izvaja na IP sloju, kjer smo morali izvesti nekatere prilagoditve obstoječe kode. Pošiljanje in prejemanje datagramov se med seboj razlikujeta, saj gre pri prvem zgolj za izbiro drugega vmesnika na terminalu MN1_1, pri drugem pa za zamenjavo ciljnega IP naslova, ki se mora izvesti na terminalu MN2_1. Zato ju v nadaljevanju obravnavamo ločeno.

Pošiljanje IP datagramov

Od trenutka uspešne vzpostavitve nove RTP povezave naprej, mora terminal MN1_1 IP datagrame pošiljati prek drugega vmesnika. Zaradi preglednejše simulacije smo se odločili, da bomo na mobilnih terminalih uporabili statično IP naslavljanje. Pri običajnem procesu usmerjanja, izbira vmesnika temelji na metriki posameznih povezav. Nižja kot je metrika, bolj ugodna je povezava. V tabeli 22 lahko vidimo nastavitve statične usmerjevalne tabele, ki smo jo uporabili na terminalu MN1_1. Iz tabele je razvidno, da bo prva izbira vmesnik, ki omogoča povezovanje z IP naslovom 190.168.1.100.

Slika 60: Statična usmerjevalna tabela mobilnega terminala MN1_1



Ob vsakem pošiljanju novega IP datagrama element pogleda v statično tabelo ter izbere ustrezen vmesnik. To se zgodi v procesu *ip_rte_central_cpu*, ki je podproces procesa *ip_dispach*, ki je odgovoren za usmerjanje. V funkciji *ip_rte_central_cpu_send_packet*, ki je definirana v procesu *ip_rte_central_cpu* se izvede pošiljanje IP datagrama na določen naslov. V naši prilagoditvi smo ob času uspešne predaje zveze izvedli zamenjavo vrednosti, ki jih mobilni terminal dobi iz statične tabele. Ob analizi pošiljanja IP datagramov prek različnih vmesnikov, smo ugotovili določene razlike, ki jih na tem mestu uporabimo. V nadaljevanju je podan del kode, ki izvede zamenjavo posameznih parametrov:

Najprej v obstoječem podatku o naslednjem IP naslovu zamenjamo posamezne vrednosti:

```
RL_next_addr_str[2]=RL_vrsta_predaje[0];
```

Nato iz tekstovne oblike zapisa IP naslova le tega spremenimo v obliko, ki jo uporablja OPNET:

```
RL_next_addr_nov=inet_address_create(RL_next_addr_str, InetC_Addr_Family_v4);
```

Na koncu še zapišemo nove vrednosti:

```
intf_ici_fdstruct_ptr->next_addr=RL_next_addr_nov;
intf_ici_fdstruct_ptr->outstrm=ex_predaja_na_intf+1;
intf_ici_fdstruct_ptr->output_intf_index=ex_predaja_na_intf;
```

Z zapisom novih vrednosti, smo dosegli, da terminal začne pošiljati pakete prek drugega vmesnika terminala MN1_1.

Prejemanje IP datagramov

Ko je nova povezava vzpostavljena, mora začeti tudi drugi mobilni terminal MN2_1 pošiljati IP datagrame prek drugega omrežja. V tem primeru smo morali spremeniti samo ciljni IP naslov. Pošiljanje IP datagramov se izvaja v procesu *ip_encap_v4*. Ta proces ima dva, za naše analize, pomembna stanja, in sicer *encap*, ki je namenjen pošiljanju IP datagramov in *decap*, ki je namenjen prejemanju IP datagramov. Potrebne spremembe smo izvedli v stanju *encap*. To storimo z naslednjim zapisom:

```
dest_addr = ex_MN1_1_intf_naslov2;
```

kjer obstoječi IP naslov zapisan v spremenljivki *dest_addr* zamenjam z IP naslovom zapisanim v zunanji spremenljivki *ex_MN1_1_intf_naslov2*.

Vhodni podatki

V elementu Inicializacija pa lahko določimo tudi ali se bodo pri simulaciji za vrednosti razmerja SNR uporabile vrednosti, ki so bile izmerjene v realnem omrežju. Vhodna datoteka mora biti v naslednji obliki:

```
110.00 8
111.00 8
112.00 8
113.00 8
114.00 10.161204187431
115.00 11.55391069228
116.00 13.214184340882
```

Kjer prvi stolpec določa simulacijski čas v sekundah, drugi stolpec pa vrednost razmerja SNR ob določenem simulacijskem času.

Iz izmerjenih vrednosti ob začetku simulacije naredimo matriko. Elemente v matriko definiramo z naslednjimi ukazi:

```
RL_line_list_ptr = op_prg_gdf_read ("snr_sim");

if (RL_line_list_ptr == OPC_NIL)
   {
      sprintf(RL_msg,"Ne morem prebrati datoteke snr_test");
      op_prg_odb_print_major(RL_msg, OPC_NIL);
    }

ex_gdf_num_rows = op_prg_list_size (RL_line_list_ptr);

RL_field_list_ptr = op_prg_str_decomp(op_prg_list_access (RL_line_list_ptr,
0), " ");

ex_gdf_num_columns = op_prg_list_size (RL_field_list_ptr);
op_prg_list_free (RL_field_list_ptr);
op_prg_mem_free (RL_field_list_ptr);

sprintf(RL_msg,"prebral fajl, vrstice = %d, stolpci = %d", ex_gdf_num_rows,
ex_gdf_num_columns);
op_prg_odb_print_major(RL_msg, OPC_NIL);

ex_traffic_matrix_vec = (float*)op_prg_mem_alloc(ex_gdf_num_rows *
ex_gdf_num_columns * sizeof(float));

for (RL_i = 0; RL_i < ex_gdf_num_rows; RL_i++)
    {
       RL_field_list_ptr =
op_prg_str_decomp(op_prg_list_access(RL_line_list_ptr, RL_i), " ");

 for (RL_j = 0; RL_j < ex_gdf_num_columns; RL_j++)
    {
      ex_traffic_matrix_vec[RL_i*ex_gdf_num_columns+RL_j] = (float)(atof
(op_prg_list_access (RL_field_list_ptr, RL_j)));
     }

op_prg_list_free (RL_field_list_ptr);
op_prg_mem_free (RL_field_list_ptr);
       }

op_prg_list_free (RL_line_list_ptr);
op_prg_mem_free (RL_line_list_ptr);
```