Zbornik radova Fakulteta tehničkih nauka, Novi Sad

UDK: 004.4:621.395
DOI: https://doi.org/10.24867/01BE38Gogic

DDOS NAPAD NA SCADA PODSISTEM SMART GRID-A

DDOS ATTACK ON SCADA SMART GRID SUBSYSTEM

Damjan Gogić, *Fakultet tehničkih nauka, Novi Sad*

Oblast – ELEKTROTEHNIKA I RAČUNARSTVO

Kratak sadržaj – *U ovom radu su analizirane posledice DDoS napada na SCADA podsistem Smart Grid-a. Za potrebe testiranja razvijena je DERMS (Distributed Energi Resource Management System) aplikacija za upravljanje distribuiranim izvorima električne energije. U okviru aplikacije su razvijene tri različite arhitekture SCADA podsistema nad kojima su izvršavani DDoS napadi. Pomoću DDoS simulatora izvršava se napad na SCADA podsistem. Tokom napada su merene performanse sistema u zavisnosti od broja napadača i različitih arhitektura SCADA podsistema.*

Ključne reči: *Distributed Denial of Service, Supervisory Control and Data Acquisition, Smart Grid*

Abstract – *This paper analyzes the consequences of DDoS attacks against SCADA subsystems in Smart Grids. For the needs of testing, a small DERMS (Distributed Energi Resource Management System) application for managing distributed power sources has been developed. Within the application, three different SCADA subsystem architectures were developed over which DDoS attacks were performed. The SCADA subsystem was attacked by a DDoS simulator. During the attack, system performance was measured for various numbers of attackers and different SCADA architectures.*

Keywords: *Distributed Denial of Service, Supervisory Control and Data Acquisition, Smart Grid*

1. UVOD

Inteligentna, pametna ili mreža budućnosti (engl. *Smart Grid*), predstavlja unapređenu verziju tradicionalnih elektroenergetskih sistema dvadesetog veka. Korišćenje novih informacionih tehnologija, omogućilo je razvoj tradicionalnih elektroenergetskih sistema u cilju efikasnije, pouzdanije i brže isporuke električne energije. Zavisnost čovečanstva od električne energije je u konstantnom porastu i iz tih razloga elektroenergetski sistemi moraju da se razvijaju velikom brzinom.

Jedan od nadolazećih izazova sa kojima mora da se suoči *Smart Grid* jeste mogućnost sajber napada prouzrokovani

povećanjem površine napada usled upotrebe modernih komunikacionih i informacionih tehnologija.

NAPOMENA:
Ovaj rad proistekao je iz master rada čiji mentor je bio dr Lendak Imre, red. prof.

Motivi sajber napada na pametnu mrežu mogu biti ekonomski, dokazivanje, nezadovoljstvo zaposlenih, industrijska špijunaža, terorizam itd.

Zanemarivanje informacione bezbednosti u kritičnim infrastrukturama (u koje spada i pametna mreža), može da omogući napadaču da se lako infiltrira u sistem, dobije pristup softveru, koji upravlja mrežom, i na taj način destabilizuje sistem i nanese ozbiljne financijske gubitke preduzeću ali i potrošačima. Pored financijskih gubitaka, napadač može da ugrozi i privatnost potrošača, prikupljanjem i zloupotrebom njihovih podataka.

2. TEORIJSKE OSNOVE

2.1. *Distributed Network Protocol* (DNP3)

U svetu računarskih mreža, protokoli definišu pravila na osnovu kojih uređaji komuniciraju jedni sa drugima. DNP3 predstavlja skup komunikacionih protokola koji se koriste za komunikaciju između dve tačke u sistemima za automatizaciju industrijskih postrojenja [4]. Protokol je razvijen od strane Westronic kompanije (danas u vlasništvu GE Harris kompanije) tokom 1990ih. Arhitektura DNP3 protokola obuhvata četiri sloja. To su fizički, *DataLink*, transportni i aplikacioni sloj.

Fizički sloj je odgovoran za razmenu poruka preko fizičkih medijuma kao što su radio, satelit, bakar, itd [4]. Pored toga, odnosi se i na stanje medija (slobodno ili zauzeto), kao i na sinhronizaciju između strana koje razmenjuju poruke.

***DataLink* sloj** [4] je zadužen za obezbeđivanje dvosmerne komunikacije između aplikacija i uređaja u polju.

Transportni sloj je zadužen da rastavi poruku sa aplikativnog sloja u jedinice podataka veličine DataLink *frame*-a, kako bi bili podesniji za transport.

Aplikacioni sloj specificira DNP3 poruke zahteva i odgovora, definiše uloge *master* i *outstation* uređaja [4].

2.2. Bezbednost

Ukoliko se posmatra bezbednost informacionih sistema tri osnovne komponente zaštite su poverljivost, integritet i raspoloživost. Izraz koji se najčešće upotrebljava za ove tri komponente je CIA triada (**C** – *confidentality*, **I** – *integrity* i **A** – *aviability*).

Poverljivost [5] je komponenta koja obezbeđuje da informacija nije otkrivena neautorizovanim licima, entitetima ili procesima.

Integritet (celovitost, neokrnjenost) [5] znači održavanje i osiguravanje tačnosti i celovitosti informacije tokom celog životnog ciklusa.

Raspoloživost (dostupnost) [5] se može definisati kao mogućnost da se do informacije ili resursa dođe na pouzdan način u vremenski prihvatljivom intervalu.

2.4.1. DoS/DDoS

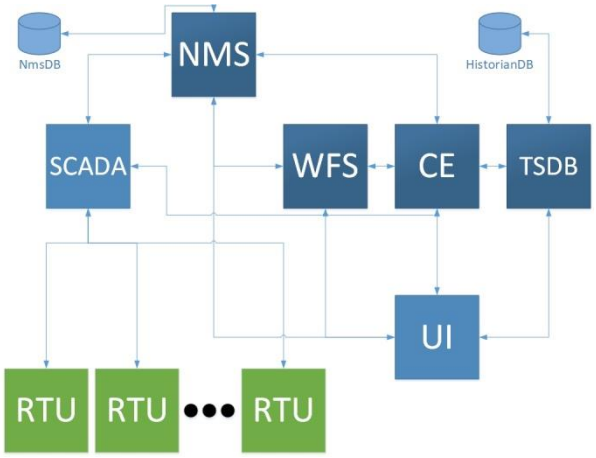
DoS (engl. *Denial of Service*) predstavlja napad koji narušava komponentu raspoloživosti. On se izvodi tako što se ciljanom sistemu šalje velika količina neželjenih poruka, koju on mora da obradi. Na taj način se iscrpljuju resursi sistema i on postaje nedostupan za sve korisnike njegovih usluga.

Ukoliko se sa jednog računara napada određeni sistem, servis ili proces radi se o jednostavnom DoS napadu, međutim, ako se napad izvodi sa više prostorno udaljenih računara tada se taj napad naziva distribuiran DoS (engl. *Distributed Denial of Service*) i često se zapisuje kao DDoS.

Prilikom primene DoS napada koristi se samo jedna IP adresa, dok se za DDoS napad koristi veliki broj zaraženih računara. Vlasnici računara sa kojih se izvodi DDoS napad često nisu svesni postojanja zlonamernog koda na njihovim računarima, koji se nazivaju *bot*-ovima a mreža takvih računara se naziva *botnet*. Zlonameran kod se širi putem internete često preko trojanaca, crva, *phishing email*-a, itd. Takav kod ne nanosi štetu računaru domaćinu, njegov zadatak je da ostane neprimetan i da služi za potrebe DDoS napada. Mrežom zaraženih računara upravlja napadač preko upravljačkog servera (engl. Command & Control – C&C server).

3. ARHITEKTURA SISTEMA

Razvijena aplikacija predstavlja *Distributed Energy Resource Management System (DERMS)* softversku platformu za nadgledanje, menadžment i regulaciju distribuiranih izvora energije. Pored toga, moguća je agregacija DER-ova po različitim kriterijumima (lokacija, tehnologija). Omogućeno je nadgledanje stanja rada svake grupe, kao i prognoza rada za svaku grupe Upravljanje radom svake grupe omogućeno je zadavanjem globalnog *setpoint*-a koji se automatski, optimalno raspoređuje na pojedinačne elemente grupe. Na slici 1 prikazana je arhitektura sistema.



Slika 1. *Arhitektura DERMS sistema*

Calculation Engine (CE) – Prikuplja analogna merenja preko SCADA komponente, generiše nadzorno upravljačke komande na zahtev korisnika sistema.

Network Model Service (NMS) - Osnovna namena NMS komponente je da ostalim komponentama u sistemu obezbedi pristup mrežnom modelu EES kroz odgovarajuće interfejse.

Remote Terminal Unit (RTU) - RTU se koristi za prikupljanje izmerenih analognih i digitalnih podataka sa uređaja u polju, i kao komandno komunikacioni kontroler za uređaje u polju.

Supervisory Control And Data Acquisition (SCADA) komponente obavlja funkcije nadzora i upravljanja fizičkom procesima realnom vremenu.

Time Series Database (TSDB) - TSDB predstavlja komponentu koji radi prikupljanje merenja očitanih sa SCADA servisa i njihovo skladištenje, pored toga radi agregaciju podataka na satnom, dnevnom, mesečnom i godišnjem nivou.

User Interface (UI) - Nadgledanje, menadžment i regulacija distribuiranih izvora električne energije omogućena je preko UI komponente.

Weather Forecast Service (WFS) – Namena WFS komponente je da ostalim komponentama omogući pristup vremenskoj prognozi. Pored trenutne vremenske prognoze servis obezbeđuje i predviđanje za sedam dana unapred sa rezolucijom od jednog sata.

4. REALIZACIJA NAPADA

Puna integracija elektroenergetskih sistema sa naprednim informacionim i komunikacionim tehnologijama, otvorila je mogućnost sajber (engl. *cyber*) napada. Od mogućih vektora napada ovde će se prikazati napad iz procesnog postrojenja.

4.1. Arhitektura napadnute komponente (SCADA)

4.1.1. SCADA komponenta bez redova

U SCADA komponenti bez redova čekanja, podaci iz svih RTU-ova se momentalno obrađuju u okviru programske niti dodeljene tom RTU-u. Svaka nit je zadužen za prihvatanje poruka, obrada, proveru alarma i obaveštavanje svih zainteresovanih strana o pristiglim promenama.

4.1.2. SCADA komponenta sa jednim redom

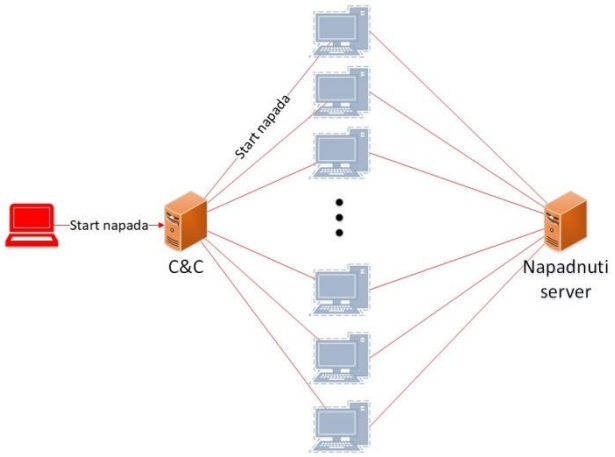
Implementacija SCADA komponente sa jednim redom zahteva da se za svaki RTU veže jedan programska nit koji prihvata podatke. Nakon što prihvati podatke, smešta ih u zajednički red čekanja i daje signal programskoj niti koji je zadužen za procesiranje podataka.

4.1.3. SCADA komponenta sa više redova

Karakteristično, za ovaj način implementacije, je da se za svaki RTU vezuje dva programske niti i jedan red čekanja. Jedna programska nit je zadužen prikupljanje podataka i njihovo smeštanje u red. Druga nit povlači i obrađuje podatke. Unapređenje se ogleda u tome što su podaci od svakog RTU-a obrađuju nezavisno jedan od drugog ali se ne može uticati na redosled izvršavanja.

4.2. Implementacija DDoS simulatora

Implementacija DDoS simulatora se oslanja na klasičnu centralizovanu klijent-server arhitekturu *botnet* mreže, gde se svaki *bot*, prilikom svoje aktivacije, javlja C&C serveru (Slika 2).



Slika 2. *Klasična klijent-server botnet arhitektura*

Komunikacije između njih je ostvarena putem WCF (engl. *Windows Communication Foundation*) *duplex* kanala. Svaki *bot* zna na kojoj se adresi nalazi C&C i prilikom svog startovanja uspostavlja WCF komunikaciju sa njim. Nakon uspostavljene komunikacije, C&C zna za tog *bot*-a i preuzima kontrolu nad njim tako što mu može komandovati da započne napad ili da ga zaustavi ukoliko je napad u toku. Prilikom komandovanja, *bot* dobija instrukciju kojom brzinom i na koliko adresa će da šalje podatke. U trenutku kada RTU izgubi konekciju sa SCADA komponentom, *bot* se aktivira i postavi na njegovo mesto ponašajući se kao regularni RTU. Poruke koje on šalje su u ispravnom DNP3 formatu, tako da SCADA ni u kom slučaju ne može da zna da li komunicira sa regularnim RTU-om ili malicioznim aplikacijom.

4.3. Scenariji i rezultati DDoS napada

U cilju da se simulira rad *Smart Grid* sistem, korišćena je *Microsoft Azure Cloud Computing Platform*-a. Na taj način dobijena je prostorna distribuiranost i nezavisnost resursa procesnog postrojenja i sistema koji njime upravlja. U okviru svakog scenarija, procesno postrojenje je simulirano sa 10 RTU-ova. Svaki RTU se izvršavao na zasebnoj virtualnoj mašini.

4.3.1. Scenario 1 – Uobičajen rad *Smart Grid* aplikacije

U okviru prvog scenarija se simulira uobičajen rad *Smart Grid* aplikacije gde SCADA komunicira se procesnim postrojenjem u kojem se ne nalazi ni jedan RTU zaražen zlonamernim kodom.

4.3.1.1. Rezultati testiranja

Rezultati testiranja izvršeni za sve tri arhitekture SCADA komponente, su identični. Zauzeće RAM memorije se je bilo statično, bez tendencije rasta, oko 42% od ukupne memorije računara na kom se sistem izvršavao. Procesor je prosečno, tokom svih pet časova rada, bio na 78% sa manjim varijacijama. Performanse sistema se mogu videti u tabeli 1.

Tabela 1. *Performanse uobičajenog rada sistema*

SCADA arhitektura	Zauzeće procesora [%]	Zauzeće RAM memorije [%]	Vreme ispada sistema
SCADA bez redova	78%	42%	-
SCADA sa jednim redom	78%	42%	-
SCADA sa više redova	78%	42%	-

4.3.2. Scenario 2 – Jedan RTU zaražen zlonamernim kodom

U okviru drugog scenarija se prikazuju se posledice po *Smart Grid* ukoliko se jedan RTU zarazi zlonamernim kodom.

4.3.2.1. Rezultati testiranja

Performanse rada sistema tokom napada prikazane su u tabeli 2. SCADA komponenta bez redova čekanja se najlošije pokazala tokom ovog testa. Jedino je u tom slučaju došlo do ispada sistema, gde je prva komponenta koja je otkazala bila *CalculationEngine*, nakon toga, otkazala je i SCADA.

Oko dva sata je bilo potrebno da se destabilizuje sistem. Međutim, na osnovu logova se moglo primetiti da, i pre nego što je otkazala, SCADA nije obrađivala sve pristigle podatke već je dolazilo do gubitka informacija.

Analizom logova, kreiranih tokom testiranja SCADA komponente sa jednim redom čekanja, može se primetiti da je već posle 10 minuta, red, u koji se smeštaju pristigli podaci, sadržao 1000 poruka koje su čekale na obradu. Taj broj se do kraja testa neprestano povećavao. Opterećenje procesora bilo oko 78%, dok se zauzeće RAM memorije blago povećavalo, što bi na duže staze dovelo do potrošnje resursa.

Implementacija SCADA komponente sa više redova pokazala je neznatno bolje rezultate u odnosu na prethodne dve arhitekture. Nakon 10 minuta rada sistema, redovi, koji prihvataju podatke sa RTU-ova sadržali su između 10 i 50 neobrađenih poruka.

Programske niti koje su zadužene za obradu podataka nisu uspevale da obrade pristigle podatke tako da se kašnjenje, na obradu, povećavalo.

Tabela 2. *Performanse sistema tokom napada*

SCADA arhitektura	Zauzeće procesora [%]	Zauzeće RAM memorije [%]	Vreme ispada sistema
SCADA bez redova	85%	39%	1h 56 min
SCADA sa jednim redom	78%	42%	-
SCADA sa više redova	70%	40%	-

4.3.3. Scenario 3 – Polovina RTU-ova zaražena zlonamernim kodom

Treći scenarijo prikazuje ponašanje SCADA komponente u slučaju kada je polovina RTU-ova, koji su pod njenim nadzorom, zaražena zlonamernim kodom.

4.3.3.1. Rezultati testiranja

Ponašanje *Smart Grid* sistema, kada se u okviru njega izvršava SCADA bez redova, je identično kao u prethodnom testu. Zauzeće procesora je iznosilo 88% dok se potrošnja memorije nije menjala. Nakon 1 sata i 50 minuta sistem je prestao sa radom.

Kada se posmatra arhitektura sistema sa jednim redom, broj zaostalih poruka, posle 10 minuta, iznosio je 5259. Posle pet sati testiranja, taj broj se povećao na 145118. Razlika u odnosu na prethodni slučaj je i ta što je nakon 2 sata došlo do prestanka rada *CalculationEngina*, međutim, on nije prouzrokovao otkaz čitavog sistema.

Tokom napada na SCADA komponentu sa više redova procesor je bio opterećen 98%. Zauzeće memorije se, do kraja testa, povećalo za 14%. Kao i u prethodnom slučaju, *CalculationEngine* je prestao sa radom nakon 2 sata od početka napada, posle toga je ručno podignut i sistem je nastavio sa radom.

Rezultati testiranja prikazani su u okviru tabele 3.

Tabela 3. *Performanse sistema tokom napada*

SCADA arhitektura	Zauzeće procesora [%]	Zauzeće RAM memorije [%]	Vreme ispada sistema
SCADA bez redova	88%	39%	1h 50 min
SCADA sa jednim redom	78%	Od 42% do 50%	2h (jedna komponenta)
SCADA sa više redova	98%	Od 40% do 54%	2h (jedna komponenta)

4.3.4. Scenario 4 – Nema regularnih RTU-ova

U okviru ovog scenarija nema ni jednog regularnog RTU-a, već su svi zaraženi zlonamernim kodom.

4.3.4.1. Rezultati testiranja

Rezultati SCADA komponente bez redova se nisu drastično menjali u odnosu na prethodne testove. Vreme kada je ceo sistem prestao sa radom je bilo oko 1 sat i 35 minuta. Zauzeće procesora u početku je iznosilo 92%.

Kada je u pitanju SCADA komponenta sa jednim redom procesor je prosečno bio opterećen 95%. Do kraja testa, potrošeno je dodatnih 38% RAM memorije. Nakon 4 sata i 16 minuta, aplikacija je prestala sa radom.

U slučaju SCADA komponente sa više redova, prosečno, 1500 poruka je bilo u svakom redu nakon 10 minuta rada. Da kraja, svaki red imao 36000 neobrađenih poruka. Procesor je konstantno radio sa 100% svojih mogućnosti dok je potrošnja RAM memorije bila u konstantnom porastu od 22%. Nakon 4h 20 minuta došlo je do ispada čitavog sistema.

Rezultati testiranja prikazani su u okviru tabele 4.

Tabela 4. *Performanse sistema tokom napada*

SCADA arhitektura	Zauzeće procesora [%]	Zauzeće RAM memorije [%]	Vreme ispada sistema
SCADA bez redova	98%	40%	1h 35min
SCADA sa jednim redom	95%	Od 39% do 77%	4h 16 min
SCADA sa više redova	100%	Od 40% do 62%	4h 10 min

3. ZAKLJUČAK

Elektroenergetski sistemi su tokom svog razvoja prešli put od tradicionalnih do naprednih (*Smart Grid*) sistema.

Jedan od osnovnih problema sa kojima se suočava pametna mreža jeste informaciona bezbednost. Kompleksnost sistema i integracija sa internetom, dvosmerna komunikacija sa velikim brojem distriburianih uređaja za prikupljanje podataka, povećali su ranjivost samog sistema.

Iz rezultata dobijeni tokom testiranja može se izvesti zaključak: bez obzira na arhitekturu SCADA komponente, dovoljan je samo jedan napadnut RTU u procesnom postrojenju kao izvor (D)DoS napada, da bi sistem postao nedostupan uz uslov da ne postoje implementirani bezbednosni mehanizmi na SCADA komponenti.

Testiranje sprovedeno u ovom radu predstavlja dobru osnovu za unapređenje bezbednosti *Smart Grid* sistema, kao i za razumevanje DDoS napada iz procesnog postrojenja preko DNP3 protokola.

4. LITERATURA

[1] J. P Arriaga., H. Rudnick, M. Rivier, „Chapter 1: Electric Energy Systems. An Overview.“, Boca Raton. CRC Press, 2009.

[2] V. Šiljkut, „Upravljanje potrošnjom u inteligentnim energetskim mrežama sa varijabilnom proizvodnjom.“ Beograd, 2014/15

[3] “Position Paper on Smart Grids”, European Regulators Group for Electricity and Gas (ERGEG) - Conclusions Paper, Jun 2010.

[4] M. Patwardhan, „DNP3: Security and scalability analysis.“ Sacramento, California State University, 2012

[5] M. Petković, „Prilog razvoju metode za detekciju napada ometanjem usluga na internetu“, Novi Sad. RS: Faculty of technical sciences, University of Novi Sad, 2018

Kratka biografija:

Damjan Gogić rođen je 1994. godine u Sanskom Mostu, Bosna i Hercegovina. Završio je srednju ekonomsku školu „Srednja ekonomska škola“ u Somboru 2013. godine. Osnovne akademske studije završio 2017. godine na Fakultet tehničih nauka u Novom Sadu.