XXIII Simpozijum o novim tehnologijama u poštanskom i telekomunikacionom saobraćaju – ***PosTel 2005,*** *Beograd, 13. i 14. decembar 2005.*

MODEL ZA MONITORING – ANALIZU KVALITETA USLUGA ZA INTERNET I MOBILNO BANKARSTVO

Bojan Stanivuković[1], Slobodan Mitrović[2]
[1] Nacionalna štedionica - banka A.D.,
[2] Saobraćajni fakultet

Sadržaj: *Kvalitet usluga u Internet i mobilnom bankarstvu u velikoj meri zavisi od performansi mrežnog sistema. U ovom radu je predstavljen model za monitoring kvaliteta usluga na osnovu praćenja rada mrežnog sistema, a čija implementacija ne zahteva dodatna ulaganja u opremu ili softver.*

Ključne reči: *Monitoring, Analiza mrežnog saobraćaja*

1. Uvod

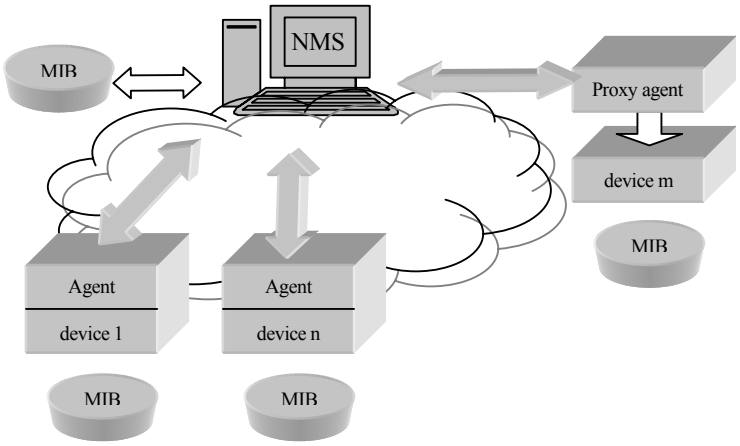
Elektronsko poslovanje bilo koje banke ili neke druge institucije ne može se zamisliti bez kvalitetnog opsluživanja, koje se zasniva na veoma prostom principu – klijenta treba uslužiti pravovremeno i efikasno. Uvođenje novih komunikacionih tehnologija je rezultiralo enormnim porastom broja klijenata koji sve svoje bankarske poslove obavljaju van šaltera banke, tj. korišćenjem Interneta i mobilne telefonije. Sa stanovišta efikasnosti bankarskog poslovanja, kvalitet usluge u ovom domenu postaje predmet prestiža na tržištu novca.

Analiza kvaliteta usluga u Internet i mobilnom bankarstvu se može vršiti pomoću sistema za monitoring mrežnog saobraćaja. Monitoring saobraćaja podrazumeva snimanje intenziteta mrežnog saobraćaja na svim radnim stanicamna, čvorištima i ulazno-izlaznim tačkama. Monitoring parametara serverskih sistema podrazumeva snimanje glavnih parametara koji pojedinačno ili u celini mogu prikazati njihov rad. Za monitoring se koriste TCP/IP protokoli iz kojih se vrši ekstrakcija pomenutih parametara.

Parametri sistema koji se mogu dobiti preko datog modela za monitoring – analizu kvaliteta usluga za internet i mobilno bankarstvo veoma su važni u procesu analize intentnog sistema i donošenja pravih odluka i sticanje prednosti na tržištu koje ima oštre zahteve i ovaj rad im je posvetio posebnu pažnju.

2. Servisi monitoringa

Prikupljanje informacija o radu jednog mrežnog sistema se, u ovom modelu, zasniva na primeni standarda za SNMP[1], RMON[2], Syslog servisa, kao i Round Robin alata. Osnovni razlog za izbor ovih servisa je njihova podržanost od strane najvećeg broja aktuelnih proizvođača hardvera i softvera. SNMP [1] je protokol aplikativnog nivoa koji služi za razmenu upravljačkih informacija između mrežnih uređaja. Pogodan je za upotrebu zahvaljujući konceptu organizacije koja se zasniva na četiri osnovna elementa: stanica (NMS[3]), agent (NMA[4]), baza (MIB[5]) i protokol (NMP[6]). Razmena podataka se vrši između agenata i stanice koja je povezana sa bazom (slika 1) . Agent može biti 'gost' bilo kog mrežnog uređaja (ruter, svič, hab, server, operativni sistem...) koja podržava SNMP. Komunikacija se vrši upotrebom UDP protokola na portovima 161 i 162. SNMP je pogodan za on-line snimanje intenziteta saobraćaja, broja ulaznih ili izlaznih paketa, broja broadcast poruka itd.



Slika 1. *Princip rada SNMP protokola*

RMON [2] je ekstenzija standardizovanih MIB-ova čija je najvažnija osobina – mogućnost kreiranja statistike analiziranjem svakog frejma na mrežnom segmentu. Ovim se može postići proaktivan monitoring u slučaju distribuiranih LAN mreža. Bitna osobina RMON-a je mogućnost lokalnog čuvanja prikupljenih podataka.

Syslog [3] je servis kojim je moguće pratiti aktivnost elementa u kome je aktivan. Pogodan je za upotrebu, bez obzira da li se radi o mrežnom uređaju, serverskom procesu ili

[1] SNMP – Simple Network Management Protocol
[2] RMON – Remote Monitor
[3] NMS – Network Management Station
[4] NMA – Network Management Agent
[5] MIB – Management Information Base
[6] NMP – Network Management Protocol

posebnoj aplikaciji. Podaci o aktivnostima se storniraju lokalno i mogu se preuzimati od strane stanice za monitoring u definisanim vremenskim intervalima ili po aktiviranju određenog događaja, poput trenutka u kojem je buffer Syslog-a na mrežnom elementu popunjen.

Round Robin alati [4] služe za standardnu statističku analizu događaja koji su zabeleženi u logovima servera ili stanica za monitoring. Njihov princip rada je "prebrojavanje" definisanih događaja koji su snimljeni u log-ovima. Statistika se neće "osvežavati" ukoliko se ne pojavi nova beleška o pojavi događaja za koje je definisano "prebrojavanje". Ova klasa alata je interesantna za primenu u monitoringu, upravo zbog svoje osobine direktne "zavisnosti" od realizacije određenih događaja. Jedan od popularnih setova alata iz ove klase je RRD Tools[7]

3. Parametri monitoringa

Kvalitet usluga u Internet i mobilnom bankarstvu u velikoj meri zavisi od performansi mrežnog saobraćaja. Zbog toga je bitno da analiza kvaliteta uključi parametre koji se obično primenjuju u analizi mrežnog sistema u poslovima administracije mreže, a to su:

- Intenzitet ukupnog saobraćaja na mreži,
- Intenziteti mrežnog saobraćaja klasifikovani po servisima koji služe za pružanje usluga prema klijentima,
- Intenziteti mrežnog saobraćaja klasifikovani po servisima koji se obavljaju u pozadinskim poslovima, tj. poslovima koji se obavljaju u okviru samog sistema banke.

Pošto su mrežni servisi okarakterisani TCP/IP portovima, monitoring određenih servisa se vrši zapravo snimanjem aktivnosti mrežnog saobraćaja, upravo, po definisanim portovima. Na primer, intenzitet Web usluga se može meriti po aktivnosti mrežnog saobraćaja prema IP adresi Web servera na portu 80, itd.

Povećanje broja transakcija po određenom tipu servisa uslovljava veći nivo iskorišćenja mrežnih resursa, kao što je ukupan nivo saobraćaja na određenim ulaznim linijama, broj ulaznih konekcija na serverima, procesorsko opterećenje servera, nivo iskorišćenja bafera na ruteru, Layer3 svičevima i drugim komponentama. Ovi nivoi mogu uticati na stepen zauzetosti sistema, što se odražava na mogućnost da, u slučaju većeg opterećenja, klijenti koji su postavili zahtev za uslugom, budu odbijeni, odnosno da se nađu u stanju otkaza, posmatrano sa aspekta teorije masovnog opsluživanja.

Intuitivno se može zaključiti da je monitoring mrežnog saobraćaja u jakoj vezi sa bezbednosnim aspektom rada mreže. Upravo, određeni modeli analize bezbednosti istraživačkih timova sa Univerziteta u Arizoni, [5],[6], su dali ideju za model kvantifikacije parametara kvaliteta posmatranih usluga.

Shodno prethodno navedenim činjenicama, možemo definisati tri stanja sistema,odnosno njegovih komponenti, posmatrano sa stanovišta zahteva za uslugom – normalno, stanje intenzivnih zahteva, stanje preopterećenosti[8].

Kvantifikacija se, pored rezultata koji su dobijaju primenom već pomenutih alata, može izvršiti sa dva faktora, faktora nivoa zahteva (FNZ) i faktora upada u sistem (CIF[9] [5]).

---

[7] http://people.ee.ethz.ch/~oetiker/webtools/rrdtool/tut/rrdtutorial.en.html

[8] stanja izvedena na osnovu literature [5]

Faktor nivoa zahteva (npr. za web server) predstavlja odnos razlike maksimalnog broja svih regularnih konekcija *(Nruk)* i normalnog broja konekcija iz sistema *(Nns)*, i razlike normalnog broja svih regularnih konekcija *(Nnsmax)* i normalnog broja konekcija iz sistema (1). Pod regularnom konekcijom se, u ovom slučaju, podrazumeva tcp/ip konekcija na portu 80 koja ne ulazi u grupu napada, a uključuje i zahteve za uslugom, dok se pod normalnom konekcijom podrazumeva isti tip konekcije, ali bez zahteva za uslugom. FNZ je prilagođena formula CIF.

$$FNZ(WebSrv, Bkp80) = \frac{|Nruk - Nns|}{|Nns\max - Nns|} \tag{1}$$

Faktor nivoa zahteva (za isti slučaj) predstavlja odnos broja konekcija u slučaju napada *(Nruk)* i normalnog broja svih regularnih konekcija *(Nnrk),* i razlike maksimalnog *(Nrkmax)* i normalnog broja svih regularnih konekcija (2).

$$CIF(WebSrv, FSkp80) = \frac{|Nfs - Nnrk|}{|Nrk\max - Nnrk|} \tag{2}$$

Navedeni faktori se mogu primeniti i u slučaju drugih parametara, na različitim tipovima mrežnih uređaja. Suština upotrebe navedenih faktora je kvantitativna vrednost kojim se može izraziti da li se određena mrežna komponenta sistema nalazi u operativnom stanju koje je prihvatljivo za klijenta, odnosno za sistem. Prihvatljive vrednosti ovih koeficijenata zavise od vrste servisa koji se izvršavaju u okviru datog sistema, kao i od vrste mrežne opreme. Da bi definicija vrednosti bila korektna, potrebno je izvršiti merenja performansi sistema po puštanju mrežnog sistema u rad. Prikupljeni podaci se, potom mogu upotrebiti u izrazu za proračun granice između normalnog stanja i stanja intenzivnih zahteva, kao i granice između stanja intenzivnih zahteva i stanja preopterećenosti.

$$V(p, m.t) = \frac{|m(t) - m_{norm}|}{\Delta p, m} \tag{3}$$

Indeks osetljivosti na napad (3) (Vulnerability index, V), predstavlja odnos razlike trenutnog nivoa saobraćaja pri napadu u trenutku t (*m(t),* tj. nivoa u stanju preopterećenosti) i nivoa regularnog saobraćaja (m_{norm}), prema minimalnoj razlici u nivou saobraćaja, potrebnoj da element mreže pređe iz jednog u drugo stanje ($\Delta p, m$). Ista formula se može primeniti za definisanje obe granice, s tim što se u prvom slučaju, za vrednost *m(t)* uzima maksimalan nivo regularnog saobraćaja, a za $\Delta p, m$ minimalni porast saobraćaja da bi sistem prešao iz normalnog stanja u stanje intenzivnih zahteva.

4. Opis modela

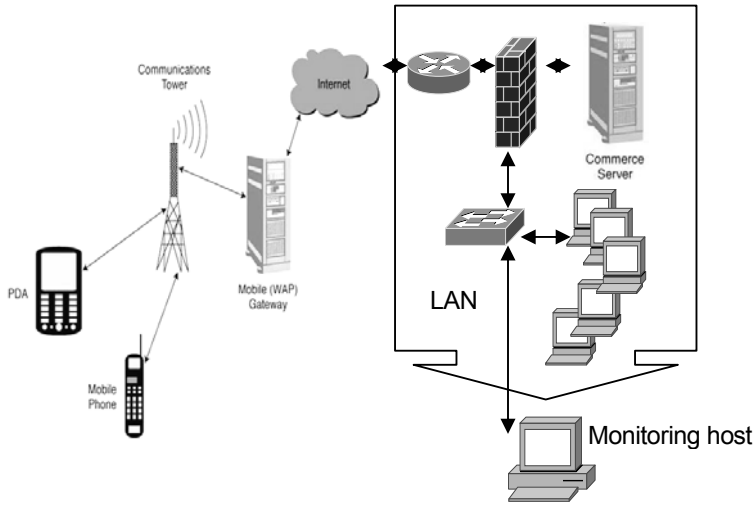
[9] CIF – Component Impact Factor

Model za monitoring i analizu usluga Internet i mobilnog bankarstva, podrazumeva realizaciju sledećih pripremnih koraka:

- Formiranje tima za monitoring, koja je u bliskoj saradnji sa administrativnim osobljem mrežnog sistema,
- Definisanje nivoa ovlašćenja za pristup mrežnom sistemu,
- Blokadu portova za sve servise van upotrebe i izvan nivoa ovlašćenja za pristup po grupama korisnika, kao i u pristupnim tačkama sistema (ruteri i sl.),
- Definisanje tačaka koncentarcija u kojima je potrebno vršiti monitoring. Preporučuje se da se monitoring vrši u svim tačkama koncentracija, zbog bliskosti zadatka sa bezbednosnim merama.
- Instalaciju servisa za monitoring, po mrežnoj infrastrukturi, u zavisnosti od vrste opreme.

Obzrom da su bankarski sistemi, zbog prirode svog posla, osetljivi sa aspekta bezbednosti, SNMP monitoring treba bazirati na SNMPv3 verziji protokola, koja podržava autentifikaciju i metode za kriptovanje. SNMP se može instalirati na svim tačkama koncentracije, kao što su upravljivi svičevi, ruteri. Ukoliko svičevi nisu upravljivi, odnosno ne podržavaju SNMP protokol, postoji mogućnost instalacije SNMP proxy agenata. Takođe, treba iskoristiti i eventualno prisustvo RMON-a.

Model podrazumeva instalaciju jednog host-a sa ulogom NMS-a koja može prikupljati podatke od agenata (slika 2.).



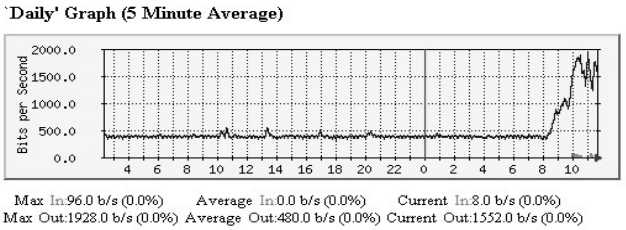
Slika 2. *Model za monitoring sistema*

Ovaj host predstavlja centralno mesto monitoringa, pa zbog toga može imati i ulogu syslog servera, da bi prikupljao podatke sa uređaja tipa firewall ili layer3 switch i sl. Na serverima se mogu postaviti Round robin alati, koji će direktno vršiti monitoring nad

servisima koji su na njima postavljeni. U tom slučaju, centralna monitoring stanica može uvesti već obrađene podatke.

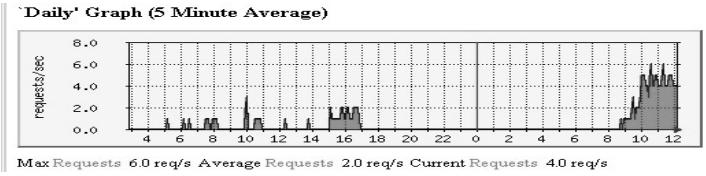
5. Primer upotrebe modela za merenje kvaliteta usluga:

Pretpostavimo da vršimo analizu kvaliteta usluga za Internet bankarstvo, tako što ćemo posmatrati Web server na kome se nalazi Web sajt za pregled tekućih računa. Pretpostavimo da je normalno opsluživanje saobraćaja okarakterisano saobraćajem čiji je grafikon prikazan na slici 3. Preseci se rade na svakih 300 sec. Stanje prikazano na slici je vezano za period nedelja-ponedeljak, poslednji presek je ponedeljak, 11:30, pre podne.



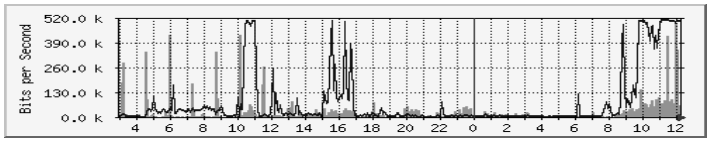
Slika 3. *Normalno stanje rada hipotetičkog Web servera*

Web server u regularnom radnom režimu emituje mnogo veći izlazni saobraćaj (plava boja - emitovanje sadržaja web sajta), od ulaznog (zelena boja – ulaz je samo adresa web lokacije). Grafikon pokazuje da je do 8 časova ujutru bilo mirovanje (broj klijenata je bio zanemarljiv). Od 8 časova, pa nadalje broj klijenata se povećava, ali je stanje Web servera normalno. Grafikon na slici 4 pokazuje broj zahteva za Internet uslugama u sekundi.



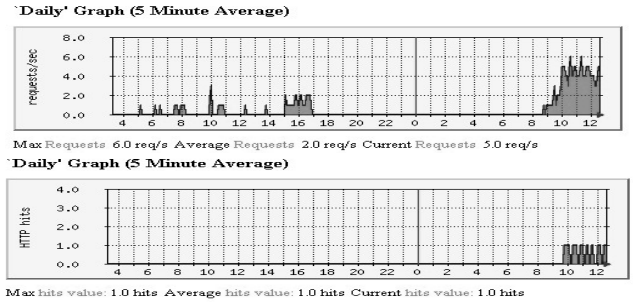
Slika 4. *Broj zahteva za uslugama Internet bankarstva, na hipotetičkom Web serveru*

Pretpostavimo da imamo slučaj u kome dolazi do problema u radu Web servera. Neka ulazno-izlazni saobraćaj ima karakteristike, prikazane na slici 5.



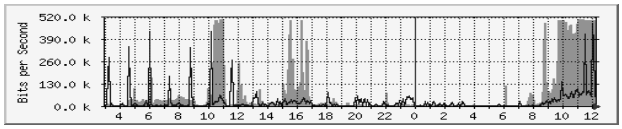
Slika 5. *Neželjene pojave na hipotetičkom Web serveru*

Može se uočiti da je u slučaju prikazanom na slici, došlo do preopterećenja servera, koji "u poslednjih sat vremena" radi sa skoro 100% kapaciteta. Zelena boja pokazuje da je broj zahteva za Internet uslugama drastično u porastu i da postoji mogućnost da neko od klijenata dobije "otkaz". Način za proveru je upoređenje broja zahteva za uslugom i broja opsluženih klijenata (slika 6).



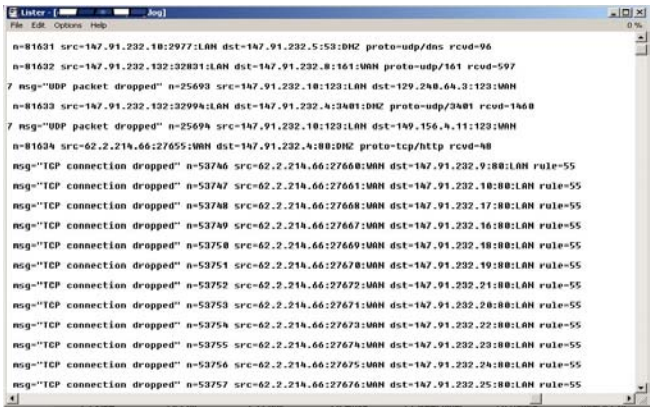
Slika 6. *Upoređenje broja klijenata koji su postavili zahtev za uslugom i broja opsluženih klijenata*

Može se uočiti da je, u ovom slučaju, došlo do otkaza klijentima i da je od 4 zahteva, samo jedan opslužen. Na sličan način se mogu utvrditi i ostale anomalije u sistemu, kao što je pojava virusa u sistemu ili neautorizovane aktivnosti (slika 7). Tada se može primetiti da je nivo ulaznog saobraćaja (zelena boja) mnogo veći od izlaznog (plava boja), posmatrano kroz globalni presek.



Slika 7. *Ponašanje saobraćaja u hipotetičkom slučaju pojave neautorizovanih aktivnosti u sistemu*

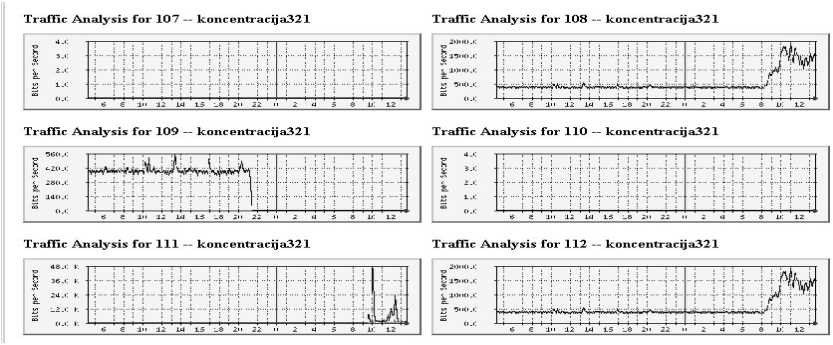
Navedeni slučaj zahteva i detaljniju analizu jer ovaj grafikon samo pokazuje "neregularno" ponašanje saobraćaja. Reakcija na ovu pojavu mora biti izvedena od strane administrativnog lica koje će izvršiti detaljniju analizu, na primer, pregledom log datoteka, koje na detaljan način beleže aktivnosti saobraćaja (slika 8).



Slika 8. *Primer Log datoteke sa neautorizovanim aktivnostima (hipotetički slučaj)*

U ovom slučaju se na primer mogu videti pokušaji dejstva neautorizovanih aktivnosti sa neke spoljne adrese (62.2.214.66). Detalj prikazane datoteke u ovom slučaju govori da su svi pokušaji odbijeni od strane zaštitnog sistema, ali isto tako mogu pokazati i suprotno. Na osnovu ovakvih podataka se mogu preduzeti odgovarajući koraci.

Slična analiza se, takođe, može primeniti i na monitoring čitavog računarskog sistema banke, pomoću kojeg se mogu utvrditi eventualne neautorizovane aktivnosti, na primer, aktivnosti van radnog vremena (slika 9).



Slika 9. *Primer monitoringa radnih stanica u sistemu*

Prikazani model se nalazi u fazi laboratorijske simulacije. U ovom modelu su vršeni preseci stanja na intervalima 300 sec, ali period ekstrakcije parametara može biti i kraći. Dodatni mehanizmi kvantifikacije (proračun i prikaz faktora FNZ i CIF) su u fazi implementacije. Za grafički prikaz su generisani skriptovi za MRTG[10].

[10] MRTG-Multi Router Traffic Grapher, http://people.ee.ethz.ch/~oetiker/webtools/mrtg/

6. Zaključak

Generalno se može zaključiti da monitoring sistema za pružanje usluga u mobilnom i Internet bankarstvu, ne predstavlja samo sredstvo za povećanje efikasnosti, već i kao neophodan vid aktivnosti u cilju obezbeđenja od neželjenih pojava. Pretpostavlja se da bi prikazana metoda, dodatnim razvojem, mogla rezultirati apsolutnom analizom stanja sistema u realnom vremenu i možda dovesti do razvoja određenih prediktivnih metoda u istom cilju.

Pomenuti model je bitan i sa bezbednosnog aspekta, jer pomaže ovlašćenom osoblju pravovremeno uočavanje potencijalnih anomalija u sistemu.

Prikazani model predstavlja pravi primer, kako se, uz minimalno ulaganje može formirati sistem koji može da pomogne u ostvarivanju vrhunskih performansi čitavog informacionog sistema banke koja želi da klijentima pruži kvalitetnu uslugu.

Literatura

[1] D. Harrington et al., "An Architecture for Describing SNMP Management Frameworks", RFC 2571, IETF, 1999.
[2] S. Waldbusser et al., "Remote Network Monitoring Management Information Base", RFC 2819, IETF, 2000.
[3] C. Lonvick et al., "The BSD syslog Protocol", RFC 3164, IETF, 2001.
[4] http://people.ee.ethz.ch/~oetiker/webtools/rrdtool/tut/rrdtutorial.en.html, 2005.
[5] S. Hariri, et al. "Impact Analysis of Faults and Attacks in Large-scale Networks". IEEE Security & Privacy, Sep/Oct Volume 1, Number 5., 2003, pp. 49-54.
[6] Guangzhi Qu, et al.,"Online Monitoring and Analysis for Self-Protection against Network Attacks", Proceedings of the International Conference on Autonomic Computing (ICAC'04), 2004.

Abstract: *Quality of mobile and Internet banking services highly depends on network efficiency level. This paper presents a model of network monitoring in purposes of analysis and monitoring in mobile and Internet banking quality of services, with low-cost implementation.*

Keywords: *Monitoring, Network Traffic analysis*

A MODEL FOR ANALYZING AND MONITORING QUALITY OF INTERNET AND MOBILE BANKING SERVICES

Bojan Stanivuković, Slobodan Mitrović