Mapiranje IEEE 802.11 bežičnih mreža u Beogradu

Dušan Švenda i Miroslav Djordjević, *Member, IEEE*

***Sadržaj* — U radu je opisano trenutno stanje bežičnih mreža standarda IEEE 802.11 u Beogradu. Izvršeno je merenje i klasifikacija detektovanih bežičnih mreža u skladu sa upotrebljenim načinom zaštite i ispitana povezanost rezultata sa tipom (proizvođačem) bežične mrežne opreme i nivoom dodatnih podešavanja implementiranih od strane korisnika.**

***Ključne reči* — Bežične mreže, sigurnost, wardriving, WEP, WiFi, WPA.**

I. Uvod

BEŽIČNI prenos podataka nudi priličan komfor korisnicima laptop računara, mobilnih telefona i pda uređaja. Povezivanje stacionarnih računara u LAN kao i računara sa perifernim uređajima postaje jednostavno, brzo i jevtino u mnogim praktičnim rešenjima koje nudi WLAN (Wireless Local Area Network) tehnologija.

Broj korisnika Wi-Fi standarda u svetu je u rapidnom porastu ako uzmemo u obzir sve načine implementacije ove tehnologije. Kamere za video nadzor, štampači, kancelarijski multifunkcionalni uređaji, mobilni telefoni, aktivna mrežna oprema, laptop računari, i razni drugi proizvodi izlaze na tržište sa ugrađenim bežičnim karticama baziranim na jednom ili više IEEE 802.11 standarda.

IEEE 802.11 standard trenutno nudi nekoliko nivoa zaštite podataka koji se prenose između AP i klijenta. Prvi implementirani protokol, nazvan Wired Equivalence Privacy (WEP) bio je uključen u prvu verziju standarda (IEEE 802.11-1997 [1]) i koristi RC4 enkripciju (generalno sigurnu metodu), koja u kombinaciji sa procesom autentifikacije i linearnošću enkripcione funkcije u odnosu na CRC otvara mogućnost otkrivanja tajnog ključa. WEP zaštita je razbijena 2001. godine [2], a kasnije su razvijene metode koje uz pomoć laptop računara mogu da otkriju WEP ključ za svega jedan minut [1]. Pošto se bežična mreža zaštićena WEP-om ne može smatrati sigurnom, 2003. godine je razvijen novi standard, nazvan WiFi Protected Access (WPA).

Poslednjih godina su uočene neke slabosti u WPA algoritmu zaštite koje omogućavaju dešifrovanje pojedinih kratkih paketa ukoliko se koristi IEEE 802.11e QoS [1], kao i generalniji man-in-the-middle napad [3] koji zahteva fizičko postavljanje napadača između AP i klijenta. Navedeni napadi ne omogućavaju otkrivanje WPA šifre, mada je nju moguće otkriti ukoliko se koristi slaba lozinka, bilo kroz napad korišćenjem rečnika (dictionary attack) ili grubom silom (brute force), odnosno ispitivanjem svih mogućih lozinki. Ukoliko je koristi jaka lozinka, WPA se, iako je protokol baziran na WEP zaštiti, trenutno smatra sigurnom tehnologijom.

U okviru IEEE 802.11i amandmana standardu, definisana je nova vrsta zaštite nazvana WPA2 ili RSN (Robust Security Network) koja, za razliku od WEP i WPA protokola, ne koristi RC4 tehniku, već je zamenjuje naprednijim AES (Advanced Encription Standard). WPA2 je, kao i WPA, podložan napadima prilikom autentifikacije (korišćenjem rečnika ili grube sile), međutim napadi predstavljeni u [1] i [3] ne mogu se implementirati, jer ne postoje slabosti RC4 algoritma.

II. Opis merenja

Merenja su vršena uz pomoć DELL Vostro A840 laptop računara, koji je bio pozicioniran na suvozačkom sedištu automobila. Trenutna pozicija određivana je uz pomoć Cellular Line Bluetooth GPS440 prijemnika, postavljenog ispod vetrobranskog stakla automobila.

Signali IEEE 802.11b/g mreža su primani pomoću TP-Link TL-WN321G bežične mrežne kartice sa USB konekcijom. Iako korišćeni računar ima ugrađenu bežičnu karticu, ona nije korišćena, pošto je ekperimentalno utvrđeno da dijagram zračenja antene u računaru ima duboke nule ukoliko se računar nalazi unutar vozila (samim tim, postoje pravci iz kojih je nemoguće ili veoma teško primati signale bežičnih mreža). Bežična kartica TP-WN321G bila je pozicionirana 60cm iznad krova automobila (pričvršćena na ugrađenu FM-antenu) čime je osigurana uniformnost zračenja u svim pravcima, odnosno umanjen uticaj karoserije automobila na dijagram zračenja. Pojačanje antene bežične kartice iznosi oko 0dBi, što je u našem slučaju predstavljalo prednost, pošto su samo relativno bliske bežične mreže bile u dometu uređaja.

U ovom radu je izvršeno pasivno snimanje i prikupljanje javno dostupnih parametara bežičnih mreža (ime mreže, MAC adresa AP, tip enkripcije, korišćeni standard, kanal na kome AP emituje,...). U skladu sa članom 302 Krivičnog zakonika [4], nije vršeno „razbijanje“ WEP zaštite, a ni napadi pomoću rečnika protiv WPA (da bi se utvrdilo da li je odabrana WPA lozinka dobro izabrana), pošto nije bilo moguće dobiti potrebnu saglasnost vlasnika mreža.

Dušan Švenda, Telekom Srbija A.D. , Takovska 2, 11000 Beograd, Srbija (telefon +381-64-1243-852, e-mail: dusansv@telekom.rs)

Miroslav Djordjević, ICT College, Zdravka Čelara 16, 11000 Beograd, Srbija (telefon +381-11-3291-220, e-mail: miroslav@ieee.org).

III. REZULTATI

Prikazani rezultati uključuju mreže detektovane u nekoliko delova Beograda. Iako istraživanjem nisu obuhvaćene sve beogradske bežične mreže, broj detektovanih mreža (2822) i ruta kojom se automobil kretao (Banjica, Rakovica, Cerak, Žarkovo, centar) omogućavaju visok nivo pouzdanosti rezultata primenjenih na celokupno područje Beograda. Zbog ograničenja upotrebljene opreme, merenjem nisu obuhvaćene mreže koje koriste IEEE 802.11a i 802.11n standarde, pri čemu treba imati u vidu da IEEE 802.11a mreže nisu veoma popularne u svetu, dok je IEEE 802.11n standard relativno nov (objavljen oktobra 2009.), tako da je oprema koja ga podržava relativno skupa a samim tim i trenutno malo zastupljena u Beogradu.

A. Korišćeni standardi

Standard koji bežična mreža koristi određen je na osnovu upotrebljene modulacije. Stariji standard (IEEE 802.11b) koristi tehniku proširenog spektra sa direktnom sekvencom (DSSS), dok noviji standard (IEEE 802.11g) upotrebljava ortogonalni frekvencijski multipleks (OFDM) [5]. Rezultati merenja prikazani su u tabeli 1.

Relativno mali broj IEEE 802.11b mreža može se objasniti činjenicom da je taj standard ratifikovan 1999. godine, u trenutku kada u Srbiji nisu postojali preveliki zahtevi za bežičnim mrežama, kao i da su uređaji bazirani na IEEE 802.11g standardu (ratifikovan nepune četiri godine nakon 802.b) bili potpuno kompatibilni sa starim standardom i veoma brzo se izjednačili po ceni sa starim uređajima.

TABELA 1: RASPODELA PO TIPU STANDARDA.

Modulacija	***Broj AP***
DSSS (IEEE 802.11b)	160 (5.7%)
OFDM (IEEE 802.11g)	2662 (94.3%)

B. Proizvođači

Tabela 2 prikazuje broj AP (i udeo u ukupnom broju) u zavisnosti od proizvođača opreme. Proizvođač opreme je određen na osnovu MAC adrese pošiljaoca (AP) koja se prenosi nezaštićeno u zaglavlju rama na MAC sloju u 802.11 standardu i javno dostupne liste MAC prefiksa [6]. U tabeli 2 prikazano je 14 najpopularnijih proizvođača, dok je merenjem detektovano 57. Proizvođači koji nisu izlistani u tabeli 2 imaju manje od 1% učešća u beogradskim bežičnim mrežama, pri čemu 36 (od 43) ima manje od 10 detektovanih AP.

Za većinu proizvođača je izvršena agregacija rezultata. Naprimer, detektovani Cisco-Linksys AP se na IEEE OUI listi [6] pojavljuju pod sledecim imenima: „Cisco“, „Cisco Systems“, „Cisco-Linksys“, „Cisco-Linksys LLC“, „Cisco-Linksys, LLC” i „The Linksys Group, Inc.”

Takođe, treba obratiti pažnju na relativno veliki broj (87, odnosno 3.1%) AP čije se MAC adrese ne nalaze na IEEE OUI listi (navedene u tabeli pod “Falsifikovan”). Čak i kada MAC adresa nije promenjena od strane korisnika („falsifikovana“), ime proizvođača dobijeno preko MAC adrese ne mora se poklapati sa imenom koje zaista stoji na samom kućištu aparata. Naprimer, uređaji čija MAC adresa odgovara proizvođaču „Askey Computer“ zapravo su bežični ADSL modem-ruter uređaji koje proizvodi Huawei (HG520x), a isporučuje ih Telekom Srbija uz svoje ADSL pakete.

TABELA 2: RASPODELA PO PROIZVOĐAČU OPREME.

Proizvođač	***Broj AP***
TP-Link	797 (28.2%)
Askey Computer	548 (19.4%)
Cisco-Linksys	338 (12.0%)
D-Link	161 (5.7%)
Intracom S.A.	121 (4.3%)
Pirelli	103 (3.6%)
Netgear	90 (3.2%)
Asustek	89 (3.2%)
Falsifikovan	87 (3.1%)
Belkin	75 (2.7%)
Siemens	62 (2.2%)
Planet	54 (1.9%)
Routerboard	34 (1.2%)
Senao	31 (1.1%)
Ostali	232 (8.2%)

C. Zaštita WLAN mreža

Vrste upotrebljene zaštite u starijim IEEE 802.11b uređajima prikazana je u tabeli 3. Skoro tri četvrtine bežičnih mreža ne upotrebljava nikakvu enkripciju, a 14% upotrebljava prevaziđenu i nesigurnu WEP enkripciju (moguće i zbog toga što uređaji ne podržavaju naprednije zaštite). Uzimajući u obzir da samo 12% IEEE 802.11b bežičnih mreža upotrebljava jaku enkripciju, nije teško zaključiti zbog čega je nekad vladalo mišljenje da su bežične mreže u Beogradu mahom nezaštićene.

TABELA 3: TIP ZAŠTITE 802.11B MREŽA.

Enkripcija	***Udeo***
Bez enkripcije	74%
WEP	14%
WPA	7%
WPA2	5%

Tabela 4 pokazuje detektovani stepen zaštite IEEE 802.11g mreža. Za razliku od IEEE 802.11b mreža, malo manje od četvrtine novijih mreža ne upotrebljava nikakvu enkripciju. Takođe, drastično je povećan broj mreža koje upotrebljavaju sigurnu enkripciju (WPA i WPA2).

TABELA 4: TIP ZAŠTITE 802.11G MREŽA.

Enkripcija	***Udeo***
Bez enkripcije	23%
WEP	20%
WPA	25%
WPA2	32%

Finalno, tabela 5 prikazuje nivoe enkripcije za AP šest proizvođača koji zajedno zauzimaju skoro tri četvrtine svih detektovanih AP. Među proizvođačima se izdvajaju „Askey Computers“ i „Intracom S.A.“, koji imaju preko 30% nezaštićenih mreža. Ovakvo odstupanje od opšteg trenda može se lako objasniti činjenicom da navedene kompanije predstavljaju proizvođače bežičnih ADSL modema-rutera koje je Telekom Srbija besplatno delio svojim korisnicima, sa inicijalno uključenim bežičnim AP. Mnogi korisnici nisu ni znali da emituju, odnosno nisu uopšte menjali konfiguraciju ADSL modema, o čemu svedoči i podatak da od nezaštićenih mreža proizvođača „Askey Computers“ 78% ima nepromenjeno inicijalno ime bežične mreže („HG520c“, „HG520i“ ili „HG520s“, u zavisnosti od verzije modema).

Bežični ADSL modemi proizvođača „Pirelli“, koje u skorije vreme korisnicima isporučuje Telekom Srbija, imaju inicijalno onemogućenu bežičnu mrežu, pa je broj nezaštićenih mreža kod ovog proizvođača smanjen na skoro polovinu prethodnog broja.

TABELA 5: ENKRIPCIJA I PROIZVOĐAČ OPREME.

Proizvođač	***Bez***	***WEP***	***WPA***	***WPA2***
TP-Link	17%	28%	14%	41%
Askey Computers	31%	23%	32%	14%
Cisco-Linksys	25%	14%	24%	36%
D-Link	13%	24%	19%	44%
Intracom S.A.	32%	12%	4%	51%
Pirelli	17%	1%	69%	14%

IV. ZAKLJUČAK

Tendencija porasta broja bežičnih mreža u Beogradu je evidentna imajući u vidu odnos broja mreža novijeg u odnosu na stariji standard. Istraživanja u budućnosti bi mogla da pokažu tačnu brzinu prirasta mreža tako što bi bilo urađeno više mapiranja istim rutama u jednakim vremenskim razmacima. Globalni razvoj IT tehnologija nije zaobičao ni Beograd pa bi se očekivana dalja ekspanzija ove tehnologije u svetu mogla očekivati i kod nas.

Bezbenost WI-FI mreža u Beogradu je iznenađujuće dobra u odnosu na očekivano stanje bezbednosti. Rezultati eventualnih budućih istraživanja bi mogli pokazati i tendenciju u zaštiti mreža, kao i stanje sigurnosti i raspodelu upotrebljenih frekvencijskih kanala najnovijeg IEEE 802.11n standarda.

ZAHVALNICA

Autori rada se zahvaljuju g. Milanu Plavšiću na velikodušnoj podeli iskustva koje je doprinelo uspešnoj realizaciji merenja.

LITERATURA

[1] Tews, E. and Beck, M., “Practical attacks against WEP and WPA”, in *Proc. of the Second ACM Conference on Wireless Network Security*, Zurich, Switzerland, 2009, pp. 79-86.

[2] J. R. Walker, “Unsafe at any key size; an analysis of the WEP encapsulation”, *IEEE Document 802.11-00/362*, Oct. 2000.

[3] T. Ohigashi and M. Morii, “A practical message falsification attack on WPA.” [Online]. Available: http://tinyurl.com/nban35

[4] “Krivični zakonik”, *Službeni glasnik RS*, 85/05, Available: http://www.parlament.gov.rs/content/cir/akta/akta_detalji.asp?Id=285&t=Z#

[5] IEEE-SA Standards Board, “IEEE 802.11-2007, Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications”, Available: http://standards.ieee.org/getieee802/download/802.11-2007.pdf

[6] Organizationally Unique Identifier (OUI) Listing, *IEEE Registration Authority*. Available: http://standards.ieee.org/regauth/oui/oui.txt

ABSTRACT

The paper presents current state of IEEE 802.11 wireless networks in Belgrade. Measurements were performed and detected wireless networks were classified according to wireless security used. Correlation of gathered results and type (manufacturer) of wireless equipment detected, as well as level of user configuration implemented is investigated.

Mapping of IEEE 802.11 wireless networks in Belgrade

Dušan Švenda and Miroslav Djordjević