

Kontrola pristupa u bežičnim mrežama naredne generacije

Bojan M. Bakmaz, *Member, IEEE*, Zoran S. Bojković, *Senior member, IEEE*

Sadržaj — Ovaj rad se bavi kontrolom pristupa kao jednim od najznačajnijih mehanizama za obezbeđivanje kvaliteta servisa u bežičnim mrežama naredne generacije. Definisana je opšti model i izvršena klasifikacija aktuelnih modela kontrole pristupa. Analizirana su dva najprihvatljivija modela kontrole pristupa za bežične mreže naredne generacije.

Ključne reči — bežične mreže, kontrola pristupa, QoS.

I. UVOD

Podrška multimedijalnim aplikacijama sa različitim zahtevima u pogledu kvaliteta servisa, u prisustvu heterogenih bežičnih tehnologija, predstavlja jedan od izazova za implementaciju budućih bežičnih komunikacionih sistema. Upravljanje resursima ima značajnu ulogu u obezbeđivanju kvaliteta servisa za ove sisteme, dok se CAC (*Call/Connection Admission Control*) u literaturi često navodi kao jedan od esencijalnih alata ove tehnike i jedan od QoS (*Quality of Service*) mehanizama u kontrolnoj ravni [1].

CAC je za prve dve generacije bežičnih sistema razvijan za samo jedan servis (prenos govora). Za bežične sisteme treće generacije (3G), koji nude veći broj servisa, razvijani su znatno napredniji i kompleksniji CAC modeli.

Od bežičnih mreža naredne generacije očekuje se podrška za znatno veći broj multimedijalnih servisa, sa različitim zahtevima u pogledu QoS [2]. Implementacija mehanizama koji obezbeđuju optimalnu kontrolu pristupa u bežičnim mrežama naredne generacije ima značajnu ulogu u obezbeđenju kvaliteta servisa i to:

- **Garantovanjem kvaliteta signala** za mreže koje su ograničene pojavom interferencije. Na primer, CDMA (*Code Division Multiple Access*) mreže su ograničene u pogledu kapaciteta, tako da veće saobraćajno opterećenje prouzrokuje smanjenje kvaliteta signala zbog interferencije. U tom slučaju, prihvataju se samo oni zahtevi koji neće smanjiti kvalitet signala za korisnike koji se već nalaze u sistemu. Kao ključni pristupni parametri mogu se deklarirati broj korisnika u posmatranoj, ili susednoj ćeliji, SIR (*Signal-to-Interference Ratio*), kao i snaga bazne stanice i mobilnog terminala na prijemu i sl.

- **Kontrolom verovatnoće gubitaka zahteva** u mrežama sa ograničenim kapacitetom linka. Smanjenje gubitak zahteva može se postići eksplicitnom rezervacijom određene količine resursa za handover zahteve. U tom slučaju, pristupni kriterijum može biti broj korisnika (grupisanih po klasama), ili procenjena verovatnoća otkaza usled handovera. Raspoloživost resursa, pri određenim uslovima, takođe može predstavljati pristupni kriterijum. Bez obzira koji se kriterijum koristi, novi zahtevi prolaze kroz znatno strožiju kontrolu pristupa, što može rezultirati povećanjem verovatnoće blokiranja zahteva.
- **Kontrolom mrežnih performansi** na nivou paketa. Preopterećenje mreže može prouzrokovati značajne poremećaje, koji se ispoljavaju u vidu povećanja kašnjenja i varijacija u kašnjenju paketa, ili smanjenja propusne sposobnosti linka. Kontrola pristupa ima značajnu ulogu u održavanju ugovorenog QoS, pri čemu broj korisnika, raspoloživost resursa i QoS parametri mogu biti korišćeni kao pristupni kriterijumi.
- **Garantovanjem brzine prenosa podataka.** Kontrola pristupa u bežičnim mrežama se može koristiti radi obezbeđivanja minimalne brzine prenosa podataka, ali se prvenstveno moraju prevazići problemi koji nastaju usled mobilnosti korisnika, limitiranog kapaciteta i uzajamne interferencije kanala.

U prvom delu rada prikazan je opšti model kontrole pristupa i izvršena klasifikacija aktuelnih modela kontrole pristupa u bežičnom okruženju. U drugom delu rada analizirani su najprihvatljiviji modeli kontrole pristupa za bežične mreže naredne generacije i date su smernice za njihovo unapređenje.

II. OPŠTI MODEL KONTROLE PRISTUPA

Opšti model kontrole pristupa u bežičnom okruženju je baziran na sledećem uslovu:

$$R + \Delta R < R_p, \quad (1)$$

pri čemu R predstavlja trenutno dodeljene resurse, ΔR povećanje resursa usled zahteva za ostvarivanje, ili nastavak komunikacije, dok R_p predstavlja predefinisani prag za raspoložive resurse. Ukoliko je uslov (1) ispunjen, zahtev će biti prihvaćen, u suprotnom, zahtev će biti odbijen, ili smešten u red za čekanje. Trenutna vrednost dodeljenih resursa se određuje na osnovu merenja performansi sistema, dok se priraštaj ΔR i optimalna

B. M. Bakmaz, Saobraćajni fakultet u Beogradu, Vojvode Stepe 305, 11000 Beograd, Srbija; (telefon: 381-11-3091230; e-mail: b.bakmaz@sf.bg.ac.yu).

Z. S. Bojković, Saobraćajni fakultet u Beogradu, Vojvode Stepe 305, 11000 Beograd, Srbija; (e-mail: zsbojkovic@yahoo.com).

vrednost praga R_p određuje statistički, bez obzira na status mreže, ali se može prilagođavati u zavisnosti od dinamike sistema.

Za TDMA (*Time Division Multiple Access*) i FDMA (*Frequency Division Multiple Access*) sisteme sa tzv. "tvrđim" kapacitetom, zauzeti kanali se mogu posmatrati kao trenutno dodeljeni resursi, dok se broj kanala koje zahteva neki poziv može posmatrati kao priraštaj ΔR . U ovom slučaju prag R_p se određuje u skladu sa zahtevanim nivoom QoS. Za sisteme sa tzv. "mekim" kapacitetom, kao što su CDMA i OFDM (*Orthogonal Frequency-Division Multiplexing*), ne postoji značajnija veza između broja korisnika i raspoloživih kapaciteta za dolazne zahteve. Za ove sisteme trenutno dodeljeni resursi se mogu dobiti na osnovu SIR na prijemu. Novi zahtev se prihvata ukoliko se SIR zahteva koji se opslužuje i novog zahteva može održati iznad prihvatljivog nivoa.

III. KLASIFIKACIJA MODELA KONTROLE PRISTUPA

Kontrola pristupa se može posmatrati kao centralizovan, ili distribuiran model. Centralizovani modeli kontrole pristupa funkcionišu na osnovu algoritma koji je smešten u nekom od elemenata mreže (npr. mobilnom komutacionom centru), gde se prikupljaju informacije iz svih ćelija, a kontrola pristupa se sprovodi daljinski, iz lokalne ćelije. U drugom slučaju, algoritam je lociran u baznoj stanici svake ćelije. U literaturi, koja se bavi ovom problematikom u bežičnim mrežama, značajna pažnja se poklanja klasifikaciji CAC modela. Aktuelni modeli kontrole pristupa mogu biti podeljeni u sledeće grupe [3]:

- kontrola pristupa na osnovu rezervacije kanala,
- kontrola pristupa na osnovu verovatnoće gubitka i blokiranja zahteva,
- kontrola pristupa bazirana na predikciji,
- kontrola pristupa na osnovu mobilnosti i
- kontrola pristupa bazirana na tarifiranju.

A. Kontrola pristupa na osnovu rezervacije kanala

Kontrola pristupa na osnovu rezervacije kanala zasniva se na principu većeg prioriteta za zahteve koji se nalaze u procesu hendovera. Ukoliko je ukupan broj raspoloživih kanala s , a broj rezervisanih kanala $s - r$, zahtev će biti prihvaćen ukoliko je broj zauzetih kanala manji od praga r , dok će zahtevi u procesu hendovera biti prihvaćeni ukoliko postoje slobodni kanali. Prema ovom modelu, prag r mora biti određen tako da verovatnoća gubitaka usled hendovera bude minimalna. Statično određivanje r faktora čini ovaj model kompleksnim i neefikasnim, dok se veća iskorišćenost kanala može postići ukoliko se vrednost ovog faktora menja u zavisnosti od stanja mreže.

Princip na osnovu koga zahtevi mogu biti prihvaćeni sa određenom verovatnoćom, koja zavisi od broja zauzetih kanala, predstavlja kontrolu pristupa na osnovu fraktalne rezervacije kanala. Prema ovom modelu, verovatnoća prihvatanja novih zahteva je manja ukoliko je broj zauzetih kanala veći i obratno. Implementacijom ovog modela mogu se izbeći zagušenja u mreži i smanjiti verovatnoća gubitaka u procesu hendovera.

B. Kontrola pristupa na osnovu verovatnoće gubitka i blokiranja zahteva

Kontrola pristupa na osnovu verovatnoće gubitka i blokiranja zahteva predstavlja jedan od decentralizovanih modela. Informacije neophodne za ostvarivanje kontrole pristupa i rezervacije resursa se razmenjuju između susednih ćelija, dok sam algoritam deluje lokalno. Maksimalan broj zahteva koji se opslužuju, N , može se izračunati na osnovu komplementarne funkcije greške:

$$P_{hd} = \frac{1}{2} \operatorname{erfc} \left(\frac{N - m}{\sigma} \right), \quad (2)$$

pri čemu je P_{hd} ciljna verovatnoća gubitaka zahteva, a m i σ označavaju srednju vrednost i varijaciju svih zahteva u posmatranoj ćeliji, koji se određuju na osnovu broja korisnika u posmatranoj i okolnim ćelijama.

Verovatnoća blokiranja zahteva $P_{nb}(t)$ u intervalu $[t-1, t]$ određuje se lokalno, iz relacije:

$$P_{nb}(t) = (1 - \omega)P_{nb}(t-1) + \omega \frac{s(t)}{r(t)} \quad (3)$$

gde $s(t)/r(t)$ predstavlja odnos blokiranih i dolaznih zahteva u intervalu $[t-1, t]$, a ω predstavlja težinski koeficijent za izračunavanje eksponencijalno otežane pokretne sredine.

C. Kontrola pristupa bazirana na predikciji

U bežičnom okruženju sa izraženom mobilnošću korisnika, razmena informacija o kontroli pristupa i rezervaciji resursa između ćelija može da izazove nepotrebno opterećenje mreže. U ovom slučaju poželjno je razviti CAC algoritme koji se oslanjaju na lokalne informacije (npr. prethodna iskorišćenost kapaciteta linka), na osnovu kojih se mogu prognozirati potrebni resursi u budućnosti.

Korišćene predikcione tehnike uglavnom se baziraju na analizi vremenskih serija (npr. ARIMA – *Auto Regressive Integrated Moving Average*) [4], [5]. Predikcija se može sprovesti direktno, na osnovu postojećih podataka, ili na osnovu kreiranog modela, korišćenjem odgovarajućih procenjenih parametara. Ovaj i prethodni CAC model su se pokazali odgovarajućim u slučaju umerene fluktuacije saobraćaja.

D. Kontrola pristupa na osnovu mobilnosti

Efikasna kontrola pristupa na osnovu mobilnosti koristi neophodne informacije o mobilnosti korisnika za procenu zahtevanih resursa u mikroćelijskom bežičnom okruženju. Ovaj princip se temelji na činjenici da svaki mobilni terminal sa aktivnom konekcijom utiče na ostale konekcije u okolini svoje trenutne lokacije. Za izračunavanje zahtevanih resursa u obzir se uzimaju informacije o dužini trajanja konekcije, trenutnoj poziciji, pravcu i brzini kretanja.

Ovaj CAC model može da poboljša proces rezervacije resursa i kontrole pristupa, međutim, proračun dolaznog saobraćaja za svaku ćeliju predstavlja komplikovanu proceduru, a razmena kontrolnih poruka u realnom vremenu i česti hendoveri, mogu značajno uticati na opterećenje linka. Zbog ograničenog kapaciteta i

nepouzdanosti bežičnog medijuma, trenutna istraživanja su usmerena ka razvoju modela za određivanje verovatnoće hendovera [6] na osnovu pomenutih informacija.

E. Kontrola pristupa bazirana na tarifiranju

Tarifiranje može imati značajnu ulogu u adekvatnom iskorišćenju bežičnih resursa. Iskorišćenje se generalno može definisati kao nivo zadovoljenja korisnika opaženim kvalitetom servisa. Iskorišćenost se, na primer, može posmatrati kao funkcija verovatnoće blokiranja i gubitaka zahteva. Međutim, sa aspekta provajdera servisa, maksimiziranje iskorišćenosti obično ne vodi ka ostvarivanju većih prihoda. Da bi se postigao veći QoS nivo, neophodno je angažovanje veće količine resursa po svakom korisniku. Nasuprot tome, za ostvarenje većeg prihoda, neophodno je minimiziranje angažovanih resursa, da bi što veći broj korisnika bio opslužen. CAC model koji se bazira na tarifiranju predstavlja kompromis između ove dve krajnosti.

Za adekvatan dinamički model tarifiranja neophodno je posmatrati optimalan dolazni tok novih zahteva, tako da se tarifa menja u zavisnosti od stanja mreže. U slučaju velikog opterećenja mreže primenjuje se tarifa najvećeg opterećenja $p(t)$, koja je znatno veća od nominalne tarife p_0 . Prema ovom modelu, funkcija zahteva koja opisuje reakciju korisnika na promenu cene ima eksponencijalni trend:

$$D[p(t)] = \exp\left(-\left(\frac{p(t)}{p_0} - 1\right)^2\right), p(t) \geq p_0 \quad (4)$$

Primenom CAC modela baziranog na tarifiranju, koji limitira broj korisničkih zahteva u časovima najvećeg opterećenja, značajno se smanjuje mogućnost zagušenja u mreži.

IV. PERSPEKTIVNA REŠENJA KONTROLE PRISTUPA ZA BEŽIČNE MREŽE NAREDNE GENERACIJE

Aktuelni modeli kontrole pristupa ne predstavljaju adekvatno rešenje za bežične mreže naredne generacije. Heterogenost bežičnih pristupnih tehnologija i zahtevi u pogledu QoS-a za veliki broj multimedijalnih aplikacija predstavljaju veliki izazov u razvoju efikasnih CAC algoritama.

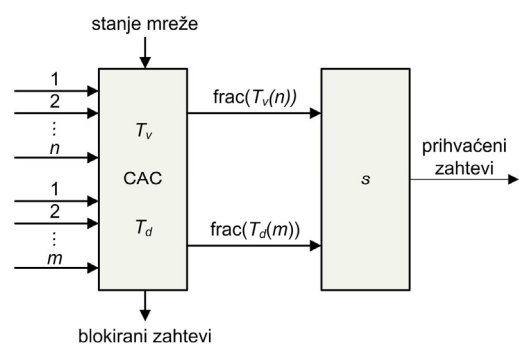
Sa aspekta kontrole pristupa, proces vertikalnog hendovera zahteva praćenje novih karakterističnih parametara, poput verovatnoće gubitka zahteva u toku vertikalnog hendovera. Novi CAC algoritmi moraju da obezbede mehanizam za prihvatanje, ili odbijanje zahteva iz različitih okruženja. U multiservisnom okruženju odluka o prihvatanju, ili odbijanju zahteva, mora biti utemeljena na raspoloživosti potrebnih resursa, ali i na ugovorenom nivou servisa. Pošto su bežične mreže naredne generacije koncipirane na ukrštenim slojevima (*cross-layers*), adekvatan CAC algoritam mora da objedini QoS performanse na nivou poziva i na nivou paketa. U ovom slučaju zahtev može biti prihvaćen isključivo ako mreža ispunjava uslove u pogledu verovatnoće gubitka, blokiranja poziva, kašnjenja, odnosno gubitka paketa.

A. Kontrola pristupa sa dvostrukim pragom

Kontrola pristupa sa dvostrukim pragom (*Dual-Threshold CAC*) [7] predstavlja optimalno rešenje za multimedijalne bežične mreže naredne generacije, jer nudi efikasan algoritam za smanjenje verovatnoće blokiranja zahteva, bez obzira da li je u pitanju prenos glasa, ili podataka. Predloženi model razmatra četiri moguće alternative za nove zahteve:

- prihvatanje obe vrste zahteva,
- prihvatanje isključivo zahteva za prenos glasa,
- prihvatanje isključivo zahteva za prenos podataka,
- odbijanje obe vrste novih zahteva.

Sa druge strane, model omogućuje pristup svim hendover zahtevima, ukoliko kapacitet ćelije to dozvoljava. Na Sl.1 je prikazan model kontrole pristupa sa dvostrukim pragom.



Sl. 1. Model kontrole pristupa sa dvostrukim pragom

Novi zahtevi za prenos glasa se kontrolišu pragom čija je vrednost određena funkcijom $m=T_v(n)$, dok je u slučaju zahteva za prenos podataka vrednost praga deklarirana funkcijom $n=T_d(m)$, uz uslov

$$m + nb \leq s, \quad (5)$$

pri čemu m predstavlja broj poziva, n broj aktuelnih sesija, b broj zauzetih kanala po sesiji, a s ukupan broj raspoloživih kanala. Za kontrolu pristupa koristi se sledeći mehanizam, koji zavisi od tipa saobraćaja i opterećenja sistema:

Zahtev za prenos glasa može biti prihvaćen ukoliko postoji makar jedan slobodan kanal i ukoliko je ispunjen uslov $m < \lfloor T_v(n) \rfloor$. U slučaju kada je slobodan samo jedan kanal i kada je $m = \lfloor T_v(n) \rfloor$, poziv će biti prihvaćen sa verovatnoćom $\text{frac}(T_v(n))$, pri čemu $\lfloor T_v(n) \rfloor$ predstavlja celobrojni deo (*integer*) vrednosti funkcije, a $\text{frac}(T_v(n))$ ostatak.

Zahtev za prenos podataka može biti prihvatljiv za sistem ukoliko je slobodno b , ili više kanala i ukoliko je ispunjen uslov $n < \lfloor T_d(m) \rfloor$. U slučaju kada je broj slobodnih kanala b i $n = \lfloor T_d(m) \rfloor$, zahtev će biti prihvaćen sa verovatnoćom $\text{frac}(T_d(m))$.

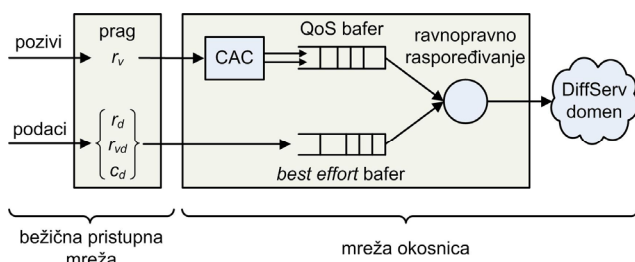
Hendover zahtevi mogu biti prihvaćeni kada postoji jedan slobodan kanal za prenos glasa, ili b slobodnih kanala za prenos podataka.

Funkcionalnost ovog modela zavisi od adekvatnog određivanja optimalnih vrednosti pragova T_v i T_d , čime se

moгу minimizirati verovatnoće blokiranja zahteva, uz zadovoljenje strogih zahteva u pogledu verovatnoće odbijanja hendover zahteva. Ovaj model je potrebno adaptirati i za slučajeve kada su dolazni zahtevi podeljeni u više od dve saobraćajne klase.

B. Dvostruka kontrola pristupa

Za QoS arhitekturu bežičnih mreža naredne generacije moguće je primeniti CAC model primenom dvostruke kontrole pristupa [3]. U modelu sa dvostrukom kontrolom pristupa (Sl. 2), CAC modul se sastoji iz dva podmodula, koji se odnose na kontrolu pristupa u bežičnim pristupnim mrežama i kontrolu pristupa u mreži okosnici. Zahtevi mogu biti prihvaćeni jedino ukoliko zadovoljavaju uslove CAC podmodula za pristupne mreže i CAC podmodula u mreži okosnici.



Sl. 2. Model dvostruke kontrole pristupa

U pristupnim mrežama kontrola pristupa se sprovodi na zahtevima koji pripadaju različitim klasama, kao i na zahtevima koji se nalaze u procesu vertikalnog hendovera. CAC podmodel za ovaj deo sistema predstavlja kontrolu pristupa na osnovu unapred definisanog praga i ima ulogu u obezbeđivanju željenog nivoa QoS, kako za pozive, tako i na paketskom nivou. Cilj kontrole u pristupnoj mreži je minimiziranje verovatnoće gubitka hendover zahteva, koji se može ostvariti prilagođavanjem vrednosti pragova za prenos glasa (r_v) i za prenos podataka (r_d). Pošto se zahtevi za prenos podataka mogu naći u procesu vertikalnog hendovera, CAC mehanizam daje veći prioritet ovim zahtevima korišćenjem praga r_{vd} , pri čemu je $r_d \leq r_{vd}$. Na osnovu toga, sledi da je broj rezervisanih kanala za hendover zahteve jednak $r_{vd} - r_d$. Prema ovom modelu, najveći prioritet imaju zahtevi koji se nalaze u procesu vertikalnog hendovera, dok najmanji prioritet imaju novi zahtevi. Zahtevi za prenos glasa mogu imati veći prioritet, ukoliko je broj kanala zauzetih prenosom podataka jednak, ili veći od vrednosti praga c_d .

U mreži okosnici periferni DiffServ ruteri poseduju dva nezavisna bafera: QoS bafer i *best effort* bafer. QoS bafer je namenjen paketima koji prenose glas, dok je drugi bafer namenjen paketima koji prenose podatke. Pretpostavka je da se paketi iz bafera opslužuju multipleksom sa vremenskom raspodelom kanala, pri čemu su vremenski slotovi fiksne dužine. Ruteri koriste mehanizam ravnopravnog raspoređivanja, koji se bazira na generalizovanom deljenju procesora (GPS - *Generalized Processor Sharing*). Ovim načinom raspoređivanja paketa postiže se virtuelna ravnopravnost, jer saobraćaj iz jednog bafera ne može uticati na performanse saobraćaja u

drugom baferu. Odnos vremena opsluživanja QoS bafera i vremena opsluživanja *best effort* bafera je jednak odnosu prioriteta koji su određeni za posmatrane tokove saobraćaja. Najveća prednost ovog modela u pogledu QoS ogleđa se u smanjenju verovatnoće gubitka zahteva u procesu hendovera u bežičnim pristupnim mrežama i kašnjenja paketa u IP-baziranoj mreži okosnici.

V. ZAKLJUČAK

Aktuelni modeli kontrole pristupa ne predstavljaju adekvatno rešenje za multiservisne, heterogene bežične mreže naredne generacije. Unapređenje analiziranih i razvoj novih optimalnih CAC modela mora biti usmeren ka dinamičkom određivanju potrebnih resursa, ugovaranju nivoa servisa i objedinjavanju QoS performansi na nivou poziva i nivou paketa.

LITERATURA

- [1] M. H. Ahmed, "Call admission control in wireless networks: A comprehensive survey", *IEEE Communications Surveys & Tutorials*, vol. 7, no. 1, First Quarter 2005, pp. 50-69.
- [2] D. Z. Deniz and N. O. Mohamed, "Performance of CAC strategies for multimedia traffic in wireless networks", *IEEE Journal on Selected Areas in Communications*, vol. 20, no. 10, Dec. 2003, pp. 1557-1565.
- [3] D. Niyato and E. Hossain, "Call admission control for QoS provisioning in 4G wireless networks: Issues and approaches", *IEEE Network*, vol. 19, no. 5, Sep/Oct. 2005, pp. 5-11.
- [4] N. Rozic and G. Kandus, "MIMO ARIMA models for handoff resource reservation in multimedia wireless networks", *Wireless Communications & Mobile Computing*, vol. 4, no. 5, Aug. 2004, pp. 497-512.
- [5] T. Zhang, et al., "Local Predictive Resource Reservation for Handoff in Multimedia Wireless IP Networks", *IEEE Journal on Selected Areas in Communications*, vol. 19, no. 10, Oct. 2001, pp. 1931-1941.
- [6] Y. Zhang, Z. H. Shao and M. Fujise, "Handoff probability in wireless mobile networks", *Proc. IEEE ICC'05*, no. 1, May 2005, pp. 3407-3411.
- [7] T-C. Chau, K. Y. M. Wong and B. Li, "Optimal call admission control with QoS guarantee in a voice/data integrated cellular network", *IEEE Transactions on Wireless Communications*, vol. 5, no. 5, May 2006, pp. 1133-1141.

ABSTRACT

This paper seeks to provide admission control as one of the most important mechanisms for obtaining quality of service in next generation wireless networks. A general model is defined and the classification of some actual models of the admission control is carried out. Then the analyses of the two most acceptable admission control models for next generation wireless networks is presented.

ADMISSION CONTROL IN NEXT GENERATION WIRELESS NETWORKS

Bojan Bakmaz and Zoran Bojkovic