P2P telefonija: Skype

Darko Bodnaruk, Janez Sterle, dr. Andrej Kos, dr. Janez Bešter
Laboratorij za telekomunikacije, Fakulteta za elektrotehniko, Univerza v Ljubljani

Povzetek — Članek predstavlja inovativen pristop k internetni telefoniji – omrežje in program Skype. Prikazana je tehnogija vsak z vsakim, ki je pomembna za širši uspeh programa v domačih in poslovnih okoljih. Predstavljene so tudi nekatere tehnične lastnosti aplikacije, kot jih je bilo moč ugotoviti iz zunanjega opazovanja delovanja programa. Prav tako se sprašujemo o varnosti take rešitve in možnosti uporabe v podjetjih.

Ključne besede — VoIP, Skype, peer-to-peer omrežja, P2P

Abstract — The article presents an innovative approach to internet telephony, used by the application Skype and its network. The underlying peer-to-peer network, which is one of the reasons for Skype's success, is outlined. Some technical features of the application, as inferred from the outside view of the application's workings, are also presented. The question whether Skype is secure and appropriate for corporate use is also asked.

Keywords — VoIP, Skype, peer-to-peer networks, P2P

I. UVOD

Tehnologija Voice over IP že dolgo obeta velike spremembe na področju govorne telefonije. Kljub velikim vložkom na področju standardizacije in vpletenosti velikih operaterjev in proizvajalcev opreme, je v zadnjem letu in pol največji zagon tehnologiji VoIP dalo novoustanovljeno podjetje Skype, ki brezplačno ponuja klice znotraj svojega omrežja, za nizko ceno pa tudi klice v omrežje PSTN oz. ISDN. Od zagona storitve Skype avgusta 2003 do danes ima ta že okrog 30 mio. registriranih uporabnikov, število prenesenih kopij pa je preseglo 100 mio.

Aplikacija Skype, ki je na voljo na platformah Windows, Linux, Mac OS X in Pocket PC, je v osnovi program za neposredno sporočanje z vgrajeno VoIP funkcionalnostjo in možnostjo prenosa datotek. Skype je zelo hitro prodrl tudi do domačih uporabnikov, saj je v nasprotju z večino ostalih rešitev VoIP zelo enostaven za namestitev in uporabo. Za širok sprejem je najbrž odločilno dejstvo, da aplikacija deluje praktično povsod, kjer jo namestimo. Za prečkanje strežnikov NAT in požarnih zidov, ki je ena večjih težav, ki jo mora tehnologija VoIP premagati za splošno uporabo, je bil uporabljen inovativen pristop. Ustanovitelj podjetja Skype, Niklas Zennström, je namreč pred tem ustanovil podjetje in program za izmenjavo datotek KaZaA. Ta sloni na tehnologiji sistemov vsak z vsakim (peer-to-peer systems – P2P) in Zennström jo je komercialno uporabil že v podjetju JoltID, kot uporabna pa se izkaže tudi za internetno telefonijo. Gre za decentralizacijo funkcij omrežja in prenašanje le-teh na končne uporabnike. S tem se zmanjšajo ozka grla oz. točke možne odpovedi sistema (»single point of failure«), hkrati pa naredi sistem zelo skalabilen.

Skype lahko označimo za t.i. »disruptive technology«, saj spreminja razmerja v telefoniji. Po besedah ustanovitelja je prišlo obdobje, ko je telefonija samo še ena izmed aplikacij in zato telekomi ne bodo več mogli zaračunavati govornih klicev. Poslovni model Skypa sloni na velikem številu uporabnikov, od katerih le del plačuje za storitve z dodano vrednostjo. Ker tehnologija P2P omogoča, da so dodatni stroški vključitve novega uporabnika praktično nič, lahko podjetje posluje z dohodkom od majhnega števila uporabnikov, ki za storitve plačuje.

V članku bo v drugem delu predstavljena arhitektura P2P in reševanje problema prehoda preko strežnikov NAT in požarnih zidov. V tretjem delu so prikazane nekatere tehnične lastnosti, ki so bile ugotovljene s preučevanjem prometa na omrežju sicer zaprte aplikacije. V četrtem delu so navedeni razlogi zakaj se podjetja pretežno še ne odločajo za uporabo programa Skype, v petem pa članek sklenemo.

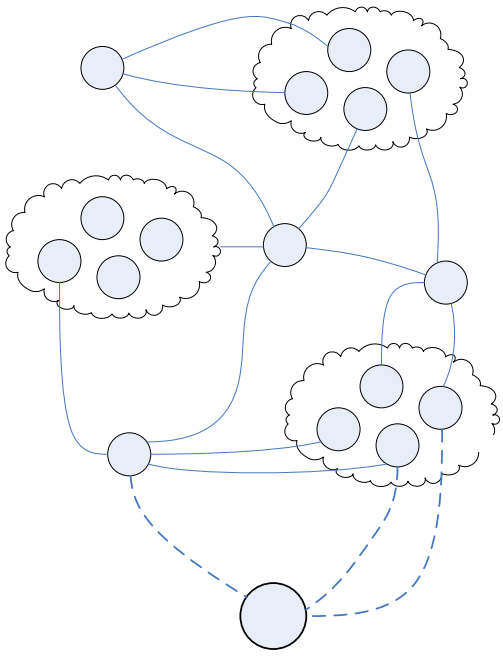
II. ARHITEKTURA PEER-TO-PEER

Omrežje Skype je prekrivno (»overlay«) peer-to-peer omrežje, saj gre za protokol nad protokoloma TCP in UDP, ki ima svoje usmerjanje in naslavljanje. Podobno kot program za izmenjavo datotek KaZaA sloni omrežje Skype na konceptu supervozlišč – gre le za enega odjemalca, vendar nekateri v omrežju opravljajo posebno vlogo. Pogoji za to, da se odjemalec (»vozlišče«) obnaša kot supervozlišče so: dovolj zmogljiv procesor, zadostna pasovna širina ter javni IP naslov.

A. *Prehajanje preko strežnikov NAT*

Pomemben problem internetne telefonije so strežniki NAT in požarni zidovi, ki preprečujejo neposredno naslavljanje odjemalcev. Taki odjemalci v omrežju pogosto prevladujejo, saj gre za pogost način za povezovanje domačih računalnikov na povezavah DSL ali osebnih računalnikov v podjetjih, ki imajo omejeno število javnih naslovov IP. Pri vzpostavljanju klica med dvema odjemalcema tako lahko naletimo na tri situacije: oba odjemalca na javnem naslovu IP, en odjemalec na javnem naslovu IP, drugi pa za strežnikom NAT oz. požarnim zidom ter oba odjemalca za strežnikom NAT ali požarnim zidom.

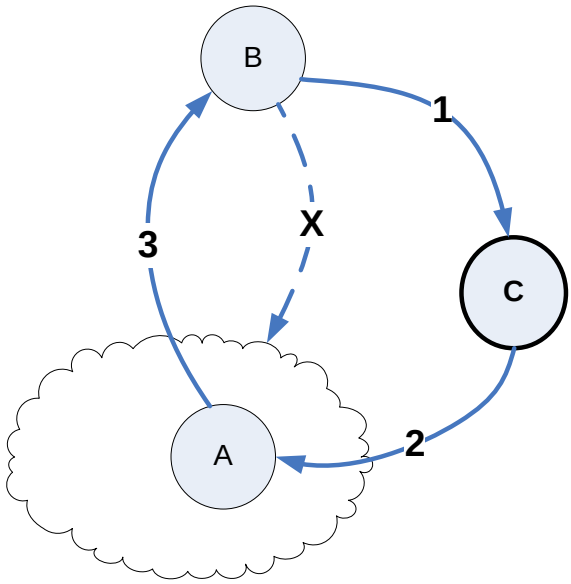
Protokoli internetne telefonije to rešujejo s posebnimi strežniki, ki posredujejo dohodni promet za taka vozlišča. Če se ti strežniki nahajajo na javnem internetu so ozko grlo sistema, saj gre vsa komunikacija z vozlišč za strežniki NAT preko njih. Če take strežnike postavimo znotraj omrežja za strežnikom NAT (t.i. »session border controller«) zahtevajo zapleteno konfiguracijo in niso primerni za domače uporabnike. Omrežje Skype problem poskuša reševati z decentralizacijo funkcije posredovanja. Namesto namenskih strežnikov posredovanje signalizacije in podatkovnega toka prevzamejo nase številna supervozlišča. Vsako običajno vozlišče v ta namen vzpostavi in drži povezavo TCP z vsaj enim supervozliščem (Slika 1).



Slika 1: Omrežje Skype - običajna vozlišča, supervozlišča in prijavni strežnik

Drugo izmed prej omenjenih situacij pri vzpostavljanju klica učinkovito rešuje koncept supervozlišč. Recimo, da je vozlišče A za strežnikom NAT, vozlišče B pa na javnem naslovu IP (Slika 2). A lahko kliče B, medtem ko B ne more neposredno klicati A. Vendar pa ima A vzpostavljeno povezavo z nekim supervozliščem C, ki ima javen naslov IP. Tako B zahtevo po komunikaciji sporoči supervozlišču C, ki to posreduje vozlišču A. Kot rečeno pa vozlišče A lahko pokliče vozlišče B. Za uporabnika je seveda vseeno oz. transparentno kako poteka vzpostavitev povezav. Supervozlišče je v tem primeru zelo malo obremenjeno saj posreduje le začetno signalizacijo.

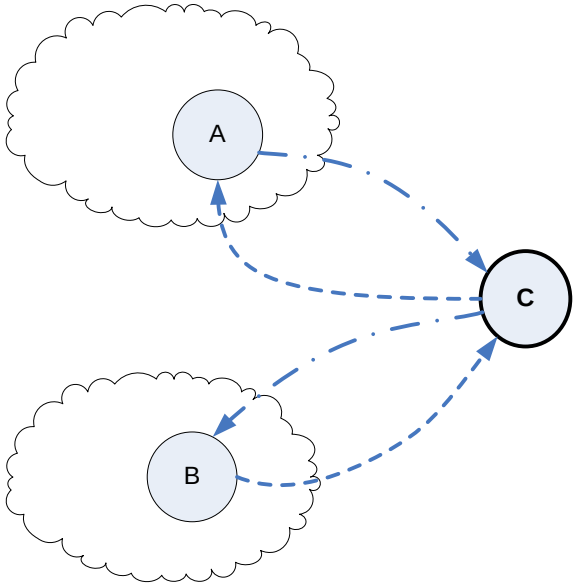
Večji problem je tretja situacija, ko sta obe vozlišči za strežnikom NAT oz. požarnim zidom (Slika 3). V tem primeru mora supervozlišče posredovati ne le signalizacijo temveč celoten podatkovni tok. To lahko supervozlišče precej obremeni, tako glede pasovne širine kot tudi procesorsko. Še posebej uporabniki, ki plačujejo glede na količino prenesenih podatkov, nimajo interesa posredovati promet za druga vozlišča. Zaenkrat v odjemalcu ni mogoče nastaviti, da se ne bi obnašal kot supervozlišče. Enak način posredovanja prometa se uporablja pri prenosu datotek, zato je hitrost prenosa v takem primeru omejena na 0.5 kB/s. Pri prenosu datotek bi namreč supervozlišče lahko zelo hitro porabilo vso pasovno širino, ki mu je na voljo, medtem ko promet pri telefoniji ne naraste tako naglo.



Slika 2: Vzpostavljanje povezave, ko je eno vozlišče na javnem naslovu IP

Ugibamo, da pri določenih vrstah strežnikov NAT odjemalci Skype uporabljajo tudi tehniko »UDP hole punching« [3]. Če strežnik NAT deluje v načinu, ki je priporočen z dokumentom RFC 3022 [4] – za enega odjemalca znotraj omrežja uporablja ista izhodna vrata pri komunikaciji z različni naslovi zunaj omrežja – je mogoče samo z izmenjavo informacij o notranjih in zunanjih naslovih IP in vratih preko supervozlišča vzpostaviti neposredno povezavo UDP. Tehnika je

poznana in jo uporabljajo nekatere internetne igre in P2P programi za izmenjavo datotek.



Slika 3: Posredovanje prometa preko supervozlišča

Za uspešno izbiro načina delovanja mora vozlišče vedeti, za kakšno vrsto strežnika NAT oz. požarnega zidu se nahaja. Skype v ta namen najverjetneje uporablja varianto protokola STUN [2].

B. *Prehajanje preko požarnih zidov*

Za transparentno prehajanje preko požarnih zidov v podjetjih uporablja odjemalec Skype več vrat, na katerih posluša mdohodni promet. Vrata UDP so izbrana naključno zaradi bolj zanesljivega delovanja pri nekaterih vrstah strežnikov NAT, posluša pa še na vratih TCP 80 in 443. Promet na teh vratih je na izhodnih požarnih zidovih praktično vedno dovoljen.

C. *Enkripcija*

Pomembna lastnost, ki je nujna za posredovanje signalizacije in podatkovnega toka preko nepoznanih vozlišč, je enkripcija kontrolne in podatkovne ravnine za vse vrste komunikacije (govor, neposredno sporočanje, prenos datotek). Spletna stran programa [1] navaja, da je za enkripcijo podatkovnega toka uporabljen enkripcijski algoritem AES (Advanced Encryption Standard) z 256-bitnimi ključi. Ti se izmenjujejo z asimetrično enkripcijo RSA s 1536- do 2048-bitnimi ključi. Javni ključi odjemalcev se preverjajo na prijavnem strežniku ob začetni prijavi v omrežje.

III. NEKATERE TEHNIČNE ZNAČILNOSTI

A. *Prijava v omrežje*

Z merjenjem prometa [5] je bilo ugotovljeno, da odjemalec ob zagonu najprej poskuša vzpostaviti povezavo z vsaj enim supervozliščem. Program hrani seznam potencialnih supervozlišč (»Host Cache«), ki je že ob inštalaciji odjemalca napolnjen z naslovi - najverjetneje naslovi stalnih vozlišč, za katere skrbi podjetje Skype (»bootstrap nodes«). Program najprej pošlje en paket UDP; če ne dobi odgovora, poskuša vzpostaviti povezavo TCP na vrata 80, zatem na vrata 443. V primeru neuspeha ta proces nekaj časa ponavlja, zatem pa javi neuspešno prijavo.

Ko odjemalec vzpostavi povezavo TCP z enim supervozliščem sledi prijava v omrežje. To je edina centralizirana funkcija v celotnem sistemu. Odjemalec se poveže na vnaprej določen prijavni strežnik, ki preveri identiteto uporabnika z uporabniškim imenom in geslom. Naloga prijavnega strežnika je skrb za unikatnost uporabniških imen v celotnem sistemu, hkrati pa je edini element omrežja, ki ga povezuje v celoto.

V naslednjem koraku prijave v omrežje vozlišče pošlje sporočila UDP na 22 različnih naslovov. Najverjetneje gre za oglaševanje prisotnosti.

B. *Iskanje uporabnikov*

Za iskanje uporabnikov Skype uporablja lastno tehnologijo Global Index. Na spletni strani je podatek, da gre za distribuirano iskanje, pri katerem je zagotovljeno, da bo uporabnik najden, v primeru da ta obstaja in se je v omrežje prijavil v zadnjih 72 urah. Najverjetneje gre za distribuirano zgoščevalno tabelo (Distributed Hash Table - DHT) [9].

Ko uporabnik v polje za iskanje vnese niz, odjemalec pošlje sporočilo supervozlišču, s katerim je povezan. Ta mu odgovori najverjetneje z naslovi na katerih se iskani uporabnik lahko nahaja. Odjemalec pošlje sporočila UDP na 4 naslove. V primeru, da ne dobi odgovora, spet kontaktira svoje supervozlišče in pošlje sporočila na 8 naslovov. Tako nadaljuje dokler uporabnika ne najde oz. preneha po določenem številu poskusov. Ni znano natančno kdaj se iskanje prekine. V primeru, da je odjemalec za požarnim zidom, ki omejuje pakete UDP, se iskanje vrši preko supervozlišča. Ker gre za distribuirano iskanje, pri tem posreduje več vozlič, ki rezultate shranjujejo. Ponovno iskanje uporabnika je pogosto hitrejše kot predhodna, saj sosednja vozlišča hranijo informacije o lokaciji iskanega.

C. *Prenos zvoka*

Kodek, ki je uporabljen za kompresijo zvoka, je iLBC. Gre za kodek podjetja Global IP Sound in je na voljo brezplačno [11]. Odlikuje ga širok frekvenčni razpon in visoka odpornost na izgubo paketov.

Merjenje prometa je pokazalo tudi nekaj značilnosti prenosa zvoka. Signalizacija je vedno potekala preko povezav TCP, neodvisno od situacije v omrežju. Prenos zvoka, vkolikor je to mogoče, poteka preko paketov UDP, velikosti 67 bytov. Uporabljena pasovna širina je povprečno 5 kB/s. V primeru posredovanja supervozlišča so bile velikosti paketov in pasovna širina podobne. V primeru požarnega zidu, ki omejuje pakete UDP, so bili paketi TCP velikosti 69 bytov, pasovna širina pa prav tako okrog 5 kB/s.

Ugotovljeno je bilo, da Skype ne uporablja izločanja tišine (»silence suppression«), saj se pri tišini uporabljena podatkovna širina ni zmanjšala. Prednosti take odločitve so v ohranjanju asociacij na strežniku NAT v primeru prometa UDP oz. preprečevanje zmanjšenja zamašitvenega okna pri povezavi TCP. [5] Sporočila so se med vozlišči izmenjevala tudi, ko je bil pogovor začasno prekinjen (»hold«). Razlogi so najbrž podobni.

Pri omejevanju prometa se je izkazalo, da je najnižja pasovna širina, pri kateri je govor še vedno razumljiv, okrog 2 kB/s v vsako smer.

Skype omogoča tudi konferenčne klice. Pri tem eno vozlišče igra vlogo mešalca zvoka. Seveda se izbere vozlišče, ki je na javnem naslovu IP, če so vozlišča v tem pogledu enakovredna, pa se izbere procesorsko najmočnejše.

IV. VARNOST

Pri vprašanju ali je Skype kot zaprta tehnologija dovolj varen za uporabo v podjetjih naletimo na kar nekaj spornih točk. Skype je namreč nemogoče omejiti na podjetje saj za svoje delovanje potrebuje prijavo na prijavni strežnik in zunanja supervozlišča.

Prva stvar je pomanjkanje dokumentacije glede enkripcije. Le okvirno je omenjeno kateri protokoli so uporabljeni, ničesar pa ne vemo o tem, kako dejansko poteka enkripcija podatkovnega toka, kako so shranjeni in zaščiteni ključi ipd. Ni jasno ali se ključi za simetrično enkripcijo AES menjajo tudi med samo sejo. Še bolj nejasna je varnost pri storitvi SkypeOut, kajti prehodi v omrežje PSTN najverjetneje niso v lasti oz. pod nadzorom podjetja Skype [7].

Sporazum o uporabi za končnega uporabnika (End User License Agreement – EULA) vsebuje nekaj nenavadnih postavk. Eksplicitno je prepovedana uporaba orodij za prisluškovanje prometu, razprševalnikov (»disassembler«), razhroščevalnikov, povratnega inženiringa (»reverse engineering«). Odjemalec Skype aktivno blokira uporabo razhroščevalnika SoftICE, saj se v primeru, da je ta na računalniku nameščen, inštalacija prekine. Zdi se da je podjetju veliko do tega, da ostane čimveč notranjega delovanja skritega. Po eni strani je to razumljivo zaradi možnosti zlorabe plačljivih storitev (SkypeOut), po drugi strani pa vzbuja nezaupanje. Znano je namreč, da je program za izmenjavo datotek KaZaA vseboval skrito funkcionalnost, ki je ob znanem P2P omrežju vzpostavila vzporedno omrežje [6].

Podjetje Skype očitno zbira vsaj nekaj statistike o klicih, čeprav gre v osnovi za decentralizirano P2P omrežje. Na osnovni spletni strani [8] je mogoče videti »živ« števec minut pogovorov, narejenih preko Skype odjemalcev v celotnem omrežju. Čeprav spletna stran trdi, da so podatki agregirani, je povsem mogoče, da se zbira več podatkov. Ti bi bili ob morebitnem vdoru v njihov sistem lahko zlorabljeni za prometno analizo.

Pri prenosu datotek se uporablja enaka enkripcija kot za vso drugo komunikacijo. To pomeni, da je tak promet nemogoče filtrirati z antivirusnimi programi na nivoju podjetja. Ker Skype odjemalec v skrajnem primeru uporabi vrata 80 oz. 443, ki se uporabljata za protokola HTTP oz. HTTPS, je praktično povsem nemogoče blokirati promet na osnovi vrat. Tako je podjetje, v katerem se uporablja Skype, na nek način »odprto« za morebitne varnostne luknje v programu ali namerno vgrajeno funkcionalnost. Problem varnostnih lukenj je sicer enak pri drugem programju, vendar pa je kombinacija zaprtokodne rešitve in kriptirane komunikacije s številnimi vozlišči širom interneta verjetno za mnoge administratorje nekoliko strašljiva.

Nekateri raziskovalci [10] so izpostavili, da vsak sistem, ki za posredovanje prometa uporablja nepoznana vozlišča, inherentno ni varen. S pomočjo povratnega inženiringa bi namreč lahko skonstruirali vozlišče, ki bi se obnašalo kot pravo, obenem pa bi prestrezalo izmenjave ključev med vozlišči za katera posreduje promet. Ta predpostavka sicer temelji na neznanem principu izmenjave simetričnih enkripcijskih ključev.

V. ZAKLJUČEK

Članek je poskušal predstaviti delovanje omrežja in odjemalcev Skype. Čeprav znan, je pristop s tehnologijo peer-to-peer inovativen in je omogočil delovanje v praktično vseh omrežnih pogojih. Skype se je s kombinacijo brezplačne telefonije preko peer-to-peer sistema, dobrega zvočnega kodeka in uporabniku prijaznega vmesnika iz še enega brezplačnega programa razvil v produkt, ki ga želijo posnemati tudi mnogi obstoječi operaterji telefonije.

Kritike izhajajo predvsem iz zaprtosti sistema, ki v kombinaciji s slabo publiciteto podjetja KaZaA istega ustanovitelja, vzbujajo sume. Prav tako podjetje Skype zelo nerado razkriva podrobnosti glede varnostnih mehanizmov, zato lahko le ugibamo o dejanski varnosti le teh. Zdi se da s skrivanjem delovanja programa želijo vezati uporabnika na njihov produkt in omrežje.

REFERENCE

[1] Skype FAQ, http://www.skype.com/help_faq.html
[2] J. Rosenberg, J. Weinberger, C. Huitema, and R. Mahy. STUN: Simple Traversal of User Datagram Protocol (UDP) Through Network Address Translators (NATs). RFC 3489, IETF, Mar. 2003.
[3] NAT Check, http://midcom-p2p.sourceforge.net/
[4] Traditional IP Network Address Translator (Traditional NAT), http://www.ietf.org/rfc/rfc3022.txt
[5] An Analysis of the Skype Peer-to-Peer Internet Telephony Protocol, http://www.cs.columbia.edu/~library/TR-repository/reports/reports-2004/cucs-039-04.pdf
[6] P2P network hidden in Kazaa downloads, http://news.zdnet.com/2100-1009_22-873416.html
[7] An analysis of Skype VoIP application for use in a corporate environment, http://www1.cs.columbia.edu/~salman/skype/Skype_Analysis_1_3.pdf
[8] http://www.skype.com
[9] http://en.wikipedia.org/wiki/Distributed_hash_table
[10] http://www.interesting-people.org/archives/interesting-people/200501/msg00235.html
[11] http://www.ilbcfreeware.org/

BIOGRAFIJA

Darko Bodnaruk (darko.bodnaruk@ltfe.org) je diplomiral leta 2002 na Fakulteti za računalništvo in informatiko Univerze v Ljubljani s področja umetne inteligence. Od leta 2002 dela v Laboratoriju za telekomunikacije na Fakulteti za elektrotehniko. Njegovo raziskovalno delo vključuje multimedijske in konvergenčne internetne aplikacije ter vgrajene sisteme.

Janez Sterle (janez.sterle@ltfe.org) je diplomiral leta 2003 na Fakulteti za elektrotehniko Univerze v Ljubljani s področja telekomunikacij. Od leta 2002 dela v Laboratoriju za telekomunikacije na Fakulteti za elektrotehniko. Njegovo raziskovalno delo je usmerjeno v preučevanje in razvoj omrežnih sistemov in storitev naslednje generacije. Od leta 2003 aktivno sodeluje tudi na uvajanju projekta izobraževalnega programa Cisco Networking Academy na Fakuleti za elektrotehniko.

Andrej Kos (andrej.kos@fe.uni-lj.si) je diplomiral leta 1996 in doktoriral leta 2003 na Fakulteti za elektrotehniko Univerze v Ljubljani, vse s področja telekomunikacij. Zaposlen je v Laboratoriju za telekomunikacije na Fakulteti za elektrotehniko. Ima veliko izkušenj na področju raziskav, razvoja, načrtovanja in analize sodobnih telekomunikacijskih sistemov in omrežij. Trenutno se najbolj posveča razvoju telekomunikacijskih omrežij in sistemov naslednje generacije, še posebno na področju internetnega protokola, večprotokolne komutacije na osnovi label in asinhronega načina prenosa. Druga njegova interesna področja zajemajo mobilne komunikacije, upravljanje omrežij in signalizacijo številka 7.

Janez Bešter (janez.bester@fe.uni-lj.si) je diplomiral leta 1979, magistriral leta 1982 in doktoriral leta 1995 na Fakulteti za elektrotehniko Univerze v Ljubljani, s področja telekomunikacij. Zaposlen je kot docent in predstojnik Laboratorija za telekomunikacije. Njegovo sedanje delo je usmerjeno v raziskave in inženiring na področju informacijske infrastrukture, vpeljevanja novih telekomunikacijskih storitev ter uporabe informacijskih tehnologij in telekomunikacij na področju e-izobraževanja. Predava predmete Osnove telekomunikacij II, Komutacijski sistemi in omrežja, Komunikacijska omrežja in storitve, Inteligentna omrežja ter Načrtovanje, modeliranje in vodenje telekomunikacijskih omrežij.