Tehničko rešenje za zaštitu privatnosti u naprednim elektroenergetskim mrežama

Srđan Đorđević, Slobodan Bojanić

***Apstrakt*—U ovom radu razmatra se problem zaštite privatnosti u smart grid mreži. Rad daje pregled najznačajnijih postojećih rešenja za zaštitu privatnosti korisnika napredne elektroenergetske mreže. Ispitana je mogućnost realizacije postupka za zaštitu privatnosti koji se zasniva na uspostavljanju kompromisa između funkcionalnosti i privatnosti. Jednostavan način da se ostvari optimalan odnos funkcionalnosti i privatnosti je potiskivanje određenih frekvencijskih komponenti napona.**

***Ključne reči*—Smart grid, napredno brojilo.**

I. UVOD

Uvođenje komunikacionih i informacionih tehnologija u tradicionalnu elektroenergetsku mrežu omogućilo je modernizaciju i razvoj nove generacije elektroenergetske mreže poznate kao smart grid. Jedan od ključnih problema u daljem razvoju napredne elektroenergetske mreže (*Smart Grid*, SG) je obezbeđivanje informacione sigurnosti. Usled umrežavanja velikog broja komponenata različite prirode i dvosmerne komunikacije koja se realizuje uz upotrebu širokog spektra fizičkih mreža na različitim nivoima značajno je povećana ranjivost sistema.

Ubrzanim razvojem savremenih informaciono-komunikacionih tehnologija značajno je povećan obim i sadržaj informacija koje se prenose komunikacionim uređajima. Povećana je i mogućnost zloupotrebe ličnih i osetljivih podataka među koje spada i povreda privatnosti. Pod povrednom privatnosti u elektronskim komunikacijama podrazumeva se sistematsko praćenje i beleženje aktivnosti i ličnih podataka određene osobe bez njenog odobrenja.

Merni podaci naprednog brojila sadrže u sebi informacije o korišćenju određenih električnih uređaja tokom vremena. Napadač bi u slučaju prikupljanja ovih podatka na komunikacionom kanalu mogao da izvede zaključke u vezi ponašanja i aktivnosti ukućana. Zaštita privatnost u smart grid mreži je intenzivno proučavana zbog značaja ove tematike. Problem zaštite privatnosti se može rešiti pravnom regulativom ili razvojem bezbednosnih tehnologija.

Sva do sada objavljena tehnička rešenja za zaštitu privatnosti korisnika SG sistema nisu razmatrala na koji način se uvođenje određenih procedura odražava istovremeno na sadržaj informacija privatnog karaktera i na tačnost podataka. Ovaj problem je prvi put obrađen u radu [1] koji daje širi teorijski okvir za model kojim se praktično uspostavlja kompromis između tačnosti i privatnosti podataka koji se prenose smart grid mrežom.

Naredno poglavlje posvećeno je problemu zaštite privatnosti korisnika smart grid mreže. U trećem poglavlju opisan je model kojim se uspostavlja veza između privatnosti i tačnosti podataka koji se prenose SG mrežom. Četvrto poglavlje daje prikaz mogućeg tehničkog rešanje za zaštitu privatnosti na SG mreži.

Srđan Đorđević– Elektronski fakultet, Univerzitet u Nišu, Aleksandra Medvedeva 14, 18000 Niš, Srbija (e-mail: srdjan.djordjevic@ elfak.ni.ac.rs).

Slobodan Bojanić – Escuela Técnica Superior de Ing. de Telecomunicación, Universidad Politècnica de Madrid, Madrid, Španija (e-mail: slobodan@die.upm.es).

II. ZAŠTITA PRIVATNOSTI

Trenutno je jedini vid zaštite od napada na privatnost korisnika smart grid mreže pravna zaštita. Ovim merama se ne može u potpunosti osigurati zaštita privatnosti već one imaju samo efekat odvraćanja od napada.

Pravna zaštita privatnosti podataka na smart grid mreži reguliše se na različite načine zavisno od zakonodavstva zemlje u kojoj se sprovodi. Evropska unija i Kanada primenjuju takozvani horizontalni režim zaštite podataka prema kojem je uspostavljen skup zakona i propisa čije se mere odnose na obradu bilo koje vrste privatnih podataka. Vremenom su odredbe ovih zakona postale primenjive i na podatke koji se prenose naprednom elektroenergetskom mrežom. U SAD je primetan nedostatak federalnih propisa za zaštitu privatnosti pri čemu je niz saveznih država usvojio zakone koji regulišu ovu problematiku. Jedna od karakteristika zakona koji se primenjuju u SAD je da je njima regulisana zaštita samo određenih podatka u određenim industrijama. Jedan od pravnih problema predstavlja činjenica da vrednosti potrošnje električne energije određenog brojila često ne mogu da se dovedu u vezu sa određenom osobom a samim tim ne mogu da budu okvalifikovani kao lični podaci.

Tehnologije za zaštitu privatnosti omogućavaju da se narušavanja privatnosti potrošača električne energije spreče pre nego što nastanu. Ovi postupci zasnivaju se na primeni protokola kojima se smanjuje količina informacija u podacima koje napredna brojila šalju komunalnim službama do nekih minimalnih vrednosti koje su neophodne za funkcionisanje sistema. U literaturi postoji više raznovrsnih tehničkih rešenja za problem zaštite privatnosti na smart gridu. Ovde će biti dat pregled najznačajnijih tehničkih rešenja koje su do sada razvijena.

Tehnika anonimizacije se zasniva na ideji da se zaštita privatnosti korisnika postigne primenom protokola koji skrivaju informacije o brojilu sa koga su podaci poslati [2]. Ovi postupci su primenjivi samo nad podacima za koje nije

neophodno specificirati izvor podataka kao u slučaju podataka za obračun potrošnje električne energije. Tehnika pouzdane obrade podataka (trusted computation) primenjuje postupak prema kojem napredno brojilo šalje koncentratoru prethodno prikupljene podatke u kojima nema privatnih informacija [3]. Ovom tehnikom je predvidjeno da se obrada i prikupljanje mernih podataka obavlja ili na samom brojilu ili od strane treće strane od poverenja.

Jedna od tehnika za poboljšanje privatnosti je perturbacija [4]. Ovim postupcima se namerno unosi grešaka u prikupljene podatke na takav način da se sačuva privatnost korisnika smart grid mreže. Unesene izmene podataka je neophodno obaviti na takav način da se zadrži neophoda tačnost za dalju obradu podataka u koncentratoru.

Proverljiva obrada (Verifiable computation) je postupak koji primenjuje autentifikacioni protokol sa nultim znanjem (*Zero Knowledge Proof*) [5]. Prednost protokola sa nultim znanjem je u postojanju anonimnosti u autentifikaciji jer ni jedna strana ne otkriva identitet. Informacije koje bi bile izvedene iz primljenih podataka ne bi mogle da se dovedu u vezu sa bilo kojim potrošačem jer nije poznat identitet pošiljaoca tih podataka.

Jedna od tehnika se zasniva na primeni homomorfne enkripcije. Glavana karakteristike ove kriptografske šeme je da omogućava primenu algebarskih operacija nad šifrovanim podacima koje odgovaraju istim operacijama nad osnovnim tekstom. Merni podaci se šifruju i šalju ka koncentratoru. Protokolom je omogućeno da se na mestu prijema podataka dešifrovanjem dobija samo zbirna vrednost merenja dok su pojedinačni podaci merenja skriveni.

III. KOMPROMIS IZMEĐU TAČNOSTI I PRIVATNOSTI

Merni podaci brojila koji su u opštem slučaju kompleksne vrednosti se odmeravaju i šalju komunalnim službama pružaoca usluga radi obračuna potrošnje ili analize podataka. Ukoliko je perioda odmeravanja dovoljno mala odmerci mernih podataka brojila mogu se interpretirati kao podaci generisani od strane slučajnoj izvora sa memorijom. Podaci merenja potrošnje električne energije nisu nezavisni od prethodno izmerenih podataka pa je stoga neophodno u modelu uvesti efekte kratkotrajnih i dugotrajnih korelacija. Dugotrajne korelacije modeluju efekat potrošnje skupa električnih uređaja na jednom mernom mestu dok kratkotrajne korelacije modeliraju obrasce ponašanja osoba koje upotrebljavaju te električne uređaje. Za potrebe modeliranja najpogodnije je primenti Gausov izvor sa memorijom. Gausova raspodela je usvojena zbog činjenice da je emipirijski pokazano da potrošnja jednog tipičnog električnog uređaja približno odgovara normalnoj raspodeli.

Neophodno je uspostaviti kvantitativno merilo količine informacija koja se prisluškuje kao i kvantitativno merilo za funkcionalnost sistema. Prijemna sekvenca u opštem slučaju predstavlja podatke dobijene perturbacijom mernih podataka da bi se smanjila količina privatnih informacija. Veličina koja meri vernost podataka izlazne sekvence je srednje kvadratno odstupanje između sekvence podataka očitanih na brojilu, X_k , i sekvence podataka očitanih na koncentratoru, $\hat{X}_k$

$$D_n = \frac{1}{n}\sum_{k=1}^{n} E\left(\left(X_k - \hat{X}_k\right)^2\right) \tag{1}$$

Gde je: E matematičko očekivanje, n broj odmeraka u sekvenci.

Da bi se procenila količina informacija koja se prisluškuje uvodi se sekvneca procenjenih vrednosti Y_k. Ovo je slučajna diskretna veličina koja je korelisana sa mernim vrednostima X_k.

Ukoliko bi bila poznata zbirna gustina verovatnoće između slučajnih sekvenci merenih i procenjenih vrednosti p_{XnYn} mogla bi da se proceni količina informacija koja se može zaključiti prisluškivanjem. Za ovu zavisnost koja nije unapred poznata autori rada [1] su usvojili linearni model. Kao kvantitaivno merilo gubitka privatnosti usvojena je sledeća funkcija:

$$L_n = \frac{1}{n} I\left(Y^n, \hat{X}^n\right) \tag{2}$$

gde je: $I(Y^n,X^n)$ uzajamna informacija između slučajnih veličina X i Y.

Brzina prenosa kroz kanal R je povezana sa funkcijama distorzije D i curenja informacija L. Potrebno je odabrati šemu kodovanja koja će uzeti u obzir ograničenja za sve tri zadate veličine. Da bi se smanjila količina informacija koja se može rekonstruisati neovlašćenim prikupljanjem podataka pošlo se od pretpostavke da treba minimizirati brzinu prenosa signala za zadatu vrednost distorzije.

Statističkom simulacijom komunikacionog sistema pokazuje se da su zahtevi koje je potrebno realizovati u prenosu podatka radi obezbeđenja zadovoljavajuće zaštite privatnosti u suprotnosti sa zahtevima kojima se postiže zadovoljavajuća funkcionalnost sistema. Odavde proizlazi da se prilikom realizacije prenosa signala može praviti kompromis između funkcionalnosti i privatnosti.

IV. TEHNIČKO REŠENJE ZA ZAŠTITU PRIVATNOSTI

Tehnike za zaštitu privatnosti koje se zasnivaju na namernom unošenju grešaka u merne podatke praktično uspostavljaju balans između tačnosti i privatnosti. Jedan širi teorijski okvir ovih postupaka, koji je dat u radu [1], daje model iz koga proizilazi da se uklanjanjem određenih spektralnih komponenti iz signala koji prikazuje potrošnju električne energije moguće ostvariti optimalno rešenje za zaštitu privatnosti.

Zaključak do koga se došlo teorijski je u skladu sa zapažanjima da u tipičnom spektru napona frekvencijske komponente malih snaga odgovaraju kratkotrajnim promenama koje nose najviše informacija o potrošaču, dok frekvencijske komponente velikih snaga najčešće odgovaraju električnim uređajima koji su uključeni duže vreme.

U tehničkog rešanje za zaštitu privatnosti koje se zasniva na primeni modela koji istovremeno obuhvata tačnost podataka i privatnost podataka potrebno je realizovati više funkcija od kojih su najznačajnije:

- Procena koje harmonike snage treba zanemariti da bi se ostvario optimalan odnos između privatnosti i tačnosti,
- Eliminisanje određenih spektralnih komponenti iz signala koji predstavlja potrošnju.

Trenutna aktivna snaga potrošača je slučajna nestacionarna veličina s obzirom da uključivanje ili isključivanje skupa električnih uređaja nije deterministički događaj. Alat za opis slučajnih veličina je autokorelaciona funkcija u vremenskom domenu i spektralna gustina snage u frekvencijskom domenu. Autokorelaciona funkcija se može odrediti iz sekvence slučajne promenjive dovoljno velike dužine. Spektralna gustina snage predstavlja diskretnu Furijeovu transformaciju autokorelacionog niza. Nakon što je utvrđena spektralna gustina snage može se ustanoviti koji harmonici nose najviše informacija. Postupak kojim bi se iz spektralne gustine snage određivali harmonici koji sadrže najviše informacije nije primenjiv u praksi s obzirom da je za procenu statističkih parametara potreban duži vremenski period.

Jedno moguće rešenje ovog problema je da se unapred urade statistički proračunu za više grupa električnih uređaja. Ovo praktično znači da je potrebno definisati više profila potrošača za koje je zajednično da imaju isti skup električnih uređaja. Najjednostavniji način da se obavi klasifikacija potrošača bila bi primena FFT nad odmercima struja i napona.

Vrednosti harmonika napona i struje tokom vremena variraju usled uključivanja ili isključivanja određenih uređaja. Najčešće vrednosti harmonika rapidno opadaju sa porastom njihovog reda usled čega ima smisla meriti i procenjivati samo harmonike do dvadesetog reda. Procena harmonika se može obaviti u frekvencijskom ili vremenskom domenu. Tradicionalni pristup harmonijskoj analizi je primena transformacije kojom se merni rezultati napona prevode u frekvencijske komponente. Uobičajena je primena diskretne Furijeove transformacije (Discrete Fourier Transform DFT) kao i njene optimizovane implementacije Brze Furijeove transformacije (Fast Fourier Transform FFT). Ukoliko se određuju individualne komponente diskretnog spektra primenjuje se Goertzel-ov algoritam [6] koji nije efikasan kao FFT ali ima drugih prednosti. Pored navedenih postupaka za harmonijsku analizu u frekvencijskom domenu se može primeniti i filtriranje pojedinih harmonika primenom filtara propusnika opsega.

Druga grupa metoda poznata kao algoritmi sinusnog podešavanja obavlja procenu parametara harmonika u vremenskom domenu. Ovim postupcima se minimizira srednja kvadratna greška između modela i mernog signala. Postoje nekoliko varijanti ovog postupka zavisno od toga da li je poznata frekvencija osnovnog harmonika i da li se harmonici izračunavaju pojedinačno ili svi istovremeno. Algoritam sa tri parametara [7] određuje parametere signala jednog harmonika polazeći od poznate vrednosti osnovnog harmonika. Ukoliko frekvencija osnovnog harmonika nije poznata primenjuje se algoritam sa četiri parametara [8] koji primenjuje iterativni optimizacioni postupak. Najbolji rezultati se ostvaruju primenom Algoritama multiharmonijskog podešavanja [9] kojim se određuju parametri svih harmonika istovremeno ali je ovaj postupak računski najzahtevniji.

Detaljni prikaz rezultata eksperimentalnih poređenja pojedinih metoda za harmonijsku analizu izvedena u skladu sa međunarodnim standardima za merenje naponskih harmonika data su u članku [10]. Rezultati pokazuju da je najveća tačnost izmerenih harmonika postignuta sa metodom multiharmonijskog podešavanja, dok je najlošije rezultate dao troparametarski algoritam. U pogledu brzine izvršavanja algoritma najbolje rezultate daje FFT, pa zatim Goertzel-ov algoritam, dok je najsporiji postupak multiharmonijskog podešavanja. Slična situacija je i u pogledu memorije potrebne za implementaciju postupka.

Imajući u vidu brzinu i tačnost postojećih algoritma za procenu harmonika napona sledi da bi najoptimalnije rešenje za ovu namenu bila primena FFT ili primena Goertzel-ovog algoritma. Prvi korak u primeni oba ova algoritma je određivanje frekvencije osnovnog harmonika, odnosno u ovom slučaju frekvencije mrežnog napona. S obzirom da frekvencija mrežnog napona nije konstantna bilo bi neophodno da se ona izdvoji filtrom propusnikom niskih frekvencija i nakon toga izmeri vremenski interval između dva prolaska kroz nultu vrednost. Sledeći korak je određivanje periode semplovanja koja bi u slučaju FFT morala da bude odabrana tako da sadrži 2^N semplova u jednoj periodi osnovnog harmonika. Odavde proizilazi da bi usled varijacija frekvencije mrežnog napona bilo neophodno stalno menjati frekvenciju semplovanja što prilično komplikuje realizaciju uređaja. I pored veće brzine FFT algoritma postupak zasnovan na Goertzel-ovom algoritmu bi za ovu namenu bio prihvatljiviji.

Vrednosti harmonika napona i struje zavise od trenutno uključenih električnih uređaja. Odavde proizilazi da je učestanost promena harmonika uslovljenja dinamikom uključivanja i isključivanja nelinearnih potrošača. Ostaje otvoreno pitanje koji je optimalni vremenski period u toku koga je neophodno uraditi procenu vrednosti harmonika snage.

Da bi se odredila snaga harmonika neophodno je da se odmerci struje i napona određene faze sempluju odvojeno. Kompleksna snaga se može izraziti u funkciji od aktivne i reaktivne snage pojedinih harmonika na sledeći način:

$$S = \sum_{k=1}^{N} S_k = \sum_{k=1}^{N} P_k + j \sum_{k=1}^{N} Q_k \tag{3}$$

gde su P_k i Q_k aktivne i reaktivne snage harmonika.

Ukoliko se prikaz mernih rezultata izmeni na takav način da se odbace određeni harmonici napona i struje dobiće se sledeće vrednosti:

$$P' = P - \sum_{k \in M} P_k \qquad Q' = Q - \sum_{k \in M} Q_k \tag{4}$$

gde je: M skup harmonika koji su zanemareni, P' aproksimirana vrednost aktivne snage, Q' aproksimirana vrednost reaktivne snage.

Relativna greška trenutne aktivne snage koja se čini odbacivanjem određenih harmonika u merenim podacima

iznosi:

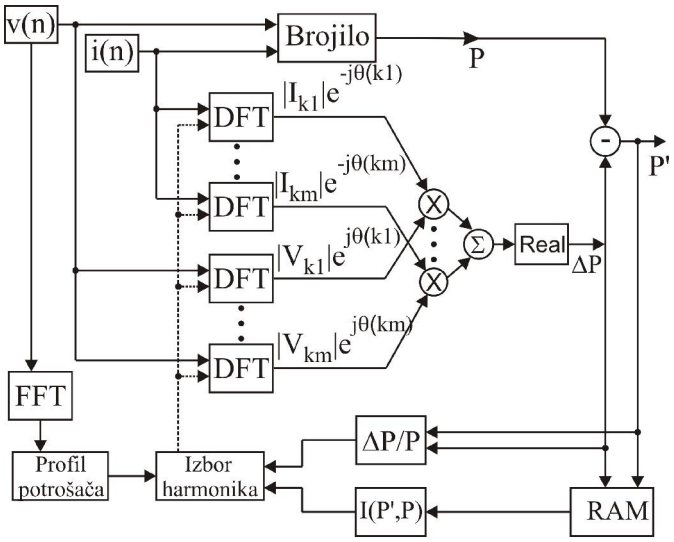
$$\delta_P = \frac{P'-P}{P} \tag{5}$$

Svi parametri potrošnje električne energije bi se izračunavali u brojilu primenom tačne vrednosti trenutne aktivne snage uključujući podatak o aktivnoj električno energiji koji se očitava nakon obračunskog perioda. Kao posledica eliminacije određenih harmonika odstupanje aproksimirane u odnosu na tačnu vrednost aktivne snage je uvek negativno. Da bi se umanjila ili eliminisala neusklađenost između profila opterećanja i aktivne električne energije bilo bi neophodno uvesti dodatne perturbacije. Ovaj problem bi mogao da se reši na taj način što bi pojedina očitavanja trenutne aktivne snage bila uvećana za određeni iznos prema unapred definisanom algoritmu tako da bude ispunjen sledeći uslov:

$$\sum_{k=1}^{M} P(k) = \sum_{k=1}^{M} P'(k) = \sum_{k=1}^{M} \left(P(k) + \Delta P(k)\right) \tag{6}$$

gde su: $P(k)$ pojedinačna očitavanja aktivne snage u brojilu, $P'(k)$ vrednosti aktivne snage koje se šalju koncentratoru, M unapred definisana dužina sekvence.

Da bi mogao da se zadovolji uslov (6) potrebno je da se nakon svakog očitavanja aktivne snage eventualno uneta namerna greška pridoda ranije uvedenim greškama. Blok šema predloženog tehničkog rešenja za zaštitu privatnosi korisnika smart grida data je na slici 1.



Sl. 1. Blok šema tehničkog rešenja za zaštitu privatnosti u naprednim elektroenergetskim mrežama.

V. ZAKLJUČAK

U radu su razmotrene mogućnosti implementacije tehnike za poboljšanje privatnosti korisnika smart grida polazeći od modela koji se zasniva na optimalnom balansu između funkcionalnosti i privatnosti. Dve najznačajnije funkcije koje bi trebalo realizovati u razmatranom tehničkom rešenju su: statistička procena harmonika snage koji se mogu zanemariti, i uklanjanje određenih spektralnih komponenti iz signala koji predstavlja potrošnju.

Imajući u vidu da tačnost statističkih proračuna u velikoj meri zavisi od vremena opservacije neko generalno rešenje koje ne bi uzimalo u obzir prethodno definisane parametre je praktično neizvodljivo. Moguće rešenje je uvođenje više profila potrošača električne energije za koje su unapred urađeni statistički proračunu u zavisnosti od zadatog skupa nelinarnih potrošača. Zaštita privatnosti se postiže uklanjanjem određenih spektralnih komponenti iz signala koji prikazuje trenutnu aktivnu snagu. Prilikom realizacije ovog postupka bilo bi neophodno osigurati da namerno uneta greška u prikazu trenutne aktivne snage bude u granicama dozvoljene tolerancije.

LITERATURA

[1] L. Sankar, S. Rajagopalan, S. Mohajer, H. Vincent Poor, "Smart Meter Privacy: A Theoretical Framework," *smart grid*, *IEEE transactions on*, vol 4, no. 2, pp. 837-846, Jun 2013.

[2] C. Efthymiou and G. Kalogridis, "Smart grid privacy via anonymization of smart metering data," 2010 First IEEE International Conference on Smart Grid Communications, pp. 238–243, 2010.

[3] S. Ruj, A. Nayak, I. Stojmenovic, "A security architecture for data aggregation and access control in smart grids," Arxiv preprint arXiv:1111.2619, 2011.

[4] C. Dwork, "The Promise of Differential Privacy: A Tutorial on Algorithmic Techniques," Foundations of Computer Science (FOCS), 2011 IEEE 52nd Annual Symposium on Digital Object 2011, pp. 1-2.

[5] B. Vaidya, D. Makrakis, H. T. Mouftah, "Authentication and authorization mechanisms for substation automation in smart grid network" *Network*, *IEEE* , vol 27, no. 1, pp. 5-11, 2013.

[6] G. Goertzel, "An algorithm for the evaluation of finite trigonometric series," *The American Mathematical Monthly*, vol. 65, no. 1, pp. 34 – 35, Jan. 1958.

[7] IEEE Std. 1057-2007. *IEEE Standard for Digitizing Waveform Recorders*, IEEE Instrumentation and Measurement Society, 2008.

[8] T. Andersson, P. Händel, "IEEE Standard 1057, Cramér-Rao bound and the parsimony principle," *IEEE Transactions on Instrumentation and Measurement*, vol. 55, no. 1, pp. 44 - 53, February 2006.

[9] P. M. Ramos, M. F. da Silva, R. C. Martins, A. C. Serra,"Simulation and experimental results of multiharmonic least-squares fitting algorithms applied to periodic signals," *IEEE Transactions on Instrumentation and Measurement*, vol. 55, no. 2, pp. 646 – 651, Apr. 2006.

[10] T. Radil and P. M. Ramos, "*Methods for Estimation of Voltage Harmonic Components, Power Quality*," Mr Andreas Eberhard (Ed.), ISBN: 978-953-307-180-0, Publisher InTech, Apr. 2011.

ABSTRACT

This paper considers the problems associated with privacy protection in smart grids. The article gives a survey of the most important existing solutions to protect customer privacy. We investigate a realization of a privacy-preserving approach that encompasses privacy-utility tradeoff into a single model. A simple but efficient solution to achieve optimal utility and privacy is to suppress low power frequency components.

A TECHNICAL SOLUTION FOR A PRIVACY-FRIENDLY SMART METERING

Srdjan Djordjević, Slobodan Bojanić