Upravljanje kvalitetom servisa i zaštitom u bežičnim ad hoc mrežama

Slavica Boštjančič Rakas[1], Valentina Timčenko[1], Borislav Đorđević[2]
[1]Telekomunikacione mreže, [2]Računarski sistemi
Univerzitet u Beogradu, Institut Mihajlo Pupin
Beograd, Srbija
slavica.bostjancic@pupin.rs, valentina.timcenko@pupin.rs, bora@impcomputers.com

***Sadržaj*—U ovom radu su predstavljene karakteristike bežičnih *ad hoc* mreža sa aspekta obezbeđivanja kvaliteta servisa i zaštite. Problemi obezbeđivanja kvaliteta servisa i zaštite najčešće se u istraživanjima razmatraju odvojeno. Međutim, bežične mreže su jako osetljive na različite vrste napada kojima se utiče na sigurnost, a čime se narušava i kvalitet servisa. U tom smislu neophodno je zajedničko sagledavanje ova dva aspekta. U radu je opisana međuzavisnost obezbeđivanja zaštite i kvaliteta servisa, na osnovu koje je predložen WPBM model za upravljanje WANET mrežama zasnovan na politikama. Funkcionalni model predložene arhitekture se sastoji od četiri entiteta za upravljanje kvalitetom servisa, resursima mreže, zaštitom i konfiguracijom mrežnih elemenata.**

Ključne riječi- bežične ad hoc mreže; PBM, QoS, zaštita.

I. UVOD

Bežične *ad hoc* mreže (WANET, *Wireless Ad hoc NETwork*) funkcionišu bez potrebe za uspostavljanjem fiksne telekomunikacione infrastrukture i centralizovane administracije pri čemu je svaki čvor istovremeno i ruter i terminal. WANET čine međusobno nezavisni, samoorganizovani čvorovi koji su odgovorni za uspostavljanje i održavanje putanja, detekciju i lociranje novih čvorova, kao i razmenu kontrolnih informacija za potrebe kontinuirane komunikacije.

Ovakve mreže mogu da obezbede komunikaciju u vanrednim situacijama, s obzirom da omogućavaju uspostavljanje komunikacije u uslovima nepostojanja fiksne mrežne infrastrukture ili kada postojeća infrastruktura nije u funkciji [1].

Karakteristike poput mobilnosti čvorova, nepouzdanosti medijuma za prenos, ograničenog kapaciteta baterije i različitosti uređaja, u velikoj meri otežavaju ostvarivanje određenog nivoa kvaliteta servisa (QoS, *Quality of Service*) i zaštite. Ovo je posebno izraženo u slučaju aplikacija koje zahtevaju dosta propusnog opsega ili malo kašnjenje.

Otvorena i aktuelna pitanja vezana za razvoj ovih mreža uglavnom se odnose na problem skalabilnosti u kontekstu realizacije sigurnosti i privatnosti komunikacije u mreži, poboljšanja efikasnosti iskorišćenja raspoloživog propusnog opsega i detekcije malicioznih aktivnosti (npr. DoS, *Denial of Service*).

Poseban problem u takvim uslovima je da se istovremeno obezbedi adekvatan nivo zaštite i kvaliteta servisa. Kvalitet servisa i zaštita su veoma važni aspekti istraživanja. Tehnike kojima se poboljšava nivo zaštite u mreži mogu negativno da utiču na postojeći nivo kvaliteta servisa, jer takve tehnike zahtevaju dodatnu potrošnju raspoloživih resursa. U literaturi se ova dva aspekta najčešće razmatraju odvojeno, međutim pokazuje se da su međusobno izrazito povezani i neophodno ih je razmatrati zajedno [2]. Osim toga, različite zlonamerne aktivnosti, kao što su napadi odbijanja servisa (DoS, *Denial of Service*) [3] ili krađa propusnog opsega, još više utiču na performanse QoS. Ipak, i pored implementacije mehanizama zaštite moguća je garancija QoS, tako da se čak i u uslovima napada ne narušava kvalitet servisa tokova saobraćaja koji nisu direktno ugroženi.

Razvoj automatizovanih i skalabilnih sistema upravljanja mrežom je najčešće usmeren ka rešavanju pitanja obezbeđivanja QoS od kraja do kraja (E2E, *End-to-End*) veze, sigurnosti i pouzdanosti, efikasnog upravljanja ograničenim resursima čvora (baterija, memorijski resursi za skladištenje informacija, resursi potrebni za obradu podataka), problema korišćenja bežičnog medijuma prenosa podataka i dr.

Jedno od perspektivnih rešenja je primena automatizovanog i skalabilnog sistema upravljanja zasnovanog na unapred definisanim politikama (PBM, *Policy Based Management*). Tako definisane politike se primenjuju za potrebe upravljanja i kontrolu mrežnih komponenata i aplikacija za obezbeđivanje zaštite, kontrole pristupa i QoS.

U poređenju sa PBM rešenjima primenjenim za potrebe upravljanja žičnim mrežama, rešenja za WANET zahtevaju obezbeđivanje dodatne pouzdanosti i efikasnosti primenjenih mehanizama.

Sistem upravljanja WANET mreža treba da bude u stanju da se prilagodi trenutnim uslovima, pri čemu je potrebno u kontinuitetu obezbeđivati kako zaštitu tako i odgovarajući nivo kvaliteta servisa, bez obzira na fluktuacije dostupnih resursa.

Ključan faktor u postizanju pouzdanog servisa je primena odgovarajućeg sistema za automatsko upravljanje zaštitom i QoS. U ovom radu je ukazano na potrebu da se ova dva aspekta posmatraju istovremeno. Predloženi sistem upravljanja WANET zasnovan je na politikama i uzima u obzir

specifičnosti WANET okruženja i karakteristike postojećih rešenja primenjenih za potrebe funkcionisanja bežičnih mreža.

II. STANJE U OBLASTI

Brojni istraživači su razmatrali specifične aspekte implementacije PBM pristupa upravljanju u različitim mrežnim okruženjima. Model PBM upravljanja resursima u radio mrežama predstavljen je u [4], dok je u [5] predložen PBM model za WANET kojim se obezbeđuje efikasno upravljanje QoS koji se zasniva na algoritmu za grupisanje čvorova u klastere.

Model hijerarhijskog i centralizovanog PBM modela za mobilne čvorove predstavljen je u [6], a obezbeđuje upravljanje servisima u heterogenim mrežama (mobilnim i bežičnim) održavajući zahtevani nivo zaštite i QoS.

Skalabilni model upravljanja WANET zasnovan na politikama opisan je u [7], a primenjuje *k-hop* tehniku klasterovanja, pri čemu se mrežni elementi konfigurišu na osnovu odgovarajuće politike upravljanja, nezavisno od konkretnih spoljnih događaja, posredstvom protokola COPS-PR (*Common Open Policy Service - for PRovisioning*).

Model za upravljanje senzorskim mrežama, SNOWMAN, predstavljen u [8], zasniva se na PBM modelu upravljanja koji je baziran na ontologijama. Time je omogućeno automatsko i dinamičko organizovanje i upravljanje senzorima koristeći predefinisane politike.

PBM arhitektura zasnovana na obezbeđivanju zaštite i kvaliteta servisa u mrežama naredne generacije (NGN*, Next Generation Networks*) predstavljena je u [9]. Predloženi model se zasniva na uvođenju pet funkcionalnih entiteta namenjenih posebno obezbeđivanju QoS, odabiru odgovarajućih politika upravljanja, upravljanju resursima mreže, konfiguraciji mreže i obezbeđivanju sigurnosti mreže.

III. BEŽIČNE AD HOC MREŽE

Bežične *ad hoc* mreže se u velikoj meri primenjuju kako za civilne tako i za vojne namene, najviše zahvaljujući fleksibilnosti, ekonomskoj isplativosti i relativno jednostavnoj implementaciji.

WANET karakteriše nekoliko slabih tačaka: (1) nepouzdanost medijuma prenosa - prisluškivanje i ubacivanje lažnog saobraćaja je moguće i bez fizičkog pristupa mrežnim entitetima; (2) osetljivost čvorova - napadači mogu da pristupe infomacijama ili da promene namenu čvora (reprogramiraju njegovo ponašanje) ili da fizički oštete odnosno unište čvor. (3) odsustvo infrastrukture - nemogućnost implementacije standardnih rešenja koja se tiču zaštite i kvaliteta servisa, jer ovi aspekti u velikoj meri zavise od međusobne saradnje čvorova, koji mogu da budu i maliciozni. (4) Dinamička promena topologije - topologija može često i brzo da se menja, pa su neophodni sofisticirani protokoli rutiranja [10].

Osnovni tipovi bežičnih *ad hoc* mreža su: (1) bežične senzorske mreže (WSN, *Wireless Sensor Network*) koje karakteriše veoma ograničeni kapaciteti baterije i procesorske snage; (2) mobilne *ad hoc* mreže (MANET, *Mobile Ad hoc NETwork*) koje u odnosu na WSN karakteriše i mobilnost čvorova i dinamička promena topologije i (3) VANET (*Vehicular Ad hoc NETwork*) koje predstavljaju podskup MANET mreža, a koje formiraju "pametna" vozila koja mogu da uspostave komunikaciju kako sa drugim takvim vozilima tako i sa fiksnom mrežnom infrastrukturom koja se nalazi pored puta [11].

Bez obzira na tip WANET, pokazalo se da je u cilju rešavanja problema koji se tiču skalabilnosti i osetljivosti, neophodno razmatranje mogućnosti integracije mehanizama zaštite i kvaliteta servisa.

A. Zaštita u bežičnim mrežama

Bežične *ad hoc* mreže su veoma osetljive na napade zbog nepouzdanog medijuma za prenos, odsustva centralizovane administracije, eventualne mobilnosti čvorova (npr. MANET, VANET) i ograničenih resursa [12], [13].

WANET treba da ispune brojne sigurnosne zahteve. *Raspoloživost* podrazumeva da servisi treba da budu uvek raspoloživi. *Intergritet podataka* pretpostavlja da bilo kakva, slučajna ili namerna, promena informacije mora da bude trenutno detektovana i po mogućnosti sprečena. *Poverljivost i privatnost* podrazumevaju zaštitu informacija u mreži od pristupa neautorizovanih entiteta. Ovakva vrsta zaštite se najčešće sprovodi različitim kriptografskim alatima. *Autorizacija* obezbeđuje pristup mreži i servisima isključivo autorizovanim mrežnim entitetima, dok je *autentifikacijom* u svakom trenutku moguća provera identiteta pošiljaoca bilo koje poruke u mreži. [10]

U osnovi, napadi mogu da se podele na spoljne i unutrašnje. Unutrašnji napadi mogu da budu destruktivniji, jer je napadač upoznat sa implementiranim politikama upravljanja, a može da poseduje i privilegovana prava pristupa.

Napadi mogu dalje se dele i na pasivne i aktivne. Pasivni napadi (analiza saobraćaja, prisluškivanje) imaju za cilj da dobiju informaciju koja se prenosi, a ne narušavaju uspostavljenu komunikaciju, dok aktivni napadi prekidaju uspostavljenu konekciju ubacivanjem lažnih paketa u mrežu (crne rupe, crvi, DoS) [13], [14].

Distribuirani DoS (DDoS, *Distributed DoS*) napadi su najagresivniji napadi, koji obično prouzrokuju prekid komunikacije, zagušenje, neispravno delovanje različitih protokola i sl. DDoS obično imaju za cilj da legitimnim korisnicima uskrate pristup servisima ili mrežnim resursima. Oslanjaju se na koordinisanu aktivnost grupe kompromitovanih čvorova koji mogu da primenjuju različite modele mobilnosti, pravce i brzinu kretanja. [15].

Savremeni sistemi za detekciju napada (IDS, *Intrusion Detection System*) obuhvataju odgovarajuće praćenje, zapisivanje i forenzičku analizu digitalnih informacija o svim aktivnostima čvorova tokom funkcionisanja mreže [16]. Ovakvi sistemi obuhvataju procedure i mehanizme za detekciju, prevenciju i reakciju u slučaju napada.

Zapisivanje događaja podrazumeva snimanje saobraćaja u realnom vremenu ili beleženje informacija o detektovanim napadima generisanjem IDS log fajlova. S obzirom na ograničene procesorske, memorijske i energetske resurse čvorova formiranje IDS log fajlova predstavlja podesniji izvor forenzičkih dokaza o detekciji napada u mreži. [17].

Bezbedna razmena informacija u mreži zasnovana je na tri komponente: *firewall* sistemi, mehanizmi detekcije napada i kripto-zaštita. Kontrola pristupa različitih korisnika moguća je definisanjem odgovarajućih korisničkih imena i lozinki za svaki čvor u mreži.

Politikom upravljanja zaštitom mora da se definiše skup informacija koje moraju da se arhiviraju (*backup*) kao i učestalost pravljanja ovakve arhive.

B. Kvalitet servisa u bežičnim mrežama

Obezbeđivanje kvaliteta servisa podrazumeva da poslata informacija bude isporučena kao i da se obezbedi bolja raspodela mrežnih resursa, a to nije jednostavno s obzirom na njihovu dinamičku prirodu WANET. Takođe, obezbeđivanje QoS u takvim mrežama zahteva implementaciju adaptivnih protokola za rutiranje i signalizaciju, koji su odgovorni za kontrolu pristupa, rezervaciju resursa, reagovanje u slučaju zagušenja u mreži kao i za ugovaranje parametara QoS. Osnovni parametri kvaliteta servisa u WANET mrežama su brzina prenosa, kašnjenje, džiter, verovatnoća gubitka paketa i stopa greške [1].

Obezbeđivanje QoS u WANET dodatno utiče na kompleksnost mobilnih čvorova i povećava potrošnju energije usled procesiranja, prosleđivanja i skladištenja podataka. QoS treba da se posmatra i uzimajući u obzir česte prekide u prenosu podataka do kojih dolazi zbog prekida komunikacije uspostavljenih konekcija. U takvim uslovima QoS treba da bude definisan kao odnos ukupnog vremena prekinute komunikacije i ukupnog vremena uspostavljene konekcije, a koji bi trebalo da bude iznad unapred definisanog praga. Treba razmotriti i implementaciju dinamičkog QoS, gde su karakteristike zagarantovanog servisa definisane rasponom vrednosti parametara QoS. U takvim uslovima promena raspoloživosti resursa kao i mogućnosti realokacije resursa neće u velikoj meri uticati na obezbeđivanje QoS.

Postojeći modeli QoS koji su već provereni u radu sa žičnim mrežama, IntServ (*Integrated Services*) i DiffServ (*Differentiated Services*), nisu u potpunosti primenljivi u WANET mrežama. [18]. IntServ model predstavlja pristup po toku saobraćaja, što znači da svaki čvor mora da ima dovoljan kapacitet za skladištenje, obradu i prosleđivanje podataka, a to nije pogodno za mreže sa ograničenim resursima. DiffServ model grupiše tokove sa sličnim zahtevima za QoS u klase, tako da omogućava jednostavnije rutiranje u jezgru mreže. Međutim dinamičkoj topologiji WANET nemoguće je tačno definisati jezgro mreže, tako da je primena i ovakvog modela komplikovana.

Obezbeđivanje QoS u WANET zahteva saradnju tri sloja protokol steka: fizički, sloj linka za podatke i mrežni sloj, tako da je za obezbeđivanje E2E QoS neophodan "cross-layer" pristup, kojim su obuhvaćene funkcije koje treba da se obezbede na više slojeva protokol steka, a odnose se na zaštitu, uštedu energije i kvalitet servisa. U tom smislu predložene su različite kombinovane arhitekture, kao što su INSIGNIA, iMAQ, SWAN, DS-SWAN, 2LQoS i CLQM.

INSIGNIA [19] predstavlja specifičan *in-band* signalizacioni protokol koji se koristi za uspostavljanje, adaptaciju i prekid E2E QoS sesije. INSIGNIA uvodi podršku adaptibilnim servisima kako bi se zadovoljio osnovni nivo QoS prilikom slanja multimedijalnih podataka u realnom vremenu. Ukoliko se u mreži oslobode odgovarajući resursi, podaci se šalju sa poboljšanim nivoom QoS.

iMAQ (*Integrated Mobile Ad hoc QoS*) predstavlja arhitekturu za prenos multimedijalnih podataka zasnovanu na kombinaciji mrežnog sloja i *middleware* servisnog sloja [20]. Mrežni sloj koristi predikcioni, lokacijski zasnovan QoS protokol rutiranja, dok *middleware* sloj od mrežnog sloja preuzima informaciju o lokaciji čvorova sa ciljem predikcije deljenja mreže, koja služi da se podaci blagovremeno preusmeravaju u mreži u zavisnosti od položaja i međusobnog rasporeda čvorova.

SWAN (*Service differentiation in stateless Wireless Ad hoc Networks*). U ovom modelu TCP (*Transmision Control Protocol*) saobraćaj u mreži je *best effort* tipa, a za UDP (*User Datagram Protocol*) *real-time* saobraćaj treba da se obezbedi odgovarajući nivo QoS [21]. SWAN koristi ugrađene algoritme za obezbeđivanje odgovarajućeg kašnjenja i propusnog opsega za *real-time* saobraćaj kroz uvođenje kontrole pristupa resursima za UDP saobraćaj.

DS-SWAN (*Differentiated Services-Stateless Wireless Ad Hoc Networks*) obezbeđuje E2E QoS u WANET mrežama koje su povezane sa fiksnom IP infrastrukturom. Predstavlja kombinaciju SWAN modela za *ad hoc* mreže i DiffServ modela za infrastrukturu žične mreže, koji međusobno sarađuju. Parametri SWAN modela se dinamički prilagođavaju uslovima kako u bežičnim tako i u žičnoj mreži. Kada kašnjenje paketa postane veće od unapred definisane vrednosti, vrši se agresivnije uobličavanje *best effort* saobraćaja [22].

2LQoS (*Two-Layered Quality of Service*) predstavlja algoritam QoS rutiranja sa diferencijacijom i uobličavanjem ulaznog saobraćaja. Otkrivanje putanje vrši se na osnovu parametara koji se odnose na potrošnju resursa (broj hopova, nivo energije, mogućnosti skladištenja) i mobilnost (stabilnost mreže), dok se izbor putanje vrši na osnovu kašnjenja i propusnog opsega. Ovim modelom predviđene su tri klase servisa [23].

CLQM (*Cross-Layer QoS Mapping*) modelom je predstavljeno preslikavanje parametara kvaliteta servisa između tri sloja protokol steka u cilju obezbeđivanja diferencijacije servisa u MANET okruženju u četiri predložene klase servisa. [24].

IV. MODEL UPRAVLJANJA KVALITETOM SERVISA I ZAŠTITOM U WANET

WPBM (W*ANET Policy Based Management*) predstavlja *overlay* arhitekturu za upravljanje QoS i zaštitom u WANET mrežama, zasnovano na politikama. *Overlay* koncept je neophodan s obzirom na to da su WANET mreže nestabilno okruženje za koje su potrebna rešenja koja mogu da odgovore na zahteve koji se odnose na nepouzdanost medijuma za prenos, pametnu raspodelu resursa i opstanak mreže.

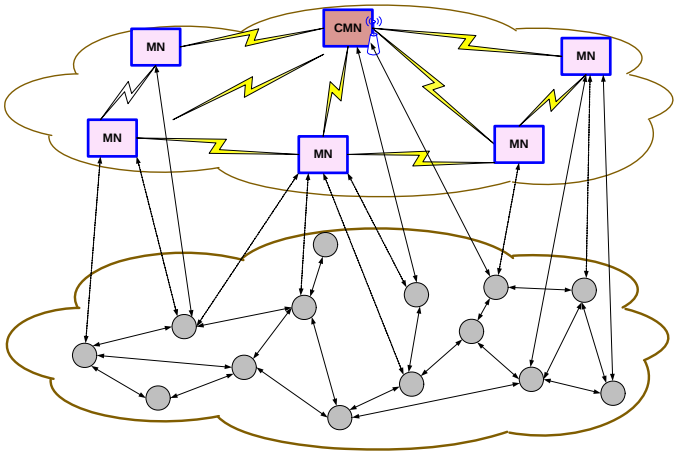
Predloženi model se zasniva na dvoslojnoj mrežnoj arhitekturi sa dva tipa čvorova i komunikacijom između čvorova na istim i različitim nivoima (Slika 1). S obzirom na veoma nepredvidivo okruženje ograničenih resursa, *overlay*

Ovaj rad je delimično finansiran od strane Ministarstva prosvete, nauke i tehnološkog razvoja Republike Srbije (TR32025, TR32037, III43002).

mrežna arhitektura omogućava optimalnu potrošnju energije, procesorskih i memorijskih resursa. Predložena arhitektura treba da obezbedi zahtevani nivo QoS i zaštite, kao i pouzdanost, skalabilnost i efikasnu raspodelu mrežnih resursa u WANET.

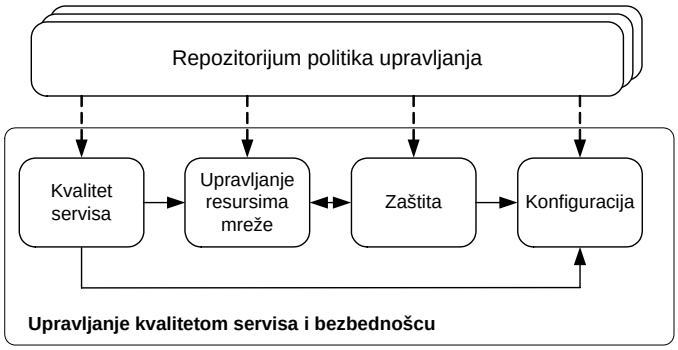
WPBM je nezavisan od veličine mreže, primenjenog protokola rutiranja, modela mobilnosti i brzine mobilnih čvorova (npr. kada su u pitanju MANET ili VANET). Čvorovi u *overlay* mreži su potpuno pouzdani, uniformno raspoređeni i sa uspostavljenim konekcijama.

Overlay mrežu čine upravljački čvorovi (MN, *Management Nodes*), dok donji nivo ove arhitekture čine regularni čvorovi. Jedan od upravljačkih čvorova se određuje kao centralni upravljački čvor (CMN, *Central Management Node*). Broj upravljačkih čvorova manji je od broja regularnih čvorova. U cilju izbegavanja pojave "single point of failure", može se definisati i redundantni centralni upravljački čvor.



Slika 1. WPBM - hijerarhijska *overlay* arhitektura.

Kako bi se produžio životni vek, čvorovi koji čine *overlay* mrežu imaju ograničenu pokretljivost i time manju potrošnju energiju. Na taj način energija služi za upravljanjem ostatkom mreže. MN čvorovi vode računa o putanjama regularnih čvorova kao i o njihovom ispravnom funkcionisanju. U ovakvim uslovima neophodno je uvođenje dinamičkog obezbeđivanja kvaliteta servisa i zaštite.



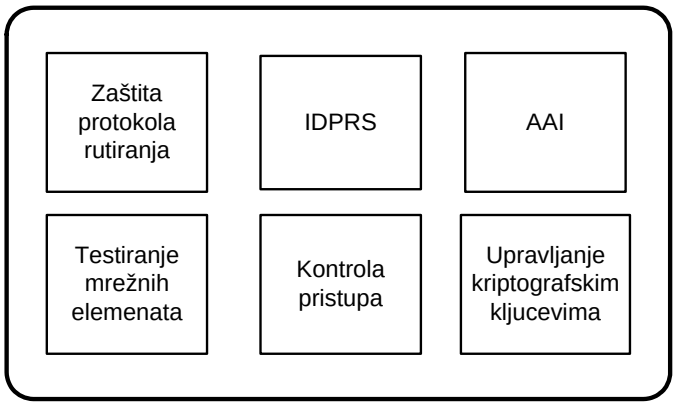
Slika 2. WPBM: funkcionalni model.

Na slici 2 prikazan je funkcionalni model WPBM arhitekture. CMN čvor prikuplja i čuva informacije i statističke podatke o događajima u mreži (detektovani napadi, *overhead* na određenim putanjama, kašnjenja i greške u komunikaciji, izveštaji o nivou zaštite, lokacije svakog čvora, promene brzine čvorova, statistika o preostalim resursima). Na osnovu takvih informacija ažuriraju se politike upravljanja, koje se sprovode u mreži. MN čvorovi u određenim trenucima šalju CMN čvoru prikupljene informacije o događajima koji su se desili u njihovom bliskom okruženju. Funkcionalni model čine četiri entiteta za upravljanje:

(1) Entitet za upravljanje kvalitetom servisa obezbeđuje različite funkcije za podršku kvaliteta servisa. Njegova funkcionalnost zavisi od raspoloživosti procesorske jedinice, propusnog opsega, memorijskih kapaciteta i raspoložive energije. Obuhvata različite QoS modele i procedure protokola za QoS rutiranje.

(2) Entitet za upravljanje resursima mreže obuhvata procedure različitih mehanizama kontrole pristupa, rezervacije resursa i estimaciju raspoloživog propusnog opsega u cilju alokacije odgovarajućeg propusnog opsega.

(3) Entitet za upravljanje konfiguracijom konfiguriše odgovarajuće parametre na osnovu informacija koje dobija od ostalih entiteta i prosleđuje ih mrežnim elementima. Konfiguracija ovih elemenata zavisi od konkretne primene mreže, modela mobilnosti i određenih ograničenja u komunikaciji.



Slika 3. Entitet za upravljanje zaštitom.

(4) Entitet za upravljanje zaštitom čini sledećih šest funkcionalnih blokova (Slika 3):

- Kontrola prihvatanja (*admission control*). Vrši procenu raspoloživih mrežnih resursa i donosi odluku o prihvatanju novih saobraćajnih tokova, a da se ne naruše garancije QoS i zaštite za postojeće tokove.
- AAI (*Authorization, Authentication, Identification*). Entitet koji je zadužen za implementaciju mehanizama za autorizaciju, autentifikaciju i identifikaciju mrežnih elemenata i njihovih aktivnosti.
- Upravljanje kriptografskim ključevima. Obezbeđuje mehanizme za dinamičko generisanje kriptografskih ključeva koji su primenjeni u različitim mehanizmima zaštite za protokole signalizacije i rutiranja.

• Zaštita protokola rutiranja podrazumeva primenu različitih procedura za bezbednu razmenu informacija za rutiranje i sigurno prosleđivanje paketa.

• IDPRS (*Intrusion Detection, Prevention, Reaction System*). Jedna od glavnih funkcija ovog funkcionalnog bloka jeste obezbeđivanje odbrane mreže u smislu prevencije, detekcije kao i reakcije na različite vrste napada [17].

• Testiranje mrežnih elemenata. Tu su implementirane različite kontrolne funkcije za detekciju grešaka u operativnim sistemima i njihovo ispravljanje.

U repozitorijumu politika upravljanja smeštene su politike koje se distribuiraju između ovih entiteta, a koje treba da se sprovedu u mreži.

V. ZAKLJUČAK

Obezbeđivanje nivoa kvaliteta servisa i zaštite je još uvek otvoren problem u oblasti WANET. Neophodno je ova dva problema posmatrati zajedno, s obzirom da obezbeđivanje odgovarajućeg nivoa jedne komponente na račun druge može da dovede do ugrožavanja pravilnog rada mreže.

U ovom radu su razmotreni postojeći problemi u oblasti obezbeđivanja kvaliteta servisa i zaštite u WANET okruženju, kao i moguća rešenja kojima bi se oba aspekta uspešno rešavala. Kao primer, predložen je sveoubuhvatni PBM model upravljanja WANET mrežama. Predložen je hijerarhijski model, čije funkcionisanje je nezavisno od veličine mreže, primenjenog protokola rutiranja i odabranog modela mobilnosti, a koji obezbeđuje funkcionisanje mreže u zavisnosti od potrebnog nivoa zaštite i kvaliteta servisa i zasnovano je na međusobnom uticaju svih definisanih funkcionalnih delova modela.

ZAHVALNICA

Ovaj rad je delimično finansiran od strane Ministarstva prosvete, nauke i tehnološkog razvoja Republike Srbije (TR32025, TR32037, III43002).

LITERATURA

[1] M. Natkaniec, K. Kosek-Szott, S. Szott, "QoS Support in Multi-Hop Ad Hoc Networks", in Wireless Network Traffic and Quality of Service Support: Trends and Standards, Eds. Lagkas, Angelidis, Georgiadis, 2010. IGI Global.

[2] A. Cizmar, J. Papaj, L. Dobos, "Security and QoS Integration Model", Computing and Informatics, vol. 31, 2012, pp. 1025–1044

[3] P. Sakarindr, N. Ansari, R. Rojas-Cessa, S. Papavassiliou, "Security-Enhanced Quality of Service (SQOS): a Network Analysis", Military Communications Conference MILCOM 2005, vol.4, Atlantic City, NJ, USA, pp. 2165 - 2171.

[4] S. Horrich, S. Ben Jamaa, P. Houze, "Policy Based RRM for Network-Terminal Decision Sharing", *IEEE Vehicular Technology Magazine*, vol. 2, no. 3, Sept. 2007, pp. 35-40.

[5] K. S. Phanse, L. A. DaSilva, S. F. Midkiff, "Design and Demonstration of Policy-Based Management in a Multi-Hop Ad Hoc Network", Ad Hoc Networks, no. 3, 2005, pp. 389-401.

[6] M. Keshariya, R. Hunt, "Architecture for Wireless Clients Operating in a Heterogeneous Mobile Environment", *Proceedings of the 8th Australian Information Security Management Conference*, Perth Western Australia, 2010, pp. 27-41.

[7] W. C. Song, S. U. Rehman, H. Lutfiyya, "A Scalable PBNM Framework for MANET Management", *Proceedings of 2009 IFIP/IEEE International Symposium on Integrated Network Management*, 2009, pp. 234-241

[8] K.-W. Lee, S.-H. Cha, "Ontology-Based Context-Aware Management for Wireless Sensor Networks", Proceedings of Advances in Computer Science, Environment, Ecoinformatics, and Education Communications in Computer and Information Science, vol. 214, 2011, pp. 353-358.

[9] V. Timcenko, S. Bostjancic Rakas, M. Stojanovic, "The Role of Service Level Agreements in NGN Security Management Systems", Proceedings of the 1st WSEAS Int. Conf. on Information Technology and Computer Networks (ITCN '12), Vienna, November 2012.

[10] R. Di Pietro, S. Guarino, N. V. Verde, J. Domingo-Ferrer, "Security in Wireless Ad-hoc Networks - A Survey", *Computer Communications*, no. 51, pp. 1-20, 2014

[11] R. Gilles Engoulou, M. Bellaiche, S. Pirre, A. Quintero, "VANET security surveys", Computer Communications, no. 44, pp. 1-13, 2014.

[12] A. Vindašius, "Security State of Wireless Networks", Elektronika Ir Elektrotechnika, vol. 71, no. 3, 2006, pp.19-22.

[13] B. Wu, J. Chen, J. Wu, M. Cardei, A Survey on Attacks and Countermeasures in Mobile Ad Hoc Networks, Wireless Network Security, Network Theory and Applications, Springer, 2007.

[14] P. Goyal S. Batra, A. Singh, "A Literature Review of Security Attack in Mobile Ad-hoc Networks", Int. Journal of Computer Applications, Vol. 9, No. 12, 2010, pp.11-15.

[15] M. Stojanovic, V. Acimovic-Raspopovic, V. Timcenko, The Impact of Mobility Patterns on MANET Vulnerability to DDoS Attacks, Elektronika Ir Elektrotechnika, No. 3 (119), March 2012, pp. 29-34.

[16] V. Timcenko, "An Approach for DDoS Attack Prevention in Mobile ad hoc Networks", Elektronika Ir Elektrotechnika, vol. 20 no. 6, 2014, pp. 150-153.

[17] V. Timčenko, M. Stojanović, "Application of Forensic Analysis for Intrusion Detection against DDoS Attacks in Mobile Ad Hoc Networks", Proceedings of the 1st WSEAS Int. Conf. on Information Technology and Computer Networks (ITCN '12), Vienna, November 2012. (Plenary lecture).

[18] M. Stojanović, V. Timčenko, S. Boštjančič Rakas, "Simulating Mobile Ad hoc Networks", in Proceedings of POSTEL 2010, Belgrade, Serbia, pp. 325 - 336. In Serbian.

[19] Z. Y. Demetrios, "A Glance at Quality of Services in Mobile Ad-Hoc Networks", Technical Report, University of California – Riverside, 2001.

[20] K. Chen, S. H. Shah, K. Nahrstedt, "Cross-Layer Design for Data Accessibility in Mobile Ad Hoc Networks", Wireless Personal Communications, pp. 49-76, Kluwer Academic Publishers, 2002.

[21] N. Sarma, S. Nandi, "Enhancing QoS Support in Mobile Ad Hoc Networks", Advances in Computer, Information, and System Sciences, and Engineering, pp. 267-273, Springer, 2006.

[22] Domingo, M. C., & Remondo, D. (2004). A cooperation model between ad hoc networks and fixed networks for service differentiation. In 29th Annual IEEE International Conference on Local Computer Networks, pp. 692-693. New York: IEEE Inc.

[23] Nikaen, N., Bonnet, C., Moret, Y., & Rai, I. A. (2002). 2LQoS - Two-layered QoS model for reactive routing protocols for mobile ad-hoc networks. In Proceedings of SCI - 6th World Multiconference on Systemics, Cybernetics and Informatics.

[24] N. Sarma, S. Nandi, "A Cross-layer QoS Mapping Framework for Mobile Ad Hoc Networks", *IETE Technical Review*, vol. 25, no. 6, 2008, pp. 346–358.

ABSTRACT

In this paper characteristics of wireless ad hoc networks have been described, in the sense of quality of service and security provisioning. Quality of service and security related issues are usually considered individualy. However, wireless ad hoc networks are higly vulnerable to different security

attacks, which can also negatively influence quality of service. Therefore, it is necessary to explore existing correlations of these aspects. We have proposed WPBM model for management of WANET networks, taking into account secury and QoS provisioning issues. Functional model of the proposed PBM approach encompasses four entities dealing with QoS, network resources, configuration and security.

QUALITY OF SERVICE AND SECURITY MANAGEMENET IN WIRELESS AD HOC NETWORKS

Slavica Bostjancic Rakas, Valentina Timcenko, Borislav Djordjevic