# Detektovanje i rešavanje incidentne situacije u domenu nadzora telekomunikacione mreže

Ivan Josifović, *Telekom Srbija a.d.*, Jelena M. Stojanović, *Telekom Srbija a.d.,* Đorđe S. Radović, *Telekom Srbija a.d.*

*Sadržaj* - **Raspoloživost i kvalitet servisa kao krajnjeg produkta predstavlja prioritet u radu svakog telekomunikacionog operatera. U radu je opisan konkretan način detektovanja incidentne situacije u domenu nadzora telekomunikacione mreže, njena brza analiza u cilju lociranja uzroka problema i proces rešavanja samog incidenta. Centralno mesto u ovim procesima zauzima operativni centar NOC (*Network Operations Center*), odgovoran za nadgledanje mreže u smislu alarma i incidenata kako bi se sprečio njihov moguć negativan uticaj na performanse mreže koje se dalje oslanjaju na kvalitet servisa kod krajnjih korisnika.**

*Ključne reči* — **servis, nadzor, kontrola kvaliteta, NOC**

## I. Uvod

Za svakog savremenog telekomunikacionog operatera veoma je važno da odgovori na zahteve svojih korisnika time što će pored širokog i raznovrsnog spektra servisa korisnicima pružiti i garantovati kvalitetan i pouzdan rad istih. U današnje vreme značajne prednosti u telekomunikacionim tehnologijama donosi heterogeno okruženje za korisnike i provajdere servisa. Ova heterogenost postoji u različitim oblastima poput tehnologija pristupa, mreža za transport, mreža za komutaciju, korisničkih terminala, aplikacija, itd. Sposobnost da se obezbedi inherentan i adaptivan kvalitet servisa u takvom heterogenom okruženju je ključ za uspeh kod sledeće generacije komunikacionih sistema. U cilju postizanja dobrih vrednosti parametara koji služe za ocenu rada kako servisa tako i celokupne mreže, QoS (*Quality of Service*) - parametri kvaliteta servisa i QoE (*Quality of Experience*) - parametri zadovoljstva prosečnog korisnika servisom u mreži, jedno od ključnih mesta zauzima nadzor rada i kontrola kvaliteta servisa. Na ovaj način se, zapravo, ogleda stvarno funkcionisanje mreže koje kao rezultat ima popularnost određenih servisa na tržištu kao i konkurentnost samog telekomunikacionog operatera. Stalni razvoj novih tehnologija i mrežne infrastrukture koju čini veliki broj uređaja različitih proizvođača zahteva dobro organizovan, centralizovan nadzor i kontrolu kvaliteta rada mreže koji se u Telekomu Srbija obavljaju u *Network Operations Center-u* (NOC).

U ovom radu opisan je konkretan način detektovanja incidentne situacije u domenu nadzora telekomunikacione mreže, njena brza analiza u cilju lociranja uzroka problema u mreži i proces rešavanja samog incidenta. Drugo poglavlje opisuje arhitekturu sistema za nadzor i kontrolu kvaliteta mreže, kao i njegove osnovne karakteristike. U trećem poglavlju opisana je jedna incidentna situacija na primeru telekomunikacionog servisa baziranog na GSM/UMTS tehnologiji i uloga NOC-a u njoj.

Ivan Josifović, Telekom Srbija a.d., Katićeva 14-18, 11000 Beograd, Republika Srbija (e-mail: ivan.josifovic@telekom.rs)

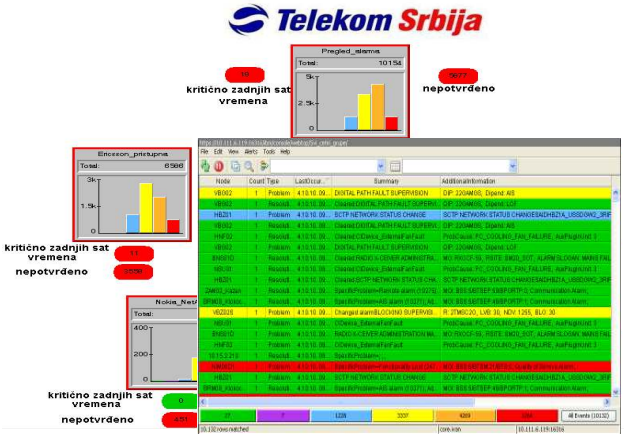
Jelena M. Stojanović, Telekom Srbija a.d., Katićeva 14-18, 11000 Beograd, Republika Srbija (e-mail: jelena.m.stojanovic@telekom.rs)

Đorđe S. Radović, Telekom Srbija a.d., Katićeva 14-18, 11000 Beograd, Republika Srbija (e-mail: djordje.radovic@telekom.rs)

## II. Sistemi za nadzor rada servisa u NOC-u

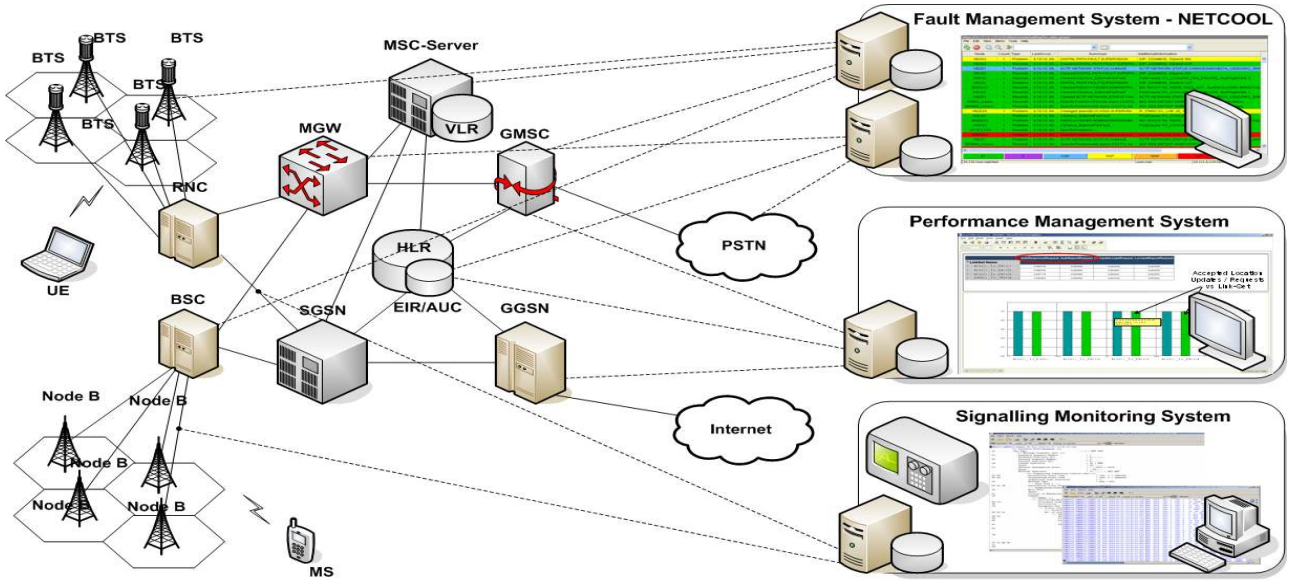
U svakom trenutku, *Network Operations Center* (NOC) ima potpunu i blagovremenu informaciju o stanju mreže i alarmima na mrežnim elementima. Nadzor možemo posmatrati kroz nekoliko domena poput: *Fault Management System* (FMS) i *Performance Management System* (PMS) u kombinaciji sa sistemima za nadzor signalizacije. Mrežni element je osnovni entitet u sistemu - uređaj. Ovaj sistem je dizajniran tako da može da podrži konstantno širenje mreže i raznovrsnost servisa.

FMS predstavlja skup funkcija (procesa) za otkrivanje, izolovanje i otklanjanje smetnji u telekomunikacionoj mreži u cilju što manjeg uticaja istih na krajnje korisnike servisa. Ovi procesi obuhvataju čuvanje i ispitivanje *log-ova* koji sadrže podatke o smetnjama u mreži, prihvatanje i delovanje na obaveštenja o detektovanju greške (alarmi), praćenje i identifikovanje kvarova, obavljanje niza dijagnostičkih testova, izveštavanje o stanju smetnje.




Sl.1. Prikaz FMS *interfeace-a* (*IBM NetCool platforma*)

U korporativnu mrežu Telekoma Srbija je implementiran *Fault Management System* (IBM NetCool platforma) koji omogućava centralizovan nadzor svih mrežnih elemenata različitih proizvođača i tehnologija, tako da su sve informacije u vezi sa greškama dostupne u realnom vremenu na jednom mestu. Sistem prikuplja informacije o stanju mrežnih elemenata, internet servisa,




Sl. 2. Prikaz arhitekture mreže i načina povezivanja uređaja za nadzor

multimedijalnih servisa, baza podataka i aplikacija. Netcool pored prikupljanja alarma sa svih mrežnih elemenata i servisnih platformi vrši njihovu analizu i korelaciju, što kao konačan rezultat daje jasnu sliku o stanju rada mreže, odnosno posmatranog servisa. Pomoću ovog sistema moguće je dobiti detaljne izveštaje o funkcionalnosti nekog mrežnog elementa.

PMS je skup alata i procesa koji omogućavaju prikupljanje, praćenje i analizu pokazatelja dobijenih sa mrežnih elemenata. Ovi pokazatelji ukazuju na normalno ili abnormalno ponašanje u mreži koje može uticati na korektno funkcionisanje servisa, a ogleda se u broju pokušaja uspostavljanja poziva, broju prekinutih poziva pre/posle uspostavljanja veze, vreme potrebno za uspostavljanje poziva, broj uspešnih/neuspešnih *Paging* procedura, broj uspešnih/neuspešnih *Handover-a* (HO) itd.

Između posmatranih parametara postoji međusobna zavisnost koja je izražena KPI/KQI (*Key Performance Indicator/Key Quality Indicator*) pokazateljima raspoloživosti servisa u mreži kao što su uspešnost uspostavljanja poziva, uspešnost *Paging* procedura, uspešnost HO-a, ukupan saobraćaj u mreži itd. Dobre vrednosti parametara KPI i KQI predstavljaju osnov na kom mogu biti zasnovani interni i eksterni SLA (*Service Level Agreements*) ugovori. Poboljšanje performansi mreže i kvaliteta servisa neminovno dovodi do boljeg iskorišćenja mreže i kvalitetnijeg funkcionisanja servisa.

Sistem za nadzor signalizacije je platforma koja pruža potpuno praćenje i kontrolisanje protokola u konvergentnim mrežama (GSM, GPRS, UMTS, SS7, VoIP) *s kraja na kraj*. Nadzor i analizu signalnih poruka je moguće ostvariti u realnom vremenu, istorijskom modu i preko sveobuhvatnih izveštaja u željenim vremenskim intervalima. Pogodnosti ovog sistema su što podatke iz mreže pretvara u konkretne informacije, utiče na kvalitet servisa (QoS) i optimizaciju mreže, smanjuje kompleksnost u upravljanju konvergentnim mrežama i servisima. Ovaj sistem omogućuje nadzor signalizacije različitih tehnologija i protokola po svim signalnim *link-ovima* između mrežnih elemenata. To je jedinstven sistem kako za domen komutacije kola, tako i za domen komutacije paketa i zbog toga je moguće pratiti celu mrežu kao jedinstvenu platformu, bez potrebe tretiranja svakog mrežnog servisa i mrežnog segmenta kao posebnog entiteta. Platformu čini centralni server koji predstavlja srce sistema, na koji su paralelno (pomoću *probe* elemenata) povezani signalni *link-ovi* između mrežnih elemenata nad kojima se vrši nadzor. Svaka signalna poruka koja se generiše pri komunikaciji unutar mreže ili pri komunikaciji mrežnih elemenata sa opremom krajnjeg korisnika beleži se na sistemu za nadzor signalizacije. Analizom ovih *dialog-a* dolazimo do lokalizacije problema kao i do njegovog rešenja.

Ovim sistemima se vrši nadzor i kontrola kvaliteta u mreži Telekoma Srbija. Na sl. 2. je prikazana uprošćena arhitektura GSM/UMTS mreže sa elementima koji učestvuju u pružanju osnovnih servisa zasnovanih na mobilnim tehnologijama *s kraja na kraj* i način povezivanja sa uređajima za nadzor. U odnosu na način prosleđivanja informacija (podataka) kroz mrežu, krajnji servisi se u okviru GSM/UMTS sistema mogu realizovati u domenu komutacije kola CS (*Circuit Switched*) i domenu komutacije paketa PS (*Packet Switched*).

Osnovni telekomunikacioni servisi predstavljaju zatvorene funkcionalne celine koje obezbeđuju krajnji servis korisniku.

U nastojanju da se korisnicima obezbedi što kvalitetniji servis, svakodnevno se prate parametri koji ukazuju na njihovo funkcionisanje. Ovi parametri se dobijaju na osnovu prefedinisanih matematičkih funkcija nad rezultatima različitih brojača po svim *interface-ima.* U daljem tekstu biće opisani neki *interface-i* i ključni parametri koji se posmatraju.

U domenu komutacije kola na pristupnom delu mobilne mreže posmatramo Iu-CS (*Circuit Switch*) i A *interface*.

A *interface* je veza unutar GSM mrežne arhitekture između BSS-a (*Base Station Subsystem*) i MSC-Server-a (*Mobile Switching Center Server*). Primarni protokoli su DTAP (*Direct Transfer Application Part*) i BSSMAP (*Base Station Subsystem Management Application Part*). Neki od mnogobrojnih parametara koji se mogu analizirati

na ovom *interface-u* su *Call Success Ratio* (procenat uspešnih poziva), *Handover Success Ratio* (procenat uspešnih *Handover-a*), *Drop Call Ratio* (procenat neregularno prekinutih poziva), *Handover failures* (razlozi neuspelih *Handover-a*) i dr.

Iu-CS *interface* je veza unutar WCDMA/UMTS mrežne arhitekture između RNC-a (*Radio Network Controller*) i MSC-Server-a. Primarni protocol je RANAP (*Radio Access Network Application Part*). Pored prethodno pomenutih KPI pokazatelja na ovom *interface-u* pratimo i RAB (*Radio Access Bearer*) *Establishment Success Ratio* (uspešnost dodele RAB-a za prenos korisničkih informacija između MSCServer/MWG-a i mobilne stanice tj. UE-a (*User Equipment*) preko WCDMA/UMTS radio mreže, *RAB Setup Time* (vreme uspostave RAB-a), *Paging Success Ratio* (procenat uspešnosti *Paging* procedure), *Location Update Success Ratio* (procenat uspešnosti *Location Update* procedure) i dr.

U domenu komutacije paketa na pristupnom delu mobilne mreže posmatramo Iu-PS (*Packet Switch*) i Gb *interface-e*.

Iu-PS *interface* je veza unutar WCDMA/UMTS mrežne arhitekture između RNC-a i SGSN-a (*Serving GPRS Support Node*), a Gb *interface* je veza unutar GSM mrežne arhitekture između BSS-a i SGSN-a. Jedni od najčešće analiziranih protokoli su RANAP (Iu-PS *interface*) i BSSGP - *Base Station System GPRS Protocol* (Gb *interface*). Parametri od značaja za analizu na ovim *interface-ima* su pored RAB *Establishment Success Ratio* , *Drop Call Ratio* i *PDP Context Success Activation Ratio* (procenat uspešnosti aktivacije PDP (*Packet Data Protocol*) *context* procedure), *Paging Success Ratio*, *Attach Success Ratio*, *Relocation Success Ratio* (procenat uspešnosti prijavljivanja korisnika na paketski deo mreže i uspešnost promene lokacije korisnika)

U *core* (jezgro) delu mreže između HLR-a i MSC/VLR-a, odnosno SGSN koristi se MAP (*Mobile Application Part*) protokol. Najčešće posmatrani parametri dobijeni sa ovih *interface-a* su *Location Update* (LU) *Success Ratio* (procenat uspešnosti LU procedure), *Routnig Area Update* (RAU) *Success Ratio* (uspešnost RAU procedure).

Na interkonekcijskim *link-ovima* (*link-ovi* koji povezuju mrežne elemente različitih operatera) kao i na *link-ovima* između centrala primarni protokoli su MAP i ISUP (*ISDN User Part*). KPI parametri koji se dobijaju sa ovih *link-ova* su ABR - *Answer to Bid Ratio*, ASR - *Answer Seizure Ratio* (procenat uspešnih poziva), *Average Length of Call* (prosečna dužina trajanja poziva), *Average Setup Time* (prosečno vreme potrebno za uspostavu veze) i dr.

Na svim signalnim *link-ovima* se prati njihovo opterećenje, za koje postoje predefinisani pragovi (*threshold-i*) čijim se prekoračenjem generišu alarmi ukazujući na neku abnormalnu situaciju.

Da bi se obezbedila potpuna dostupnost i funkcionalnost servisa potrebno je obezbediti konstantan nadzor svih mrežnih elemenata, njihovu konektivnost i nadzor aplikativnih *layer-a* koji sačinjavaju jednu servisnu arhitekturu. Najvažniju ulogu u incidentnim situacijama ima brzina odziva na detektovani incident i proces upravljanja datom informacijom. To obezbeđuju jasno predefinisane procedure rada i neprekidni nadzor servisne arhitekture 24/7 (24 sata dnevno / 7 dana u nedelji).

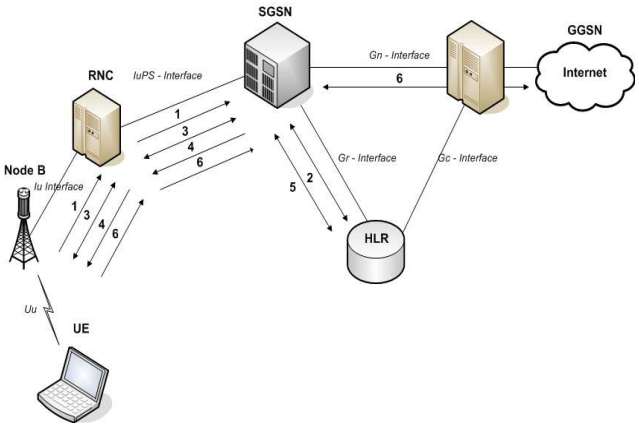
Na sl. 2. je, takođe, prikazan princip nadzora jednog osnovnog servisa u mreži Telekoma Srbija. FMS prikuplja alarme i informacije sa svih mrežnih elemenata, PMS vrši statistička merenja na istim, dok sistem za nadzor signalizacije prikuplja informacije o protokolima pomoću kojih komuniciraju mrežni elementi. Iako na slici izgleda da su ova tri sistema međusobno odvojena i nezavisna, njihova uzročno-posledična veza je evidentna u svakodnevnom nadzoru rada i kontroli kvaliteta servisa, što je opisano u III poglavlju.

## III. DETEKTOVANJE I REŠAVANJE INCIDENTNE SITUACIJE

U ovom poglavlju ćemo ilustrovati način detektovanja, lokalizaciju problema i njegovo rešavanja na primerima najzastupljenijih osnovnih servisa:

- Bežični prenos paketskog saobraćaja (Sl. 3)
- Bežični prenos govornog saobraćaja (Sl. 4)

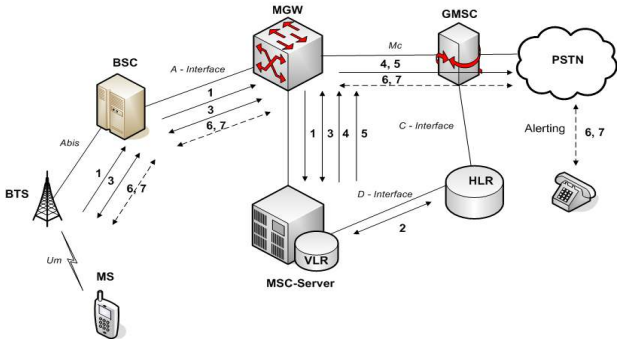
UE (*User Equipment*), u našem primeru radna stanica (laptop), koristi servis prenosa paketskog saobraćaja putem HSDPA modema i SIM karticu sa *postpaid* korisničkim profilom. Slanjem zahteva za prijavu na mrežu (*Attach Request*) UE inicira proceduru prijave uređaja na UMTS mrežu. SGSN prvo vrši autentikaciju korisnika (na osnovu parametara koje je dobio od HLR/AUC), a zatim informiše HLR o novoj lokaciji korisnika servisa i od njega dobija podatke o pretplatničkom profilu. Nakon toga korisniku je omogućeno korišćenje željenog servisa (*Activation PDP Context*), što je prikazano na slici 3.




Sl. 3. Prikaz elemenata i procedura funkcionisanja servisa - Bežični prenos paketskog saobraćaja

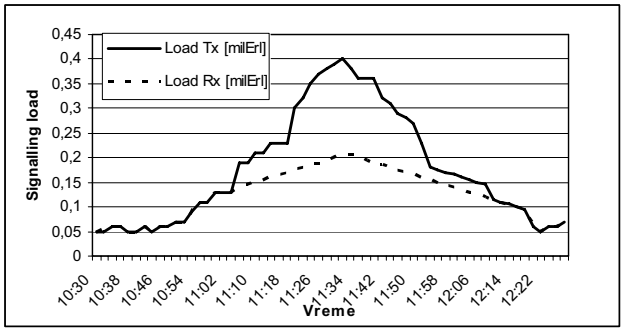
MS (*Mobile Station*), u našem primeru mobilni telefon sa SIM karticom i *postpaid* korisničkim profilom, koristi govorni telefonski servis u GSM modu. Smatraćemo da je telefon ranije već prijavljen na mrežu. Nakon zahteva za uspostavu poziva (*mobile originating connection request*) potrebno je da MSC-Server/VLR na koji je korisnik prijavljen izvrši autentikaciju korisnikovog identiteta, posle čega korisnik započinje proceduru uspostave poziva ka biranom broju.

U daljem tekstu su opisane etape u detektovanju, lokalizaciji i rešavanju problema koji utiče na rad servisa.



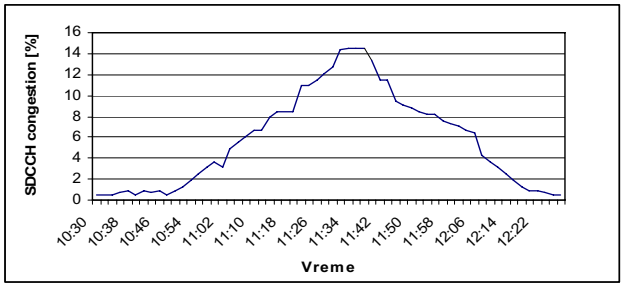

Sl. 4. Prikaz elemenata i procedura funkcionisanja servisa - Bežični prenos govornog saobraćaja

Na NetCool-u (*Fault Management System-u*) je uočen alarm sa MSC-Server-a o prekoračenim unapred definisanim *Threshold-ima* koji ukazuju na prevelik broj neuspelih autentikacija korisnika, kao i alarm o pređenom *Threshold-u* opterećenja signalnog *link-a* između MSC-Server-a i HLR-a.




Sl.5. Prikaz opterećenja signalnog linka

Brza ali detaljna analiza uočenih alarma je ostvarena u datom primeru pomoću *Performance Management System-a* i sistema za nadzor signalizacije. Na osnovu dobijenih statističkih izveštaja sa PMS-a primećeno je zagušenje na radio delu mreže, konkretno na SDCCH (*Stand-alone Dedicated Control Channel*) kanalu koji je odgovoran za kontrolu signalizacije na pristupnom delu mobilne mreže (Sl. 6.).




Sl. 6. prikaz merenja SDCCH congestion

Na osnovu predefinisanih *dialog-a* toka servisa pomoću sistema za nadzor signalizacije pristupilo se dubljoj analizi signalnih poruka i protokola potrebnih za normalno funkcionisanje servisa. Svakoj komunikaciji UE/MS sa mrežom prethodi autentikacija korisnikovog identiteta, pa se pomenuti problem odmah odrazio na sve zahteve korisnika (*Attach/Location Update* – procedura prijave korisnika na mrežu, *Call Setup* – procedura uspostave poziva, *Handover* – procedura promene mrežnog elementa koji opslužuje korisnika). Na signalizaciji je razjašnjen veliki broj neuspelih zahteva za *Location Update* i *Call Drop-ova* sa razlogom neuspešne autentikacije. Taj zaključak je problem fokusirao na deo mreže između MSC-Server-a i HLR-a preko koga se razmenjuju signalne poruke sa AUC registrom odgovornim za autentikaciju korisnika.

Iz dalje analize signalnih poruka i statističkih izveštaja proistekao je konačan zaključak da HLR ne obrađuje većinu poruka i na njih ne šalje odgovor nakon čega predefinisani tajmeri na MSC-Server-ima ističu, što se odražava da zahtevi korisnika za uspostavom servisa bivaju odbijeni.

Ovaj konkretan problem se odrazio na kratkotrajan otežan rad servisa, ali je zahvaljujuću FMS, PMS, sistemu za nadzor signalizacije i jasno definisanim procesima u najkraćem mogućem roku rešen, čime je korisniku bio ponovo raspoloživ kvalitetan servis.

## IV. Zaključak

Pružanje raspoloživog, pouzdanog i kvalitetnog servisa nije jednostavno, ali kao rezultat ima zadovoljne korisnike, popularne servise i konkuretnost samog operatera na telekomunikacionom tržištu. Za nadzor i kontrolu kvaliteta servisa, kao i detektovanje, lokalizaciju i rešavanje nastalih smetnji u mreži treba uzeti u obzir puno platformi i alata koji na prvi pogled izgledaju nezavisni, iako u opisanom primeru je evidentna njihova neraskidiva veza. Pri tome mora se voditi računa da vreme delovanja bude što je moguće kraće, ali da dijagnostikovanje bude precizno i tačno.


[1] ETSI TS 23.107 Technical Specification Group Services and System Aspects; Quality of Service (QoS) concept and architecture.
[2] ETSI TS 102 250-6 v1.2.1, "Speech processing, transmission and quality aspects; QoS aspects for popular services in GSM and 3G networks"; October 2004.
[3] Ericsson WCDMA/UMTS System Overview, Ericsson Radio Systems AB, Stockholm, 2001.
[4] Josif G. Ghetie, "Fixed-Mobile Wireless Networks Convergence: Technologies, Solutions, Services", Cambridge U. P., 2008.
[5] SGSN Rel 7. Operation and Maintenance, NSN academy, 2008
[6] GPRS Signalling, Ericsson Radio Systems AB, Stockholm, 2002.
[7] UMTS Performance Measurement, A Practical Guide to KPIs for the UTRAN Environment, Ralf Kreher, Germany 2006.
[8] WCDMA Signaling in the Core Network, Ericsson 2006.
[9] WCDMA RAN Protocols and Procedures, Ericsson 2006.



## Abstract

Availability and quality of service as final goal is priority of each telecommunication operator. In this paper has been described a specific way of detecting incident in domain of supervising of telecommunication network, its quick analysis in order to alocate the cause of problem in the network and the processes of resolving the incident. Central role in these processes takes NOC (Network Operations Center), which is responsible for monitoring the network in terms of alarms and incidents in order to avoid their possible negative impact on the network performance and on the quality of service for end users.


## DETECTION AND RESOLUTION OF INCIDENT IN DOMAIN OF TELECOMMUNICATION NETWORK MONITORING


Ivan Josifović, Jelena M. Stojanović, Đorđe S. Radović