XXXI Simpozijum o novim tehnologijama u poštanskom i telekomunikacionom saobraćaju – PosTel 2013, Beograd, 3. i 4. decembar 2013.

PRINCIPI REALIZACIJE IP MREŽA ZA PODRŠKU DALJINSKOG UPRAVLJANJA ELEKTROENERGETSKIM OBJEKTIMA

Mirjana Stojanović [1], Jasna Marković-Petrović [2]
[1]Saobraćajni fakultet u Beogradu, [2] PD "HE Đerdap" - HE "Đerdap 2" Negotin

Sadržaj: *U radu su prvo prikazane opšte karakteristike sistema daljinskog upravljanja u elektroprivredi, a zatim su detaljnije opisani savremeni SCADA (Supervisory Control and Data Acquisition) sistemi, koji se zasnivaju na TCP/IP modelu i Ethernet tehnologiji. Oni su najčešće integrisani u zajedničku IP mrežu, koja se koristi i za realizaciju drugih servisa za operativne i poslovne potrebe elektroprivrednog preduzeća. Diskutovani su kritični zahtevi za integraciju SCADA sistema u IP mrežu. Sledi prikaz simulacione analize uticaja distribuiranih DoS (Denial of Service) napada na performanse SCADA sistema. Na kraju rada su razmatrana rešenja zaštite IP baziranih SCADA sistema, sa posebnim osvrtom na značaj kvantitativne analize sigurnosnog rizika pri projektovanju sistema zaštite.*

Ključne reči: *Daljinsko upravljanje, kvalitet servisa, SCADA, sigurnost, VPN.*

1. Uvod

Funkcija daljinskog upravljanja elektroenergetskim sistemom postavlja specifične zahteve za telekomunikacione servise, koje karakteriše prenos heterogenih podataka u realnom vremenu i van realnog vremena (pogonskih podataka). Komunikacija se ostvaruje između centara upravljanja različitih nivoa, kao i između centara upravljanja i objekata elektroenergetskog sistema, i to na nivoima elektrana, mreže prenosa i distributivnih mreža. Novi komunikacioni zahtevi pojavljuju se u sklopu funkcionisanja tržišta električne energije: podaci za obračun razmene energije, proračun raspoloživih kapaciteta prenosa, izrada programa razmena i realizovanja energetskih transakcija. Imajući to u vidu, koncepcija tradicionalnih SCADA (*Supervisory Control and Data Acquisition*) sistema proširena je EMS (*Energy Management System*) i DMS (*Distributed Management System*) sistemima, koji pretpostavljaju koncept distribuiranih centara upravljanja u integrisanom mrežnom okruženju.

Savremeni telekomunikacioni sistemi za podršku daljinskog upravljanja zasnivaju se na otvorenim standardima, a prvenstveno na TCP/IP modelu i Ethernet tehnologiji. Ove tehnologije omogućuju i pristup podacima SCADA sistema preko pretraživača Weba. Daljinsko upravljanje se najčešće realizuje posredstvom zajedničke IP mreže, u koju su integrisani i drugi telekomunikacioni servisi za operativne i poslovne

potrebe elektroprivrednog preduzeća. U ovom radu su analizirani preduslovi za integraciju daljinskog upravljanja u elektroprivrednu IP mrežu: diferencijacija nivoa kvaliteta servisa (*Quality of Service*, QoS), međusobna izolacija saobraćaja koji potiče od različitih aplikacija, bezbednost i pouzdanost.

Rad je organizovan na sledeći način. Drugo poglavlje sadrži prikaz arhitekture SCADA sistema i pregled standardizovanih komunikacionih protokola za podršku sistema daljinskog upravljanja. U trećem poglavlju su diskutovani kritični zahtevi za integraciju sistema daljinskog upravljanja u IP mrežu. U četvrtom poglavlju je prikazana analiza performansi SCADA sistema u uslovima distribuiranog DoS napada. Peto poglavlje posvećeno je tehnikama zaštite i metodama procene sigurnosnog rizika. Šesto poglavlje obuhvata zaključna razmatranja.

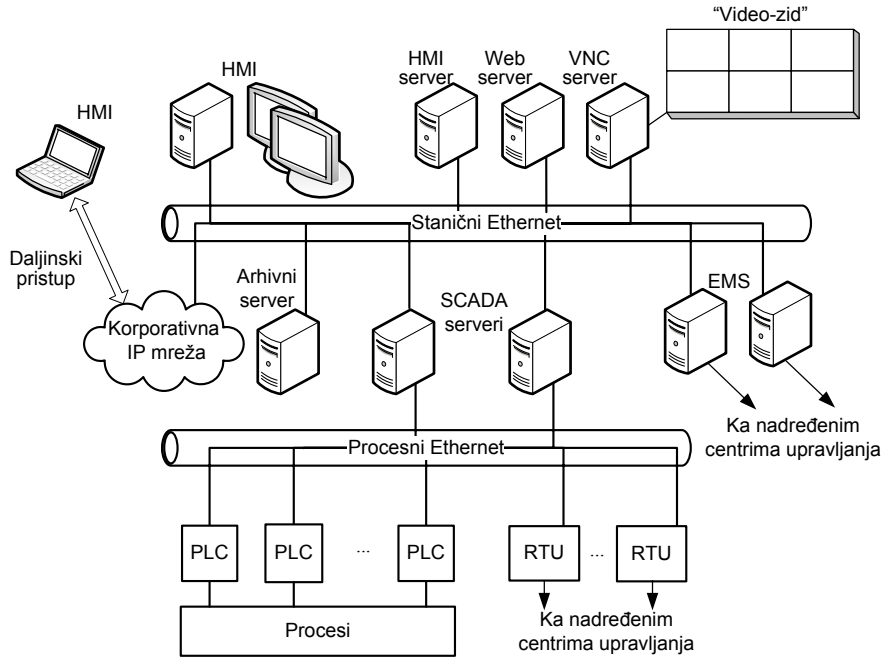
2. Arhitektura sistema daljinskog upravljanja i pregled standardizovanih protokola

SCADA sistem obezbeđuje pravovremene i tačne informacije o procesu i stanju pogona u elektroenergetskim postrojenjima, što doprinosi efikasnom, pouzdanom i bezbednom nadzoru i upravljanju, kao i optimizaciji procesa proizvodnje, prenosa i distribucije električne energije. Na taj način se postižu i manji operativni troškovi. Glavni zadatak je da obezbedi operateru sredstvo i način upravljanja visoko automatizovanim procesom. Neophodan je pregled celokupnog sistema sa lako dostupnim relevantnim informacijama o stanju procesa kako bi se omogućila pravovremena akcija operatera. SCADA/EMS sistem se sastoji iz više podsistema [1]:

- Podsistem daljinskih telemetrijskih jedinica (*Remote Terminal Units*, RTUs) i programabilnih logičkih kontrolera (*Programmable Logic Controllers*, PLCs)[1], povezanih na merne pretvarače i senzore u procesu, preko kojih se vrši prikupljanje analognih i digitalnih veličina, kao i izdavanje upravljačkih naloga procesu u vidu digitalnih komandi ili zadavanjem analognih vrednosti neke veličine;
- Komunikacioni podsistem, koji obezbeđuje vezu između centralne stanice i udaljenih terminala sa jedne strane i korisnika sa druge;
- Centralni podsistem, koji obuhvata skup servera sa bazama podataka, aplikativnim softverom i softverom za vizuelizaciju, npr. VNC (*Virtual Network Computing*);
- Interfejs između operatera i sistema (*Human Machine Interface*, HMI), koji obezbeđuje grafički prikaz i kontrolu procesa;
- Podsistem za obradu i arhiviranje podataka, kreiranje i distribuciju dispečerskih izveštaja i ostale zahteve korisnika sistema;
- Podsistem za merenje i obračun razmene energije (EMS).

Većinu savremenih SCADA sistema karakteriše formiranje posebne podmreže, povezane sa korporativnom mrežom elektroprivrednog preduzeća. Operaterska mesta mogu se implementirati i u klijentima poslovne mreže, posredstvom Web aplikacija. Primer arhitekture SCADA sistema u elektroenergetskom objektu prikazan je na slici 1.

[1] Kod većine proizvođača PLC je uređaj opštije namene od RTU, odnosno može se primenjivati za kontrolu različitih industrijskih procesa i lako se konfiguriše za različite funkcije.



Slika 1. *Primer arhitekture SCADA sistema u elektroenergetskom objektu.*

Komunikacioni podsistem treba da obezbedi pouzdan prenos i razmenu informacija između RTU jedinica i centra upravljanja, koristeći telekomunikacione tehnologije visokih performansi. On ima mogućnost rada u modu ciklične prozivke, kada centar upravljanja periodično proziva i prikuplja podatke od konektovanih daljinskih jedinica, kao i u modu komunikacije na zahtev, koja se inicira registrovanjem unapred definisanih događaja od strane daljinske jedinice. Da bi se osigurao pouzdan prenos podataka i eliminisali efekti elektromagnetskih smetnji, kao medijum prenosa u okviru elektroprivrednog objekta prvenstveno se koriste optička vlakna. Komunikacija između daljinskih jedinica i centra upravljanja može se obavljati radio linkovima, iznajmljenim telefonskim linijama ili posredstvom optičkih vlakana postavljenih unutar zaštitne užadi po dalekovodima (*Optical Ground Wire*, OPGW).

Standardizovane komunikacione arhitekture za SCADA/EMS/DMS su IEC[2] 870-5, IEC 870-6 i EPRI[3] UCA (*Utility Communications Architecture*) 2.0, a UCA rad na standardizaciji objektnih modela je nastavljen kroz definisanje serije standarda IEC 61850. Osim navedenih protokola, u širokoj upotrebi su industrijski standardi Profibus DP i MODBUS, namenjeni za komunikaciju PLC kontrolera u udaljenim sistemima (npr. turbinska regulacija agregata, sistem za temperaturnu kontrolu agregata).

Protokoli serije **IEC 870-5** definišu aplikacioni sloj, sloj linka za podatke i fizički sloj. Namenjeni su razmeni podataka u realnom vremenu između RTU i centra upravljanja, u sistemima koji zahtevaju kratko vreme odziva, u uslovima malog

[2] International Electrotechnical Commission.
[3] Electric Power Research Institute.

propusnog opsega komunikacionog kanala, često u prisustvu različitih oblika elektromagnetske interferencije, a ograničeni su na višestruke veze tačka-tačka i zvezdasto-petljaste konfiguracije. Osnovni protokol ove serije, 870-5-101, podržava nebalansirani (*master/slave*) i balansirani režim prenosa podataka. Podacima se mogu dodeliti dva nivoa prioriteta u prenosu. Protokol obezbeđuje periodično i sporadično (spontano) ažuriranje podataka, kao i sinhronizaciju.

IEC 870-5-103 je unapređena varijanta protokola 101 u pogledu mehanizama za transfer fajlova. Predstavlja prateći standard koji obezbeđuje interoperabilnost opreme za telezaštitu i kontrolnog sistema u transformatorskoj stanici. IEC 60870-5-104 je takođe unapređena varijanta protokola 101, koja predviđa TCP/IP interfejs za povezivanje na LAN i različite tipove WAN mreža. Standard definiše protokole za prenos podataka preko Etherneta i serijskom vezom (*Point-to-Point Protocol*, PPP).

Standardi serije **IEC 870-6** definišu protokole za daljinsko upravljanje kompatibilne sa OSI referentnim modelom. Osnovna ideja je da se razvoj protokola specifičnih za daljinsko upravljanje ograniči na aplikacioni sloj, odnosno na definisanje aplikacionog servisnog elementa za daljinsko upravljanje (*Telecontrol Application Service Element*, TASE). Aktuelna verzija je TASE2, definisana standardima 870-6-503 (servisi i protokoli), 870-6-802 (objektni modeli) i 870-6-702 (aplikacioni profil). Namenjen je za razmenu podataka u realnom vremenu, obračun razmene energije, daljinsko upravljanje, operatorske poruke i daljinsko izvršavanje programa.

IEC 61850 *(Communication Networks and Systems in Substations)* je globalni standard za informacione modele i razmenu informacija u oblasti automatizacije transformatorskih stanica. Automatizovani sistem je skup povezanih inteligentnih elektronskih uređaja, koji međusobno razmenjuju informacije u cilju realizacije procesa kao što su zaštita, nadgledanje, merenja i funkcionisanje elektroenergetskog objekta (npr. sabirnica, transformator ili vod). Standard uvodi objektno orijentisan pristup modelovanju funkcija postrojenja, a u cilju interoperabilnosti opreme različitih proizvođača neophodno da se definišu modeli svih poznatih funkcija i tipova podataka struktuiranih u tri hijerarhijska kontrolna nivoa: nivoa stanice, nivoa polja i nivoa procesa. Modeli su prilagođeni potpuno distribuiranim sistemima, u kojima su tipovi podataka definisani prema odgovarajućim funkcionalnim elementima kao što su prekidači, rastavljači, merni transformatori itd. Standard je podeljen na više delova koji opisuju različite aspekte komunikacione mreže transformatorske stanice, kao što su:

- Opšti i specifični funkcionalni zahtevi za komunikaciju u transformatorskoj stanici;
- Identifikacija servisa, modela podataka, protokola aplikacionog sloja i nižih slojeva;
- Specifikacija formalne opisne tehnike SCL (*Substation Configuration description Language*) na osnovu koje se obezbeđuje standardni format konfiguracionih fajlova, odnosno detaljni formalni opis konfiguracije sistema;
- Apstraktna prezentacija podataka i servisa odnosno kreiranje objekata/instanci podataka i servisa koji su nezavisni od primenjenih protokola nižih slojeva;
- Preslikavanje apstraktnih servisa u konkretne protokole, kao što su MMS (*Manufacturing Messaging Specification*), Ethernet i dr.;
- Metodologija testiranja saglasnosti (konformnosti) implementacija sa standardima;
- Komunikacija između transformatorskih stanica;
- Komunikacija između centra upravljanja i transformatorske stanice.

Standard **IEC 61970** (*Energy Management System Application Program Interface*) definiše principe povezivanja aplikacija za EMS sisteme, razvijenih na različitim programskim jezicima, operativnim sistemima i modelima podataka. Standard definiše apstraktni, objektni informacioni model (*Common Information Model,* CIM), koji stvara preduslove za integrisanje konfiguracionih podataka iz raznih delova sistema upravljanja putem njihove razmene u opšte prihvaćenom XML formatu.

3. Kritični zahtevi za integraciju daljinskog upravljanja u IP mrežu

Opšti preduslovi za integraciju heterogenih servisa u zajedničku IP-baziranu mrežu elektroprivrednog preduzeća su: pravilno projektovanje mreže, podrška različitih nivoa QoS, određeni stepen međusobne izolacije servisa i stvaranje uslova za bezbedan rad mreže kroz implementaciju odgovarajuće politike zaštite. Za donošenje odluke o stepenu i strategiji integracije servisa presudni su tehno-ekonomski faktori, mada mogu da budu značajni i zakonski normativi specifični za pojedine države, kao i komunikacioni zahtevi koji se pojavljuju u međunarodnoj interkonekciji elektroenergetskih sistema.

Međunarodna organizacija CIGRÉ[4] propisuje sledeće zahteve za QoS parametre daljinskog upravljanja: vreme prenosa ≤ 1s, protok ≤ 2Mb/s i raspoloživost > 99,98% [2]. Na osnovu takvih zahteva, CIGRÉ kvalifikuje daljinsko upravljanje kao "nekritičan servis u realnom vremenu", koji se može implementirati u IP mrežama i integrisati sa drugim telekomunikacionim servisima. O tome svedoče i praktična iskustva elektroprivrednih kompanija u SAD, Japanu, Švedskoj, Švajcarskoj, Španiji, Portugaliji i drugim zemljama, a poslednjih godina se IP-bazirani sistemi daljinskog upravljanja intenzivno realizuju i u Elektroprivredi Srbije [3]. Detaljnija razmatranja o principima modelovanja i projektovanja multiservisnih mreža u elektroprivredi mogu se pronaći u [4], gde su predstavljeni i rezultati iscrpne simulacione studije o integraciji heterogenih servisa (daljinsko upravljanje, VoIP, video-konferencije i tradicionalni Internet servisi), principima klasifikacije saobraćaja i izboru optimalne discipline opsluživanja paketa u cilju podrške različitih nivoa kvaliteta servisa.

Primena IP virtuelnih privatnih mreža (*Virtual Private Network*, VPN) je ekonomično rešenje za elektroprivredne mreže sa integrisanim servisima, jer omogućuje razdvajanje saobraćaja koji potiče od različitih aplikacija (bez potrebe za formiranjem fizički odvojenih podmreža), različite nivoe QoS i zaštitu informacija posredstvom *IP Security* protokola [3]. VPN servisi obično se konfigurišu u sklopu elektroprivredne IP mreže zasnovane na sopstvenoj infrastukturi komutacije i prenosa. Pri tome se mogu koristiti VPN sa pristupom na sloju 2 (L2) ili na sloju 3 (L3). Organizacija CIGRÉ je 2007. godine realizovala međunarodni projekat o implementaciji operativnih servisa posredstvom IP VPN [5]. Istraživanjem su obuhvaćeni SCADA/EMS, komunikacija između centara upravljanja, alarmni sistemi u transformatorskim stanicama, operativna telefonija, razmena električne energije, upravljanje telekomunikacionim sistemom, *outsourcing* i dr. U projektu su predstavljena iskustva jednog broja svetskih elektroprivrednih kompanija i ukazano je na područja primene IP VPN.

S obzirom na značaj daljinskog upravljanja za funkcionisanje elektroprivrednog preduzeća i sistema u celini, sigurnost servisa predstavlja imperativ u projektovanju i eksploataciji IP mreže. Tipične pretnje savremenim SCADA sistemima su zlonamerni

[4] Conseil International des Grand Réseaux Électriques.

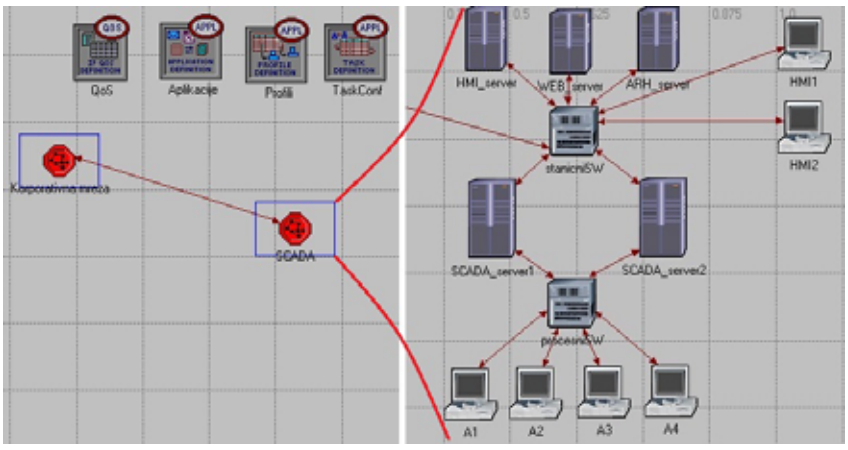
programi, unutrašnji i spoljašnji napadi. Zlonamerni korisnici koriste poznate osetljivosti ICT sistema, ali i specifične nedostatke u mehanizmima zaštite SCADA sistema kao što su: greške u operativnom sistemu, zanemarivanje autentifikacije, daljinsko konfigurisanje, povezanost sa drugim mrežama, primena bežičnih veza, izostanak primene antivirusnih softvera, nepostojanje sistema za otkrivanje napadača i ljudski faktor (nedovoljno iskustvo, nedovoljno fizičko obezbeđenje lokacija) [6]. Sistematizacija napada na SCADA sisteme i prikaz evidentiranih napada na industrijske kontrolne sisteme u svetu može se pronaći u [7].

4. Analiza performansi SCADA sistema u uslovima DDoS napada

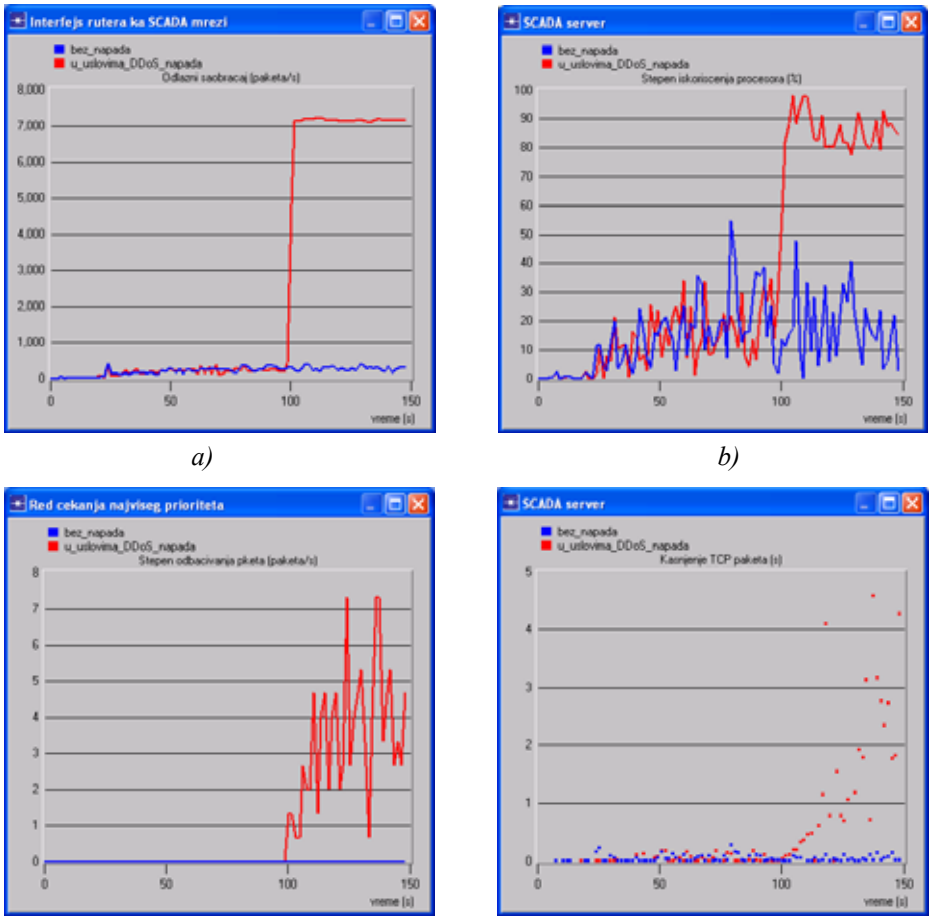
Odbijanje servisa (*Denial of Service*, DoS) je napad u kome se legitimnim korisnicima onemogućuje pristup servisima ili resursima mreže. Ovaj tip napada može se vršiti u različitim formama na bilo kom sloju protokol steka. Posebno je teško otkriti i sprečiti distribuirane DoS (DDoS) napade u kojima više napadača istovremeno napada metu (npr. neki vitalni mrežni server). 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 propusni opseg dela mreže [8].

Analiza performansi SCADA sistema u uslovima DDoS napada izvršena je simulacijom, pomoću programskog paketa *OPNET IT Guru Academic Edition* [9]. Detaljan prikaz analize dat je u [10]. Simulirana mreža je sastavljena od korporativne podmreže i podmreže SCADA sistema, kao što je prikazano na slici 2. Podmrežu SCADA sistema čine: (1) stanični deo sa Web serverom, arhivnim serverom, HMI serverom i računarima za vizuelizaciju procesa (HMI1 i HMI2) i (2) procesni deo sa daljinskim jedinicama za upravljanje agregatima i pomoćnim sistemima elektrane. SCADA serveri imaju dualne mrežne interfejse, po jedan za povezivanje sa staničnim odnosno procesnim delom podmreže. Korporativni deo mreže sačinjava 50 klijentskih računara.

U simulacionom modelu definisane su tri grupe saobraćajnih tokova: saobraćaj unutar SCADA podmreže, saobraćaj između korporativne podmreže i SCADA podmreže i saobraćaj kojim je simuliran DDoS napad.



Slika 2. *Topologija simulirane mreže (OPNET).*



a) *b)*

c) *d)*

Slika 3. *Degradacija performansi SCADA sistema u uslovima DDoS napada: a) odlazni saobraćaj ka SCADA podmreži; b) iskorišćenje procesora SCADA servera; c) stepen odbačenih paketa (SCADA saobraćaj); d) kašnjenje (SCADA saobraćaj).*

SCADA saobraćaj je simuliran pomoću tri profila zasnovana na FTP (*File Transfer Protocol*) izvorima, koji koriste TCP protokol:

- Profil 1 – slanje rezultata merenja iz pogona ka centru upravljanja: vreme ponavljanja događaja je konstantan kratak period, a količina podataka odgovara uniformnoj raspodeli u opsegu manjih vrednosti;
- Profil 2 – razmena signala alarma i komandi između centra upravljanja i pogona: saobraćaj se generiše u skladu sa Poasonovom raspodelom;
- Profil 3 – razmena dispečerskih izveštaja između SCADA sistema: vreme ponavljanja je konstantan duži period, a količina podataka odgovara uniformnoj raspodeli (veći fajlovi).

Saobraćajni tokovi između korporativne podmreže i SCADA podmreže potiču od Web aplikacija pomoću kojih se na klijentima korporativne mreže dobija vizuelni

prikaz procesa i potrebni izveštaji, podataka koji se prenose ka centrima daljinskog upravljanja i usled pristupa serverima za potrebe konfigurisanja sa klijenata korporativne mreže. Ovaj tip saobraćaja je modelovan korišćenjem standardnih aplikacija (Database, FTP, Web) u sedam različitih profila.

DDoS napad je simuliran "plavljenjem" mreže UDP paketima iz 20 izvora (lociranih u korporativnoj mreži), koji generišu saobraćaj konstantnog protoka.

Saobraćaj u korisničkoj ravni je podeljen u četiri klase, a SCADA saobraćaj se opslužuje sa najvišim prioritetom. U mrežnim uređajima se primenjuje disciplina ravnomernog opsluživanja paketa sa težinskim faktorima (*Weighted Fair Queuing*, WFQ), u kojoj se tokovima saobraćaja dodeljuju težinski faktori, srazmerno rezervisanom propusnom opsegu.

Simulirana su dva scenarija: scenario bez napada na infrastrukturu IP mreže i scenario sa prethodno opisanim DDoS napadom na aplikacionom sloju. Rezultati simulacije koji pokazuju degradaciju performansi SCADA sistema u uslovima DDoS napada prikazani su na slici 3. DDoS napad počinje u trenutku $t = 100s$, a slika 3a) prikazuje saobraćaj koji se upućuje SCADA podmreži. Veliki intenzitet dolaznog zlonamenog saobraćaja prouzrokuje blokadu resursa SCADA servera (mete napada), što se vidi kroz stepen iskorišćenja procesora u opsegu 80-100% , na slici 3b). Od početka napada, usled zagušenja, počinje i odbacivanje paketa na interfejsu rutera ka delu mreže u kojoj se nalazi meta napada, pa se stepen odbačenih paketa koji pripadaju SCADA saobraćajnom toku povećava i iznosi približno 3,6% ukupnog saobraćaja u redu najvišeg prioriteta, slika 3c). Istovremeno se povećava i kašnjenje u obradi zahteva legitimnog saobraćaja, koje dostiže i do 4,5s kao što je ilustrovano na slici 3d). To je znatno iznad prihvatljivih granica za sistem daljinskog upravljanja i predstavlja još jedan pokazatelj ozbiljne degradacije performansi servisa u uslovima napada.

5. Zaštita SCADA sistema i procena sigurnosnog rizika

Upravljanje zaštitom ICT sistema podrazumeva definisanje politike zaštite i izbor odgovarajućih mehanizama zaštite. Pri tome je potrebno da se sprovede analiza osetljivosti sistema, analiza i procena rizika, izbor i implementacija mehanizama zaštite i praćenje njihove efikasnosti [6]. Zaštita IP-baziranih SCADA sistema zasniva se na primeni poznatih preventivnih i reaktivnih tehnika kao što su: analiza dnevnih aktivnosti, upravljanje lozinkama, biometrijske tehnike, implementacija zaštitnih zidova (*firewall*) za filtriranje saobraćaja između poslovnih sistema i SCADA mreža, simetrična kriptografija, primena L2 i L3 IP virtuelnih privatnih mreža, primena različitih tipova sistema za otkrivanje napadača (*Intrusion Detection System*, IDS) i primena tehnika forenzičke analize digitalne evidencije radi otkrivanja zlonamernih aktivnosti u mreži [11].

Otkrivanje zlonamernih programa i njihova eliminacija u SCADA sistemima predstavlja problem zbog velikih procesorskih zahteva koji usporavaju rad. Pokretanje antivirusnih programa i ažuriranje pripadajućih baza podataka, skeniranje sistema u potrazi za zlonamernim kodom i slične akcije zahtevaju procesorske resurse koji često nisu dostupni svim komponentama SCADA sistema. Neki od problema koji se mogu javiti kod primene *firewall*-ova su povećanje kašnjenja u prenosu upravljačkih informacija, složenost održavanja i nedostatak *firewall*-ova kompatibilnih sa pojedinim protokolima koji se primenjuju u SCADA sistemima.

Pri projektovanju zaštite IP-baziranih sistema daljinskog upravljanja treba uraditi detaljnu analizu sigurnosnog rizika, koja se zatim periodično ponavlja (delimično ili u celini) tokom eksploatacije i nadgradnje sistema. Takav zadatak je složen i zahteva značajna ulaganja. Veoma je teško ili čak nemoguće identifikovati sve pretnje i proceniti verovatnoću njihovog dešavanja. Potencijalna posledica je neodređena ili netačna estimacija troškova u slučaju različitih vrsta otkaza izazvanih napadima na sistem. Procena ulaganja u poznate tehnologije zaštite kao što su *firewall* i antivirusni softver je jednostavnija, jer je ekonomija takvih tehnologija dobro poznata. Problem se pojavljuje pri investiranju u nove tehnologije i proizvode, kada je teško da se proceni opravdanost ulaganja, kao i da li eventualna dobit zavisi od očekivane učestanosti napada, štete prouzrokovane napadom i efikasnosti tehnologije da spreči napad ili ublaži posledice.

Analiza sigurnosnog rizika može biti kvalitativna ili kvantitativna [12]. Kvalitativna analiza pretpostavlja metode koji izražavaju gubitke kao subjektivnu meru, npr. stepen rizika procenjuje se kao nizak, srednji ili visok. Kvantitativna analiza zasniva se na matematičkom pristupu (numerička analiza, statističke metode) pomoću koga se rizik izražava numeričkim vrednostima određenih veličina. To mogu biti ekonomske kategorije kao što su očekivani godišnji gubitak, povrat investicija i dr. Druga mogućnost je da se rizik kvantifikuje u zavisnosti od učestanosti napada i njihovog uticaja na performanse servisa [13].

6. Zaključak

Daljinsko upravljanje karakteriše se kao nekritičan servis u realnom vremenu, što znači da se telekomunikacioni zahtevi mogu realizovati u zajedničkoj IP mreži, uz uslov da postoji diferencijacija kvaliteta servisa po klasama i da je SCADA saobraćaj izolovan od ostalih tipova saobraćaja u mreži. Protokoli specifični za daljinsko upravljanje razvijaju se na aplikacionom sloju (uključujući modele i prezentaciju podataka) i koriste TCP/IP stek. IP VPN su ekonomično rešenje za realizaciju SCADA/EMS i komunikacije između centara upravljanja, zahvaljujući razdvajanju različitih tipova saobraćaja bez formiranja podmreža, podršci QoS i zaštiti informacija.

Jedna od posledica evolucija arhitekture sistema daljinskog upravljanja je osetljivost na različite vrste infrastrukturnih napada. Napadi kao što je DoS/DDoS potencijalno ugrožavaju vitalne funkcije elektroenergetskog sistema. Primena pojedinih standardnih tehnika zaštite utiče na degradaciju performansi SCADA sistema, a za neke vrste napada ne postoje pouzdani mehanizmi zaštite. Poželjno je da se izvrši kvantitativna analiza sigurnosnih rizika pri projektovanju zaštite sistema daljinskog upravljanja, kao i tokom njegove eksploatacije. Neophodan je i razvoj novih metoda za procenu sigurnosnog rizika, prilagođenih specifičnostima sistema daljinskog upravljanja.

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

Literatura

[1] D. Bailey, E. Wright, *Practical SCADA for Industry*, Elsevier, Oxford, 2003.
[2] "Integrated Service Networks for Utilities", CIGRÉ Technical Brochure TB 249, WGD2.07, 2004.

[3] "Studija razvoja telekomunikacionog sistema privrednog društva za distribuciju električne energije Elektrodistribucija Beograd d.o.o.", Institut Mihajlo Pupin, 2010.
[4] J. Marković-Petrović, "Principi projektovanja multiservisnih IP mreža u elektro-privredi", magistarska teza, Elektrotehnički fakultet u Beogradu, 2011.
[5] "Operational Services Using IP Virtual Private Networks", CIGRÉ Technical Brochure TB 321, TFD2.10, 2007.
[6] R. L. Krutz, *Securing SCADA Systems*, Wiley Publishing Inc., 2006.
[7] B. Zhu et al., "Taxonomy of Cyber Attacks on SCADA Systems", *Proc. of the 2011 IEEE Int. Conferences on Internet of Things, and Cyber, Physical and Social Computing,* Dalian, China, 2011, pp. 380-388.
[8] T. Peng et al., "Survey of Network-Based Defense Mechanisms Countering the DoS and DDoS Problems", *ACM Computing Surveys*, vol. 39, no. 1, article 3, 2007.
[9] OPNET IT Guru Academic Edition. [Online]. www.opnet.com/university_program/ itguru_academic_edition/
[10] J. Marković-Petrović, M. Stojanović, "Analysis of SCADA System Vulnerabilities to DDoS Attacks", *Proc. of the TELSIKS 2013*, Niš, October 2013.
[11] J. Marković-Petrović, M. Stojanović, "Zaštita telekomunikaciono-informacionog sistema u elektroprivredi", *Zbornik radova 15. Simpozijuma Upravljanje i telekomunikacije u EES*, CIGRÉ Srbija, RD2–03, Donji Milanovac, oktobar 2012.
[12] T. Tsiakis, "Information Security Expenditures: A Techno-Economic Analysis", *Int. Journal of Computer Science and Network Security*, vol. 10, no. 4, 2010, pp. 7-11.
[13] G. Dondossola et al., "Cyber Risk Assessment of Power Control Systems – A Metrics Weighed by Attack Experiments", *2011 IEEE Power and Energy Society General Meeting*, San Diego, CA, July 2011.

Abstract: *In this paper, we first provide an overview of remote control system in power utilities. Further focus is on the advanced Supervisory Control and Data Acquisition (SCADA) systems, which are based on the TCP/IP model and the Ethernet technology. They are typically integrated into a common IP-based network, which is used for implementing a number of operating and corporate services in power utilities. Critical requirements for SCADA integration have been discussed, including quality of service and security. The impact of distributed Denial of Service attacks to SCADA system performance has been analyzed through a comprehensive simulation. Finally, we address security mechanisms as well as the importance of a proper security risk analysis.*

Keywords: *Remote control, quality of service, SCADA, security, VPN.*

IMPLEMENTATION PRINCIPLES OF IP-BASED NETWORKS SUPPORTING POWER CONTROL SYSTEMS

Mirjana Stojanović, Jasna Marković-Petrović