

IDPS TEHNOLOGIJE U INDUSTRIJSKIM SISTEMIMA DALJINSKOG UPRAVLJANJA

Mirjana Stojanović¹, Jasna Marković-Petrović²

¹Saobraćajni fakultet u Beogradu, ²PD "HE Đerdap" - HE "Đerdap 2" Negotin

Sadržaj: *U radu su prvo opisane ključne funkcije sistema za detekciju i prevenciju napada (Intrusion Detection and Prevention Systems, IDPS), opšte metodologije detekcije napada i tipovi IDPS tehnologija. Zatim su analizirani specifični zahtevi industrijskih sistemima daljinskog upravljanja za IDPS i karakteristike telekomunikacionog saobraćaja u ovim sistemima, koje su relevantne za tehnike detekcije anomalija. Sledi prikaz karakterističnih arhitektura IDPS projektovanih za industrijske sisteme daljinskog upravljanja. Na kraju je ukazano na značaj procene bezbednosnog rizika pri projektovanju IDPS sistema i tokom njegove eksploatacije.*

Ključne reči: *Detekcija napada, prevencija napada, procena rizika, SCADA.*

1. Uvod

Usvajanje otvorenih komunikacionih standarda, korišćenje otvorenih softverskih platformi, povezanost sistema upravljanja sa drugim mrežama, daljinski pristup i dostupnost tehničkih informacija su razlozi zbog kojih je informaciono-komunikaciona infrastruktura savremenih industrijskih sistema daljinskog upravljanja (*Industrial Control Systems, ICS*) podložna različitim vrstama sajber napada. Posebno su osetljivi SCADA (*Supervisory Control and Data Acquisition*) sistemi, a to su distribuirani sistemi daljinskog nadzora i upravljanja koji prikupljaju i analiziraju informacije o industrijskom procesu i stanju pogona, u realnom vremenu. Sistematičan prikaz i analiza mogućih pretnji, kao i osetljivosti ICS na napade može se pronaći u literaturi [1], [2].

Poslednjih godina su veoma aktuelna istraživanja i razvoj rešenja sistema za detekciju i prevenciju napada (*Intrusion Detection and Prevention Systems, IDPS*) namenjenih za ICS mreže. Strogi zahtevi za rad u realnom vremenu i integritet podataka, pravilni uzorci telekomunikacionog saobraćaja i ograničen skup korišćenih protokola su polazni faktori za projektovanje i implementaciju specifičnih, sofisticiranih IDPS sistema. Veliki broj rešenja je još na nivou prototipskih implementacija, ili je tek u fazi verifikacije simulacijom ili u laboratorijskim uslovima. Cilj rada je da ukaže na specifičnosti IDPS sistema u ICS mrežama, na značaj razvoja takvih sistema, kao i planiranja ulaganja u IDPS, u procesu projektovanja i eksploatacije sistema zaštite.

Rad je organizovan na sledeći način. Drugo poglavlje sadrži kratak pregled opštih karakteristika IDPS tehnologija. U trećem poglavlju su analizirane specifičnosti ICS koje su relevantne za projektovanje i implementaciju IDPS sistema. Četvrto poglavlje obuhvata prikaz četiri arhitekture IDPS u industrijskim sistemima daljinskog upravljanja. U petom poglavlju je ukazano na značaj procene bezbednosnog rizika pri projektovanju i održavanju IDPS sistema. Šesto poglavlje obuhvata zaključna razmatranja.

2. Opšta svojstva IDPS tehnologija

Sistemi za detekciju napada (IDS) i sistemi za prevenciju napada (IPS) imaju mnogo zajedničkih svojstava, a administratori najčešće mogu da blokiraju preventivna svojstva IPS proizvoda, čime se njihova funkcionalnost svodi na IDS. Zbog toga se u literaturi obično sreće zajednički naziv – sistemi za detekciju i prevenciju napada (IDPS).

IDPS tehnologije razlikuju se prvenstveno po tipu događaja koje prepoznaju i po metodologiji koju koriste za identifikaciju incidenata [3]. Osim nadzora i analize događaja, IDPS tipično obuhvata i snimanje informacija o događajima, obaveštavanje administratora o važnim događajima putem upozorenja (alarma) i generisanje izveštaja.

Klasifikacija po tipu događaja obuhvata sledeće četiri grupe: (1) mrežni IDPS – nadgleda saobraćaj u pojedinim segmentima mreže i analizira aktivnosti mrežnih i aplikacionih protokola u cilju identifikacije sumnjivih aktivnosti; (2) bežični IDPS – nadgleda saobraćaj u bežičnoj mreži i analizira odgovarajuće MAC protokole; (3) IDPS za analizu ponašanja mreže – analizira mrežni saobraćaj sa ciljem identifikacije pretnji koje generišu neuobičajeni saobraćajni tokovi, kao što su DDoS (*Distributed Denial of Service*) napadi, neke forme malicioznog softvera ili narušavanje bezbednosnih politika i (4) IDPS u hostu – nadgleda karakteristike jednog hosta i događaja u njemu u cilju detekcije incidenata.

Metodologije za detekciju incidenata mogu biti: zasnovane na detekciji potpisa (*signature-based*), zasnovane na detekciji anomalija (*anomaly-based*) i zasnovane na analizi stanja protokola (*stateful protocol analysis*). Najveći broj IDPS tehnologija koristi više metodologija detekcije, zasebnih ili integrisanih, u cilju što tačnije detekcije širokog spektra napada.

Metodi zasnovani na detekciji potpisa porede nadgledane događaje sa potpisima (uzorcima koji odgovaraju poznatoj pretnji) u cilju identifikacije mogućih incidenata. Ovi metodi su vrlo efikasni u detekciji poznatih pretnji, ali i potpuno neefikasni u uslovima novih ili nepoznatih pretnji, kao i modifikovanih napada.

Metodi zasnovani na detekciji anomalija zasnivaju se na upoređivanju nadgledanih događaja sa listom aktivnosti koje su unapred definisane kao normalne, u cilju identifikacije značajnijih odstupanja. IDPS ima statičke ili dinamičke profile koji reprezentuju normalno ponašanje korisnika, hostova, mrežnih konekcija, ili aplikacija. Inicijalni profil generiše se tokom perioda treninga, koji obično traje nekoliko dana ili nedelja. Razvijen je veliki broj metoda za detekciju anomalija, koji mogu biti: statistički, zasnovani na *data mining*-u, zasnovani na znanju i zasnovani na mašinskom učenju [4]. Glavna prednost metoda zasnovanih na detekciji anomalija je visok stepen efikasnosti detekcije nepoznatih pretnji. Međutim, pogrešno uključivanje malicioznih aktivnosti u profile je tipičan problem ovih metoda. Drugi problem pri generisanju profila je pitanje tačnosti, a posledica je kompleksnih aktivnosti u mreži.

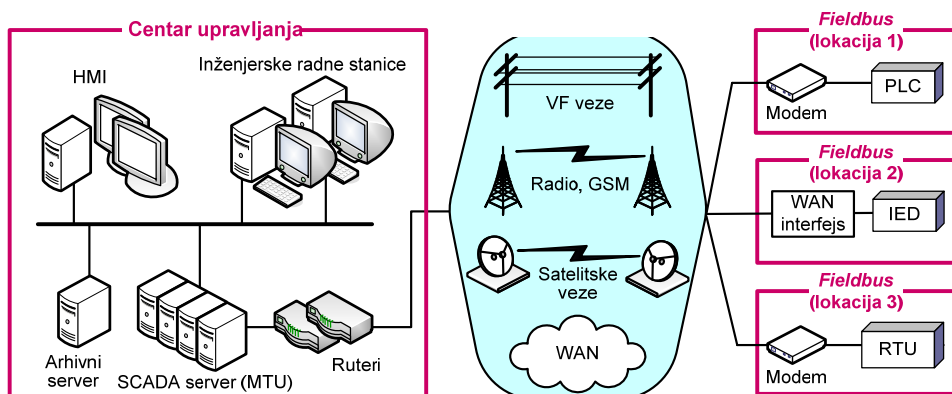
Metodi zasnovani na analizi stanja protokola upoređuju nadgledane događaje sa unapred određenim profilima, generisanim na osnovu definicija aktivnosti protokola za svako stanje protokol-automata. Drugim rečima, oni koriste univerzalne profile koje definišu organizacije za standarde i/ili proizvođači softvera. Ovi metodi mogu da identifikuju neregularne nizove poruka, kao što je ponavljanje iste komande, ili zadavanje komande kojoj nije prethodila komanda predviđena specifikacijom protokola. Njihov glavni nedostatak je intenzivno korišćenje procesorskih i memorijskih resursa zbog snimanja stanja velikog broja istovremenih sesija i složene analiza tih stanja.

IDPS tehnologije ne obezbeđuju potpuno tačnu detekciju napada. Stepenn tačnosti sistema opisuje se pomoću dva parametra: procenat normalnih aktivnosti koje su detektovane kao maliciozne (*False Positives*, FPs) i procenat malicioznih aktivnosti koje nisu detektovane, već su smatrane normalnim (*False Negatives*, FNs). Sistem je utoliko tačniji ukoliko su vrednosti FP i FN manje (u idealnom sistemu je FP=0 i FN=0). U većini IDPS sistema, redukcija FN povećava procenat FP i obrnuto. Često se usvaja bezbednosna politika kojom se smanjuje FN, na račun potencijalnog povećanja procenta FP. To znači da će biti detektovan veći broj malicioznih događaja, ali i da su potrebni dodatni analitički resursi da se izvrši diferencijacija FP od malicioznih događaja. Podešavanje tačnosti IDPS sistema vrši se promenljivim konfiguracionim parametrima.

Prevenција napada je odziv na detektovane pretnje pokušajem da se spreči njihova realizacija. Postoji nekoliko tehnika odziva: (1) IDPS zaustavlja napad raskidom mrežne konekcije ili korisničke sesije koja se koristi za napad, blokiranjem pristupa meti napada sa naloga ili IP adrese koja pripada napadaču, ili blokiranjem svih pristupa meti napada; (2) IDPS teži da poremeti napad promenom konfiguracije, promenom kontrolnih parametara ili generisanjem dodataka (*patches*) za softver uređaja i (3) IDPS menja sadržaj napada, uklanjajem ili zamenom malicioznih delova.

3. Specifičnosti industrijskih sistemima daljinskog upravljanja relevantne za IDPS

Vremenska kritičnost ICS (posebno SCADA sistema) je posledica zahteva da se pravovremeno reaguje na određene događaje i paralelnog izvršavanja različitih funkcija, jer se radi o distribuiranim sistemima sa geografski dislociranim komponentama.



Slika 1. Opšta blok šema SCADA sistema.

Na slici 1 prikazane su komponente i opšta konfiguracija SCADA sistema. Lokalna mreža u centru upravljanja povezuje SCADA server (*Master Terminal Unit*, MTU), inženjerske radne stanice, arhivni server, HMI (*Human Machine Interface*) server i konzole, kao i rutere i/ili svičeve za komunikaciju sa daljinskim stanicama. Centar upravljanja prikuplja i analizira informacije od daljinskih stanica (*fieldbus*-ovi na različitim lokacijama), prezentuje ih na HMI i generiše akcije na osnovu detektovanih događaja. Centar upravljanja je odgovoran i za opšte alarme, analizu trendova i generisanje izveštaja. U podsistemu daljinskih telemetrijskih jedinica (*Remote Terminal Units*, RTUs), programabilnih logičkih kontrolera (PLC) i inteligentnih elektronskih uređaja (IED) vrši se lokalna kontrola mernih pretvarača i nadzor senzora. Komunikacioni podsistem povezuje centar upravljanja sa podsistemom daljinskih stanica i omogućuje operateru daljinski pristup *fieldbus*-ovima za potrebe dijagnostike i otklanjanja otkaza. Za komunikaciju se koriste standardni ili namenski protokoli, preko veza tipa "tačka-tačka" ili širokopojasne IP-bazirane mreže.

Problem bezbednosti kontinualnog sistema koji radi u realnom vremenu zahteva sveobuhvatno razmatranje i holističko razumevanje bezbednosti mreže, teorije upravljanja i fizičkih sistema [5], [6]. Ultimativni cilj je da se ostvare zahtevane performanse u realnom vremenu, po principu 7 dana/24 časa, u realističnom okruženju u kome regularno ponašanje koegzistira sa otkazima sistema, uslovima okruženja, ljudskim greškama, ali i sajber napadima.

Aspekti relevantni za projektovanje IDPS su: vreme odziva sistema, pravovremena isporuka svih bitnih podataka i ažurnost podataka (podaci su validni samo u određenom intervalu vremena). Važan je i redosled ažuriranja podataka sa senzora, posebno ako oni vrše nadzor istog procesa ili korelisanih procesa. Redosled dolaska podataka u centar upravljanja igra značajnu ulogu u prezentaciji dinamike procesa i utiče na donošenje ispravnih odluka, bilo da se radi o algoritmu upravljanja (softveru) ili o operateru koji nadgleda industrijski proces.

Saobraćaj u ICS mrežama karakteriše se pravilnim uzorcima i relativno ograničenim skupom protokola. Ta svojstva su inherentno pogodna za razvoj i primenu tehnika zasnovanih na detekciji anomalija. U nastavku su navedena osnovna svojstva saobraćaja u ICS mrežama:

- **Koristan protok.** Stabilnost protoka je karakteristična za ICS mreže. Promene protoka mogu da budu indikacija događaja koji zahtevaju visok intenzitet saobraćaja (skeniranje, DoS napad, otkazi/greške u radu).
- **IP adrese i brojevi portova.** U ICS mrežama koje koriste statičko dodeljivanje adresa, očekuje se da soketi (parovi "IP adresa:Port") budu konstantni. Pojava novog soketa ukazuje na aktiviranje novog servisa, ali i na potencijalni napad.
- **Prosečna dužina paketa.** Većina sistema na nivou *fieldbus*-a generiše pakete poznate dužine, sa jasnom statistikom prosečne dužine. Zbog toga, prosečna dužina paketa predstavlja dobar pokazatelj normalnog ponašanja ili anomalije.
- **Merenje vremena.** Vreme prenosa i intervali međudolazaka paketa iz svih mrežnih čvorova su sadržajni podaci za detekciju napada u ICS mrežama. To proističe iz strogih zahteva za rad u realnom vremenu, posebno na nivou *fieldbus*-a. Vremenske karakteristike saobraćaja i pridružena statistika pokazuju pravilnosti i ujedno se razlikuju od saobraćaja tipičnih aplikacija u korporativnim mrežama i mrežama provajdera.

- **Smer toka podataka.** Smer toka podataka pokazuje koji sistem inicira konekciju. U tipičnoj operaciji, poznato je koji sistem inicira uspostavu veze. Kada se veza uspostavi, količina podataka koju jedan sistem šalje drugom je predvidljiva, sa velikom verovatnoćom, posebno kada je u pitanju poznat servis. Odstupanje od takvog ponašanja obično ukazuje na anomaliju.
- **Trajanje konekcije.** Trajanje konekcije je tipično za TCP protokol. S obzirom na ograničen broj servisa u ICS mreži, trajanje konekcija ima veoma malu varijansu.
- **Format i sadržaj korisnog segmenta.** Korisni segmenti (*payloads*) paketa koji potiču od ICS aplikacija su najčešće precizno definisani. Promene formata korisnog segmenta ukazuju na moguće anomalije u ponašanju sistema. Isto tako, uočene anomalije u sadržaju korisnog segmenta mogu da budu indikatori za detekciju pogrešne konfiguracije sistema ili malicioznih aktivnosti.
- **Preslikavanje MAC adresa u IP adrese.** Preslikavanje MAC adresa u IP adrese vrši se u svakom LAN-u u cilju detekcije promena hardverskih komponenata. Pojava nove MAC adrese ukazuje na instalaciju novog hardvera u mreži. S obzirom da se i MAC adrese mogu falsifikovati, korisne su za detekciju lažnog predstavljanja. One takođe pomažu administratoru da vodi evidenciju o legitimnom hardveru u sistemu.
- **Tipovi i konfiguracija protokola.** Protokoli koji se koriste u ICS mreži su precizno definisani i ograničeni. Prisustvo novih protokola u saobraćaju ukazuje na ozbiljne promene u mreži. Konfiguracija protokola je najčešće statička, a bira se tako da garantuje najbolje performanse mreže. Nadzor konfiguracionih parametara protokola omogućuje da se detektuju loše konfigurisani servisi i maliciozne aktivnosti.
- **Konektivnost.** Broj konekcija u ICS mreži je uglavnom permanentan, a konektivnost pojedinih čvorova zavisi od njihove uloge u mreži. Varijacije konektivnosti čvorova, srednje vrednosti konektivnosti (na nivou mreže) i raspodele konektivnosti mogu da budu indikatori malicioznih aktivnosti.

4. Prikaz karakterističnih arhitektura IDPS projektovanih za ICS mreže

4.1. Sistem za detekciju napada na Modbus TCP protokol stek

Modbus je namenski ICS protokol, zasnovan na komunikaciji klijent-server. Modbus klijent je nadređeni uređaj koji šalje upit Modbus serveru. Upit sadrži kôd funkcije, kojim se definiše traženi servis i listu pridruženih parametara, koja obuhvata adrese odredišta i bliži opis zahteva. Funkcije Modbus klijenta obuhvataju očitavanje diskretnih ulaza (na nivou bita) ili registara (na nivou 16-bitnih reči), upisivanje vrednosti na odgovarajuće izlaze i dijagnostičke funkcije za servere. Kada server primi i procesira zahtev, formira i šalje odgovor klijentu. Odgovor je ili pozitivan (normalan) ili negativan (obaveštenje da se desila greška ili izuzetak). Modbus upiti i odgovori koduju se u odgovarajuće jedinice podataka, koje se zatim enkapsuliraju ili u serijski protokol na sloju linka za podatke ili u TCP/IP stek (tada se skup protokola naziva "Modbus TCP").

U [7] su predložene tri tehnike za detekciju napada na Modbus TCP protokol stek, koje su verifikovane implementacijom prototipa.

Prva tehnika zasniva se na analizi stanja protokola, a usredsređena je na formate poruka. Izvršeni su kategorizacija i opis Modbus TCP zahteva i odgovora, polazeći specifikacije Modbus aplikacionog protokola i uputstva za implementaciju Modbus TCP.

Osnovna provera obuhvata specifikaciju pojedinih polja u Modbus porukama. Na primer, kôd funkcije je polje dužine jednog bajta. Za opseg vrednosti Modbus TCP upita R važi:

$$\forall R \in \text{ModbusTCPRequest} \rightarrow \text{funCodeField}(R) \in \{1 - 8, 15 - 16, 65 - 66\}.$$

Sledi unakrsna provera vrednosti polja, zato što opseg prihvatljivih vrednosti jednog polja može da zavisi od vrednosti drugog polja. Na primer, za očitavanje 1-bitnog ulaza (*Read coils*), kôd funkcije=1, a dužina poruke (*lenField*) je fiksna i iznosi 6 bajtova:

$$\forall R \in \text{ModbusTCPRequest} \rightarrow \text{if funCodeField}(R)=1 \text{ then lenField}(R)=6.$$

Složenije specifikacije obuhvataju više upita ili odziva. U regularnoj Modbus transakciji, vrednosti nekoliko polja u upitu moraju da se podudare sa vrednostima odgovarajućih polja u odzivu. Specifikacija sadrži i druge relacije između pojedinih polja u upitu i odzivu, zavisno od kodova funkcija. Na primer, pri očitavanju ulaznih registara (*Read input registers*), vrednost polja u upitu kojim se definiše broj registara treba da bude jednaka polovini vrednosti polja kojim se definiše broj bajtova u odgovarajućem odzivu (registri su 16-bitne reči). Takvo pravilo je korisno za detekciju preliivanja bafera.

U prototipskoj implementaciji razvijena su *Snort*¹ pravila za detekciju narušavanja nekih od pomenutih specifikacija. Definisani su skupovi regularnih i nevažećih kodova Modbus funkcija. Zatim su razvijena *Snort* pravila za detekciju Modbus upita koji sadrže kodove funkcija iz skupa nevažećih kodova. Pored pravila za kodove funkcija, razvijena su *Snort* pravila za druge atribute, kao što su identifikatori protokola, dužine paketa (ili pojedinih polja), kodovi izuzetaka, adrese i dr.

Druga tehnika takođe se zasniva na analizi stanja protokola, a podrazumeva modelovanje i formiranje skupa očekivanih uzoraka komunikacije između različitih komponenata Modbus mreže. Na primer, u regularnoj komunikaciji, Modbus serveri ne iniciraju uspostavu TCP veze, već samo odgovaraju na zahteve dobijene od Modbus klijenata. Iako se *Snort* može koristiti za detekciju narušavanja pravila izvedenih iz Modbus specifikacija, problem je što je na taj način teško opisati svojstva saobraćaja koja zahtevaju analizu više paketa. U [7] je, umesto *Snort*-a, korišćen jezik za specifikaciju i verifikaciju – PVS². Iskorišćeno je svojstvo PVS da omogućuje kodovanje i kompilaciju izvršnih specifikacija. Razvijen je formalni model Modbus sistema koji definiše dozvoljeni skup upita i očekivanih odziva, a zatim je generisan izvršni PVS model Modbus saobraćaja. Model definiše predikate kao što su **valid_request(r)** koji proverava da li je paket **r** prihvatljiv upit za uređaj **D**, i **valid_response(r,s)** koji proverava da li je **s** prihvatljiv odziv na upit **r**. Pošto su ti predikati izvršni, mogu se jednoznačno koristiti za detekciju napada: kada se uređaju **D** pošalje paket **r**, aktivira se **valid_request(r)**. Ako je rezultat – **false**, generiše se alarm. Slično važi za proveru regularnosti odziva **s** na upit **r**.

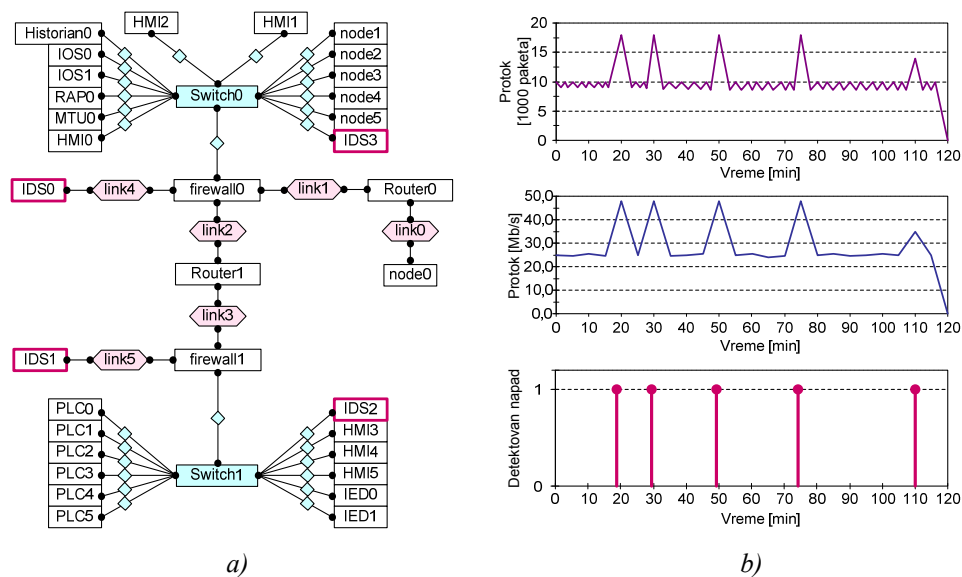
¹ *Snort* je mrežni IDS sa slobodno dostupnim kodom (<http://snort.org>). Zasniva se na relativno jednostavnom jeziku za specifikaciju zloupotreba i potpisa napada. U većini slučajeva, potpisi se kodiraju samo jednim *Snort* pravilom, kojim se definišu krajnje tačke veze i atributi paketa.

² PVS (*Prototype Verification System*) je jezik i automatizovano okruženje za formalnu specifikaciju i verifikaciju sistema (dostupan je na sajtu <http://pvs.csl.sri.com/>).

Treća tehnika zasnovana je na detekciji anomalija, a polazi od specifikacije očekivanih uzoraka komunikacije između komponenata mreže. Tehnika je prezentovana na primeru specifikacije politike pristupa serverima, odnosno definisanja pravila međusobne komunikacije u mreži. Na osnovu toga su definisana *Snort* pravila, pomoću kojih se mogu detektovati odstupanja od pomenutih politika.

4.2. Sistem za detekciju anomalija zasnovan na modelima konekcija

SPEAR (Systematic aPproach for connEction pAtteRn-based anomaly detection) je pristup za detekciju anomalija, zasnovan na modelima konekcija u SCADA sistemima [8]. Metodologija obuhvata: (1) ekstenziju Netlab³ klijenta, koji se koristi za formiranje SCADA mreže zbog pogodnog grafičkog interfejsa; (2) modelovanje topologije mreže zasnovano na široko rasprostranjenom, slobodno dostupnom simulatoru *ns-2* i (3) generisanje konfiguracionih fajlova za nekoliko sistema za detekciju anomalija zasnovanih na *Snort*-u.



Slika 2. Primer funkcionisanja algoritma *SPEAR*: a) Topologija SCADA sistema (*Netlab*) i b) detekcija napada (*Snort*) (adaptirano iz [8]).

Netlab klijent ima ugrađene komponente za formiranje topologije, definisanje protokola i generisanje saobraćaja u IP mrežama. Ekstenzija Netlab klijenta obuhvata komponente specifične za SCADA sistem: modem, HMI, PLC, IED, RTU, SCADA master i dr. Opis mreže obuhvata sve njene komponente i saobraćaj između njih. Pored toga, korisnik može manuelno da modeluje IDS zasnovan na detekciji anomalija. IDS se

³ Grafički korisnički interfejs zasnovan na jeziku Java. Omogućuje konstruisanje heterogenih topologija i specifikaciju svojstava saobraćaja (protok, kašnjenje). Kada je topologija definisana, može se eksportovati u fajl za simulator *ns-2* ili prebaciti u interaktivni čvor, sa mogućnošću promene parametara. Slobodno dostupan na sajtu: <http://www.emulab.net/netlab/client.php3>.

može povezati na dva načina: (1) na svičeve, kao regularni čvor mreže i (2) ili između LAN-ova, kao što se povezuju ruteri. Kada je opis mreže završen, grafički korisnički interfejs ga eksportuje u *ns-2* fajl (zajedno sa operativnim sistemom za svaki host). Taj fajl se procesira pomoću algoritma implementiranog na jeziku *Python*. Izlaz algoritma su *Snort* pravila pomoću kojih se mogu detektovati anomalije na modelima konekcija.

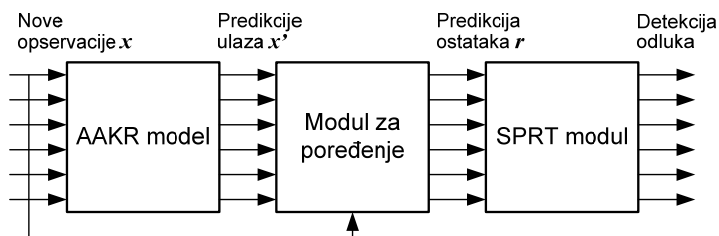
Evaluacija predloženog pristupa izvršena je simulacijom, na primerima karakterističnih topologija SCADA sistema [2]. Posle generisanja *Snort* pravila prethodno opisanim algoritmom, iskorišćeno je svojstvo simulatora *ns-3* da eksportuje simulirani saobraćaj u fajlove koji sadrže realne pakete, generisane iz modelovanog (legitimnog i malicioznog) saobraćaja. Zatim su identične topologije reprodukovane u *ns-3* i aktiviran je određeni broj generatora saobraćaja protoka 1Mb/s, tokom intervala od 2 časa. Saobraćaj su sačinjavali legitimni i maliciozni tokovi, pri čemu je maliciozni saobraćaj, kratkog trajanja, generisan u slučajnim intervalima. Primer topologije SCADA sistema, simulacije i detekcije napada ilustrovan je na slici 2.

Rezultati eksperimenata su pokazali da *Snort* detektuje napad pri svakoj pojavi saobraćajnog *burst*-a. Pošto su uzorci SCADA saobraćaja predvidljivi na svakoj konekciji, procenat detektovanih napada je 100%, bez pojave FP i FN. Algoritam je ispitan i na većim topologijama, koje su se sastojale od 10 do 100 LAN-ova, a pokazano je da vreme izvršavanja približno linearno zavisi od broja LAN-ova.

4.3. Primena statističkih tehnika podesnih za nadzor kritičnih sistema

Primena statističkih tehnika za detekciju anomalija, originalno razvijenih za nadzor kritičnih sistema kao što su nuklearne elektrane, predložena je u [9]. Prvo se vrši *on-line* trening da bi se formirali profili regularnog saobraćaja. Profili se opisuju specifičnim vektorima – indikatorima sistema, kao što su iskorišćenje linka, opterećenje procesora i neuspešno prijavljivanje sistemu. Profili se zatim klasifikuju zavisno od doba dana, dana u nedelji, vikenda/praznika itd. Alarm se generiše ako su novi podaci o mrežnom saobraćaju izvan unapred definisanog intervala poverenja za snimljene profile.

Eksperimentalno okruženje sačinjavaju SUN serveri i radne stanice. Simulirano je nekoliko tipova DoS napada na server. Podaci za inicijalnu analizu dobijeni su sa *auditing* sistema na SUN serveru, koji obezbeđuje statistiku o saobraćajnim tokovima sa ulaza i izlaza servera, kao i o radu hardvera. Za nadzor saobraćaja mogu se koristiti i različiti slobodno dostupni softverski paketi, kao što je NETTOP.



Slika 3. Dijagram sistema za detekciju anomalija [9].

Na slici 3 je prikazan blok-dijagram sistema za detekciju anomalija. Ulazni vektor x opisuje unapred određena svojstva koja reprezentuju ponašanje mreže.

Tehnikom autoasocijativne regresije jezgra (*Auto-Associative Kernel Regression*, AAKR) vrši se predikcija korektnih verzija ulaza, \mathbf{x}' . Korektnne verzije konstruišu se poređenjem trenutnih opservacija sa ranijim opservacijama koje označavaju normalno ponašanje. Ostaci (reziduumi) predikcije formiraju se poređenjem opservacija sa predikcijama modela. Reziduumi sadrže odstupanja od normalnog ponašanja, koja ukazuju na anomalije, odnosno na potencijalni napad. Na reziduume se primenjuje test odnosa statističkih verovatnoća (*Statistical Probability Ratio Test*, SPRT) da se odredi sa kojom verovatnoćom rezidualni niz reprezentuje normalno ponašanje odnosno anomaliju (modovi H_0 i H_1 , respektivno). Prvo se izračunava odnos verovatnoća na sledeći način:

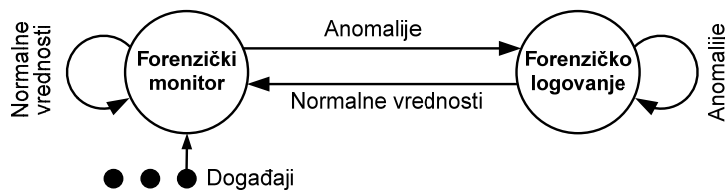
$$L_n = \frac{P(\{x_n\}/H_1)}{P(\{x_n\}/H_0)}, \quad (1)$$

gde $\{x_n\}$ predstavlja niz od n uzastopnih opservacija vektora \mathbf{x} . Konačna odluka donosi se poređenjem sa pragom koji uzima u obzir verovatnoće FP i FN.

On-line sistem za nadzor je realizovan pomoću softvera zasnovanog na MATLAB-u, koji obezbeđuje skup funkcija za aplikacije nadzora procesa i opreme. Ovaj sistem za prikuplja više od 60 promenljivih, kojima su iskazane statističke informacije o mrežnom saobraćaju i operativnom hardveru. Posle početnih testova ispostavilo se da je, za simulirane tipove DoS napada, relevantan samo mali broj promenljivih, kojima je iskazano iskorišćenje procesora i prosečno opterećenje u minutu. Trening se sastoji od 1000 opservacija odabranih u normalnim uslovima rada, dok je skup testova sačinjen od ukupno 300 opservacija, u normalnim uslovima rada i u uslovima napada.

4.4. Sistem zasnovan na forenzičkom monitoru događaja

Pristup opisan u [10] zasniva se na realizaciji forenzičkog monitora pomoću konačnog automata, koji funkcioniše kao agent za konstantno nadgledanje događaja u SCADA mreži. Forenzička analiza SCADA sistema u realnom vremenu usredsređena je na fizičke elemente povezane *fieldbus*-om, LAN mrežu kontrolera i supervizorski LAN.



Slika 4. Konačni automat u funkciji SCADA monitora u realnom vremenu [10].

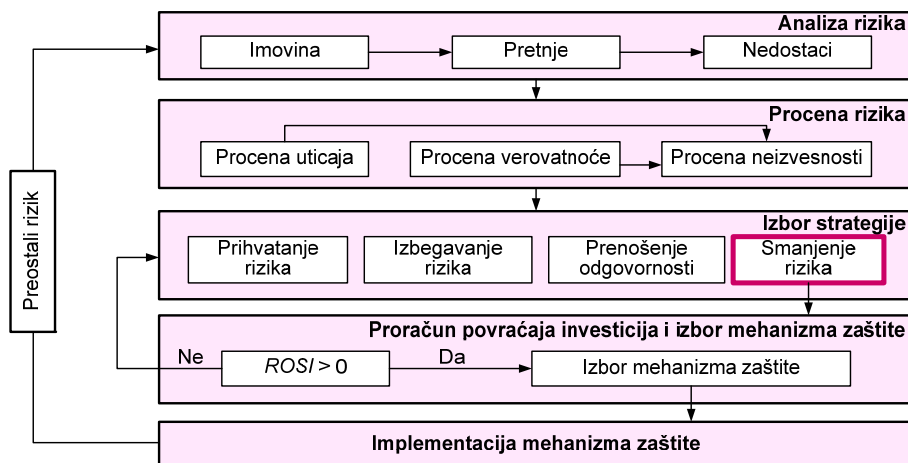
Automat sa dva stanja (forenzički monitor i forenzičko logovanje, slika 4) je softverski agent koji vrši kontinuiran nadzor stanja SCADA sistema i ispituje systemske promenljive, *tag*-ove senzora, mrežni saobraćaj i izvršavanje komandi. Ako agent detektuje da je očitana vrednost van opsega regularnih vrednosti, automatski se prebacuje u forenzički režim rada i inicira logovanje forenzičke informacije. U idealnom slučaju bio bi potreban poseban *backup* sistem za kontinuiranu ekstrakciju anomalija iz SCADA *tag*-ova i formiranje zapisa o svakom takvom događaju. Primeri zapisa su: opterećenje procesora, nazivi i vrednost senzora, stanja fizičke i virtuelne memorije, stanja diskova i

mrežnih drajvova, stanja mrežnih promenljivih, spisak aktivnih memorijskih procesa, nazivi izvršnih procesa, radni direktorijum, komandna linija, identifikatori korisnika, konekcije, tok izvršavanja komandi, deskriptori fajla, itd. Kada sistem počne da očitava normalne vrednosti, vraća se u stanje forenzičkog monitora i prekida logovanje.

SCADA sistem uobičajeno očitava svaki senzor ili upravljački registar sistema (*tag*). Učestanost logovanja varira od 300ms do 1s. Sistem ima i do 40000 *tag*-ova, kada generiše približno 400 gigabajta podataka u periodu od 24 časa. Prethodna kalkulacija izvedena je pod pretpostavkom da je prosečna dužina zapisa oko 120 bajtova. Drugim rečima, pored akvizicije podataka u realnom vremenu, problem predstavlja i obrada velike količine podataka. To zahteva manipulaciju upitima za baze podataka, kao i proces brzog prihvatanja i upisa koji treba da izvršava proces forenzičkog logovanja dok istovremeno novi podaci pristižu u sistem.

5. Procena bezbednosnog rizika pri projektovanju IDPS sistema

Uzimajući u obzir evidentnu potrebu za razvojem i implementacijom specifičnih IDPS sistema u ICS mreži, poželjno je da se pri projektovanju sistema zaštite izvrši procena bezbednosnog rizika, sa ciljem da se odredi optimalan nivo ulaganja. Upravljanje rizikom je kontinualan proces (slika 5), a svi koraci se ciklično ponavljaju, kako zbog preostalog rizika tako i zbog stalnog unapređenja, proširenja sistema i potencijalne pojave novih nedostataka i pretnji. Strategija smanjenja rizika, odnosno definisanje prihvatljivog rizika, je optimalna pri odlučivanju o investicijama u sistem zaštite ICS [11].



Slika 5. Proces upravljanja bezbednosnim rizikom [11].

Pregled i analiza metoda za procenu bezbednosnog rizika ICS mogu se pronaći u literaturi [11], [12]. Pokazalo se da opšti kvantitativni metodi procene rizika u informaciono-komunikacionim sistemima, zasnovani isključivo na ekonomskim kategorijama, nisu adekvatni za ICS, zbog toga što ne uzimaju u obzir specifičnosti u aspektima pouzdanosti, zahteva za kvalitet servisa i primenjenih protokola.

U radu [13] predložili smo metod procene bezbednosnog rizika u slučaju DDoS napada na infrastrukturu SCADA sistema i postupak *cost-benefit* analize za preporučenu primenu IDPS mehanizma zaštite. Metod predlaže kombinovanje kvantitativnog i kvalitativnog pristupa. Procena bezbednosnog rizika se zasniva na matematičkom pristupu i ekonomskim parametrima, a obuhvata proračun očekivanog godišnjeg gubitka (*Annual Loss Expectancy, ALE*) i povraćaja investicija u zaštitu (*Return On Security Investment, ROSI*). Kvalitativni pristup se ogleda u definisanju težinskih koeficijenata, koji kvantifikuju uslove u kojima se dogodio napad, a zavise od brojnih tehn-ekonomskih faktora. Pomenuti metod definiše preduslove za određivanje ovih koeficijenata, a to su analiza statističkih podataka i definisanje ključnih indikatora performansi (*Key Performance Indicator, KPI*) u skladu sa zahtevanim performansama koje obezbeđuju ostvarenje poslovnih ciljeva. Definisanje prihvatljivog praga za *ROSI* omogućuje donošenje odluke o optimalnom ulaganju u zaštitu SCADA sistema.

6. Zaključak

Zahtevi za kvalitet servisa, karakteristike telekomunikacionog saobraćaja i primenjeni aplikacioni protokoli uslovljavaju razvoj i implementaciju specifičnih rešenja IDPS u industrijskim sistemima daljinskog upravljanja. Pokazuje se da su metodi zasnovani na detekciji anomalija najpogodniji za primenu u takvim IDPS sistemima. Iako su statističke tehnike najopštije u smislu portabilnosti u različita operativna i komunikaciona okruženja, neophodna su "kustomizovana" rešenja, prilagođena specifičnostima konkretne ICS mreže. Pravilna procena bezbednosnog rizika u fazama planiranja, projektovanja i reinženjeringa sistema zaštite značajno doprinosi optimizaciji ulaganja u odgovarajuće mehanizme zaštite, uključujući i specifična IDPS rešenja.

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

Literatura

- [1] B. Zhu, A. Joseph, A. Sastry, "A Taxonomy of Cyber Attacks on SCADA Systems", in *Proc. of the 2011 Int. Conf. on the Internet of Things and the 4th Int. Conf. on Cyber, Physical, and Social Computing*, Dalian, China, 2011, pp. 380-388.
- [2] K. Stouffer, J. Falco, K. Scarfone, "Guide to Industrial Control Systems (ICS) Security", NIST Special Publication 800-82 Rev. 1, 2013.
- [3] K. Scarfone, P. Mell, "Guide to Intrusion Detection and Prevention Systems", NIST Special Publication 800-94, 2007.
- [4] V. Jyothsna, V. V. Rama Prasad, K. Munivara Prasad, "A Review of Anomaly based Intrusion Detection Systems", *International Journal of Computer Applications*, Vol. 28, No.7, 2011, pp. 26-35.
- [5] B. Zhu, S. Shankar, "SCADA-specific Intrusion Detection/Prevention Systems: A Survey and Taxonomy", in *Proc. of the 1st Workshop on Secure Control Systems (SCS)*, Stockholm, Sweden, 2010.

- [6] M. Mantere, M. Sailio, S. Noponen, "Network Traffic Features for Anomaly Detection in Specific Industrial Control System Network", *Future Internet*, Vol. 5, Issue 4, 2013, pp. 460-473.
- [7] S. Cheung et al., "Using Model-based Intrusion Detection for SCADA Networks", in *Proc. of the SCADA Security Scientific Symposium*, Miami Beach, FL, 2007.
- [8] D. A. Rusu, B. Genge, C. Siaterlis, "SPEAR: A Systematic Approach for Connection Pattern-based Anomaly Detection in SCADA Systems", *Procedia Technology*, Vol. 12, 2014, pp. 168-173.
- [9] D. Yang, A. Usynin, J. Wesley Hines, "Anomaly-Based Intrusion Detection for SCADA Systems", in *Proc. of the 5th Int. Topical Meeting on Nuclear Plant Instrumentation, Control and Human Machine Interface (NPIC & HMIT 2006)*, Albuquerque, NM, 2006.
- [10] P. Taveras, "SCADA Live Forensics: Real Time Data Acquisition Process to Detect, Prevent or Evaluate Critical Situations", in *Proc. of the 1st Annual Int. Interdisciplinary Conference (AIIC 2013)*, Azores, Portugal, 2013, pp. 253-262.
- [11] J. Marković-Petrović, M. Stojanović, "Analiza metoda za procenu bezbednosnog rizika SCADA sistema", *Zbornik radova 16. simpozijuma CIGRE Srbija – Upravljanje i telekomunikacije u elektroenergetskom sistemu*, Kladovo, 2014.
- [12] A. A. Cárdenas et al., "Attacks Against Process Control Systems: Risk Assessment, Detection, and Response", *Proc. of the 6th ACM Symposium on Information, Computer and Communications Security*, Hong Kong, 2011, pp. 355-366.
- [13] J. Marković-Petrović, M. Stojanović, "An Improved Risk Assessment Method for SCADA Information Security", *Elektronika Ii Elektrotehnika*, Vol. 20, No. 7, 2014, pp. 69-72.

Abstract: *In this paper, we first explain key functions of the Intrusion Detection and Prevention Systems (IDPS), general intrusion detection methods, as well as the existing IDPS technologies. We further analyze specific requirements of industrial control systems concerning IDPS, with the features of telecommunication traffic in such systems that are relevant for anomaly-based detection techniques. A survey of distinctive IDPS architectures designed for industrial control systems has also been provided. Finally, we point out the importance of security risk assessment during the design and operation of an IDPS system.*

Keywords: *Intrusion detection, intrusion prevention, risk assessment, SCADA.*

IDPS TECHNOLOGIES FOR INDUSTRIAL CONTROL SYSTEMS

Mirjana Stojanović, Jasna Marković-Petrović