Skrivanje topologije i medija menadžment u VoIP mrežama korišćenjem SBC kontrolera

Dragan Botić, Siniša Vujčić
Direkcija za tehniku
Mtel a.d. – Telekom Srpske
Banja Luka, RS, BiH
dragan.botic@mtel.ba, sinisa.vujcic@mtel.ba

Dejan Nemec
Departman za energetiku, elektroniku i telekomunikacije
Fakultet tehničkih nauka, Univerzitet u Novom Sadu
Novi Sad, Srbija
denem@uns.ac.rs

Sažetak — **Uloga SBC kontrolera u VoIP mrežama je višestruka i obuhvata: grupu funkcija periferne odbrane (kontrola pristupa, skrivanje topologije mreže, prevencija DoS/DDoS napada), grupu funkcija koje rješavaju dostupnost krajnjih tačaka mreže (NAT/FW prelaz, *interworking* ili *repair* protokola), kao i funkcionalnosti medija menadžmenta, medija monitoringa i QoS-a. Cilj ovog rada je da prikaže SBC funkcionalnosti skrivanja topologije mreže iz grupe funkcija periferne odbrane kao i medija monitoring i medija menadžment funkcionalnosti, ukaže na njihovu važnost u očuvanju tržišne pozicije mrežnih operatora i zaštite vlastitih resursa od neovlaštenog korišćenja i/ili zloupotrebe. U cilju razumijevanja potencijalnih problema koji mogu nastati upotrebom SIP protokola u javnim telekomunikacionim mrežama, opisan je i opšti način funkcionisanja SBC kontrolera.**

Ključne riječi – SBC; VoIP; SIP; SDP; UA, B2BUA; NAT

I. UVOD

Dinamičan razvoj telekomunikacionog tržišta, pojava novih servisa, sve većeg broja operatora, uporedo sa brzim tehnološkim promjenama dovodi do promjena u topologiji mreže, uvođenja novih elemenata u mrežu. Jedan od tih elemenata je i SBC (*Session Border Controller*). Od njegove pojave pa do danas neprestano raste broj funkcionalnosti koje on izvršava u mreži. Ove funkcionalnosti u stvari predstavljaju rješenja za probleme koji se javljaju u VoIP (*Voice over Internet Protocol*) mrežama u uslovima konvergencije telekomunikacionih mreža i postepenog prelaska govornih servisa sa TDM (*Time-Division Multiplexing*) tehnologije na VoIP tehnologiju i dominacije SIP (*Session Initiation Protocol*) protokola u VoIP mrežama [1].

Razvoj SIP protokola je bio opterećen s jedne strane postojećim mrežnim okruženjem i postojećim tehnologijama sa kojima je trebalo zadržati konekciju, a sa druge strane potrebom za novim inovativnim pristupom u rješavanju problema nastalih u novom mrežnom okruženju sa novim servisima i novim tehnologijama. Razvoj SIP protokola je tekao u etapama. Svaka sledeća revizija je uz razvoj novih i unapređenje postojećih funkcionalnosti rješavala i uočene nedostatke iz prethodnih revizija. Jedan od krupnijih nedostataka SIP protokola, čija priroda je u *end-to-end* komunukaciji, je činjenica da se tokom razvoja računalo na brži tempo iskorišćenja IPv4 (*Internet Protocol version 4*) adresnog prostora i ranije uvođenje IPv6 adresnog prostora u upotrebu, čime bi problem NAT (*Network Address Translation*) prelaza prestao da postoji. Međutim pošto se IPv4 adresni prostor zadržao duže od predviđenog, trebalo je riješiti taj problem. U ovim uslovima se na telekomunikacionom tržištu javlja SBC kontroler koji u svom skupu funkcionalnosti sadrži i rješenje za ovaj sistemski nedostatak SIP protokola – NAT prelaz [2]. Drugi nedostaci SIP protokola su se ticali samog dizajna protokola. Brojni apstraktni pojmovi kao što su *dialog, session, transaction,* itd. nisu imali jedinstvene, nedvosmislene identifikatore koji im se pridružuju. Broj njihovih kombinacija u zaglavlju SIP poruka dovodio je do smanjivanja interoperabilnosti. Neki od njih su riješeni kasnijim revizijama SIP protokola uvođenjem dodatnih parametara (*branch*, *session-id,* itd.), dok je za druge rješenje pronađeno u SBC funkcionalnosti *protocol repair*. Sledeći nedostatak SIP protokola je činjenica da, u početku implementacije, komponente koje su razvijene da rade pod SIP-om nisu uobzirile potrebu za zaštitom od neovlaštenog pristupa mrežnim resursima. Taj aspekt sigurnosti je takođe, počeo da rješava SBC implementirajući funkcionalnost kontrole pristupa. Ova funkcionalnost je vezana i za način registracije korisnika koji se, takođe, odvijaju preko SBC-a i SBC ima uvid u podatke o registraciji uključujući i vrijeme trajanja registracije. Na ovaj način je SBC počeo izvršavati sigurnosne funkcije u mreži. Sljedeći aspekt upotrebe SBC-a je bio zakonsko presretanje, LI (*Lawful Interception*) [3]. U početnoj fazi je predmet zakonskog presretanja bio govorni servis u fiksnoj i mobilnoj mreži, potom su stvorene pretpostavke za zakonsko presretanje i *data* servisa (*e-mail*). SBC prve generacije su bili namjenski nemodularni uređaji koji su rješavali problem sigurnog pristupa pretplatnika operatorovim PSTN (*Public Switched Telephone Network*) gejtvejima, podžavajući funkcionalnosti skrivanja topologije mreže i NAT prelaz. Druga generacija SBC uređaja je bila tehnološki naprednija i podržavala je kompleksnije tokove poziva, kao i video komunikaciju. U ovoj generaciji su podržane funkcionalnosti DoS (*Denial of Service*) prevencija, zaštita od preopterećenja, IPSec (*IP Security*) protokol, *fraud* prevencija. SBC se pored kontrole pristupa (UNI SBC – *User Network Interface SBC*), počinje koristiti i u svrhu kontrole i

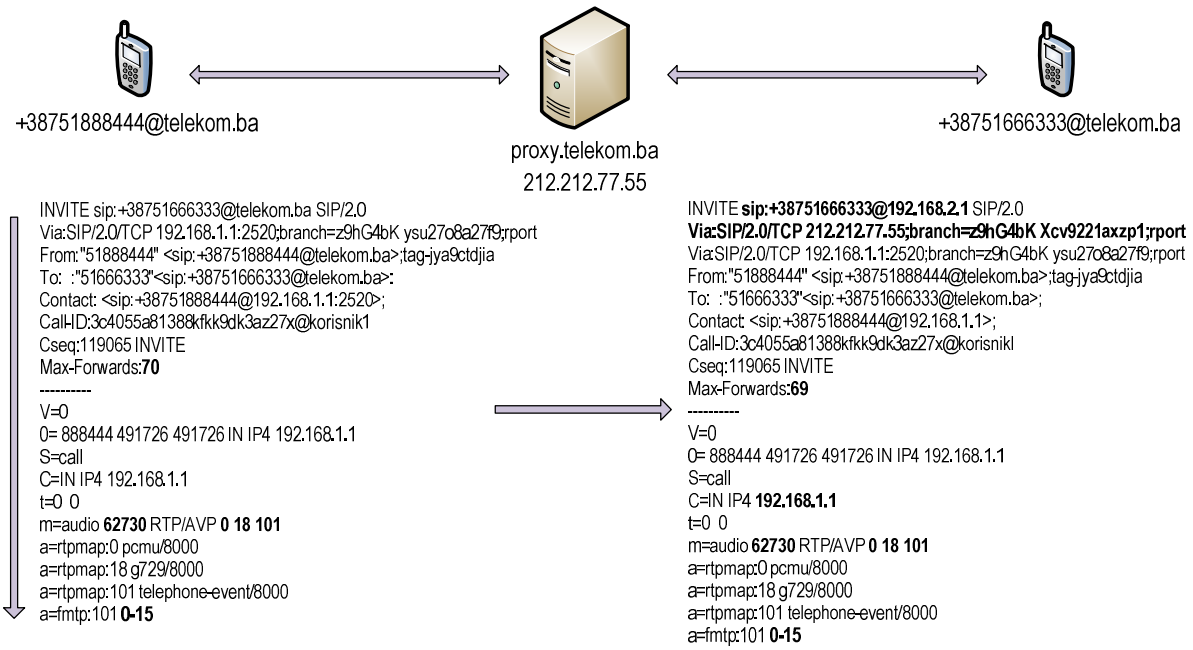
zaštite saobraćaja koji dolazi kroz razmjenu sa drugim operatorima, (NNI SBC – *Network Network Interface SBC*), kao i u *enterprise* scenariju. Zbog mogućnosti povećanja performansi i skalabilnosti SBC se hardverski dijeli na namjenske komponente za obradu signalizacionih i medija tokova, koji međusobno komuniciraju koristeći protokole kao što je MEGACO [1].

Ova modularnost omogućava operatorima nezavisno planiranje kapaciteta i funkcionalnosti medija i signalizacionih modula. U uslovima novog mrežnog okruženja nastalog stalnim razvojem telekomunikacionih mreža, javljaju se potrebe za razvojem novih funkcionalnosti kao i potreba za migracijom nekih postojećih funkcionalnosti sa pojedinih mrežnih elemenata na SBC. SBC funkcionalnosti se danas nude kao virtuelna rješenja koja mogu biti instalisana na operatorovom hardveru u okviru *cloud* rješenja. Od proizvođača SBC-a se očekuje da ponude otvorene interfejse koji će omogućiti laku integraciju u postojeću infrastrukturu korištenu za prenos multimedijalnih servisa.

II. OPŠTI NAČIN FUNKCIONISANJA SBC-A

Na sl. 1 prikazan je tok SIP INVITE poruke između pozivajućeg i pozvanog učesnika, UA (*User Agent*) preko proksi servera [4]. Prikazan je pojednostavljen model gdje se između pozivajućeg i pozvanog UA nalazi samo jedan proksi server. Zadatak proksi servera je da identifikuje lokaciju pozvanog UA na osnovu IP adrese i proslijedi zahtjev za pozivom (INVITE poruku) ka njoj, pri tome u *Via* polje zaglavlja dodaje svoju adresu kao indikator koji ukazuje na put kojim se odgovor treba vratiti. *Proxy* ne mijenja informacije o dijalogu, kao što su *tag* polje u *From* liniji zaglavlja, *Call-id* ili *Cseq* polje. *Proxy* takođe ne mijenja informacije prisutne u tijelu SIP poruke. Tokom faze inicijalizacije sesije UA-i razmjenjuju SIP poruke koje sadrže SDP (*Session Description Protocol*) tijelo poruke sa adresama na koje pojedini UA očekuju da medija bude isporučena, odnosno to su adrese preko kojih će se razmjenjivati saobraćaj [5]. Nakon uspješno završene faze inicijalizacije sesije, UA-i mogu direktno razmjenjivati mediju bez posredovanja proksija. SBC-ovi se javljaju u različitim konfiguracijama, opremljeni različitim funkcionalnostima, zavisno od potreba operatora i ciljeva koji se žele postići. U opštem slučaju mogu se identifikovati određena svojstva koja su zajednička za većinu SBC uređaja implementiranih kao B2BUA (*Back-to-Back User Agent*).

B2BUA kao i proksi server dijele SIP transakciju u dva dijela. Jedna strana je okrenuta ka UAC-u (*User Agent Client)* i radi kao server, druga je okrenuta ka UAS-u (*User Agent Server*) i radi kao *client*. Dok *Proxy* uobičajeno čuva stanje informacija vezanih za aktivne transakcije, B2BUA-i čuvaju informacije vezane za aktivne dijaloge (npr. pozivi u toku). Ovo znači da će proksi prilikom prijema SIP zahtjeva čuvati informacije o njemu toliko dugo dok se transakcija ne završi, odnosno dok ne stigne odgovor na poslani zahtjev. Neposredno poslije toga informacije vezane za ovu transakciju će biti obrisane. B2BUA će stanje informacija držati za vrijeme trajanja dijaloga, tj. po završetku (terminaciji) poziva ove informacije će biti obrisane [6].



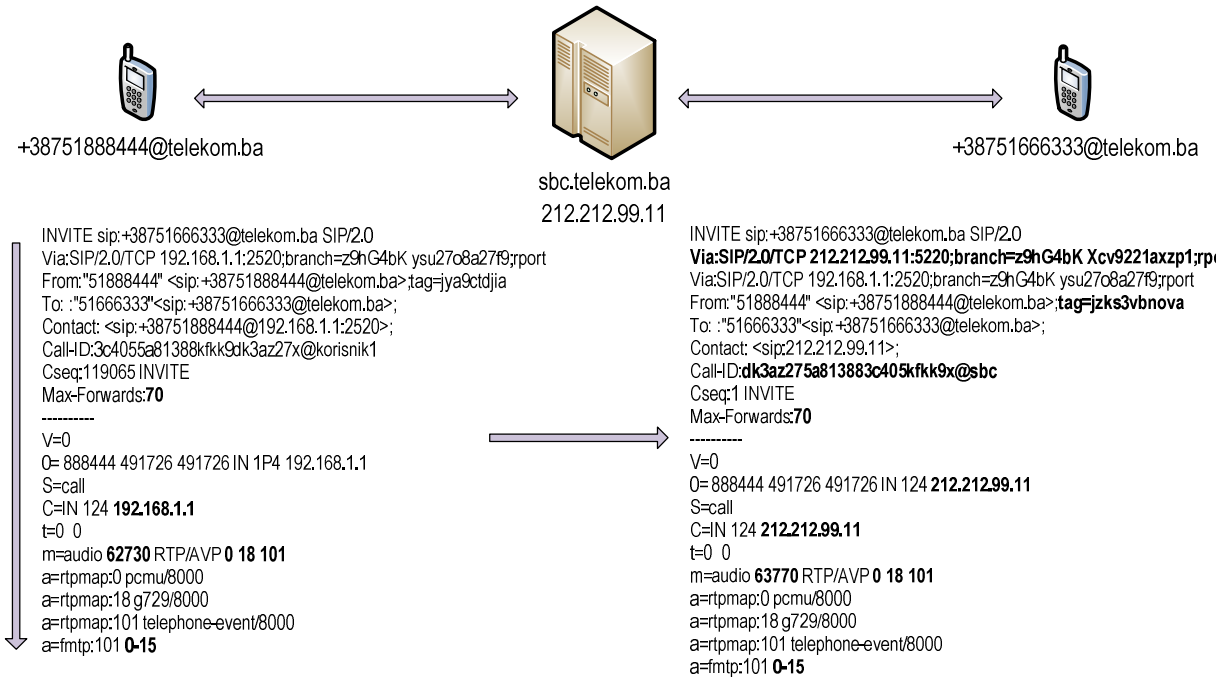
Slika 1. Pojednostavljen SIP *call flow* sa proksi serverom kao posrednikom

Na sl. 2 prikazan je pojednostavljen tok SIP poziva ali u ovom slučaju je između pozvanog i pozivajućeg UA posrednik SBC umjesto proksi servera.

SBC radi kao B2BUA tako da se ponaša kao UAS prema pozivajućem UA, a kao UAC prema pozvanom UA. U ovom slučaju SBC terminira poziv koji je generisao pozivajući UA i

generiše novi poziv ka pozvanom UA. INVITE poruka koju SBC šalje u postupku generisanja novog poziva više nije referencirana na pozivajućeg UA. INVITE poruka koju sada šalje SBC ka proksiju sadrži *Via* i *Contact* polje SIP zaglavlja koje ukazuje da je SBC pošiljaoc poruke, a ne više pozivajući UA. SBC takođe rukuje informacijama u navedenim poljima *Call-Id* i *From.* U slučaju kada je SBC konfigurisan da vrši nadzor nad medija saobraćajem tada on vrši promjenu adresnih informacija sadržanih u „c" i „m" linijama SDP tijela poruke. Osim SIP poruka preko SBC-a će prelaziti i audio i video paketi. Kako INVITE poruka poslana od strane SBC-a uspostavlja novi dialog, SBC će takođe vršiti upis novih vrijednosti, za polja *Cseq* i *Max-Forwards* [7].

Moguće su i opcije u kojima SBC ne vrši promjenu informacija vezanih za dijalog, čak u posebnim slučajevima, ni promjenu adresnih informacija.



Slika 2. Pojednostavljen prikaz SIP *call flow*-a sa SBC-om kao posrednikom

III. SKRIVANJE TOPOLOGIJE MREŽE

Svrha skrivanja topologije mreže je u ograničavanju informacija o vlastitoj mreži, koje bi mogle postati dostupne korisnicima koji pristupaju iz vanjskih, stranih mreža. Mrežni operatori imaju zahtjeve za ovom funkcionalnošću, zato što ne žele da IP adrese njihove *core* opreme (proksi serveri, gejtveji, aplikacioni serveri, softsvičevi, IMS *(IP Multimedia Subsystem),* servisne platforme i drugi mrežni elementi) budu vidljive izvana [8]. Razlozi leže u mogućoj izloženosti ove opreme DoS/DDoS (*Distributed DoS*) napadima, mogućoj zloupotrebi i neovlaštenom korištenju resursa mreže od strane drugih operatora u određenim saobraćajnim situacijama. Takođe, postoje i razlozi skrivanja unutrašnje arhitekture i organizacije mreže od konkurenata pa čak i od partnera. U nekim slučajevima korisnici žele sakriti adrese svoje opreme, odnosno modifikovati SIP poruke koje mogu sadržati privatne statičke adrese.

Najčešći način skrivanja topologije mreže je skidanje *Via* i *Record-Route* polja iz SIP zaglavlja, kao i promjena sadržaja *Contact* polja i *Call-ID*-a. Međutim, na mjestima na kojim se koriste IP adrese umjesto naziva domena u SIP zaglavlju, to se ne može uraditi na taj način. Takva polja su npr. *From* i *To*. SBC može zamijeniti ove IP adrese sa vlastitom IP adresom ili imenom domena.

Naravno, pored postavljanja SBC-a na ulazu u mrežu, postoje i drugi načini skrivanja informacija o topologiji mreže. Jedan od načina je i korišćenje UA *privacy* mehanizma, gdje UA može olakšati prikrivanje mrežne topologije, ali to nije tema ovog rada.

Skrivanje topologije mreže korišćenjem SBC-a u scenariju nepostojanja saglasnosti, odnosno "ne znanje" korisnika nosi određene probleme. Ova funkcionalnost je bazirana na *hop-by-hop* povjerljivom modelu, za razliku od *end-to-end* modela po kom funkcioniše SIP protokol. Promjena parametara u pojedinim porukama SIP zaglavlja, bez pristanka korisnika, mogla bi potencijalno modifikovati ili promijeniti korisničke informacije koje se tiču privatnosti, sigurnosti i uticati na aplikacije višeg nivoa koje ostvaruju komunikaciju s kraja na kraj koristeći SIP protokol.

UA nema mogućnost da razlikuje MITM (*Man-In-The-Middle*) napad od aktivnosti SBC-a. Funkcionalnost skrivanja mrežne topologije ne radi dobro sa *Authenticated Identity Management* mehanizmom u scenariju u kom SBC nema neku vrstu saglasnosti korisnika. *Authenticated Identity*

Management mehanizam je baziran na *hash* vrijednosti koja se izračunava na osnovu vrijednosti parametara: *From*, *To*, *Call-ID*, *CSeq*, *Date* i *Contact* polja SIP zaglavlja, plus vrijednost parametara iz cijelog tijela poruke. Ako SBC ne obezbjeđuje servis autentifikacije može doći do promjene sadržaja navedenih polja SIP zaglavlja**.** Npr. mijenja se sadržaj *Contact* polja u SIP zaglavlju. Ovo za rezultat ima nemogućnost *end-to-end* komunikacije, jer se *hash* vrijednost sada izračunava na osnovu promijenjenih parametara i neće se poklopiti sa očekivanom. Ovo je riješeno tako što je SBC opremljen funkcionalnošću koja obezbjeđuje servis autentifikacije.

Kao rezultat uspostave SIP sesije, krajnjim korisničkim tačkama biće poznate IP adrese na koje će slati, odnosno sa kojih će primati medija sadržaj. Ovo znači da će npr. korisnik koji koristi SIP protokol za uspostavu veze sa PSTN brojem znati IP adresu PSTN gejtveja koji je odgovoran za povezivanje VoIP servisa sa PSTN mrežom. Takođe, tokom faze uspostave sesije proksi serveri će upisati svoje adrese u *Via* polje SIP zaglavlja. Moguća je zloupotreba ovih informacija od strane pojedinih korisnika, kako u cilju napada na proksi servere operatora i onemogućavanje servisa, tako i zloupotreba mogućnosti direktnog pristupa PSTN gejtvejima, neovlašteno korišćenje resursa, npr. generisanja saobraćaja koji neće biti korektno tarifiran.

Da bi se sakrili podaci o elementima unutrašnje mreže operatora, sve poruke koje šalju elementi unutrašnje mreže se prenose ka spoljnjim mrežama preko SBC-a. SBC mijenja podatke u poljima SIP zaglavlja upisijući u njih svoje podatke. Nadalje će u poljima SIP zaglavlja kao što su *Contact*, *Record-Route* i sličnim, kao i u tijelu poruke egzistirati samo adrese SBC-a.

U narednom primjeru funkcionalnosti skrivanja topologije mreže, SBC radi kao B2BUA (*Back-to-Back User Agent*) i uklanja sve informacije o topologiji mreže, kao npr. unešene vrijednosti za *Via* i *Record-Route* polja iz odlaznih poruka.

Posmatraće se sledeći mogući scenario: SBC (*sbc.telekom.ba*) prima INVITE zahtjev iz vlastite, unutrašnje mreže (*inner network*), što je u ovom slučaju mreža mrežnog operatora. U datom primjeru *+38751888444@telekom.ba* u procesu uspostave poziva šalje INVITE poruku ka *+38751666333@telekom.ba*. SBC, koji se nalazi na putanji ove poruke, prima originalnu poruku u obliku u kom ju je *+38751888444@telekom.ba* poslao.

Na sl. 3 dat je prikaz originalne SIP poruke pre skrivanja topologije mreže.

```
INVITE sip:+38751666333@telekom.ba SIP/2.0
Via: SIP/2.0/UDP proxy3.telekom.ba;branch z9hG4bK48j0w174131.1
Via: SIP/2.0/UDP proxy2.telekom.ba;branch z9hG4bK18an6i9234172.1
Via: SIP/2.0/UDP proxy1.telekom.ba;branch z9hG4bK39bn2e5239289.1
Via: SIP/2.0/UDP 192.168.1.1;branch z9hG4bK92fj4u7283927.1
Contact:<sip:+38751888444@192.168.1.1:2520>;
Record-Route: <sip: proxy3.telekom.ba;lr>
Record-Route: <sip: proxy2.telekom.ba.com;lr>
Record-Route: <sip: proxy1.telekom.ba;lr>
```

Slika 3. Prikaz INVITE *Request* poruke pre skrivanja topologije mreže

SBC izvršava funkciju skrivanja topologije mreže, tako što uklanja sva postojeća *Via* i *Record-Route* polja u zaglavlju SIP poruke i postavlja umjesto njih *Via* i *Record-Route* polja sa vlastitim SIP URI-jem (*Uniform Resource Identifier*). Sl. 4 prikazuje izgled izmijenjene SIP poruke.

```
INVITE sip:+38751666333@telekom.ba SIP/2.0
Via: SIP/2.0/UDP sbc.telekom.ba;branch=z9hG4bK92es3w230129.1
Contact: :<sip:+38751888444@l92.168.1.1:2520>;
Record-Route: <sip: sbc.telekom.ba;lr>
```

Slika 4. Izgled INVITE *Request* poruke poslije skrivanja topologije mreže

Kao i proksi server koji upisuje *Record-Route* parametar pri prosleđivanju SIP poruka i SBC rukuje svim pojedinačnim porukama u okviru datog SIP dijaloga. Ako SBC, iz nekog razloga, bude restartovan moguć je gubitak dijela informacija koje su bile u postupku obrade u tom trenutku. Npr. slučaj u kom je obrada informacija nasilno prekinuta usljed gubitka napajanja SBC-a. Tada SBC neće biti u stanju da ispravno rutira pristigle poruke. Priroda nastalog problema će zavisiti od dijela informacija koje su izgubljene u ovom događaju.

Ovo je bio primjer skrivanja topologije mreže, odnosno informacija o mrežnim elementima *core* mreže operatora. Po-red skrivanja mrežne topologije SBC može izvršavati funkciju skrivanja identiteta, odnosno informacija vezanih za identitet korisnika. Prilikom skrivanja identiteta korisnika SBC mijenja vrijednost u polju *Contact* SIP zaglavlja, kao i u drugim poljima koja sadrže informacije vezane za identitet korisnika. U SIP zaglavlju su definisana sljedeća polja koja sadrže informacije o identitetu korisnika: "*Contact*", "*P-Asserted-Identity*", "*Referred-By*", "*Identity*" i "*Identity-Info*".

IV. MEDIJA MONITORING I MEDIJA MENADŽMENT

Nadgledanje i upravljanje medija saobraćajem *(Media Traffic Management)* je funkcija kontrole medija strimova. Mrežni operatori mogu zahtijevati da ove funkcionalnosti budu aktivirane u cilju kontrole saobraćaja prenošenog kroz vlastitu mrežu. *Media Traffic Management* pomaže i u kreiranju različitih vrsta *billing* modela za različite servise. Npr. video telefonija može biti i jeste tarifirana drugačije od čisto govornih servisa, takođe omogućava operatorima korišćenje određenih kodeka, pri čemu su zahtjevi za propusnim opsegom različiti, što za posljedicu može imati i različitu tarifu. Jedan od dodatnih slučaja korišćenja *Media Traffic Management*-a je zakonsko presretanje saobraćaja u okviru zakonskih regulativa. Funkcionalnost zakonskog presretanja saobraćaja je prvo i najčešće primjenjivana kod govornog servisa, mada tehnološke mogućnosti i zakonske regulative obuhvataju i druge oblike saobraćaja, odnosno pojedine vrste servisa u okviru njih. Kontrola *e-mail* servisa u svrhu zakonskog presretanja postepeno je ušla u upotrebu. Mrežni operatori posjeduju tehničku infrastrukturu koja im to omogućava. To su SIP proksi serveri koji rade kao B2BUA, a koji mogu biti i posebni mrežni elementi ili je ta funkcionalnost implementirana u okviru SBC-a, pri čemu su zakonski preduslovi podrazumijevani.

U opštem slučaju su medija tokovi nezavisni od signalizacionih tokova, tj. medija i signalizacioni tokovi ne moraju da prelaze iste putanje. Međutim kada u mreži postoji SBC, medija pri ulasku u mrežu prelazi preko SBC-a prilikom čega SBC, pored modifikacije polja u SIP zaglavlju, vrši i modifikaciju opisa sesije u tijelu poruke. Modifikacijom opisa sesije SBC može isforsirati slanje medija tokova preko određenih linkova na kojima će biti zadovoljeni zahtjevi za određenim QoS (*Quality of Service*) nivoom ili osigurati da pretplatnik koristi samo određene, dozvoljene kodeke pri realizaciji datog servisa. Važno je napomenuti da SBC nema direktne veze sa ruting topologijom i da SBC ne radi promjenu rezervacije propusnog opsega u TE (*Traffic Engineering*) tunelima niti ima direktnu interakciju sa ruting protokolima (npr. RIP – *Routing Information Protocol*, OSPF – *Open Shortest Path First*).

Pojedini operatori ne žele upravljati saobraćajem, ali ga žele nadgledati, kako bi osigurali informaciju o stepenu ispunjenja uslova iz SLA (*Service Level Agreements*) prema svojim korisnicima ili partnerima. Sa stanovišta SBC-a, potrebni preduslovi za nadgledanje saobraćaja su iste kao i za upravljanje saobraćajem, s tim da se razlikuje sam postupak kao i rezultati.

SBC-ovi su funkcionalno osposobljeni za rad sa „*lost* BYE" problemom. Radi se o scenariju u kom jedna od krajnjih tačaka otkaže u toku trajanja sesije. SBC može detektovati da je slanje medije prekinuto i poslati BYE poruku za obe strane u svrhu čišćenja zaostalih stanja vezanih za raskinutu sesiju u elementima mreže koji su posredovali u prosleđivanju sesije kao i u krajnjim tačkama.

Jedan od mogućih oblika *Media Traffic Management*-a je SBC terminiranje medija tokova i SIP dijaloga generisanjem BYE zahtjeva. Ova vrsta procedure može biti zastupljena u situaciji kada *prepaid* korisniku ponestane kredita. Medija menadžment će osigurati da korisnik ne može ignorisati BYE zahtjev generisan od strane SBC-a i da ne može nastaviti slanje medije i nakon isteka kredita.

Implementacija *Media Traffic Management*-a na ovaj način zahtijeva mogućnost pristupa i modifikacije SDP-a *(Session Description Protocol)* od strane SBC-a. Prilikom uspostave sesije parametri sesije mogu biti ponuđeni od strane pozivajućeg UA u okviru INVITE poruke i prihvaćeni u ponuđenom ili redukovanom obliku u okviru 200 OK poruke od strane pozvanog UA, ili ponuđeni u okviru 200 OK poruke od strane pozvanog UA, a prihvaćeni u okviru ACK poruke od strane pozivajućeg UA. Shodno tome ovaj pristup neće funkcionisati ako UA vrši kriptovanje ili na drugi način obezbjeđuje zaštitu integriteta tijela poruke u *end-to-end* komunikaciji. Modifikacija poruke ili tijela poruke bez saglasnosti ili pristanka pretplatnika dovodi do situacije u kojoj UA nema načina da razlikuje SBC akciju od MITM *(Man-In-The-Middle)* napada. Ovo je u suprotnosti sa *Authenticated Identity Management*-om. Rješenje je implementacija *Authenticated Identity Management* funkcionalnosti u okviru skupa SBC funkcionalnosti.

Ako prenos medije nije odrađen na odgovarajući način može doći do prekida rada funkcija kao što su ECN (*Explicit Congestion Notification*) i PMTUD (*Path Maximum Transmition Unit Discovery*). Prenos medije može vrlo lako dovesti do prekida pojedinih funkcionalnosti IP i transportnog sloja koje zavise od pravilne konfiguracije pojedinih polja u zaglavljima ovih protokola. Posebno osjetljiva polja su ECN i ToS (*Type of Service*), kao i DF (*Don't Fragment*) bit.

Način na koji *Media Traffic Management* funkcioniše otežava uvođenje novih servisa. Potrebno je da SBC bude opremljen tako da može da podrži nove oblike komunikacija. Jedan od uslova je mogućnost nadgradnje SDP protokola prije puštanja u rad novog servisa, što je dodatni zahtjev pri puštanju novih servisa.

Ako SBC vrši usmjeravanje više medija strimova kroz centralne tačke u mreži, to lako može uzrokovati značajne količine dodatnog saobraćaja ka ovim tačkama, što može stvoriti usko grlo u mreži i uzrokovati zagušenje pojedinih linkova. U ovoj situaciji SBC može poslati poruke koje korisnik neće moći primiti i identifikovati kao i poruke koje dolaze u okviru dijaloga sa *peer* entitetom ili sa SIP *Registrar* ili *Proxy* serverom. Zbog toga je potrebno izvršiti proračun saobraćaja koji će se usmjeravati preko pojedinih mrežnih elemenata, uključujući i SBC, kako bi se obezbijedili optimalni resursi koji garantuju funkcionisanje sistema i poštovanje SLA za pojedine korisnike i pojedine servise i u uslovima maksimalnog opterećenja mreže.

Primjer upravljanja saobraćajem može biti prikazan na sljedeći način. Neka SBC radi kao B2BUA, pod kontrolom je operatora i nalazi se na medija putanji, odnosno medija tokovi su usmjereni ka SBC-u. U praksi SBC vrši modifikaciju opisa sesije u SIP poruci. SBC prima medija saobraćaj od jednog UA i prosljeđuje ga ka drugom UA. Pri prenosu medije u suprotnom pravcu SBC izvršava identične operacije. Kao što je ranije pomenuto ograničavanje tipa kodeka je oblik *Media Traffic Management*-a. SBC ograničava izbor kodeka u postupku dogovaranja, tj. razmjene ponuda i odgovora između UA. Kao rezultat procesa dogovaranja o parametrima prenosa, vrši se modifikacija opisa sesije. Poslije usaglašavanja i modifikacije opisa sesije SBC vrši provjeru da li su parametri medija strima u saglasnosti sa dogovorenim. Ako se medija strim razlikuje od dogovorenog, SBC ima mogućnost da raskine sesiju i/ili podigne alarm.

Razmotriće se scenario gdje SBC prima INVITE zahtjev iz vanjske meže, u ovom slučaju je to pristupna mreža (*Access scenario* [3]). Sl. 5 daje prikaz SDP opisa sesije primljene SIP poruke.

U ovom slučaju, SBC izvršava funkciju *Media Traffic Management*-a modifikujući „m" (*media*) liniju i uklanjajući jednu „a" (*attribute*) liniju u skladu sa eksternim ograničenjima. Sl. 6 daje prikaz opisa sesije usaglašenog sa eksternim ograničenjima, odnosno mogućnostima, u jednom od koraka usaglašavanja.

```
v=0
o=888444 491726 491726 IN IP4 192.168.1.1
c=IN IP4 192.168.1.1
m=audio 49230 RTP/AVP 96 98
a=rtpmap:96 L8/8000
a=rtpmap:98 L16/16000/2
```

Slika 5. Sadržaj SDP-a u zahtjevu za prioritetizaciju *Media Traffic Management*-a

```
v=0
o=888444 2890844526 2890842807 IN 1P4 192.168.1.1
c=IN IP4 192.168.1.1
m=audio 49230 RTP/AVP 96
a rtpmap:96 L8/8000
```

Slika 6. Izgled opisa sesije nakon izvršene *Media Traffic Management* funkcije

Problemi se mogu pojaviti prilikom puštanja u rad novih servisa. Svi SBC elementi u mreži bi trebali biti *upgrade*-ovani zajedno sa krajnjim korisničkim uređajima. Važno je napomenuti da su mogući problemi sa poljima zaglavlja koja se odnose na npr. funkcionalnost skrivanja topologije mreže.

Određena proširenja koja ne zahtijevaju aktivne manipulacije SDP-om mogu biti uspješno implementirana bez *upgrade*-a postojećih SBC elemenata u mreži [9]. U slučajevima potrebe za *upgrade*-om mora se voditi računa da se ne ugroze postojeći servisi.

V. ZAKLJUČAK

U uslovima sve oštrije konkurencije na rastućem telekomunikacionom tržištu, za ispunjavanje ugovorenih obaveza o isporuci servisa (SLA), nužno je konstantno nadgledanje i kontrola parametara mreže i isporučenog servisa, kako bi se osigurao nivo dostupnosti i kvalitet isporučenog servisa naveden u SLA. SBC funkcionalnosti nadgledanja i upravljanja medija strimovima i QoS-om u potpunosti ispunjavaju ove zahtjeve i u scenariju kontrole pristupa (UNI SBC) i u scenariju razmjene saobraćaja sa drugim operatorima (NNI SBC). Za očuvanje i unapređenje konkurentske pozicije na telekomunikacionom tržištu i zaštitu od neovlaštenog i/ili zlonamjernog korišćenja resursa vrlo je bitna implementacija funkcije skrivanja topologije mreže. Ova funkcionalnost je uspješno realizovana u okviru periferne zaštite pozicioniranjem SBC-a između *core* i pristupne mreže mrežnog operatora, odnosno u graničnom području između mreža različitih operatora. Kako bi se obezbijedilo normalno funkcionisanje SBC mrežnog elementa, u oba navedena scenarija, potrebno je izvršiti proračun saobraćaja koji se preko njega usmjerava, u uslovima maksimalnog mrežnog opterećenja i osigurati mrežne resurse za optimalan rad svih elemenata u mreži.

Može se zaključiti da je funkcija nadgledanja i menadžmenta medija strimova, kao i finkcija skrivanja topologije mreže uspješno realizovana u okviru SBC funkcionalnosti i da predstavlja jedno od mogućih rješenja za ovaj rastući problem. Preporuka je da se dalje istraživanje nastavi u pravcu integracije SBC funkcionalnosti u *cloud* rješenje.

LITERATURA

[1] D. Nemec, D. Vukobratović, V. Crnojević, Č. Stefanović, "Tehnologija VoIP sistema", Katedra za telekomunikacije i obradu signala, Fakultet tehničkih nauka, Novi Sad, 2007.

[2] R. Mahy, P. Matthews, J. Rosenberg, "Traversal Using Relays around NAT (TURN): Relay Extensions to Session Traversal Utilities for NAT (STUN)", RFC 5766, IETF, 2010.

[3] D. Botić, D. Nemec, S. Vujčić, "Analiza funkcionalnosti SBC kontrolera u različitim scenarijima primjene", XXIII Festival informatičkih dostignuća INFOFEST 2016, Festivalski katalog, Ministarstvo za informaciono društvo i telekomunikacije Crne Gore, pp. 122-129, Budva, Septembar 2016.

[4] J. Rosenberg, H. Schulzrinne, G. Camarillo, A. Johnston, J. Peterson, R. Sparks, M. Handley, E. Schooler, "SIP: Session Initiation Protocol", RFC 3261, IETF, 2002.

[5] M. Handley, V. Jacobson, C. Perkins, "SDP: Session Description Protocol", RFC 4566, IETF, 2006.

[6] Andrew Prokop, "The Back-to-Back User Agent (B2BUA)", https://andrewjprokop.wordpress.com/2013/12/27/the-back-to-back-user-agent-b2bua/, December, 2013.

[7] J. Hautakorpi, G. Camarillo, R. Penfield, A. Hawrylyshen, M. Bhatia, "Requirements from Session Initiation Protocol (SIP) Session Border Control (SBC) Deployments", RFC 5853, IETF, 2010.

[8] 3GPP, "IP Multimedia Subsystem (IMS)"; Stage 2, 3GPP TS 23.22810.0.0, Mart 2010

[9] M. Handley, V. Jacobson, C. Perkins, "SDP: Session Description Protocol", RFC 4566, IETF, 2006.

ABSTRACT

SBC controllers in VoIP networks have several functions that includes: function group for peripheral defense (access control, hiding network topology, prevention of DoS/DDoS attacks), functions that solve availability of network endpoints (NAT/FW transversal, interworking and repair protocol) and functionality of media management, media monitoring and QoS. This paper present SBC functionality of hiding network topology from the group of peripheral defense functions as well as media monitoring and media management functionality, marking their importance in maintaining the market position of network operators and the protection of own resources against unauthorized use and/or abuse. In order to understand the potential problems that may arise using SIP protocol in public telecommunications networks, in this paper general mode of operation of SBC controller is described.

HIDING TOPOLOGY AND MEDIA TRAFFIC MANAGEMENT IN VOIP NETWORKS USING SBC

Dragan Botić, Dejan Nemec, Siniša Vujčić