doi: 10.46793/EEE24-1.42B

Originalni naučni rad
UDK 621.31:519.87

Estimacija stanja u elektroenergetskom sistemu sa PMU uređajima i maliciozni napad injektiranjem loših merenja i njegova detekcija

Vladimir Bečejac*, Miloš Đorđević*, Nemanja Jelenić*, Mihajlo Marković*, Miloš Mosurović**

* AD Elektromreža Srbije
** Srpska berza električne energije Seepex

Rezime **-** Ovaj rad istražuje značaj primene metode estimacije stanja u elektroenergetskim sistemima, posebno fokusirajući se na ulogu PMU (Phasor Measurement Unit) uređaja. Prikazane su osnovni principi i prednosti estimatora stanja u odsustvu PMU merenja, a zatim se analizira kako PMU merenja značajno unapređuju preciznost estimacija stanja. Kroz detaljan pregled, istaknute su ključne karakteristike PMU uređaja i kako njihovi sinhronizovani podaci doprinose boljem kvalitetu estimacije stanja. U radu se istražuju bezbednosni aspekti estimacije stanja, posebno se fokusirajući na maliciozni napad injektiranjem lažnih merenja (FDIA). Kroz konkretan primer, demonstrirano je kako FDIA napad može značajno uticati na tačnost estimacija stanja, uvodeći netačne podatke u sistem. Razmatrana je i strategija detekcije ovakvih napada pomoću analize reziduala.

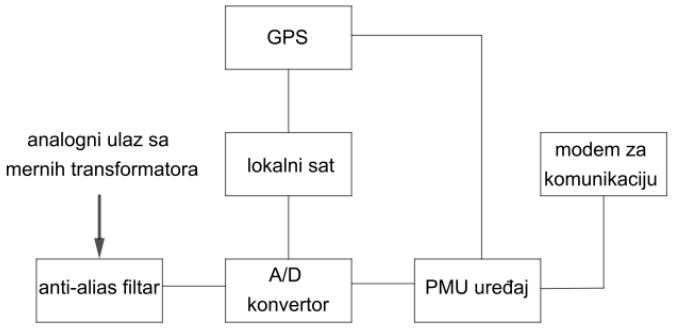
Ključne reči - estimacija stanja, PMU, FDIA

I UVOD

Estimator stanja (ES) funkcioniše tako što određuje stanje elektroenergetskog sistema (EES) na temelju njegovog matematičkog modela i dostupnih merenja. U skladu sa mrežnim modelom, ES pronalazi rešenje koje je što moguće bliže stvarnim merenjima. Ova aplikacija je od vitalnog značaja u operativnim centrima. Međutim, ES koji se oslanja isključivo na PMU merenja nije praktičan zbog visokih troškova implementacije i dugoročnih ulaganja u SCADA/EMS sistem koji je dugo vremena bio ključan za estimaciju stanja [1]. Realniji pristup je iskoristiti postojeća SCADA/EMS i PMU merenja kako bi se poboljšao kvalitet estimacije stanja. Radovi na ovu temu često koriste tehnike podržane teorijom i simulacijama. Međutim, postoje izazovi u odabiru relevantnih podataka iz obimne količine pristiglih informacija, kao i problemi s konvergencijom tradicionalnog elektroenergetskog sistema koji se oslanja na PMU podatke. Često se u estimaciji stanja koristi Njutn-Rapsonov metod, ali ovaj pristup ignorisanja članova većeg od drugog stepena u Tejlorovom razvoju ima smisla samo uz dobro odabran početni trenutak [2]. S obzirom na različitu učestalost PMU i SCADA merenja u ES-u, izbor početnog trenutka i konvergencija postaju problematični. Ignorisanje članova većeg od drugog stepena u Tejlorovom razvoju nije dovoljno za adekvatnu polinomnu aproksimaciju tokova snaga. Neki drugi algoritmi, poput Gaus-Zajdelovog, mogli bi biti neprihvatljivi za velike sisteme zbog brzine konvergencije. Radi prevazilaženja problema integracije PMU i SCADA merenja, sprovedeno je mnogo istraživanja [3,4,5,6,7].

II SINHROFAZORSKA TEHNOLOGIJA

Govoriti o PMU tehnologiji i procesima u današnjem vremenu je izazovno s obzirom na raznolikost pristupa svakog proizvođača koji želi da istakne svoje konkurentske prednosti na tržištu. Ipak, u osnovi, svi PMU uređaji dele određene karakteristike koje će biti istaknute u ovom pregledu. Ti uređaji se sastoje od nekoliko ključnih modula: računarskog, za prikupljanje podataka i za sinhronizaciju. Svaki PMU uređaj obuhvata analogne ulaze, sposobnost filtriranja, digitalizacije, sinhronizacije, digitalnu obradu i komunikacijske mogućnosti.



Slika 1. Blok šema PMU uređaja

Na slici 1 je prikazana struktura tipičnog PMU uređaja [8]. Analogne ulaze koristimo kako bismo prikupili trofazni signal sa sekundarnih naponskih i strujnih mernih transformatora za dalju analizu. Iako je suštinski PMU uređaj mikroprocesorska zaštita, on se razlikuje od klasičnih zaštita po tome što može prikupljati signale struje i napona sa različitih izvora u trafostanici. Da bi se ovi signali dalje obradili, neophodno je da prođu kroz analogno-digitalnu konverziju (A/D). U tu svrhu, početni signali se često redukuju korišćenjem oslabljivača ili instrumentalnih transformatora (obično na naponske nivoe od ± 10 V i strujne nivoe od nekoliko ampera, u zavisnosti od specifikacija proizvođača). Kako bi se izbegli alijas efekti, period odabiranja mora zadovoljiti Nikvistov kriterijum, što podrazumeva korišćenje anti-alijas filtera. Moderni PMU uređaji često koriste višestruko uzorkovanje (tzv. *oversampling*) sa visokim stopama odsecanja (*cut-off frequency*) unutar analognih anti-alijas filtera kako bi se postigla veća fleksibilnost i efikasnost. Digitalni decimacioni filteri se koriste za uzorkovanje signala sa manjom frekvencijom, čime se postiže integrisani digitalni anti-alijas

filter [8] zajedno sa analognim anti-alijas filtrom. Ovakva struktura omogućava stabilniji rad PMU uređaja u različitim uslovima temperature i sporiji proces starenja, uz poboljšani kvalitet signala. Svi odbirci koji se dobijaju u opisanom procesu imaju vremenske značke (*time tag*). Sat koji vrši njihovo dodeljivanje je baždaren prema GPS vremenu koje se dobija od strane GPS satelita raspoređenih u šest orbitalnih ravni.

Na kraju procesa, iz PMU uređaja izlazi vremenski sinhronizovani signal koji se telekomunikacionim putevima dovodi do sledećeg uređaja u hijerarhiji - PDC uređaja (*Phasor Data Concentrator*) koji ima ulogu da prikuplja, vrši obradu i odbacuje loše podatke primljene sa svih primljenih signala iz PMU uređaja. Za velike sisteme kada jedan PDC uređaj nije dovoljan, postavlja se više njih, a onda se signali iz PDC-ova dovode na super PDC uređaj. Za bilo kakav vid analize se pristupa PDC ili super PDC uređaju preko neke od razvijenih aplikacija npr. WAMS, o kojoj će biti reči u odeljku o primeni sinhrofazorske tehnologije. Treba napomenuti da je komunikacija na nivou PMU - PDC dvosmerna. Sa PDC uređaja se na PMU uređaj mogu poslati konfiguracione poruke, najčešće vezane za striming proces. Komunikacija se odvija preko fiber-optičkih kablova koji imaju ogroman kapacitet za prenos podataka.

III WLS ESTIMACIJA STANJA

Statička procena stanja se može opisati kao proces pronalaženja vrednosti promenljivih stanja koje minimizuju kvadratnu sumu razlika između izmerenih i stvarnih vrednosti veličina, gde su te vrednosti funkcija vektora promenljivih stanja [9,10,11]. Pri tom, svakoj razlici, koja se naziva rezidual merenja, mora se pridružiti odgovarajuća težina. Inicijalna jednačina za WLS algoritam je data sa:

$$\mathbf{z} = \mathbf{h}(\mathbf{x}) + \mathbf{e},$$

gde je **z** *m* – dimenzioni vektor merenja, vektor **h** ima *m* nelinearnih funkcija i vektor stanja, **x**, koji se sastoji od *n* promenljivih. Vektor **e** predstavlja vektor grešaka merenja. Kriterijumska funkcija koja se posmatra je oblika

$$J(\mathbf{x}) = \sum_{i=1}^{m} \frac{\left(z_i - h_i(x)\right)^2}{R_{ii}} = \left[\mathbf{z} - \mathbf{h}(\mathbf{x})\right]^T \mathbf{R}^{-1} \left[\mathbf{z} - \mathbf{h}(\mathbf{x})\right]. \quad (1)$$

Cilj WLS algoritma je minimizacija prethodno postavljene kriterijumske funkcije (1). Sa **R** je označena matrica kovarijansi merenja preko relacije $R = \mathrm{cov}\{e\} = \mathrm{diag}\{\sigma_m{}^2\}$. Estimacija vektora promenljivih stanja se iterativno dobija rešavanjem sistema jednačina:

$$\mathbf{G}\left(\mathbf{x}^{(k)}\right)\Delta\mathbf{x}^{(k)} = \mathbf{H}^T\left(\mathbf{x}^{(k)}\right)\mathbf{R}^{-1}\left(\mathbf{z} - \mathbf{h}\left(\mathbf{x}^k\right)\right)$$
$$= \mathbf{H}^T\left(\mathbf{x}^{(k)}\right)\mathbf{R}^{-1}\Delta\mathbf{z}^{(k)},\ k = 0,1,2...$$
$$\Delta\mathbf{x}^{(k)} = \mathbf{x}^{(k+1)} - \mathbf{x}^{(k)}$$

gde je sa **G** označena matrica pojačanja u *k*-toj iteraciji, **H** je Jakobijeva matrica u *k*-toj iteraciji, dok je priraštaj vektora merenja u *k* – toj iteraciji dat sa $\Delta\mathbf{z} = \mathbf{z} - \mathbf{h}\left(\mathbf{x}^{(k)}\right)$.

IV NAPADI NA ELEKTROENERGETSKI SISTEM

Elektroenergetski sistem je ključni infrastrukturni resurs koji, poput mnogih drugih, može biti meta različitih vrsta hakerskih napada. Evo nekoliko potencijalnih hakerskih napada na elektroenergetski sistem, zajedno sa osnovnim objašnjenjem o svakom:

- *Denial-of-Service* (DoS) napadi: Ovi napadi ciljaju da onesposobe elektroenergetski sistem preplavljujući ga sa velikim brojem zahteva, čime se sprečava normalno funkcionisanje. To može dovesti do prekida u isporuci električne energije.
- Napadi na SCADA sistem: SCADA (*Supervisory Control and Data Acquisition*) sistemi se koriste za nadzor i upravljanje elektroenergetskim sistemom. Napadi na ove sisteme mogu omogućiti napadačima pristup kontrolama sistema, što može dovesti do neovlašćenog manipulisanja i oštećenja opreme ili prekida u snabdevanju energijom.
- Napadi na mrežnu infrastrukturu: Napadi na mrežnu infrastrukturu elektroenergetskog sistema mogu ciljati rutere, prekidače i druge mrežne komponente kako bi se poremetio komunikacioni protokol sistema. To može ometati komunikaciju između različitih delova sistema, što može dovesti do problema u upravljanju i isporuci električne energije.
- Fizički napadi: Ovi napadi uključuju fizičko oštećenje infrastrukture elektroenergetskog sistema, poput sabotaže transformatora, prekidača ili drugih ključnih komponenti. Takvi napadi mogu prouzrokovati ozbiljne prekide u snabdevanju električnom energijom i zahtevni su za oporavak.
- Fišing i društveni inženjering: Napadači mogu pokušati da dobiju pristup osetljivim informacijama ili sistemima elektroenergetskog sistema putem fišinga (*phishing*), slanjem lažnih e-mailova ili druge manipulativne komunikacije. Ovo može dovesti do neovlašćenog pristupa sistemima ili krađe korisničkih podataka.
- Malware napadi: *Malware* (zlonamerni softver) može biti korišćen za infekciju računara ili drugih uređaja unutar elektroenergetskog sistema. Ovi napadi mogu omogućiti napadačima pristup osetljivim informacijama ili čak daljinsku kontrolu nad sistemima.
- Napadi na IoT uređaje: Sa sve većim brojem pametnih uređaja povezanih u elektroenergetski sistem (npr. pametni brojila), napadači mogu ciljati ove uređaje radi poremećaja sistema ili krađe podataka.

U ovom radu će se razraditi napad na SCADA sistem. Ovi sistemi igraju ključnu ulogu u nadzoru, upravljanju i automatizaciji različitih procesa unutar elektroenergetskog sistema, uključujući distribuciju, prenos i generaciju električne energije. Evo nekoliko načina na koje napadi na SCADA sisteme mogu biti izvedeni i potencijalne posledice:

- Neovlašćeni pristup: Napadači mogu pokušati da dobiju neovlašten pristup SCADA sistemima putem raznih tehnika, uključujući iskorišćavanje ranjivosti u softveru, upotrebu ukradenih korisničkih podataka ili korišćenje naprednih tehnika kao što su napadi *brute force*. Kada dobiju pristup, napadači mogu imati mogućnost da manipulišu postavkama sistema, izvrše komande ili promene parametre koji kontrolišu elektroenergetski sistem.
- Manipulacija podacima: Napadači mogu promeniti ili uništiti podatke koji se prikupljaju i obrađuju u SCADA sistemima. Ovo može rezultirati pogrešnim očitavanjima, netačnim procenama i odlukama zasnovanim na nepouzdanim informacijama. Na primer, napad na SCADA sistem koji kontroliše distribuciju električne energije može rezultirati pogrešnim upravljanjem opterećenjem mreže ili nepotrebnim isključenjem snabdevanja.
- Otkazivanje rada sistema: Napadači mogu izazvati otkazivanje rada SCADA sistema ili sprečiti normalno funkcionisanje putem različitih tehnika, kao što su distribuirani DoS napadi ili napadi na ranjivosti sistema. Ovo može uzrokovati ozbiljne prekide u snabdevanju električnom energijom, naročito ako se ne može brzo intervenisati i oporaviti.
- Lažne komande i kontrole: Napadači mogu emitovati lažne komande ili manipulisati kontrolama SCADA sistema kako bi izazvali neželjene efekte ili čak štetu na opremi. Na primer, mogućnost da se lažno otvore ili zatvore prekidači u elektroenergetskom sistemu može dovesti do prekida u snabdevanju energijom ili oštećenja opreme.
- Krađa podataka: Napadači mogu ciljati SCADA sisteme radi krađe osetljivih podataka, kao što su informacije o infrastrukturi, operativnim procedurama ili korisničkim podacima. Ove informacije mogu se koristiti za dalje napade ili za stvaranje drugih bezbednosnih rizika.

Napadi na SCADA sisteme mogu imati ozbiljne posledice po funkcionalnost, sigurnost i pouzdanost elektroenergetskog sistema. Stoga je ključno da se preduzmu odgovarajuće mere zaštite, uključujući stalno praćenje sistema, primenu sigurnosnih zakrpa, obuku osoblja i implementaciju sigurnosnih protokola kako bi se smanjila ranjivost na ove vrste napada.

V ESTIMACIJA STANJA SA PMU MERENJIMA

PMU merenja se koriste za prikupljanje fazorskih podataka o stanju elektroenergetskog sistema (EES) u realnom vremenu. Ova merenja se šalju do koncentratora fazorskih podataka putem specijalnog protokola kako bi se vremenski sinhronizovala i dalje distribuirala do kontrolnog centra. Međutim, jedan od izazova koji se javlja je skladištenje velike količine informacija koje se generišu u kratkom vremenskom periodu, što predstavlja zahtev za naprednim SCADA/EMS sistemima.

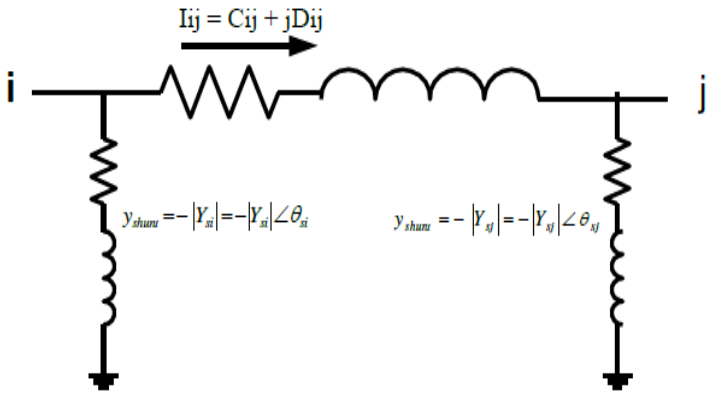
Najčešći način korišćenja PMU merenja je upoređivanje fazorskih uglova napona između različitih čvorova u mreži sa prethodno definisanim vrednostima. Ako su razlike između ovih uglova veće od predefinisanih granica, generiše se alarm koji obaveštava dispečera o mogućim problemima u stabilnosti EES-a.

Pored upotrebe u estimaciji stanja radi poboljšanja robustnosti, observabilnosti i tačnosti mreže, PMU merenja takođe imaju značajnu ulogu u analizi tranzijentnih pojava koje su omogućene visokom frekvencijom merenja. Iako bi idealno bilo da postoji PMU merenje u svakom čvoru EES-a, zbog visokih troškova ova merenja se postavljaju samo na pažljivo odabrane lokacije, koristeći napredne algoritme za optimizaciju postavljanja [14].

Iako PMU merenja pružaju detaljne informacije o stanju sistema, klasična SCADA merenja i dalje imaju važnu ulogu, posebno za praćenje promena koje se ne dešavaju tako često. Stoga, integracija visokofrekventnih PMU merenja sa klasičnim SCADA merenjima zahteva napredne tehnike za estimaciju stanja koje mogu efikasno upravljati ovim različitim tipovima podataka.

U statičkoj estimaciji stanja, koristi se princip baferovanja PMU merenja kako bi se uvažila njihova tačnost i pouzdanost. Ovaj princip podrazumeva čekanje između dva uzastopna izvršavanja WLS estimacije stanja kako bi se formirala srednja vrednost i varijansa PMU fazorskih merenja. Ovo omogućava da se bolje iskoristi informacija dobijena iz PMU merenja i da se smanji uticaj mogućih privremenih fluktuacija u merenjima.

PMU uređaj ima sposobnost da meri fazor napona u čvoru u koji je instaliran i sve fazore struja koje iz tog čvora izlaze. Ako definišemo y_{shunt} kao otočnu admitansu, a sa y rednu admitansu, fazor struje može biti predstavljen u pravougaonom obliku, kao što je prikazano na slici 2. Veličine C_{ij} i D_{ij} su definisane sa:



slika 2. Pi zamenska šema

$$C_{\text{ij}} = |V_i Y_{si}|\cos(\delta_i + \theta_{si}) + |V_j Y_{ij}|\cos(\delta_j + \theta_{ij}) - |V_i Y_{ij}|\cos(\delta_i + \theta_{ij})$$

$$D_{\text{ij}} = |V_i Y_{si}|\sin(\delta_i + \theta_{si}) + |V_j Y_{ij}|\sin(\delta_j + \theta_{ij}) - |V_i Y_{ij}|\sin(\delta_i + \theta_{ij})$$

gde je vektor stanja dat sa $x = [V_1, V_2, ..., V_N]^T$. Jakobijan matrice merenja H koje odgovara aktivnom i reaktivnom delu struje je:

$$\frac{\partial C_{ij}}{\partial V_j} = |Y_{si}|\cos(\delta_i + \theta_{si}) - |Y_{ij}|\cos(\delta_i + \theta_{ij})$$

$$\frac{\partial C_{ij}}{\partial V_j} = |Y_{ij}|\cos(\delta_i + \theta_{ij})$$

$$\frac{\partial C_{ij}}{\partial \delta_i} = -|V_i Y_{si}|\sin(\delta_i + \theta_{si}) + |V_i Y_{ij}|\sin\left(\delta_i + \theta_{ij}\right)$$

$$\frac{\partial C_{ij}}{\partial \delta_j} = -|V_i Y_{ij}|\sin(\delta_j + \theta_{ij})$$

$$\frac{\partial D_{ij}}{\partial V_i} = |V_{si}|\sin(\delta_j + \theta_{ij}) - |Y_{ij}|\sin\left(\delta_i + \theta_{ij}\right)$$

$$\frac{\partial D_{ij}}{\partial V_j} = |Y_{ij}|\sin(\delta_j + \theta_{ij})$$

$$\frac{\partial D_{ij}}{\partial \delta_i} = |V_i Y_{si}|\cos(\delta_i + \theta_{si}) - |V_i Y_{ij}|\cos\left(\delta_i + \theta_{ij}\right)$$

$$\frac{\partial D_{ij}}{\partial \delta_i} = |V_j Y_{ij}|\cos\left(\delta_j + \theta_{ij}\right)$$

Vektor merenja sadrži efektivnu vrednost napona, ugao fazora napona, koeficijente C_{ij} i D_{ij}, kao i informacije o snagama injektiranja, tokove aktivne i reaktivne snage. Uobičajeno je da su merenja dobijena iz PMU uređaja tačnija i preciznija u poređenju sa tradicionalnim merenjima. Stoga se očekuje da će merenja obavljena uz pomoć PMU uređaja generisati preciznije i tačnije rezultate u poređenju sa procenama tradicionalne tehnike. Vektor stanja i podaci merenja mogu biti izraženi u pravougaonim koordinatama. Merenje napona može biti izraženo kao $V=E+\mathrm{j}F$, a struje kao $I=C+\mathrm{j}D$. Takođe, sa $g_{ij}+\mathrm{j}b_{ij}$ su označeni parametri redne admitanse, a sa $g_{si}+\mathrm{j}b_{si}$ parametri otočne admitanse. Struja od čvora i ka čvoru j može biti izražena sada kao:

$$I_{ij} = \left[\left(V_i - V_j\right)\left(g_{ij} + \mathrm{j}bij\right)\right] + \left[V_i\left(g_{si} + \mathrm{j}b_{si}\right)\right]$$
$$= V_i\left[\left(g_{ij} + \mathrm{j}b_{ij}\right) + \left(g_{si} + \mathrm{j}b_{si}\right)\right] - V_j\left(g_{ij} + jb_{ij}\right)$$

. Vektor merenja z je izražen preko $z=h(x)+e$ a preko pravougaone forme:

$z = \left(H_r + jH_m\right)\left(E + jF\right) + e$, gde je $H = H_r + \mathrm{j}H_m$, $x = E + \mathrm{j}F, z = A + \mathrm{j}B$. Parametri A i B mogu se izraziti kao $A = H_r E - H_m F$, $B = H_m E + H_r F$, a u matričnoj formi:

$$\begin{bmatrix} A \\ B \end{bmatrix} = \begin{bmatrix} H_r & -H_m \\ -H_m & H_r \end{bmatrix}\begin{bmatrix} E \\ F \end{bmatrix} + e$$

.

Tada, estimirane vrednosti se mogu dobiti rešavajući linearnu jednačinu

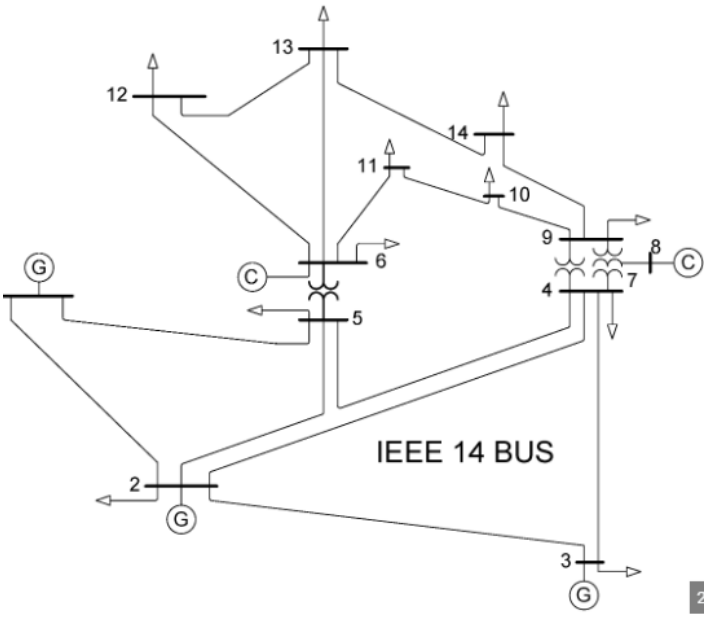
$\Delta \tilde{x} = \left(H^T R^{-1} H\right)^{-1} H^T R^{-1} \Delta z = G^{-1} H^T R^{-1} \Delta z$, tada je nova matrica H data sa:

$H_{new} = \begin{bmatrix} H_r & -H_m \\ -H_m & H_r \end{bmatrix}\begin{bmatrix} E \\ F \end{bmatrix} + e$, pa se ima

$$\tilde{x} = \begin{bmatrix} \tilde{E} \\ \tilde{F} \end{bmatrix} = \left(H_{new}{}^T R^{-1} H_{new}\right)^{-1} H_{new}{}^T R^{-1} \begin{bmatrix} A \\ B \end{bmatrix}.$$

U pogledu pouzdanosti i tačnosti sistema, PMU može pružiti preciznije merne podatke. Više slučajeva će biti testirano dodavanjem PMU uređaja tradicionalnom setu merenja. Simulacije su sprovedene na IEEE sistemu sa 14 čvorova **(**slika 3). Smatra se da su PMU uređaji postavljeni u čvorove 2, 6, 7 i 9.

U tabelama 1 i 2 su prikazani rezultati estimacije stanja. Zbog ograničenja prostora u radu, izostavljen je detaljan opis parametara mreže, uključujući snage injektiranja i ostalih relevantnih podataka.



Slika 3: IEEE mreža sa 14 čvorova

Tabela 1. Fazori napona u čvorovima bez PMU

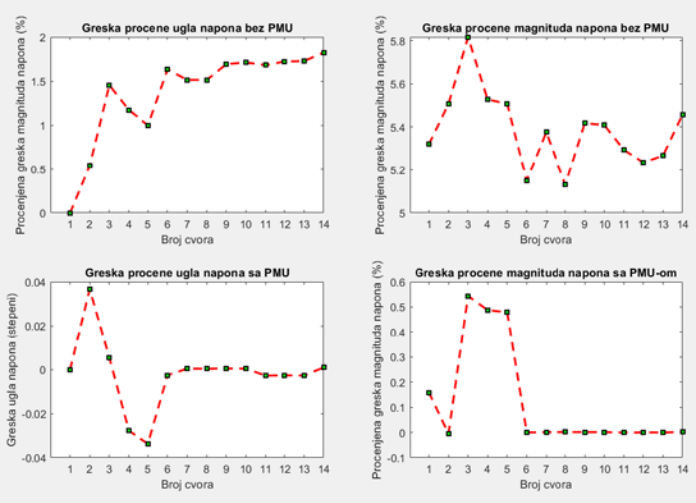
Broj čvora	Napon (r.j.)	Ugao (stepeni)
1	1,0068	0
2	0,9899	-5,0258
3	0,9518	-12,7546
4	0,9579	-10,2142
5	0,9615	-8,7264
6	1,0185	-14,4443
7	0,9919	-13,2372
8	1,0287	-13,2371
9	0,9763	-14,8206
10	0,9758	-15,0364
11	0,9932	-14,8553
12	1,0009	-15,2946
13	0,994	-15,3285
14	0,9647	-16,0727

Na slici 4 su prikazane greške koje se prave sa i bez PMU uređaja. Možemo videti da se kvalitet estimacije stanja sa PMU

uređajima značajno popravlja.

Tabela 2. Fazori napona u čvorovima sa PMU

Broj čvora	Napon (r,j,)	Ugao (stepeni)
1	1,0584	0
2	1,0451	-5,0258
3	1,0046	-12,7546
4	1,0083	-10,2142
5	1,0118	-8,7264
6	1,0700	-14,4443
7	1,0457	-13,2372
8	1,0800	-13,2371
9	1,0305	-14,8206
10	1,0299	-15,0364
11	1,0461	-14,8553
12	1,0533	-15,2946
13	1,0466	-15,3285
14	1,0193	-16,0727



Slika 4. Greške procene ugla napona sa i bez PMU uređaja

VI UNSCENTED KALMAN FILTER

Uobičajeni Kalman filter može naići na poteškoće u obradi izrazito nelinearnih funkcija koje opisuju odnos između merenja i stanja sistema, kao što je slučaj u proceni stanja elektroenergetskih sistema. Linearizacija ovih funkcija korišćenjem proširenog Kalman filtera često može dovesti do nepreciznih rezultata ili čak do divergencije algoritma. Iterativna primena proširenog Kalman filtera može rešiti ove probleme, ali uz dodatno vreme izvršenja algoritma. Oba pristupa takođe mogu imati problema sa stvaranjem matrica Jakobijana, što dodatno komplikuje proces [13].

Unscented Kalman filter (UKF) pristupa rešavanju problema nelinearnosti na drugačiji način. Umesto linearizacije funkcija, ovaj filter koristi selektovane uzorke tačaka koji tačno reflektuju pretpostavljenu raspodelu stanja sistema. Ovi uzorci se direktno propagiraju kroz originalne nelinearne funkcije, a zatim se koriste za dobijanje srednje vrednosti i kovarijanse stanja sistema. Ideja je da je lakše aproksimirati Gauss-ovu raspodelu nego proizvoljnu nelinearnu funkciju, što omogućava tačnije procene stanja sistema. Ovaj pristup ne zahteva formiranje matrica Jakobijana i Hesijana, što dodatno pojednostavljuje algoritam.

Unscented Kalman filter funkcioniše na sličan način kao prošireni Kalman filter (EKF) u smislu osnovnih koraka. Oba algoritma se sastoje od dva glavna koraka:

- Predikcija: U ovom koraku, trenutno stanje sistema se predviđa na osnovu tranzicione funkcije (koja opisuje kako se sistem razvija tokom vremena) i prethodnog stanja sistema. Ovaj korak generiše procenu stanja sistema u sledećem vremenskom koraku.
- Korekcija/Ažuriranje: Nakon što su dostupna merenja za trenutni vremenski korak, sistem vrši korekciju ili ažuriranje procene stanja koristeći ova merenja. Ovaj korak koristi informacije o merenjima kako bi se poboljšala procena stanja sistema.

Ovi koraci se iterativno ponavljaju kako bi se sistem dinamički pratio kroz vreme, uzimajući u obzir kako tranzicione funkcije, tako i informacije dobijene iz merenja. Oba filtra, kako EKF tako i UKF, su osmišljena kako bi rešio problem estimacije stanja u nelinearnim sistemima, ali se razlikuju u načinu linearizacije i propagacije informacija o stanju sistema. Estimirani vektor promenljivih stanja u trenutku $t_{n-1}(\tilde{x}(t_{n-1})$ njemu odgovarajuća matrica kovarijansi $R_{\tilde{x}}(t_{n-1})$ se proširuje srednjom vrednošću $E\{v(t_n)\}=0$ i matricom kovarijansi greške tranzicionog perioda:

$$\tilde{\boldsymbol{x}}(t_{n-1}) = [\hat{\boldsymbol{x}}^T(t_{n-1}) \quad \mathbf{0}]^T$$
$$\tilde{\boldsymbol{R}}_{\tilde{\boldsymbol{x}}}(t_{n-1}) = \begin{bmatrix} \boldsymbol{R}_{\tilde{\boldsymbol{x}}}(t_{n-1}) & \mathbf{0} \\ \mathbf{0} & \boldsymbol{R}_{\boldsymbol{v}}(t_n) \end{bmatrix}$$
$$\tilde{n} = 2n$$

gde $\tilde{n}$ predstavlja broj elemenata proširenog vektora promenljivih stanja, $R_{\tilde{x}}(t_{n-1})$ a predstavlja proširenu matricu kovarijansi. Sigma tačke, kojih ima $\tilde{2n+1}$ i njihovi težinski faktori se određuju kao:

$$\chi^i(t_{n-1}) = \begin{cases} \tilde{\mathbf{x}}(\mathrm{t_{n-1}}) + \mathrm{B_i}, & \mathrm{i} = 0, \\ \tilde{\mathbf{x}}(\mathrm{t_{n-1}}) + \mathbf{B_i}, & \mathrm{i} = 1, \ldots, \tilde{\mathrm{n}} \\ \tilde{\mathbf{x}}(\mathrm{t_{n-1}}) - \mathbf{B_{i-\tilde{n}}}, & \mathrm{i} = \tilde{\mathrm{n}}+1, \ldots 2\tilde{\mathrm{n}}. \end{cases}$$
$$W_i^s = \begin{cases} \mathrm{k}/(\tilde{\mathrm{n}}+\mathrm{k}), & \mathrm{i} = 0, \\ 1/[2(\tilde{\mathrm{n}}+\mathrm{k})], & \mathrm{i} = 1, \ldots, 2\tilde{\mathrm{n}}. \end{cases}$$
$$W_i^c = \begin{cases} \mathrm{k}/(\tilde{\mathrm{n}}+\mathrm{k}) + (1-\alpha^2+\beta), & \mathrm{i} = 0, \\ 1/[2(\tilde{\mathrm{n}}+\mathrm{k})], & \mathrm{i} = 1, \ldots, 2\tilde{\mathrm{n}}. \end{cases}$$

gde je $\mathbf{B}_i$ i – ta kolona matrice $\mathbf{B} = \sqrt{\left(\tilde{n}+\kappa\right)\tilde{\mathbf{R}}_{\tilde{x}}\left(t_{n-1}\right)}$, zatim α - koeficijent koji uključuje prethodno znanje o distribuciji vektora promenljivih stana, k - parametar skaliranja, W_i^s je težinski faktor koji se odnosi i – tu sigma tačku i koristi za proračun prediktovanog vektora promenljivih stana i matrice kovarijansi. Prediktovane sigma tačke se dobijaju propagacijom prethodno odabranih sigma tačaka kroz tranzicionu funkciju $f\left(x\left(t_{n-1}\right)\right)$ koja opisuje kako se sistem razvija tokom vremena. Ove sigma tačke se koriste za

procenu predikcije vektora promenljivih stanja u trenutku t_n. Nakon propagacije, dobija se prediktovanu srednju vrednost i kovarijanse:

$$\overline{\boldsymbol{\chi}}^i(t_n) = \boldsymbol{f}(\boldsymbol{\chi}^i(t_{n-1}))$$

$$\overline{\boldsymbol{x}}(t_n) = \sum_{i=0}^{2\tilde{n}} W_i^s \overline{\boldsymbol{\chi}}^i(t_n)$$

$$\boldsymbol{R_x}(t_n) = \sum_{i=0}^{2\tilde{n}} W_i^c (\overline{\boldsymbol{\chi}}^i(t_n) - \overline{\boldsymbol{x}}(t_n))\,(\overline{\boldsymbol{\chi}}^i(t_n) - \overline{\boldsymbol{x}}(t_n))^T$$

Unscented Kalman Filter u estimaciji stanja u energetskim sistemima se sastoji iz nekoliko koraka:

- Inicijalizacija: Proces počinje inicijalizacijom početnog stanja sistema. Ovo može uključivati postavljanje inicijalnih vrednosti promenljivih stanja, kao i inicijalizaciju kovarijacione matrice koja opisuje nesigurnost u početnom stanju.
- Predikcija: Prvi korak u svakoj iteraciji je predikcija sledećeg stanja sistema. To se postiže propagacijom trenutnog stanja sistema kroz tranzicionu funkciju *f*(*x*), koja opisuje evoluciju sistema tokom vremena. Koristi se i kovarijaciona matrica šuma procesa kako bi se uzela u obzir nesigurnost u predikciji.
- Generisanje sigma tačaka: Zatim se generišu sigma tačke, koje su odabrane tačke u prostoru stanja koje odražavaju statističku raspodelu stanja sistema. Ove tačke se biraju tako da što bolje opisuju raspodelu stanja i njegovu nesigurnost.
- Predikcija sigma tačaka: Svaka od sigma tačaka se zatim propagira kroz tranzicionu funkciju kako bi se dobile predikcije stanja u sledećem vremenskom koraku.
- Procena predikcije stanja: Nakon propagacije, procenjuje se srednja vrednost i kovarijansa predikcije stanja. Ovo se radi na osnovu prediktovanih sigma tačaka.
- Ažuriranje: Kada stignu novi mereni podaci, ažurira se procena stanja sistema. To se postiže kroz dva koraka:
- Generisanje sigma tačaka merenja: Koristeći procenjenu srednju vrednost i kovarijansu stanja, generišu se sigma tačke merenja kroz funkciju merenja, koja opisuje kako stanje sistema utiče na merene veličine.
- Ažuriranje stanja: Mereni podaci se zatim koriste za ažuriranje procene stanja sistema. Ovo se postiže proračunom težinskih faktora za svaku sigma tačku, koji se zatim koriste za procenu novog stanja sistema.
- Ponavljanje iteracija: Ovi koraci se ponavljaju za svaki novi vremenski korak, pri čemu se procena stanja sistema kontinuirano ažurira na osnovu novih merenja i predikcija.

Ovaj proces omogućava estimaciju stanja sistema u realnom vremenu, uzimajući u obzir kako merene podatke tako i nesigurnost u modelu sistema i merenjima.

VII MALICIOZNI NAPADI NA ESTIMATOR

Pretpostavlja se da postoji *m* broj mernih uređaja koji pružaju *m* merenja $z_1, ..., z_m$ i da postoji *n* promenljivih stanja $x_1, ..., x_n$. Odnos između ovih *m* merenja i *n* promenljivih stanja može se karakterisati matricom $m \times n$ koju će se označiti sa H. Uopšteno, matrica H elektroenergetskog sistema određuje se topologijom i impedansama vodova sistema. Takođe pretpostavlja se da napadač može imati pristup matrici H ciljanog elektroenergetskog sistema i može ubacivati maliciozna merenja u kompromitovane mere kako bi narušio proces procene stanja.
Razmatraju se dva moguća cilja napada: nasumične napade ubacivanja lažnih podataka, u kojima napadač ima za cilj da pronađe bilo koji vektor napada koji može rezultirati pogrešnom procenom promenljivih stanja, i ciljane napade ubacivanja lažnih podataka, u kojima napadač teži pronalaženju vektora napada koji može ubaciti specifičnu grešku u određene promenljive stanja. Iako potonji napadi mogu potencijalno prouzrokovati više štete sistemu, prvi su lakši za izvršenje

Pored osnovnog opisa napada ubacivanja lažnih podataka, koriste se i sledeća dva verovatna scenarija napada kako bi olakšali diskusiju o tome kako napadač može konstruisati vektore napada kako bi zaobišao trenutne pristupe za detekciju loših merenja. Međutim, napadi ubacivanja lažnih podataka nisu ograničeni na ove scenarije napada.

Scenario I – Ograničen pristup mernim uređajima. Napadaču je dozvoljen pristup samo određenim mernim uređajima zbog različitih fizičkih zaštita mernih uređaja. Na primer, merni uređaji locirani u podstanicama sa fizičkom kontrolom perimetra mogu biti znatno teže dostupni u poređenju sa onima koji se nalaze u zaključanoj kutiji izvan zgrade.

Scenario II – Ograničeni resursi za kompromitovanje mernih uređaja. Napadaču su ograničeni resursi potrebni za kompromitovanje mernih uređaja. Na primer, napadač ima resurse da kompromituje samo do k mernih uređaja (od svih mernih uređaja). Zbog ograničenih resursa, napadač može takođe želeti da minimizira broj mernih uređaja koji će biti kompromitovani.

Analiza Scenarija I

U ovom scenariju, napadač ima ograničen pristup samo određenim mernim uređajima zbog različitih nivoa fizičke zaštite tih uređaja. Ova ograničenja znače da napadač može manipulisati samo merenjima na uređajima do kojih može fizički pristupiti ili na koje ima digitalni pristup. To bi mogli biti merni uređaji koji su manje zaštićeni ili se nalaze na periferiji mreže, umesto onih koji se nalaze unutar dobro čuvanih podstanica.

Selekcija ciljanih uređaja: Napadač prvo identifikuje uređaje do kojih može pristupiti. Ovo zahteva prethodno poznavanje mreže i njenih bezbednosnih mehanizama.

Analiza matrice H: Napadač analizira matricu H koja karakteriše odnos između mernih uređaja i promenljivih stanja sistema. Ovo zahteva poznavanje ili procenu topologije mreže i impedansi vodova.

Konstrukcija vektora napada: Na osnovu dostupnih informacija o matrici H, napadač konstruiše vektor napada koji je dizajniran da, kada se primeni na kompromitovane uređaje, izazove željenu pogrešnu procenu stanja u sistemu. Ovaj proces uključuje selekciju odgovarajućih vrednosti za manipulaciju merenja na dostupnim uređajima kako bi se izazvala specifična greška u procenjenim promenljivama stanja bez otkrivanja.

Implementacija napada: Napadač zatim implementira napad ubacivanjem konstruisanog vektora napada u merni sistem,

izmenom merenja na ciljanim uređajima.

Otkrivanje i odbrana: Iako ovaj pristup omogućava napadaču da izvede FDIA (*False Data Injection Attack*), postoji rizik od otkrivanja ukoliko sistem za detekciju loših merenja identifikuje anomalije u izmenjenim podacima.

Potreba za detaljnim znanjem: Uspešna implementacija napada zahteva detaljno znanje o mreži, uključujući topologiju i parametre sistema, što može da bude izazovno za napadača da obezbedi bez unutrašnjeg izvora ili naprednih tehnika izviđanja.

Scenario I pokazuje da čak i sa ograničenim pristupom, napadači mogu efikasno izvesti FDIA ako pažljivo odaberu ciljane merne uređaje i precizno konstruišu vektor napada. Međutim, uspeh ovakvog napada zavisi od sposobnosti napadača da se neopaženo infiltrira i manipuliše mernim sistemom, kao i od njihove sposobnosti da precizno procene ili pristupe ključnim informacijama o mreži.

Analiza Scenarija II

Ovaj scenario pretpostavlja situaciju u kojoj napadač mora efikasno upotrebiti svoje ograničene resurse da maksimizira uticaj napada na sistem.

Napadač mora pažljivo odabrati koje merne uređaje će kompromitovati kako bi maksimizovao efekat napada. S obzirom na ograničeni broj uređaja koje može efektivno kompromitovati, napadač treba da odredi koja merenja imaju najveći uticaj na procenu stanja sistema. To zahteva razumevanje veza između mernih uređaja i ključnih promenljivih stanja na koje napadač želi da utiče.

Nakon odabira ciljanih mernih uređaja, napadač konstruiše vektor napada koristeći dostupne informacije o konfiguraciji sistema i matrici H. Ovo uključuje proračunavanje promena koje treba napraviti na izabranim merenjima kako bi se izazvala željena greška u procenama stanja sistema. Efektivnost ovog koraka zavisi od sposobnosti napadača da pristupi tačnim i detaljnim informacijama o sistemu.

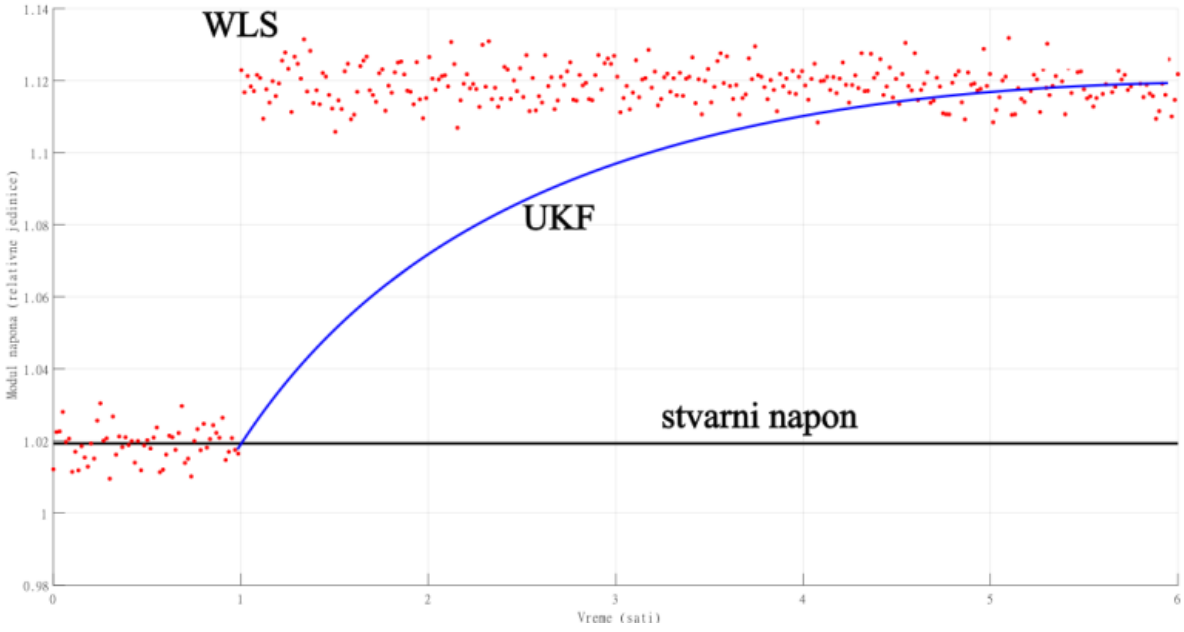
Za razliku od Scenarija I, gde je fokus na fizičkim ili digitalnim ograničenjima pristupa mernim uređajima, Scenarij II istražuje kako napadač može optimizovati upotrebu ograničenih resursa. Napadač mora balansirati između broja mernih uređaja koje želi da kompromituje i potrebe da ostane ispod radara detekcijskih sistema. Ovo često zahteva sofisticirane strategije i duboko poznavanje sistema da bi se identifikovali "slabi" merni uređaji čija kompromitacija može proizvesti disproporcionalno veliki uticaj na procenu stanja.

VIII PRIMER NAPADA

Pretpostavlja se da napadač ima neograničeno znanje o svim neophodnim parametrima sistema i da ima neograničene resurse. Napadač želi da injektiranjem loših merenja promeni napon u čvoru br. 5 za 1 relativnu jedinicu. Pretpostavimo da napad počinje u prvom satu. Ukoliko bi se za detekciju koristila samo statička WLS estimacija stanja, ona ne prati dinamiku sistema tj. ne zavisi od rezultata iz prošlosti. Kako napadač ima neograničeno znanje i resurse, on može odabrati takav vektor napada koje bi prošao kroz Hi-kvadrat test za identifikaciju loših merenja, kao i test na maksimalni normalizovani rezidual merenja. Međutim, ukoliko se koristi i dinamička estimacija stanja i to UKF algoritam, maliciozni napad neće biti preslikan odmah na napon u čvoru, već će se ka vrednosti koju napadač želi kretati postepeno.

U ovom primeru je zato iskorišćen vektor reziduala promenljivih stanja i to dobijenih od statičke WLS i dinamičke UKF estimacije:

$$\mathrm{Res} = \tilde{x}_{WLS}(t_n) - \tilde{x}_{UKF}(t_n).$$



Slika 5. Prikaz rezultata simulacije

Normalizovani vektori reziduala promenljivih stanja se dobija deljenjem apsolutne vrednosti vektora reziduala promenljivih stanja sa kvadratnim korenom vrednosti dijagonalnih članova matrice kovarijansi promenljivih stanja iz UKF algoritma:

$$\mathrm{Res}_{nor} = \frac{\left|\mathrm{Re}\,s\left(t_n\right)\right|}{\sqrt{R_x\left(t_n\right)}}.$$

Sada se detekcija malicioznih napada vrši isto kao i detekcija loših merenja: poređenjem maksimalnih normalizovanih reziduala. Postavlja se pitanje praga kada je maliciozni napad detektovan. Obično je to od 30 do 40 r.j. Na slici 5 su prikazani grafici stvarnog napona u čvoru br. 5. Može se primetiti da WLS estimacija do prvog sata prilično dobro prati stvarnu vrednost napona, a UKF se skoro poklapa sa stvarnom vrednosti napona. U prvom satu se događa maliciozni napad i kako WLS estimacija ne zavisi od prošlosti, ona odmah uzima novu vrednost, dok se UKF estimacija postepeno približava i uzima vrednost koju napadač želi tek nakon 4 sata. Primenom normalizovanog vektora reziduala promenljivih stanja se dobija da je u prvom satu on jednak 404, što je značajno iznad 30 do 40 r.j. i možemo reći da je napad detektovan.

IX Zaključak

Uvođenje Phasor Measurement Units (PMU) uređaja unelo je revolucionarne promene u način na koji se vrši estimacija stanja u elektroenergetskim sistemima, donoseći značajna poboljšanja u preciznosti, brzini i pouzdanosti detekcije i identifikacije stanja mreže. PMU uređaji, merni instrumenti nove generacije, omogućavaju merenje električnih veličina u mreži, kao što su naponi i struje, sa visokom tačnošću i u realnom vremenu, pružajući time detaljan uvid u trenutno stanje mreže. Ključna poboljšanja kvaliteta estimacije stanja zahvaljujući PMU uređajima su povećana preciznost, a zahvaljujući visokoj tačnosti merenja faza i amplituda koje PMU uređaji pružaju, moguće je postići znatno precizniju estimaciju stanja elektroenergetske mreže. Ovo doprinosi boljem razumevanju dinamike sistema i poboljšava pouzdanost operativnih odluka. Takođe, PMU uređaji omogućavaju skoro trenutno praćenje promena u mreži zahvaljujući sposobnosti merenja u realnom vremenu. Ova karakteristika je ključna za brzo reagovanje na iznenadne poremećaje u mreži, omogućavajući efikasnu stabilizaciju sistema. Integracijom podataka sa PMU uređaja, sistemi za estimaciju stanja mogu efikasnije identifikovati i isključiti loša merenja, smanjujući uticaj grešaka i povećavajući pouzdanost procena stanja. PMU podaci, zbog svoje visoke tačnosti i kratkih vremenskih intervala merenja, pružaju dodatni sloj zaštite protiv napada na sisteme za estimaciju stanja, uključujući napade ubacivanjem lažnih podataka (FDIA). Upotrebom PMU podataka, sistem može brže i efikasnije detektovati anomalije koje mogu ukazivati na prisustvo malicioznih aktivnosti. PMU uređaji su posebno korisni u dinamičkim estimatorima stanja, kao što je UKF, omogućavajući detaljniju analizu promenljivosti i dinamike mreže. Ovo je posebno važno u kontekstu sve većeg učešća obnovljivih izvora energije i povećane potrebe za upravljanjem varijabilnosti i nepredvidivosti u mreži.

Istraživanje u fokusu pokazuje da postojeće metode za detekciju i identifikaciju loših merenja u elektroenergetskim sistemima nisu dovoljno otporne na sofisticirane oblike malicioznih napada, kao što su napadi ubacivanja lažnih podataka (FDIA). Ključni problem leži u tome što se tradicionalne tehnike oslanjaju na analizu reziduala merenja, što napadačima omogućava da manipulišu sistemom tako da indukuju greške u procenjene vrednosti ciljanih promenljivih stanja, a da pritom ostanu neotkriveni. Napadači mogu da iskoriste poznavanje Jakobijeve matrice sistema za precizno usmeravanje svojih napada, simultano menjajući vrednosti određenih skupova merenja. Ovo čini promene nedetektovanim za tradicionalne metode detekcije. Ovi napadi predstavljaju realnu pretnju sa potencijalno ozbiljnim posledicama, s obzirom na sve učestalije hakerske napade na infrastrukturu energetskih sistema. Zbog toga je u radu predstavljena nova tehnika koja kombinuje statičku i dinamičku estimaciju stanja, koristeći nelinearni dinamički estimator stanja zasnovan na Unscented Kalman Filter (UKF) algoritmu. UKF je izabran zbog svoje sposobnosti da se efikasno nosi sa izrazito nelinearnim sistemima. Predložena metoda koristi kratkoročnu prognozu potrošnje i proizvodnje energije za konstrukciju tranzicione matrice, što omogućava preciznije predviđanje promenljivih stanja i smanjuje grešku tranzicionog procesa. Za detekciju FDIA koristi se nova metrika zasnovana na poređenju normalizovanih reziduala promenljivih stanja iz statičke i dinamičke estimacije stanja sa unapred definisanim pragom. Ovaj pristup omogućava detekciju napada čak i kada su promene indukovane napadom minimalne i nalaze se unutar uobičajenih grešaka estimatora stanja. Ovaj inovativni algoritam detekcije testiran je na test mrežama i pokazao se efikasnim u detektovanju FDIA, potvrđujući neophodnu osetljivost na različite intenzitete napada. Predstavljena metoda ne samo da unapređuje sigurnost i pouzdanost estimacije stanja u elektroenergetskim sistemima već i naglašava važnost kontinuiranog razvoja i prilagođavanja bezbednosnih mehanizama za zaštitu kritične infrastrukture od malicioznih napada.

Literatura/References

[1] Gomez-Exposito, A., Abur, A., Rousseaux, P., de la Villa Jaen, A., Gomez-Quiles, C. On the use of PMUs in power system state estimation, in Proc. *Proceedings of the 17th Power Systems Computation Conference (PSCC 2011*, Stockholm, 22-26 August 2011. https://www.academia.edu/72290650/On_the_use_of_PMUs_in_power_system_state_estimation?auto=download [pristupljeno 04.02.2024]

[2] Oh, H. Situational Awareness with PMUs and SCADA, 2017. https://doi.org/10.48550/arXiv.1706.00795

[3] Overbye, T., Sauer, P., DeMarco, C., Lesieutre, B., Venkatasubramanian, M. Using PMU data to increase situational awareness: Final Project Report, Power System Engineering Research Center (PSERC) Publication 10-16, 2010. https://pserc.wisc.edu/wp-content/uploads/sites/755/2018/08/S-36_Final-Report_Sept-2010.pdf [pristupljeno 04.02.2024]

[4] Giri, J., Parashar, M., Trehern, J., Madani, V. The situation room: Control center analytics for enhanced situational awareness, IEEE Power and Energy Magazine, Vol. 10, No. 5, pp. 24-39, 2012. https://doi.org/10.1109/MPE.2012.2205316

[5] Korres, G.N., Manousakis, N.M. State estimation and bad data processing for systems including PMU and SCADA measurements, Electric Power Systems Research, Vol. 81, No. 7, pp. 1514-1524, 2011. https://doi.org/10.1016/j.epsr.2011.03.013

[6] Das, K., Hazra, J., Seetharam, D. P., Reddi, R. K., Sinha, A. K. Real-time hybrid state estimation incorporating SCADA and PMU measurements, in Proc. *3rd IEEE PES Innovative Smart Grid Technologies Europe (ISGT Europe)*, Berlin, Germany, pp. 1-8, 14-17 October 2012. https://doi.org/10.1109/ISGTEurope.2012.6465749

[7] Avila-Rosales, R., Rice, M. J., Giri, J., Beard, L., Galvan, F. Recent experience with a hybrid SCADA/PMU on-line state estimator, in Proc. *2009 IEEE Power & Energy Society General Meeting* , Calgary, Canada, pp.1-8, 26-30 July 2009. https://doi.org/10.1109/PES.2009.5275954

[8] Phadke, A.G., Thorp, J.S. *Synchronized Phasor Measurements and Their Applications*, Springer 2008.

[9] Abur, A., Exposito, A. *Power System State Estimation: Theory and Implementation*, New York: Marcel Dekker, 2004

[10] Schweppe, F. C., Wildes, J. Power System Static-State Estimation, Part I: Exact Model, IEEE Transactions on Power Apparatus and Systems, Vol. 89, pp. 120-125, 1970. https://doi.org/10.1109/TPAS.1970.292678

[11] Mijušković, N., Vlaisavljević, D. Statička Estimacija Stanja Elektroenergetskog Sistema - Pregled Metoda, Beograd: EPS, 1996.

[12] Liu, Y., Ning, P., Reiter, M.K. False Data Injection Attacks Against State Estimation in Electric Power Grids, ACM Transactions on Information and System Security, Vol. 14, No. 1, pp. 1-33, 2011. https://doi.org/10.1145/1952982.1952995

[13] Živković, N. *Detekcija malicioznih napada na elektroenergetski sistem korišćenjem sinergije statičkog i dinamičkog estimatora stanja*, Univerzitet u Novom Sadu, Fakultet tehničkih nauka, 2019.

[14] Kumar, J., Rai J.N., Vipin vp., Aurora. B.B., Singh C.K. Improvement in power system state estimation by use of phasor measurement unit, International journal of engineering research and technology (IJERT), Vol.1, No. 8, pp. 1-6, 2012. https://www.ijert.org/research/improvement-in-power-system-state-estimation-by-use-of-phasor-measurement-unit-IJERTV1IS8201.pdf [pristupljeno 08.02.2024]

AUTORI/AUTHORS

dr Vladimir Bečejac - PhD elektrotehnike i računarstva, EMS AD, vladimir.becejac@ems.rs, ORCID 0000-0002-2679-9354
Miloš Đorđević - MS inženjer elektrotehnike i računarstva, EMS AD, milos.djordjevic@ems.rs, ORCID 0009-0001-6118-5104
Nemanja Jelenić - diplomirani inženjer elektrotehnike i računarstva, EMS AD, nemanja.jelenic@ems.rs, ORCID 0009-0004-1878-7726
Mihajlo Marković - diplomirani inženjer elektrotehnike i računarstva, EMS AD, mihajlo.markovic@ems.rs, ORCID 0009-0002-9604-5432
Miloš Mosurović - MS inženjer elektrotehnike i računarstva, SEEPEX, milos.mosurovic@seepex-spot.rs, ORCID 0009-0005-3237-9734

State Estimation in the Power System with Phasor Measurement Units and Malicious Attacks through Injection of Inaccurate Measurements and Its Detection

Abstract **-** This manuscript explores the significance of state estimation methods in electric power systems, with a particular focus on the role of Phasor Measurement Units. In the manuscript is presented the basic principles and advantages of state estimators in the absence of PMU measurements, followed by an analysis of how PMU measurements significantly enhance the accuracy of state estimations. Through a detailed review, we highlight the key characteristics of PMUs and how their synchronized data contributes to improved state estimation quality. The paper investigates the security aspects of state estimation, specifically focusing on malicious attacks through the injection of false measurements (FDIA). Using a concrete example, it is demonstrated how an FDIA attack can significantly impact the accuracy of state estimations by introducing inaccurate data into the system. The manuscript also considers a strategy for detecting such attacks through residual analysis.

Index Terms **-** State estimation, Phasor Measurement Unit (PMU), False Data Injection Attack (FDIA)