PRIMENA FORENZIČKE ANALIZE U SISTEMIMA ZAŠTITE SAVREMENIH IP MREŽA

Mirjana Stojanović [1,2], Valentina Timčenko [3]
[1]Saobraćajni fakultet u Beogradu, [2] Elektrotehnički fakultet u Beogradu
[3] Institut Mihajlo Pupin u Beogradu

Sadržaj: *Forenzička analiza obuhvata identifikaciju, prikupljanje, analizu i prezentaciju digitalne evidencije (dokaza) radi otkrivanja neovlašćenih ili zlonamernih aktivnosti u mreži. U radu su prvo opisane IP traceback tehnike koje se koriste u Internetu za rekonstrukciju putanje od mete do napadača. Zatim su prikazani koncepti "honeypot" i "honeynet" – mrežnog uređaja i mreže projektovanih da budu osetljivi na različite vrste napada, sa ciljem da se tako identifikuju napadači i analizira njihovo ponašanje. Sledi razmatranje problema forenzičke analize u bežičnim mrežama. Posebno su prikazani primeri algoritama za forenzičku analizu u mobilnim ad hoc mrežama.*

Ključne reči: *Digitalna evidencija, forenzička analiza, sistem za detekciju napada.*

1. Uvod

Forenzička analiza telekomunikacione mreže obuhvata identifikaciju, prikupljanje, analizu i prezentaciju digitalne evidencije (dokaza) radi otkrivanja neovlašćenih ili zlonamernih aktivnosti. Faze forenzičkog istraživanja su: prikupljanje i čuvanje evidencije o događajima u mreži, ispitivanje i analiza prikupljenih podataka, vizuelizacija i prezentacija rezultata. Proces analize prikupljenih podataka predstavlja jezgro forenzičkog istraživanja, jer teži izvođenju zaključaka o kritičnim detaljima sigurnosnog incidenta u mreži, kroz rekonstrukciju vremena, mesta, detalja napada i identifikaciju napadača [1]. Proces može obuhvatati analizu trendova, grupisanje srodnih sadržaja, fuziju podataka, korelaciju, prepoznavanje uzoraka i detekciju anomalija u saobraćaju. Forenzičku analizu karakteriše prikupljanje dokaza "post mortem", kao i činjenica da svi istražitelji ne moraju da budu ICT eksperti, odnosno da se dokazi moraju prezentovati u formi koja je prihvatljiva stručnjacima različitih profila [2], [3].

Algoritmi forenzičke analize implementiraju se u sklopu sistema za detekciju napada (*Intrusion Detection System*, IDS) ili koriste podatke iz ovih sistema. IDS je centralizovani ili distribuirani sistem (uređaj, aplikacija) koji vrši nadzor mreže radi detekcije zlonamernih aktivnosti i generiše izveštaje na osnovu prikupljenih podataka. Stepen efikasnosti IDS sistema i pridruženih algoritama za forenzičku analizu tipično se

opisuje pomoću dva parametra: procenat normalnih aktivnosti koje su detektovane kao maliciozne (*false positives*, FP) i procenat malicioznih aktivnosti koje nisu detektovane, već su smatrane normalnim (*false negatives*, FN). Očigledno je da je IDS sistem utoliko efikasniji ukoliko su vrednosti FP i FN manje (u idealnom sistemu je FP=0 i FN=0). Pored toga, za efikasan IDS je važno da vreme detekcije napada bude što kraće.

Statistička analiza više od 2000 realnih FP i FN alarma u Internetu [4], izvršena na osnovu podataka prikupljanih u periodu oktobar 2009–februar 2011. godine, pokazala je sledeće rezultate: (1) FP alarmi su dominantni i čine više od 92% svih grešaka u IDS; (2) oko 91% FP alarma nije posledica problema u sistemu zaštite, već potiču od neadekvatne politike upravljanja i (3) približno 93% FN alarma potiče od varijacija dobro poznatih napada, kao što su napadi na SQL servere, "crvi" (*worms*) i prelivanje bafera (*buffer overflow*).

Forenzička analiza se sprovodi na različitim slojevima protokol steka i odnosi na različite tipove napada. U Internetu su dobro poznate tehnike i alati za forenzičku analizu zlonamernih aktivnosti nad sistemom elektronske pošte i pretraživačima Weba [5]. "*Sniffer*" je zajednički naziv za klasu softverskih paketa namenjenih prikupljanju odlaznog i dolaznog saobraćaja mrežnog uređaja (na nivou IP paketa), a koriste se kao važni izvori informacija IDS sistema.

Značajan porast bežičnih, a posebno mobilnih komunikacija postavlja niz novih zahteva za sisteme zaštite. Neki od problema, koji nisu prisutni u tradicionalnom Internetu, odnose se mobilnost napadača, mobilnost elemenata IDS sistema, problem dostavljanja prikupljenih podataka centru IDS sistema i, konsekventno, probleme nepotpune evidencije događaja [6]. Razvoj tehnika i alata za forenzičku analizu u ovakvim mrežama je tek u začetku.

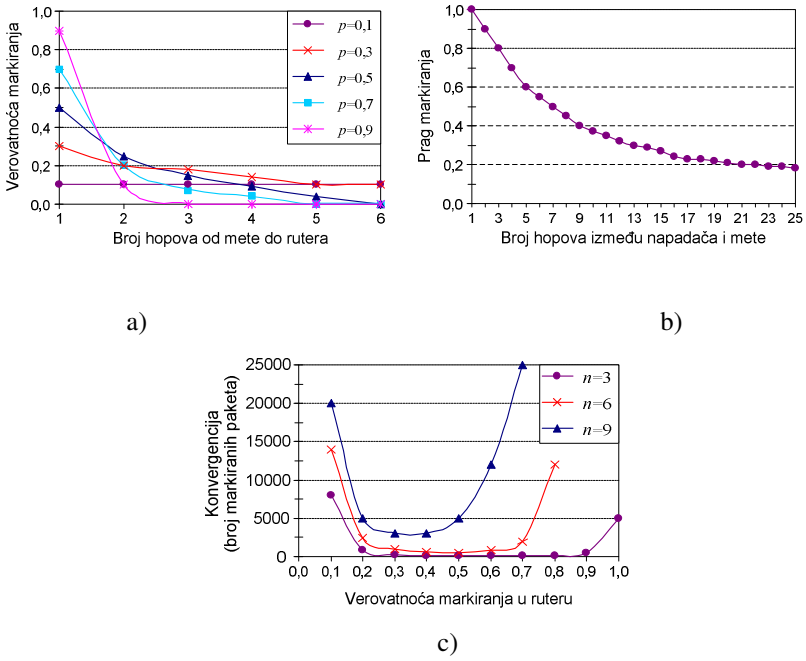
Ovaj rad je organizovan na sledeći način. Drugo poglavlje sadrži pregled IP *traceback* tehnika koje se koriste u Internetu za rekonstrukciju putanje od mete do napadača. U trećem poglavlju predstavljeni su koncepti *"honeypot"* i *"honeynet"* – mrežnog uređaja i mreže projektovanih da budu osetljivi na različite vrste napada, sa ciljem da se tako identifikuju napadači i analizira njihovo ponašanje. U četvrtom poglavlju razmatrani su problemi forenzičke analize u bežičnim mrežama. Peto poglavlje sadrži primere algoritama za forenzičku analizu u zaštiti mobilnih ad hoc mreža (*Mobile Ad hoc NETwork*, MANET). Šesto poglavlje obuhvata zaključna razmatranja.

2. IP traceback

Pretpostavimo da je $P = h_1 \rightarrow h_2 \rightarrow \ldots \rightarrow h_i \rightarrow h_{i+1} \rightarrow \ldots \rightarrow h_n$ putanja podataka između hostova h_1 i h_n. Problem IP *traceback*-a definiše se na sledeći način: ako je poznata IP adresa hosta h_n, treba identifikovati IP adrese hostova h_{n-1}, …, h_1. Ako su h_1 i h_n izvor i meta napada respektivno, putanja P se naziva "putanja napada".

Rekonstrukcija putanje napada od mete do napadača nije jednoznačno određen proces zbog mogućeg maskiranja napadača na različitim slojevima TCP/IP steka i/ili kompromitovanja tranzitnih hostova. Tehnike **testiranja linkova** [7], [8] započinju *traceback* od rutera koji je najbliži meti napada i rekurzivno određuju *upstream* linkove preko kojih je prenet saobraćaj napadača. Međutim ove tehnike uspešne su samo ako je napad u toku i ne mogu se primenjivati "post-mortem".

Tehnike **markiranja paketa** zasnovane su na ideji da se u jednom trenutku uzima jedan uzorak putanje, odnosno jedan ruter na putanji napada (umesto zapisa cele putanje). U zaglavlju paketa definiše se polje *Node* koje je dovoljne veličine da smesti adresu jednog rutera. Na primer, u IPv4 je to 32-bitna vrednost u okviru polja *Options* u zaglavlju. Kada primi paket, ruter će upisati sopstvenu IP adresu u polje *Node* sa verovatnoćom p. Pod pretpostavkama da je poslat dovoljan broj paketa i da je putanja stabilna, meta će primiti najmanje jedan uzorak od svakog rutera na putanji napada. Verovatnoća da će ruter R_i markirati paket i da nijedan od *downstream* rutera neće markirati taj isti paket je strogo opadajuća funkcija udaljenosti (broja hopova) od mete. Ako je verovatnoća markiranja p ista u svim ruterima, verovatnoća prijema paketa koga je markirao ruter udaljen d hopova od mete je $p(1-p)^{d-1}$. Slika 1a) ilustruje verovatnoću prijema paketa koga je markirao ruter udaljen d hopova ($d = 1,2,...,6$), za različite vrednosti individualne verovatnoće markiranja p.

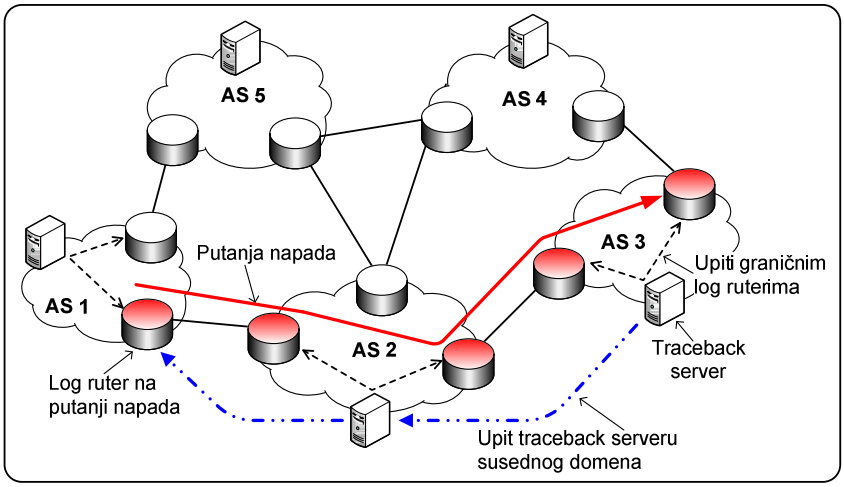


Slika 1. *Tehnike markiranja paketa u ruteru: a) verovatnoća markiranja u zavisnosti od broja hopova; b) prag markiranja u zavisnosti od broja hopova na putanji napada; c) konvergencija za putanje napada sa različitim brojem hopova (adaptirano iz [5]).*

Prag markiranja definiše se kao najmanja verovatnoća dodeljena svakom ruteru na putanji sa ciljem da se, sa verovatnoćom 99%, garantuje da će najmanje jedan ruter na putanji markirati paket. Prag markiranja opada sa povećanjem broja hopova. Što je veći broj tranzitnih rutera, veća je verovatnoća da će neki od njih markirati paket. Na slici 1b) prikazane su vrednosti praga markiranja za broj hopova u rasponu od 1 do 25.

Konvergencija se definiše kao najmanji broj paketa neophodan da se identifikuje niz rutera koji obrazuju putanju napada. Da bi se utvrdio redosled rutera na putanji napada posmatra se broj markiranih paketa u svakom ruteru. Ruter najbliži meti imaće najveći broj markiranja, dok će ruter najbliži napadaču imati najmanji broj markiranja. Da bi se odredila putanja napada sastavljena od n hopova (*meta* $\rightarrow R_{n-1} \rightarrow \ldots \rightarrow R_i \rightarrow R_{i-1} \ldots \rightarrow R_2 \rightarrow R_1 \rightarrow$ *napadač*), treba da budu ispunjena sledeća dva uslova: (1) meta treba da primi pakete tako da je svaki ruter na putanji napada obeležio najmanje jedan paket i (2) broj paketa koje je markirao ruter R_i mora da bude veći od broja paketa koje je markirao R_{i-1}. Konvergencija, u suštini, predstavlja najmanji broj paketa koji meta treba da primi da bi prethodna dva uslova bila ispunjena.

Vrednost konvergencije zavisi od verovatnoće markiranja paketa u svakom ruteru i broja hopova na putanji napada. Na slici 1c) prikazane su vrednosti konvergencije (merene sa intervalima poverenja 95–97%) u zavisnosti od verovatnoće markiranja paketa u ruteru, za putanje napada sa 3, 6 i 9 hopova. Uočava se da je, za dati broj hopova na putanji napada, konvergencija minimalna za određeni opseg vrednosti verovatnoća markiranja paketa. Vrednost praga markiranja se smanjuje sa povećanjem broja hopova zbog toga što istovremeno raste verovatnoća markiranja paketa u nekom od rutera na putanji napada. Konvergencija se povećava sa povećanjem broja hopova na putanji napada. Kako se broj hopova povećava, potrebno je više vremena da stignu paketi koje markiraju ruteri bliži napadaču (velika je verovatnoća da su veći broj paketa ponovo markirali *downstream* ruteri na putanji napada). Da bi se smanjilo vreme konvergencije na putanjama sa većim brojem hopova, važno je da verovatnoće markiranja paketa u pojedinačnim ruterima budu što manje.



Slika 2. *Arhitektura višedomenskog IP traceback sistema: rekurzivni režim rada [9].*

Sledeća grupa *IP traceback* tehnika zasniva se na **analizi informacija iz log fajlova** u ruterima. U cilju redukcije vremena procesiranja i memorijskog prostora, primenjuju se različite tehnike filtriranja informacija sadržanih u log fajlovima. Često se primenjuje statistička analiza zasnovana na različitim pretpostavkama o pojavi anomalija

u saobraćaju usled prisustva saobraćaja napadača. Tako tehnike spektralne analize polaze od pretpostavke da saobraćaj napadača ne ispoljava periodičnost, Kolmogorovljev test se zasniva na pretpostavci o visokoj korelaciji saobraćaja napadača, dok se analiza vremenskih nizova ograničava na poznate napade [8].

Analiza informacija iz log fajlova je veoma kompleksan zadatak ako se zahteva praćenje putanje IP paketa kroz nekoliko administrativnih domena. *AS-level Single Packet Traceback* (AS-SPT) tehnika, predložena u [9], zasniva se na praćenju paketa pomoću log informacija u graničnim ruterima domena. U svakom domenu postoji *traceback* server za potrebe nadgledanja graničnih rutera u kojima se izvršavaju log operacije. Ovaj server je istovremeno glavna tačka kontakta za *traceback* upite od lokalnih i udaljenih korisnika. *Traceback* server čuva informacije o serverima susednih domena. Kada stigne upit za praćenje, server ga prosleđuje svim graničnim ruterima u svom domenu. Ako posmatrani paket samo prolazi (tranzitira) kroz domen, *traceback* server dobija odgovarajuće obaveštenje i od ulaznog i izlaznog rutera. Komunikacija sa serverima susednih domena može se odvijati na dva načina: (1) rekurzivni režim, kada se upit sukcesivno prosleđuje prethodnim domenima na putanji napada, kao što je ilustrovano na slici 2 i (2) iterativni režim, kada se šalje odziv na prethodno dobijeni upit, sa prikupljenim informacijama.

3. Honeypot i Honeynet

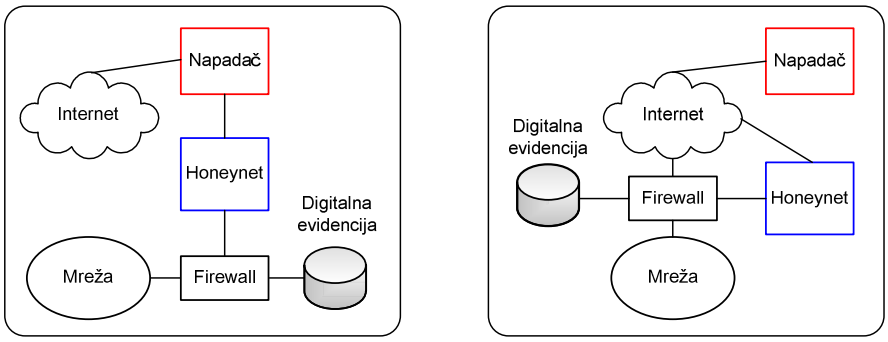
Honeynet Project [10] je jedna od vodećih neprofitabilnih međunarodnih organizacija, osnovana 1999. godine i posvećena istraživanju najnovijih napada i razvoju slobodno dostupnih alata za poboljšanje bezbednosti Interneta. Istraživanja se sprovode pomoću posebno projektovanih uređaja (*honeypot*) i mreža (*honeynet*).

Honeypot je mrežni hardver i/ili softver koji je namerno projektovan tako da bude osetljiv na različite vrste napada, sa ciljem da se pomoću njega identifikuje, posmatra i analizira ponašanje napadača [11]. Fizičke realizacije su raznovrsne: od pasivnog serverskog *socket*-a na transportnom sloju do kompletnog hardversko-softverskog sistema. Često je cilj da *honeypot* bude `''`mamac`''` postavljen na Internet kao legitimni sistem koji nudi servise. Svaka veza koju spoljni entitet uspostavlja sa *honeypot*-om smatra se, sa velikom verovatnoćom, pasivnim ili aktivnim napadom. Slično tome, odziv *honeypot*-a ukazuje da je potencijalni napadač aktivan. Forenzička analiza aktivnosti *honeypot*-a manje je podložna pojavi FP i FN alarma od analize klasičnih IDS sistema. Osim toga, oni su korisni za detekciju i analizu napada koji još nisu dovoljno ispitani ili nisu ranije viđeni.

Honeynet je mreža *honeypot*-ova sa visokim stepenom interakcije, što znači da obezbeđuje realne operativne sisteme za interakciju sa napadačima. Sav dolazni i odlazni saobraćaj se kontroliše, registruje i snima. Mreža implementira vrstu *firewall* uređaja koji je namenjen zaštiti realnog Interneta od napada koji iz nje proističu, a naziva se ***honeywall***. Zaštita se sprovodi ograničavanjem broja konekcija na sat, ograničavanjem propusnog opsega raspoloživog napadačima, presretanjem i modifikacijom zlonamernih paketa koji ciljno napadaju osetljive tačke drugih sistema i dr.

Konfiguracija *honeynet*-a zasniva se na serijskoj ili paralelnoj arhitekturi, kao što je prikazano na slici 3. U serijskoj arhitekturi, *honeynet* filtrira sav odlazni i dolazni saobraćaj realne mreže koja je potencijalna meta napada. Ako je *honeynet*

kompromitovan, *firewall* realne mreže generiše odgovarajuće alarme. Na taj način je realna mreža potpuno zaštićena od direktnih napada, na račun većeg kašnjenja svakog odlaznog i dolaznog paketa. U paralelnoj arhitekturi su *honeynet* i realna mreža paralelno povezani na Internet. Na taj način se ne unosi dodatno kašnjenje, ali je realna mreža direktno izložena napadima. Zbog toga se u *firewall*-u realne mreže primenjuju stroga pravila filtriranja. *Honeynet* analizira sav dolazni saobraćaj i po potrebi rekonfiguriše *firewall* zavisno od rezultata sprovedene forenzičke analize.



a) b)

Slika 3. *Konfiguracije honeynet-a: a) serijska arhitektura; b) paralelna arhitektura.*

Virtuelni *honeynet* implementira koncept *honeynet*-a u jednom sistemu, a može se realizovati u samostalnoj ili hibridnoj varijanti. Samostalna varijanta podrazumeva simulaciju funkcija *honeynet*-a na jednom računaru i ima niz prednosti u pogledu portabilnosti, ekonomičnosti i održavanja. Ograničenja se prvenstveno odnose na softver odnosno operativni sistem specifičan za računar na kome se izvršava virtuelni *honeynet*. Hibridna varijanta je kombinacija klasičnog *honeynet*-a i odgovarajućeg softvera za vizuelizaciju. *Firewall* uređaji i komponente IDS sistema implementirani su u fizički odvojenim uređajima, ali se svi *honeypot*-ovi virtuelno izvršavaju (simuliraju) na jednoj mašini. Svaki virtuelni *honeypot* može se fleksibilno konfigurisati za različite servise koji su potencijalna meta napada. Sa povećanjem broja *honeypot*-ova uvećava se i verovatnoća da će biti prikupljene relevantnije informacije o napadu. Na primer, najveći broj zahteva za uspostavu TCP konekcija generiše se i šalje slučajno izabranim odredištima (IP adresama). Identifikacija da su takvi zahtevi deo napada može se izvršiti tek kada je TCP konekcija uspostavljena i već primljeni segmenti koji sadrže maliciozni saobraćaj. Verovatnoća takvih događaja raste sa brojem *honeypot*-ova.

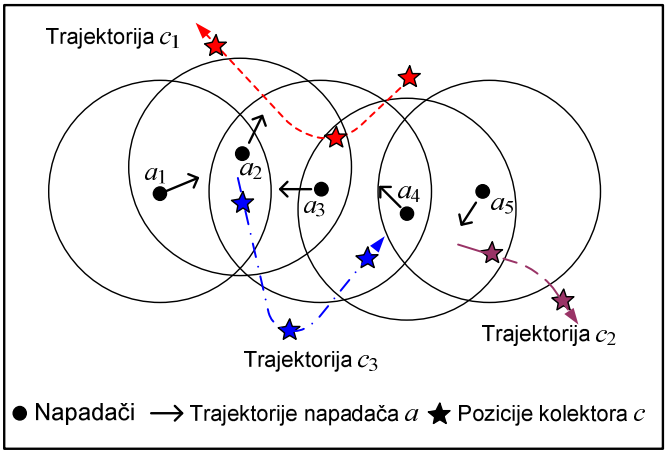
4. Problemi forenzičke analize u bežičnim mrežama

Uporedo sa sve masovnijom instalacijom bežičnih mreža pojavljuje se niz novih bezbednosnih problema, koji uopšte ne postoje u žičnom okruženju [12]. Većina ozbiljnih problema tiče se privatnosti informacija, jer se one prenose kroz bežični medijum kome se slobodno pristupa. Tipični napadi su: krađa identiteta (''krekovanje'' bežičnog pristupa Internetu), presretanje paketa, snimanje razgovora, krađa privatnih informacija,

napad na tačku pristupa da bi se blokirao pristup drugih računara Internetu i konfigurisanje tačke pristupa tako da omogući krađu poverljivih informacija (*phishing*).

Nove vrste napada uslovljavaju i primenu novih tehnika zaštite. U tradicionalnoj žičnoj mreži, napadaču je veoma teško da potpuno ukloni tragove svojih aktivnosti. To nije slučaj sa bežičnim mrežama. Digitalna evidencija (dokazi) teško se prikuplja, a lako oštećuje ili čak uništava. Neophodno je da se ustanovi detaljna standardna operativna procedura za prikupljanje digitalnih dokaza i forenzičku analizu [3], [6].

Većina novih rešenja IDS sistema u bežičnim mrežama zasniva se na kooperativnoj ili hijerarhijskoj arhitekturi [13]. U kooperativnoj arhitekturi je IDS entitet instaliran u svakom čvoru, a susedni čvorovi razmenjuju informacije ako je potrebno da razreše određene dileme. Hijerarhijska arhitektura implementira višeslojni pristup podelom mreže na klastere, od kojih svaki sadrži posebno opremljen centralni čvor (*cluster-head*) na kome se izvršava relativno složen softver za detekciju napada. Nezavisno od arhitekture, u mobilnim mrežama i napadači i IDS entiteti menjaju lokacije tokom napada, odnosno ulaze ili izlaze iz međusobnih zona pokrivanja, kao što je ilustrovano na slici 4.



Slika 4. *Varijacija topologije mreže.*

Kada su napadi mobilni, napadač može da menja identitet, poziciju, lokaciju i tačku pristupa. To znači da se podaci o mobilnosti moraju uzeti u obzir pri modelovanju aktivnosti napadača. Da bi se efikasno prikupljale informacije o mobilnosti, potrebno je da skup pouzdanih entiteta IDS sistema (kolektorskih čvorova) bude raspoređen po celoj mreži. Ti čvorovi mogu biti aktivni entiteti (koji ujedno vrše potrebne analize podataka) ili samo pasivni kolektori. U svakom slučaju, moraju da budu opremljeni za nadzor, prijavljivanje i praćenje događaja povezanih sa kretanjem čvorova, varijacijama topologije, romingom i *handoff*-om, kreiranjem klastera i dr. U bežičnim senzorskim mrežama, kolektorski čvorovi moraju da budu opremljeni dodatnim procesorskim, energetskim i komunikacionim resursima. Posebno je značajno da sami kolektori budu pouzdani i bezbedni, s obzirom na zadatak da čuvaju i eventualno procesiraju poverljive informacije.

Tokom napada su moguće sledeće situacije: (1) svi kolektori mogu da detektuju određeni događaj i generišu izveštaj o njemu; (2) grupa kolektorskih čvorova detektuje događaj i izveštava o njemu, a ostali čvorovi su van dometa napadača, mete i tranzitnih čvorova koji rutiraju saobraćaj napadača ili (3) događaj ostaje neregistrovan jer zona propagacije napada nije bila pokrivena kolektorskim čvorovima. Efikasna analiza scenarija napada u takvim okolnostima podrazumeva razvoj i primenu tehnika korelacije, filtriranja i agregacije prikupljenih podataka.

U hijerarhijskom IDS sistemu neophodna je pouzdana isporuka prikupljene evidencije centralnom čvoru. Usled efekta mobilnosti, ne može se sa sigurnošću garantovati uspostava putanje između kolektora i centra IDS sistema. Distribuirani pristup analizi dokaza nema problem dostupnosti, ali centralizovani pristup značajno redukuje procenat FP i FN alarma.

U bežičnim senzorskim mrežama, neaktivni čvorovi su u tzv. *sleep* režimu (kada ne emituju nikakve podatke) radi uštede energije. Kolektori moraju da budu svesni tog svojstva da bi se izbegla pogrešna detekcija neaktivnih čvorova kao malicioznih. U slučaju da kolektori uđu u *sleep* režim neće biti sposobni da doprinesu radu IDS sistema.

Uspešna rekonstrukcija scenarija napada na osnovu nepotpune evidencije zahteva formalne tehnike za generisanje hipoteza kako bi se osigurala tolerancija sistema na podatke koji nedostaju. To ujedno omogućuje istraživanje scenarija koji obuhvataju nepoznate tehnike napada ili koriste nepotpunu evidenciju. Hipotetičke akcije mogu se generisati na osnovu poznavanja ponašanja sistema pri odzivu na akcije korisnika.

5. Primeri algoritama za forenzičku analizu u zaštiti MANET od DDoS napada

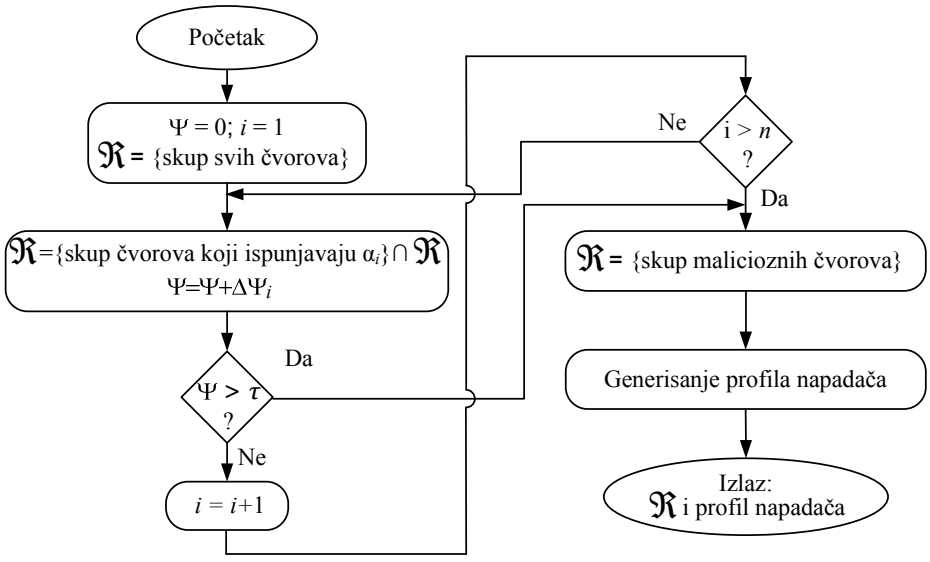
MANET je distribuirani sistem mobilnih čvorova koji se slobodno i dinamički sami organizuju u proizvoljne, privremene i ad hoc mrežne topologije, bez unapred obezbeđene komunikacione infrastrukture i centralne administracije. Zbog takvih svojstava ove mreže su vrlo osetljive na različite tipove napada, a posebno na distribuirane DoS napade (*Distributed Denial of Service*, DDoS). Tipičan DDoS napad izvodi se ''plavljenjem'' u kome grupa napadača koordinisano upućuje saobraćaj ka meti, sa ciljem da blokira glavne resurse mete ili da iscrpi raspoloživi mrežni propusni opseg. U DDoS napadu na MANET, napadač obično kompromituje određeni broj mobilnih čvorova, koji postaju tzv. ''zombi'' čvorovi. Svaki zombi generiše saobraćaj sličan legitimnom u pogledu intenziteta i veličine paketa. To znači da se snažan napad konstituiše koordinacijom više zombija. Tada je moguće da "plavljenje" ne bude usmereno na određeni MANET čvor (metu) nego da teži blokadi cele mreže [14]. DDoS napad se može izvesti na bilo kom sloju protokol steka što se manifestuje zagušenjem medijuma, prekidom logičkih linkova ili greškama u funkcionisanju protokola rutiranja, transportnih i aplikacionih protokola [15]. Osim broja zombija, na osetljivost MANET mreže značajno utiču način i brzina kretanja čvorova [16].

Evidencija događaja u mreži može se dobiti na osnovu snimanja realnog saobraćaja ili iz log fajlova u IDS sistemu (ili *firewall* uređajima). Zahtev da svaki MANET čvor snima saobraćaj u realnom vremenu je teže izvodljiv, s obzirom na ograničene procesorske, memorijske i energetske resurse čvorova. To znači da su, u najvećem broju slučajeva, log fajlovi podesniji izvor forenzičkih dokaza. Svaki zapis u IDS log fajlu obično je na nivou jednog paketa, a obuhvata informacije kao što su: IP

adresa izvora i odredišta, vremenski pečat (trenutak prijema paketa), tip transportnog protokola i dr.

U [14] je predložen analitički model za ispitivanje statističkih karakteristika uzoraka saobraćaja koji omogućuje da se detektuju anomalije i identifikuje DDoS napad. Pretpostavljen je napad na mrežnom sloju u kome napadači zloupotrebljavaju *broadcast* mehanizam u proceduri rutiranja tako što teže da paralizuju mrežu generisanjem velikog broja identičnih zahteva za uspostavljanje ruta (*Route REQuest*, RREQ). Druga pretpostavka je da IDS entitet postoji u svakom čvoru i održava log fajl sa osnovnim informacijama o svakom primljenom paketu (adrese izvora i odredišta, vremenski pečat). Definisana su dva kriterijuma detekcije koja se mogu kvantifikovati: prvi se odnosi na detekciju velikog broja identičnih RREQ paketa u sukcesivnim intervalima aktivnosti IDS, a drugi na detekciju generisanja saobraćaja velikog intenziteta (protoka). Kvantitativne vrednosti pomenutih kriterijuma detekcije zapravo predstavljaju nizove slučajnih promenljivih, čije se varijacije mogu modelovati pomoću sekvencijalne detekcije tačke promene. Cilj je da se utvrdi da li je posmatrani niz promenljivih statistički homogen, a ako to nije slučaj određuje se trenutak u kome se dogodila promena. Za takve potrebe iskorišćen je poznati algoritam CUSUM (*CUmulative SUM control chart*), koji posmatra varijacije srednje vrednosti u vremenu. On zatim izračunava kumulativnu sumu odbiraka slučajne promenljive, a kada ta suma premaši unapred definisani prag smatra se da se dogodila promena (napad).

Algoritam forenzičke analize predložen u [17] predviđen je za hijerarhijski model IDS sistema, a zasniva se na metodu eliminacije (slika 5).

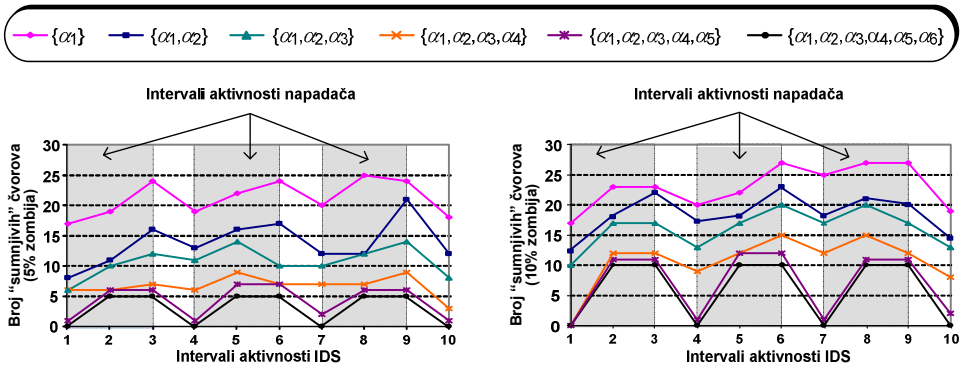


Slika 5. *Algoritam za forenzičku analizu DDoS napada u MANET (adaptirano iz [17]).*

Skup potencijalno malicioznih čvorova $\mathfrak{R}$ inicijalno obuhvata sve MANET čvorove. Unapred je definisan skup sukcesivnih kriterijuma $\{\alpha_1, \alpha_2, ..., \alpha_n\}$ za filtriranje

log fajla. Pretraživanje se obavlja iterativno, sa najviše *n* iteracija. Posle svake iteracije, iz skupa $\Re$ se eliminišu čvorovi koji ne ispunjavaju odgovarajući kriterijum pretrage. To znači da posle iteracije *i*, koja odgovara kriterijumu α_i , skup $\Re$ predstavlja grupu potencijalno malicioznih čvorova, koji ispunjavaju kriterijume $\{\alpha_1, \alpha_2, ..., \alpha_i\}$. Za ocenu malicioznosti mobilnog čvora uveden je faktor Ψ ($0 \le \Psi \le 1$), koji se inicijalno postavlja na vrednost 0, a zatim uvećava za unapred definisanu vrednost $\Delta\Psi_i$ posle svake iteracije *i*. Proces pretraživanja log fajla završava se kada vrednost faktora Ψ dostigne administrativno definisani prag τ ili kada se iscrpi skup svih kriterijuma pretrage, zaključno sa α_n . Posle analize zajedničkih svojstava malicioznih čvorova (IP adrese, veličina paketa, tip transportnog protokola, period aktivnosti itd.) generiše se profil napadača.

Iscrpna simulaciona analiza sprovedena je na modelu *Manhattan Grid* mreže sa 100 čvorova i jednim IDS centrom. Simuliran je DDoS napad na aplikacionom sloju, sa 5 i 10 zombija, koji sinhronizovano i povremeno generišu pakete istog tipa i veličine prema jednom odredištu (meti). Filtriranje log fajla vrši se pomoću skupa od šest sukcesivnih kriterijuma, koji označavaju: α_1 – aktivnost čvora, α_2 – zajedničku adresu odredišta, α_3 – isti tip transportnog protokola, α_4 – sličnu veličinu paketa, α_5 – eliminaciju kontrolnih paketa na nižim slojevima i α_6 – iste intervale generisanja saobraćaja.



a) b)

Slika 6. *Postupak detekcije DDoS napada za slučajeve: a) 5% zombi čvorova; b) 10% zombi čvorova (adaptirano iz [17]).*

Na slici 6 je prikazan postupak detekcije napada i broja potencijalno malicioznih čvorova, sukcesivnim uključivanjem kriterijuma $\alpha_1 - \alpha_6$. Značajna aktivnost grupe čvorova (kriterijum α_1) uočava se u tri intervala vremena, a zatim se uključivanjem kriterijuma $\alpha_2 - \alpha_4$ redukuje broj ''sumnjivih'' čvorova. Posle filtriranja log fajla pomoću kriterijuma α_5 i α_6 zaključuje se da je reč o povremenim

sinhronizovanim aktivnostima, identifikuje skup zombija $\Re$, kao i intervali njihove aktivnosti.

6. Zaključak

Tehnike forenzičke analize kontinuirano se razvijaju, primenjuju i unapređuju u današnjem Internetu, na različitim slojevima protokol steka i za različite tipove napada. U žičnim mrežama primenjuje se određeni broj dobro razvijenih alata za analizu napada na elektronsku poštu, pretraživače Weba, kao i IP *traceback* tehnike, koje otkrivaju putanje napada u smeru od mete ka napadaču. Koncepti *honeypot* i *honeynet* zasnivaju se na ideji da se instaliraju uređaji odnosno mreža koji su osetljivi na napade, sa ciljem da "privuku" napadače i namerno izazovu napade. Takav pristup je veoma efikasan za detekciju i analizu novih napada ili napada koji još nisu dovoljno ispitani.

U radu je posebna pažnja posvećena problemima sa kojima se suočava forenzička analiza napada na mobilne bežične mreže, kada se podaci o mobilnosti moraju uzeti u obzir pri modelovanju aktivnosti napadača. Problem se dodatno usložnjava ako su kolektori podataka mobilni kada je moguće da pojedini događaji ostanu neregistrovani, jer zona propagacije napada trenutno nije pokrivena kolektorskim čvorovima. Pored evidentne potrebe za standardizacijom procedura za prikupljanje digitalnih dokaza i forenzičku analizu, neophodan je razvoj formalnih tehnika za generisanje hipotetičkih akcija napadača u uslovima nepotpune digitalne evidencije. Takođe su predstavljena dva algoritma forenzičke analize DDoS napada u mobilnim ad hoc mrežama, zasnovana na pretraživanju i analizi log fajlova u IDS sistemu.

Zahvalnica. Rad je finansiran od strane Ministarstva prosvete, nauke i tehnološkog razvoja Republike Srbije (projekti tehnološkog razvoja TR 32025 i 36002).

Literatura

[1] E. Casey, "Network Traffic as a Source of Evidence: Tool Strengths, Weaknesses, and Future Needs", *Digital Investigation*, vol. 1, no. 1, 2004, pp. 28-43.

[2] A. Patel, S. Ó Ciardhuáin, "The Impact of Forensic Computing on Telecommunications", *IEEE Comm. Magazine*, vol. 38, no. 11, 2000, pp. 64-67.

[3] Y-S. Yen, I-L. Lin, A. Chang, "A Study on Digital Forensics Standard Operation Procedure for Wireless Cybercrime", *International Journal of Computer Engineering Science (IJCES)*, vol. 2, no. 3, 2012, pp. 26-39.

[4] C-Y. Ho, Y-C. Lai, I-W. Chen, F-Y. Wang, W-H. Tai, "Statistical Analysis of False Positives and False Negatives from Real Traffic with Intrusion Detection/ Prevention Systems", *IEEE Comm. Magazine*, vol. 50, no. 3, 2012, pp. 146-154.

[5] N. Meghanathan, S. Reddy Allam, L. A. Moore, "Tools and Techniques for Network Forensics", *International Journal of Network Security & Its Applications* (IJNSA), vol. 1, no. 1, 2009, pp. 14-25.

[6] S. Rekhis, N. Boudriga, "Formal Reconstruction of Attack Scenarios in Mobile Ad Hoc and Sensor Networks", *EURASIP Journal on Wireless Communications and Networking*, 2011. Available at: http://jwcn.eurasipjournals.com/content/2011/1/39.

[7] A. Chakrabarti, G. Manimaran, "Internet Infrastructure Security: A Taxonomy", *IEEE Network*, vol. 16, no. 6, 2002, pp. 13-21.
[8] T. Peng, C. Leckie, K. Ramamohanarao, "Survey of Network-Based Defense Mechanisms Countering the DoS and DDoS Problems", *ACM Computing Surveys*, vol. 39, no. 1, article 3, 2007.
[9] T. Korkmaz, C. Gong, K. Sarac and S. Dykes, "Single Packet IP Traceback in AS-level Partial Deployment Scenario", *International Journal of Security and Networks*, vol. 2, no. 1/2, pp. 95-108, 2007.
[10] The Honeynet Project. Available at http://www.honeynet.org.
[11] F. Pouget, M. Dacier, "Honeypot-based Forensics", in *Proc. of the AusCERT Asia Pacific Information Technology Security Conference 2004*, Brisbane, 2004.
[12] A. Vindašius, "Security State of Wireless Networks", *Elektronika Ir Elektrotechnika*, no. 7 (71), 2006, pp. 19–22.
[13] C. Xenakis, C. Panos, I. Stavrakakis, "A Comparative Evaluation of Intrusion Detection Architectures for Mobile Ad Hoc Networks", *Computers & Security*, vol. 30, no. 1, 2011, pp. 63-80.
[14] Y. Guo, I. Lee, "Forensic Analysis of DoS Attack Traffic in MANET", in *Proc. of the 4th Int. Conf. on Network and System Security*, Melbourne, 2010, pp. 293-298.
[15] M. Stojanović, V. Timčenko, S. Boštjančič Rakas, "Intrusion Detection Against Denial of Service Attacks in MANET Environment", in *Proc. of the POSTEL 2011*, Belgrade, December 2011, pp. 201-212.
[16] M. Stojanović, V. Aćimović-Raspopović, V. Timčenko, "The Impact of Mobility Patterns on MANET Vulnerability to DDoS Attacks", *Elektronika Ir Elektrotechnika*, no. 3 (119), 2012, pp. 29-34.
[17] V. Timčenko, M. Stojanović, "Application of Forensic Analysis for Intrusion Detection against DDoS Attacks in Mobile Ad Hoc Networks", in *Proc. of the 1st WSEAS Int. Conf. on Information Technology and Computer Networks (ITCN '12)*, Vienna, November 2012. (Plenary lecture).

Abstract: *Network forensics encompasses identification, collection, investigation and presentation of the digital evidence in order to detect unauthorized or malicious activities. In the first part of the paper, we address IP traceback techniques, which are used in the Internet for reconstruction of the attack path, from the victim to the attacker. Further, the concepts of ''honeypot'' and ''honeynet'' have been explained. They represent device and network intentionally designed to be vulnerable to different types of attacks, with the objective to identify attackers and analyze their behavior. In the second part of the paper, the issues of forensic analysis in wireless networks have been considered. Finally, we present the examples of forensic algorithms in mobile ad hoc networks.*

Keywords: *Digital evidence, forensic analysis, intrusion detection system*