SIGURNOSNI ASPEKTI NAPREDNIH ELEKTROENERGETSKIH MREŽA

Srđan Đorđević, *Elektronski fakultet u Nišu, srdjan.djordjević@elfak.ni.ac.rs*
Slobodan Bojanić, *Universidad Politecnica de Madrid, slobodan@die.upm.es*

Sadržaj – *U ovom radu dat je kratak pregled najznačajnijih sigurnosnih problema u smart grid mrežama. Izložena su i najvažnijih tehnička rešenja za njihovo prevazilaženje. Nadogradnja tradicionalne elektroenergetske mreže dovodi do povećanja efikasnosti i pouzdanosti elektroenergetskog sistema ali se u isto vreme uvodi brojne potencijalne sigurnosne ranjivosti. Analizirane su najvažnije sigurnosne ranjivosti smart grid sistema sa posebnim osvrtom na sajber sigurnost. Rad opisuje i kriptografske tehnike neophodne za zaštitu od sajber napada.*

1. UVOD

Napredna elektroenergetska mreža (*Smart Grid,* SG) predstavlja nadogradnju tradicionalnog elektroenergetskog sistema (EES) kojom se uz pomoć niza novih funkcionalnosti izlazi u susret kako trenutnim tako i budućim potrebama svih entiteta priključenih na elektroenergetsku mrežu. Integracijom postojeće elektroenergetske mreže (EEM) sa softverom, savremenim informacionim i komunikacionim tehnologijama osavremenjuje se EES i povećava njegova efikasnost, pouzdanost i kapacitet. Uvođenje SG sistema, međutim, dovodi do niza novih sigurnosnih rizika koji se moraju detaljno razmotriti s obzirom na činjenicu da zaštita električne mreže ima veliki socijalni značaj.

SG odlikuje veća kompleksnost u odnosu na klasičnu EEM usled umrežavanja velikog broja dodatnih komponenata različite prirode. Na ovaj način povećana je ranjivost sistema na napade sa dva aspekta. Sa jedne strane povećan je broj pristupnih tačaka sa kojih se razmenjuju informacije u elektroenergetskom sistemu. Drugi aspekt je umrežavanje komponenata različite prirode koja ima za posledicu međusobnu interakciju različitih tehnologija što predstavlja dodatni sigurnosni rizik. Praktično je nemoguće u sistemu takvih dimenzija i kompleksnosti garanotovati bezbednost u svakom podsistemu.

Sjedinjavanje SG sistema sa informacionim sistemima i mrežama predstavlja dodatan faktor koji unosi široki spektar bezbednosnih pretnji. Sastavni deo sistema je raznovstan softver čije funkcije su od kontrole i estimacije do proračuna cena usluga. Softver koji održava sistem je izložen potencijalnom dejstvu malicioznih kodova čiji cilj može da bude i izmena način na koji funkcioniše sistem. Prekid u komunikaciji ili radu softvera koji upravlja sistemom može da ima za posledicu nestanak električne energije a u ekstremnim slučajevima da prouzrokuju havarije i povrede.

Problem informacione bezbednosti elektroenergetskog sistemu je novije prirode kao i standardizacija koja se bavi ovom problematikom. U sastavu IEC (*International Electrotechnical Commission)* organizacije je i tehnički komitet zadužen za razvoj standarda za razmenu informacija elektroenergetskih i drugih srodnih sistema. Naziv ovog tehničkog komiteta je T57 . Unutar ovog tehničkog komiteta funkcioniše više radnih grupa od kojih je svaka odgovorna za razvoj standarda u određenom domenu. Skup standarda koji se tiču sigurnosti podataka i komunikacija nosi oznaku IEC62351.

Aktivnosti kojima se ugrožava bezbednost SG sistema se zavisno od karaktera mogu okvalifikovati kao sajber napadi ili kao fizički napadi. Postojeći mehanizmi i mere zaštite SG sistema daju zadovoljavajuće rezultate na isključvio sajber ili fizičke napade. Algoritmi za informacionu bezbednost ne uzimaju u obzir posledice koje sajber napad može da ima na fizička svojstva sistema i obrnuto algoritmi za fizičku bezbednost ne poseduju potpuni uvid u informacionu infrastrukturu sistema. Odavde proizilazi da metodi fizičke i informacione zaštite SG mreže nisu dovoljni da obezbede zaštitu od svih napada. Pojavljuje se potreba za razvojem sajber-fizičkih modela i metoda kojima bi se uspešno zaštitio sistem od svih vrsta napada uključujući i hibridne napade [1].

U narednom poglavlju razmotreni su prioriteti najznačajanijih ciljeva zaštite SG sistema. Prikaz kriptografskih metoda koje se primenjuju u naprednoj eleketroenergetskoj mreži dat je u trećem pogavlju. Četvrto poglavlje posvećeno je aspektima implementacije „pametnog brojila" kojima se sprovode neophodne mere bezbednosti.

2. CILJEVI ZAŠTITE SG SISTEMA

Neophodno je obezbediti da sve mere preduzete u cilju povećanja bezbednosti EEM ne utiču na kontinualno snabdevanje električnom energijom. Najznačajniji ciljevi zaštite podataka u EEM su:

- Raspoloživost resursa
- Integritet podataka
- Tajnost podataka

Raspoloživost resursa predstavlja najznačajniji bezbednosni cilj u SG u celini kao i najvećem broju komponenata elektroenergetskog sistema jer se njime obezbeđuje funkcionalnost sistema. Drugi sigurnosni servis po značaju je integritet podataka odnosno zaštita od neovlašćenog, nepredviđenog ili nenamernog modifikovanja podataka. Upravljanje EES obavlja se na osnovu podataka prikupljenih sa brojnih senzora i agenata. Svako neautorizovano modifikovanje ili umetanje ulaznih podataka može da se odrazi na kvalitet električne energije ili da izazove kvarove i oštećenja u EES.

Gubitak tajnosti podatka nosi manje sigurnosnih rizika u odnosu na dostupnost i integritet. Procenjuje se da uvođenje SG povećava količinu podatak koja se prenosi električnom mrežom za jedan red veličine. Među podacima koji se prenose SG mrežom nalazi se i velika količina informacija koja u prošlosti nije prikupljana. Pojavljuje se problem zaštite korisnika mreže od sistemskog posmatranja, beleženja aktivnosti i ličnih podataka odnosno problem zaštite privatnosti [2]. Pored informacija korisnika potrebno je zaštititi i informacije davaoca usluga kao i proizvođača opreme.

Značaj koji imaju pojedini sigurnosni servisi na bezbednost sistema zavisi od tipa komponente i tipa podataka nad kojim se primenjuju. Radi organizovanja efikasnih mera zaštite potrebno je odrediti prioritete sigurnosnih servisa za pojedine komponenete i tipove podataka.

Istraživanja bezbednosti u SG sistemu najčešće predstavljaju nezavisne analize bezbednosti pojedinih komponenata sistema. Ovakav pristup je razumljiv kada se ima u vidu veličina i kompleksnost SG sistema. Najznačanije oblasti istraživanja bezbednost SG sistema, prema [3], su:

SCADA sistemi, modeli estimacije stanja, komunikacioni protokoli, pametna brojila.

Praćenje i upravljanje fizičkim aspektima elektroenergetske mreže obavlja se sistema za nadzor i upravljanje. Postoji više vrsta ovih sistema od kojih se najviše koriste *SCADA* (*Supervisory Control and Data Acquisition*) sistemi koji predstavljaju objedinjenje sistema za akviziciju podataka i sistema za daljinsko upravljanje. U tradicionalnim EES nije postojala potreba za uvođenjem bezbednosnih mera u sistemima za nadzor i upravljanje jer su ovi sistemi bili praktično izolovani. Za razliku od tradicionalnih u naprednim elektroenergetskim sistema postoji razmena podata između SCADA sistema i ostalih komponenata mreže što predstavlja veliki bezbednosni rizik. Narušvanje funkcionisanja SCADA sistema može da dovede do oštećenja veoma skupe opreme a u nekim situacijama i do povređivanja ljudi. Najznačajniji cilj mera bezbednosti u ovim sistema je obezbeđivanje neprekidnog napajanje sistema.

Sastavna komponenta SCADA sistema je model estimacije stanja čija je namena modeliranje podataka senzora i agenata. Primena ovog modela omogućava kontrolu fizičkih svojstava sistema u cilju očuvanja stablinosti. Najveći bezbednosni problem za modele estimacije stanja predstavlja zaštita od ubacivanja lažnih podataka obzirom da je veoma komplikovano razdvojiti lažne podatke od tačnih. Drugi bezbednosni problem može da bude nedovoljan kapacitet komunikacionog kanala. Ciljievi zaštite modela estimacije stanja su raspoloživost resursa i integritet podataka.

Unutar SG mreže analogna mehanička brojila zamenjena su digitalnim meračima potrošnje električne energije koji imaju mogućnost zapisa potrošnje i dvosmerne komunikacije prema kontrolnom centru. Ovo čini razliku između napredna merne infrastrukture (*Advanced Metring Infrastrucutre* – AMI) i tradicionalnog sistema za očitavanje potrošnje.

Najznačajniji sigurnosni servisi za ovu komponentu SG su integritet i tajnost. Prvi cilj zaštite se podrazumeva jer se njime ozbeđuje da očitavanja "pametnog brojila" ne budu izmenjena. Tajnost podatak je takođe bitna jer su već razvijeni postupci kojima se na osnovu očitanih vrednosti potrošnje električne energije može odrediti koji su električni uređaji korišćeni u kom vremenskom razdoblju. Radi osiguranja privatnosti korisnika potrebno je umanjiti količinu informacija koja se prikuplja od strane kućnih uredjaja i svesti je isključivo na informacije koje su neophodne da bi udaljeni entitet mogao da obavi potreban zadatak. Raspoloživost pametnog brojila je mnogo manje kritična u odnosu na druge komponente SG sistema imajući u vidu da se dozvoljena latencija ovog uređaja izražava u satima.

Komunikacija između velikog broja komponenata u SG sistemu iziskuje primenu više različitih komunikacionih protokola. Postoje dva zanačajna problema u vezi sigurnosti komunikacionih protokola. Jedan se tiče potrebe da se poveže više komponenata koje uzajamno imaju veoma različite komunikacione zahteve. Drugi problem ogleda se u činjenici da SG treba da se integriše sa nasleđenim i zastarelim EES za koji ne postoji bezbednosna podrška. Sigurnosni ciljevi za komunikacione protokole zavise od komponenata koje međusobno komuniciraju i podataka koji se razmenjuju.

Da bi se uspešno obavilo projektovanje ili testiranje SG sistema neophodno je razviti hardverski ili softverski model kojim je moguće simulirati funkcionisanje celokupnog sistema. Simulacija SG sistema predstavlja izazov zbog veličine i složenosti. Na ovaj način mogu se sagledati razne aspekti SG sistema uključujući procenu bezbednosnih rizika.

Uticaj koji imaju pojedini sigurnosna servisa na bezbednost SG sistema zavisi od tipa informacija nad kojima se primenjuju. Informacije koje pametno brojilo razmenjuje sa kontrolnim centrom mogu se svrstati u tri kategorije:

- informacije o cenama
- kontrolne komande
- podaci pametnog brojila.

Pored tri tipa informacija koje se prenose kominikacionim kanalom treba razmotriti i zaštitu softvera. Pregled prioriteta pojedinih sigurnosnih ciljeva u zavisnosti od tipa informacija dat je u tabeli 1.

Tajnost podataka je najvažnija obezbediti kada se razmenjuju podaci pametnog brojila. Ovi podaci sadrže informacije privatnog karaktera na osnovu kojih se mogu ustanoviti obrasci korišćenja pojedinih kućnih uređaja. Tajnost ostala dva tipa podataka kao i softvera nema veliki značaj jer su te informacije obično javno dostupne.

Integritet softvera je od kritičnog značaja jer bi instaliranjem zloćudnog softvera napadač bio u mogućnosti da kontroliše bilo koju komponentu mreže ili uređaj. Integritet podataka je od značaja za sve podatke koji se prenose komunikacionim kanalom. Izmena podataka o ceni odnosno tarifi može da ima za posledicu nekontrolisani porast potrošnje.

Raspoloživost informacija i električne energije je od ključnog značaja za bezbednost SG mreže. Da bi sistem mogao normalno da funkcioniše u svim situacijama neophodna je raspoloživost softvera kao i kontrolnih komandi. Informacije o cenama su bitne jer bi njihov izostanak mogao da ima finansijske i pravne implikacije. Ovaj sigurnosni servis nije od značaja za podatke brojila jer ne postoji potreba za njihovim neprekidnim očitavanjem.

Tabela 1. *Prikaz prioriteta sigurnosnih servisa*

Prioritet S. S.	Informacije o cenama	Kontrolne komande	Podaci brojila	Softver
Tajnost podataka	Nizak	Nizak	Srednji	Nizak
Integritet podataka	Visok	Visok	Visok	Visok
Raspoloživost	Visok	Visok	Nizak	N/A

3. PRIMENA KRIPTOGRAFSKIH METODA U NAPREDNOJ ELEKTROENERGETSKOJ MREŽI

Sigurnost SG sistema nije moguće obezbediti isključivo primenom kriptografskih algoritmi, jer oni pružaju samo tajnost podataka koji se razmenjuju komunikacionim kanalima. Kriptografski algoritmi čine deo ukupnog postupka koji osigurava informacionu sigurnost. Da bi se razmenjivali šifrovani podaci neophodno je postojanje protokola kojim bi bili definisani kriptografski algoritami, dužine ključeva, procedure za autentifikaciju entiteta itd.

Integritet poruka, odnosno konzistentnost i tačnost poruka, obezbeđuje funkcija za sažimanje ili heš funkcija (hash). Od ulaznog niza proizvoljne dužine generiše se niz znakova fiksne dužine. Heš algoritam treba da obezbedi da bude praktično nemoguće iz dva ulazna niza dobiti istu heš vrednost. Ovim postukom se efikasno detektuju uobičajene greške prilikom transfera podataka. Najrasprostranjeniji heš algoritmi u protokolima i aplikacijama bili su SHA-1 i MD5. Međutim ovi algoritmi se sada smatraju nesigurnim.

Da bi se uspešno obavila razmena podataka na komunikacionoj liniji neophodno je ostvariti uzajamnu identifikaciju (autentifikaciju) izvora informacija. Autentifikacija se može realizovati na dva načina:

1. Primenom tajnog ključa
2. Primenom digitalnog potpisa

Ukoliko se za autentifikaciju koristi tajni ključ neophodno je obezbediti skup ključeva za svaki uređaja kao i razmenu ovih ključeva između uređaja. Pored toga što je koordinacija ovog postupka veoma komplikovana ne postoji ni ekonomska opravdanost za njegovo korišćenje.

Postupak autentifikacije primenom digitalnog potpisa je jednostavniji za realizaciju i ekonomski opravdaniji. Svaki od uređaja ima tajni ključ koji se formira u toku postupka instalacije kao i jedan sertifikat za upravljanje ključevima. Tehnika digitalnog potpisa za kriptovanje koristi tajni ključ enteta koji šalje poruku dok se za dekriptovanje primenjuje javni ključ istog entiteta. Ovakav pristup je opravdan jer je od primarnog značja verifikacija uređaja koji šalje poruku a ne zaštita sadržaja poruke. Uobičajena je primena HMAC (*Hash-based Message Authentication Code*) algoritma prema kome se potpisivanje (kriptovanje) obavlja nad sažetkom poruke koji se dobija primenom neke od heš fukcija. Ovako potpisani sašetak poruke (message digest) šalje se zajedno sa izvornom porukom. Na ovaj način istovremeno se obezbeđuje integritet podataka i autentifikacija poruke.

Zaštita tajnosti podataka koji se prenose komunikacionom linijom realizuje se primenom simetričnih kriptografskih algoritama. Osnovna odlika ovih algoritama je da za šifrovanje i dešifrovanje poruka obe strane koriste isti ključ. Najčešće korišćeni standardi bili su DES (*Data encryption Standard*) i njegova kasnija verzija AES (*Advanced encryption standard*). Najznačajniji nedostatak simetričnih algoritama za kriptovanje poruka je problem distribucije ključeva odnosno potreba da oba entiteta poseduju jedinstven simetrični ključ koji bi trebao da se razmeni preko zaštićenog kanala. Pored toga ova vrsta algoritama nameće potrebu za vrlo velikim brojem ključeva jer je neophodno obezbediti poseban ključ za svaki par entiteta.

Asimetrični kriptografski algoritmi koriste različite ključeve za kriptovanje i dekriptovanje. Ova dva ključa su povezana preko jedinstvene jednosmerne funkcije na takav način da poruka enkriptovana sa jednim brojem može da se dekriptuje primenom drugog broja. Primenom ovakvog pristupa otklonjeni su najvažniji nedostaci simetričnih kriptografskih algoritama. Trenutno postoje dva matematička pristupa u asimetričnoj kriptografiji. Najšire poznat je RSA (Rivest, Shamir and Adleman) kriptosistem [4] koji se zasniva na određenim svojstvima prostih brojeva (faktorisanju velikih brojeva) pri čemu se izvorni tekst tretira kao niz prirodnih brojeva. RSA uobičajeno koristi ključ od 1024 ili više bitova.

Noviji pristup je kriptografski sistem zasnovan na eliptičkim krivama (*Elliptic Curve Cryptography* - ECC) [5] koji se zasniva na algebarskim strukturama eliptičkih krivih u konačnom polju. Ovaj algoritam za isti nivo sigurnosti koristi ključeve znatno manje dužine u odnosu na RSA algoritam. Upotrebom manjih ključeva povećava se brzina izvršavanja i smanjuje potrošnja. Postoji veliki broj hardverskih implementacija ECC kriptosistema publkovanih u literaturi [6]. Većina poznatih implementacija namenjena je postizanju većih brzina uz upotrebu značajnijih resursa.

Asimetrična kriptigrafija je u odnosu na simetričnu kriptografiju znatno sporija i zahtevnija jer koristi ključeve veće dužine. Zbog ovih svojstava asimetrična kriptografija se ne primenjuje za enkripciju veće količine podataka već uglavnom kao sastavni deo protokola i aplikacija koje zahtevaju poverljivost i overavanje identiteta. Najoptimalnije rešenje je istovremena primena simetričnih i asimetričnih algoritama za prenos podataka u smart grid mreži. Asimetrični algoritam se koristi samo dok se ne uspostavi veza a nakon toga se prenos podataka obavlja znatno efikasnijim simetričnim kriptografskim algoritmom.

Jedan od značajnih problema u asimetričnim kriptografskim sistemima je provera autentičnosti poruke, odnosno procedura kojom bi se sa sigurnošću utvrdio identitet entiteta koji šalje poruku. Da bi se sprečila mogućnost zloupotrebe neophodno je da entieti koji međusobno komunicijraju provere uzajamno identitet primenom digitalnog sertifikata.

Upravljanje javnim ključevima odvija se unutar infrastrukture javnog ključa (*Public Key Infrastructure* - PKI). PKI čine hardver, softver i procedure koje su neophodne za upravljanje, generisanje, skladištenje i distribuciju kriptografskih ključeva i digitalnih sertifikata. Imajući u vidu da SG predstavlja mrežu velikih dimenzija na koju je priključen ogroman broj uređaja i organizacija neophodno je da sistem za upravljanje ključeva ispuni određene uslove. Pre svega potrebno je da sistem bude fleksibilan, zatim da pruža odgovarajuću sigurnost kao i najveći mogući stepen efikasnosti. Sastavni deo PKI je sertifikacionom telo (*Certificate Authoritiy* - CA) koje funkcioniše kao treća strana od poverenja. CA najpre vrši autentifikaciju krajnjih korisnika, najčešće posredstvom registracionih tela (*Registration Authority*, RA), nakon čega izdaje digitalni sertifikat koji garantuje identitet korisnika jer povezuje javni ključ sa njegovim vlasnikom. Učesnici u komunikaciji razmenjuju ove digitalne sertifikate kako bi dokazali svoj identitet.

Dva najviše korišćena standarda za PKI su X.509 i PGP (*Pretty Good Privacy*). Značajna odlika X.509 modela je hijerarhijska struktura sertifikacionih tela i takozvani lanac poverenja. Prilikom provere sertifikata uređaja neophodno je ispitati da li je sertifikat validan odnosno da li je istekao. Ova provera se obavlja na osnovu pripadnosti listi opozvanih sertifikata (*Certification Revocation List* - CRL). Pored toga potrebno je ispitati i da li je sertifikat izdat od strane pouzdanog sertifikacionog tela.

Zaštićeni komunikacioni kanal uspostavlja se primenom sigurnosnog protokola koji treba da obezbedi tajnost, integritet podataka i autentifikaciju entiteta. Integritet poruka ostvaruje se primenom heš funkcija, zaštita tajnosti podataka primenom simetričnih kriptografskih algoritama, dok se autentifikacija odnosno provera identiteta strana koje komuniciraju postiže primenom digitalnog potpisa i digitalnih sertifikata. Najčešće primenjivan sigurnosni protokol za razmenu informaciju u SG mrežana je TLS (*Transport Layer Security*) singurnosni protokol. Poverljivost podataka u razmeni podataka primenom TLS protokola definisana je standardom IEC 62351-3. Prema ovom standardu implementacija bi trebala da podržava višestruka sertifikaciona tela, dvosmernu razmenu sertifikata, najmanje AES-128 enkripciju.

4. REALIZACIJA MERA ZAŠTITE NAPREDNOG BROJILA

Zaštita naprednog brojila predstavlja veliki bezbednosni izazov imajući u vidu da se nalazi na korisničkoj strani i samim tim je fizički dostupan evenutalnom napadaču koji može direktno da stekne materijalnu korist narušavanjem podataka. Ovi uređaji bi trebali da budu opremljeni dodatnim komponentama čija je namena fizička zaštita kao i sprečavanje hardverskih ili softverskih otkaza. Neophodno je

da kriptoprocesor i njegova memorija budu realizovani sa fizičkom otpornošću na napad (tamper resistance) čime bi se očuvala sigurnost kriptografskih ključeva i podataka za autentifikaciju [7].

Potrebno je da napredno brojilo poseduju ugrađene procedure heš funkcije, simetričnog kriptografskog algoritma, asimetričnog kriptografskog algoritma, kao i proceduru za upravljanje ključevima [8]. Uvođenjem alternativnih kriptografskih algoritama i postupaka autorizacije i autentifikacije povećava se bezbednost i postiže se veća fleksibilnost uređaja.

Procedure i dužine ključeva koje obezbeđuju dovoljan nivo zaštite SG sistema definisane su standardima. Tabele 2, i 3 daju prikaz preporuka NIST (*National Institute of Science and Technology*) za heš algoritme, asimetrične kriptografske algoritme i simetrične kriptografske algoritme respektivno. Tabele prikazuje i preporučene dužine ključeva. Veća dužina ključa znači veću bezbednost ali je potrebno obezbediti da kriptoprocesor poseduje dovoljnu procesorsku moć i dovoljno memorije da memoriše kriptografski materijal.

Tabela 2. *Preporuka za heš algoritme u smart grid mrežama prema* SP 800-57 *i* SP 800-131

Algoritam	2011-2029	nakon 2030
Secure Hash Algorithm (SHA)	SHA-224	SHA-256, SHA-384, SHA-512

Tabela 3. *Preporuka za asimetrične kriptografske algoritme prema* SP 800-57 *i* SP 800-131

Algoritam	2011-2029	nakon 2030
Advanced Encryption Standard (AES)	AES-128, AES-192, AES-256	AES-128, AES-192, AES-256
Triple-Data Encryption Standard (TDES)	TDES sa tri ključa	Isključena je mogućnost primene

Preporučuje se da svaki od uređaja poseduje jedinstvene ključeve i akreditive. Ovom merom se obezbeđuje da eventualno razbijanje ključa jednog uređaja nema posledice na bezbednost ostalih uređaja u SG mreži. Jedna od mera koju treba preduzeti je i periodično osvežavanje i ažuriranje tajnih informacija.

Da bi se uspešno obavilo generisanje ključeva u pojedinim operacijama kriptografskih algoritama neophodna je upotreba kvalitetnog izvora pseudo-slučajnih brojeva. Generatori pseudoslučajnih brojeva (*Pseudorandom number generators*, PRNG) su praktično algoritmi koji na osnovu ulaznog niza slučajnih brojeva generišu niz brojeva koji se zbog svog determinističkog karaktera naziva niz pseudoslučajnih brojeva. Početni niz slučajnih brojeva koji se naziva ključ (*seed*) dobija se u generatoru slučajnih brojeva (*Random number generators*, RNG). Zaštita od kriptoanalitičkog napada u velikoj meri zavisi od adekvatnog izbora slučajnog događaja iz koga se generiše početni niz brojeva jer je izlazni niz moguće reprodukovati samo ukoliko se poznaju početne vrednosti [9]. Algoritmi generatora pseudoslučajnih brojeva su javno dostupni.

5. ZAKLJUČAK

Integracija tradicionalne EEM sa informacionim i komunikacionim tehnologijama nametnula je brojne bezbednosne probleme. Sagledavanje bezbednosti SG sistema je veoma kompleksan zadatak. U ovom radu dat je sažet pregled nekih mera bezbednosti u naprednoj elektroenergetskoj mreži sa akcentom na informacionu bezbednost. Dat je i generalni prikaz mera zaštite koje je potrebno uzeti u obzir prilikom projektovanja pametnog brojila.

Implementacija i primena kriptografija u obezbeđivanju informacione sigurnosti je detaljno dokumentovana i podržana brojnim standardima. Međutim njena primena u sistemima za kontrolu i upravljanje je relativno nova. Standardi koji se odnose na sajber sigurnost i interoperabilnost SG sistema još uvek nisu u potpunosti razrađeni.

ZAHVALNOST

Rezultati prikazani u ovom radu ostvareni su u okviru projekta TR 32004 čiju realizaciju finansira Ministarstvo nauke Republike Srbije.

LITERATURA

[1] Yilin Mo, T.H.-J. Kim, K. Brancik, D. Dickinson, Heejo Lee, A. Perrig, B. Sinopoli, "Cyber–Physical Security of a Smart Grid Infrastructure, " *in Proc. IEEE*, Vol. 100, No. 1, Jan. 2012, pp. 195-209.

[2] S. Bojanić, O. Nieto-Taladriz, S. Djordjević, "Privacy Issues in Smart Grids," *Proceedings of Small System Simulation Symposium* 2012, Niš, pp. 135-140.

[3] Todd Baumeister, "Literature review on smart grid cyber security," Technical Report, University of Hawaii at Manao, Dec. 2010.

[4] R. L. Rivest, A. Shamir, L. Adleman., "A method for obtaining digital signtures and public-key cryptosystems". *Comm. ACM*, Vol 21, pp. 120-126, 1978.

[5] N. Koblitz, "Elliptic curve Cryptosystems," *Mathematics of Computation*, Vol. 48, No. 177, 1989, pp. 203–209.

[6] L. Batina, S. B. Ors, B. Preneel, J. Vandewalle, "Hardware architecture for public key cryptography," Integration, the VLSI journal, Vol. 34, No. 6, pp. 1-64, 2003.

[7] J. Naruchitparames, M. Gunes, C. Evrenosoglu, "Secure communications in the Smart Grid," *The Journal of Grey System*, Vol. 1, No. 1, 1989, pp. 1–24.

[8] V. B. Litovski, P. M. Petković, S. Bojanić, "Cryptography and the Grid," Zbornik Radova Druge Konferencije o bezbednosti informacionih sistema, Forum BISEC 2010, Beograd, pp. 93-98.

[9] Swapna Iyer, "Cyber Security for Smart Grid, Cryptography, and Privacy," International Journal of Digital Multimedia Broadcasting, Vol. 2011.

[10] A.E. Bryson and Y.C. Ho, *Applied Optimal Control*, New York: Wiley, 1975.

[11] B.K. Bose, "Sliding mode control of induction motor," in *Proc. IEEE Ind. Appl. Soc. Annu. Meeting*, 1985, pp. 479-486.

Abstract – This paper represents brief overview of the most important Smart Grid security issues and key solutions for addressing security concerns. Upgrading of the traditional electrical power grid increases overall efficiency and reliability but at the same time it introduces many potential security vulnerabilities into the system. This paper will focus on these threats and risks especially relating to cyber security. Furthermore, we describe common cryptography techniques that are required to overcome cyber attacks.

SMART GRID SECURITY VURNELABILITES

Srđan Đorđević, Slobodan Bojanić