doi: 10.46793/EEE26-3.35C

*Originalni naučni rad*
UDK 621.316.1:004.056

# Maliciozni napadi na estimator stanja u distributivnim mrežama: Analiza izvodljivosti napada u uslovima male redundanse merenja

**Stefan Čubonović[*], Dragan Ćetenović[*], Nikola Vojnović[**], Aleksandar Ranković[*]**

[*] Fakultet tehničkih nauka u Čačku, Univerziteta u Kragujevcu
[**] Fakultet tehničkih nauka Univerziteta u Novom Sadu

***Rezime*** - U poslednjoj deceniji je intenzivirana upotreba informaciono-komunikacionih tehnologija u distributivnim mrežama. Takve tehnologije su izložene rizicima od malicioznih sajber napada, što predstavlja pretnju po rad distributivnih mreža. Jedna od mogućih meta takvih napada u distributivnim mrežama je i estimator stanja. Klasični algoritmi za detekciju loših podataka, među kojima se najčešće sreću statističke metode kao sto su $\chi^2$ test ili test najvećeg normalizovanog reziduala, ne mogu da detektuju maliciozne napade injektiranjem lažnih podataka (false data injection attacks - FDIAs) ukoliko su ovi vešto prikriveni. Međutim, zbog male redundanse merenja karakteristične za distributivne mreže, napadači su u problemu da prikriju napad, pa ga u tom slučaju čak i klasični algoritmi za detekciju loših podataka mogu prepoznati. To omogućuje detekciju FDIAs bez dodatnih finansijskih ulaganja koja bi iziskivala implementacija sofisticiranih rešenja. Ovaj rad se bavi analizom izvodljivosti FDIAs u distributivnim mrežama, nastojeći da dovede u vezu izvodljivost napada i redundansu merenja. Rezultati analize se mogu upotrebiti da ukažu operatoru distributivnog sistema da li postoji potreba za sofisticiranim tehnikama za detekciju FDIAs ili ne, a zavisno od merne infrastrukture mreže kojom operator upravlja.

***Ključne reči*** - BDD, FDIA, pseudo merenja, WLS

## I UVOD

Savremeni koncept distributivne mreže ne označava samo fizičku infrastrukturu prenosa i distribucije električne energije, već i njenu integraciju sa informaciono-komunikacionim tehnologijama. Tradicionalna infrastruktura dopunjena je sa naprednim mernim uređajima, uređajima energetske elektronike i komunikacionim kanalima, omogućavajući dvosmerni protok podataka i nadzor u realnom vremenu. Uređaji kao što su PMU (eng. *phasor measurement units*) omogućavaju prikupljanje i razmenu informacija o stanju mreže u gotovo svakom trenutku. Međutim, upravo te nove tehnologije otvaraju vrata novim pretnjama, a to su sajber napadi. Takvi napadi su sofisticirano dizajnirani tako da mogu ozbiljno ugroziti stabilnost i sigurnost celog EES-a. Primeri ovakvih incidenata odavno nisu samo teorijska konstrukcija već i realan scenario. Napad na ukrajinsku elektrodistributivnu mrežu 2015. godine [1], poznat kao BlackEnergy napad, doveo je do masovnog nestanka struje. Slični pokušaji su zabeleženi i u Sjedinjenim Američkim Državama [2] i nekim Evropskim zemljama [3], što potvrđuje da sajber bezbednost predstavlja jedan od ključnih izazova savremenih EES-a. Razvijeni su brojni algoritmi za detekciju loših podataka (*bad data detection* – BDD), među kojima dominiraju statističke metode kao što su $\chi^2$ test i LNR (*largest normalized residual*) test [4, 5]. Ovi testovi, iako najviše korišćeni i efikasni u detekciji loših podataka, mogu pokazati određena ograničenja u slučaju izuzetno naprednih i dobro koordinisanih napada, kao što je maliciozni napad injektiranjem lažnih podataka (*false data injection attacks* - FDIA) [6]. Iako se ovakvi napadi u teoriji mogu konstruisati tako da ostanu neprimećeni od strane tradicionalnih detektora loših podataka, u distributivnim mrežama ograničena merna redundansa može značajno smanjiti mogućnost njihove izvodljivosti, što u dosadašnjim istraživanjima nije u potpunosti razmatrano. Stoga se postavlja pitanje: „Da li je realizacija pažljivo dizajniranih FDIA napada moguća u odsustvu kontrole nad pseudo merenjima?“.

Ovaj rad ima 6 delova. Nakon uvoda, u drugom delu rada, prikazana je teorijska osnova koja se odnosi na metod minimizacije sume otežanih kvadrata reziduala merenja (*weighted least squares* - WLS) u estimaciji stanja (*state estimation* - SE), standardne testove loših podataka ($\chi^2$ i LNR) i osnovne principe dizajniranja FDIA napada. Treći deo opisuje karakteristike korišćene distributivne mreže, tipove merenja i način implementacije napada. Četvrti deo odnosi se na rezultate i analizu, sa posebnim akcentom sa posebnim akcentom na analizu uslova pod kojima FDIA napadi mogu ili ne mogu proći nezapaženo kroz tradicionalne detektore u uslovima ograničene merne redundanse. U petom delu dat je zaključak ovog istraživanja. Šesti deo predstavlja pregled korišćene literature.

## II TEORIJSKA OSNOVA PRIMENJENIH METODA

U ovom delu prikazani su osnovni teorijski koncepti neophodni za razumevanje ostatka rada. Najpre, se razmatra problem SE u EES-ima, sa posebnim akcentom na WLS metodu, koja u praksi predstavlja standardni pristup. Nakon izvršene SE sprovodi se detekcija loših podatka, zbog toga je neophodno da se upoznamo sa tradicionalnim metodama, $\chi^2$ test i LNR test, koje se koriste za identifikaciju merenja sa neuobičajenim odstupanjima. Na kraju, se uvodi pojam FDIA i objašnjava osnovni princip njihovog načina izvođenja.

### *II.1 Estimacija stanja WLS metodom*

Cilj SE je da kroz matematički model i dostupna merenja proceni vektor stanja posmatranog dela EES-a. Vektor stanja se obično definiše poznavanjem amplituda napona $|V_i|$ i faznih stavova napona $\theta_i$ po čvorovima u tom sistemu. Procena ovih veličina je

važna, jer poznavajući njih možemo stvoriti tačnu sliku o stanju posmatranog dela EES-a. Suprotno, ako su ove veličine kompromitovane greškama ili namernim napadima ceo sistem postaje nepouzdan. Zbog toga SE predstavlja važan deo savremenog sistema za nadzor i upravljanje.

WLS metoda zasnovana na minimizaciji sume otežanih kvadrata reziduala merenja je najkorišćenija u praksi. Cilj optimizacije je pronaći vektor stanja $x$ koji će minimizirati funkciju cilja (jednačina 1), najčešće upotrebom iterativnog Njutn-Rapsnovog postupka [8]:

$$J(\boldsymbol{x}) = [\boldsymbol{z} - \boldsymbol{h}(\boldsymbol{x})]^T \boldsymbol{R}^{-1} [\boldsymbol{z} - \boldsymbol{h}(\boldsymbol{x})]. \quad (1)$$

gde su:

- $\boldsymbol{z}$ – vektor merenja;
- $\boldsymbol{x}$ – vektor stanja ($|V_i|$ i $\theta_i$);
- $\boldsymbol{h}(\boldsymbol{x})$ – nelinearna vektorska funkcija koja povezuje vektor stanja i vektor merenja;
- $\boldsymbol{R} = \boldsymbol{W}^{-1}$ – matrica kovarijansi grešaka merenja;
- $\boldsymbol{W}$ – težinska matrica, inverzna matrici kovarijansi grešaka merenja.

Nelinearna vektorska funkcija $\boldsymbol{h}(\boldsymbol{x})$ zasniva se na datom skupu jednačina (2) injektiranja i tokova snaga [5]:

$$\begin{aligned} P_i &= |V_i| \sum_{j=1}^{n} |V_j| \left(G_{ij} \cos\theta_{ij} + B_{ij} \sin\theta_{ij}\right) \\ Q_i &= |V_i| \sum_{j=1}^{n} |V_j| \left(G_{ij} \sin\theta_{ij} - B_{ij} \cos\theta_{ij}\right) \quad (2) \\ P_{ij} &= |V_i|^2 G_{ij} - |V_i| |V_j| (G_{ij} \cos\theta_{ij} + B_{ij} \sin\theta_{ij}) \\ Q_{ij} &= -|V_i|^2 B_{ij} - |V_i| |V_j| (G_{ij} \sin\theta_{ij} - B_{ij} \cos\theta_{ij}) \end{aligned}$$

Iz prethodno navedenih izraza (2) jasno je da promena magnitude ili faznog ugla napona utiče na vrednosti injektiranja i tokova snaga, što predstavlja osnovu za razumevanje strukture napada vektora analiziranog u daljem tekstu rada.

Efikasnost WLS estimacije prisutna je u prenosnim mrežama sa bogatom mernom infrastrukturom. Međutim, u distributivnim mrežama broj merenja je često osiromašen, što značajno smanjuje redundansu merenja i čini proces osetljivijim na greške i napade. Upravo zbog toga, analiza WLS metode predstavlja osnovu za razumevanje ranjivosti sistema na FDIA napade.

*II.2 $\chi^2$ test detekcije loših podataka*

Jedna od najčešće korišćenih BDD metoda u procesu SE je $\chi^2$ test. Ovaj test se zasniva na statističkom ispitivanju veličine reziduala, odnosno razlike između izmerenih i procenjenih vrednosti merenja. Funkcija cilja u WLS metodi ima oblik:

$$J(\boldsymbol{x}) = [\boldsymbol{z} - \boldsymbol{h}(\boldsymbol{x})]^T \boldsymbol{R}^{-1} [\boldsymbol{z} - \boldsymbol{h}(\boldsymbol{x})] = \boldsymbol{r}^T \boldsymbol{W} \boldsymbol{r}. \quad (3)$$

Gde je $\boldsymbol{r} = \boldsymbol{z} - \boldsymbol{h}(\boldsymbol{x})$ vektor reziduala merenja. Funkcija $J(\boldsymbol{x})$ generalno prati $\chi^2$ raspodelu sa stepenom slobode jednakim broju merenja umanjenom za broj stanja [5]:

$$J(\boldsymbol{x}^*) \sim \chi^2(m - n), \quad (4)$$

gde su $m$ broj merenja, $n$ broj promenljivih stanja i $\boldsymbol{x}^*$ rešenje problema procene stanja dobijeno primenom WLS metode.

Ideja testa podrazumeva da se u slučaju kada je vrednost funkcije cilja $J(\boldsymbol{x}^*)$ veća ili jednaka od unapred definisanog praga $\tau_{\chi^2}$, zaključuje da u merenjima postoji loš podatak (test je pozitivan). U suprotnom, kada je vrednost funkcije cilja $J(\boldsymbol{x}^*)$ manja od unapred definisanog praga $\tau_{\chi^2}$, pretpostavlja se da su sva merenja konzistentna (test je negativan). Izbor prave vrednosti praga $\tau_{\chi^2}$ je izuzetno bitan, jer premala vrednost može dovesti do lažne detekcije postojanja lošeg podatka, a prevelika vrednost može sakriti postojanje lošeg podatka. Prednost $\chi^2$ testa ogleda se u jednostavnoj primeni. Međutim, ovaj test pruža samo globalni indikator postojanja loših podataka, bez informacija o njihovoj tačnoj lokaciji. Zbog toga se u praksi često kombinuje sa dodatnim metodama, kao što je LNR test, koje omogućavaju identifikaciju konkretnih merenja odgovornim za odstupanje.

*II.3 LNR test detekcije loših podataka*

Za razliku od $\chi^2$ testa, koji predstavlja globalni indikator konzistentnosti merenja, LNR test omogućava identifikaciju konkretnih merenja koja su potencijalno degradirana. Suština metode je da se izračunaju normalizovani reziduali svih merenja u posmatranom delu EES-a i da se najveći od njih upredi sa unapred zadatim pragom. Normalizovani reziduali definišu se sledećim izrazom [5]:

$$r_i^N = \frac{r_i}{\sqrt{\sigma_{r_i}^2}}, \quad (5)$$

gde su $r_i$ rezidual *i*-tog merenja, a $\sigma_{r_i}^2$ njegova varijansa.

Vrednost unapred definisanog praga $\tau_{LNR}$ najčešće iznosi 3 [5]. Međutim, postoje i drugi načini definisanja statičkog [8] ili dinamičkog praga [9], ali Bez obzira na način odabira, logika testa je sledeća: „Ukoliko vrednost najvećeg normalizovanog reziduala premaši zadati prag, odgovarajuće merenje se označava kao loše.“. Prednost LNR testa ogleda se u njegovoj sposobnosti lokalizacije merenja koje izaziva nekonzistentnost. Međutim, pokazano je da LNR test, kao i $\chi^2$ test, može biti ranjiv na pažljivo projektovane FDIA napade, posebno u distributivnim mrežama gde je broj merenja ograničen.

*II.4 Maliciozni napad injektiranjem lažnih podataka (FDIA)*

Poseban oblik sajber napada usmeren na proces SE u posmatranom delu EES-a predstavlja FDIA. Ideja ovih napada jeste da delovanje napadača ostane nevidljivo za tradicionalne testove, poput $\chi^2$ i LNR testa. Za projektovanje ovakvih napada nije potrebno poznavati celokupnu sliku posmatranog dela EES-a, već je dovoljno poznavanje samo vektora merenja. Promene u vektoru merenja se pažljivo biraju tako da reziduali ostaju konzistentni čime se zaobilaze pomenuti testovi detekcije loših podataka. Posledica toga je da operator dobija izobličenu, ali naizgled validnu sliku stanja posmatranog dela EES-a.

Posmatrajmo standardni SE model:

$$z_i = h_i(x_i) + e_i, \quad (6)$$

pri čemu je:

- $z \in R^m$ – vektor merenja,
- $x \in R^n$ – vektor stanja,
- h(·) – nelinearna vektoska funkcija i
- $e \sim N(0, R)$ – vektor greške merenja za koji se smatra da

prati Gausovu raspodelu sa nultom srednjom vrednošću i kovarijansnom matricom R.

Da bi FDIA bio uspešan, u literaturi se često prave sledeće pretpostavke [7], [10]:

- napadač može pristupiti merenjima u realnom vremenu u posmatranom delu EES-a (područje S), definisanom skupom čvorova;
- napadač ima mogućnost da izmeni sva merenja unutar tog dela EES-a;
- napadač poseduje apriori znanje o topologiji sistema i parametrima vodova u posmatranom delu mreže.

U praksi ove pretpostavke predstavljaju idealan scenario, čija je ostvarivost u distributivnim mrežama sa ograničenom mernom infrastrukturom često upitna.

Neka je $m_s$ skup indeksa merenja u području $S$, a $I_S$ skup indeksa pripadajućih stanja. Tada se merenje $\boldsymbol{z}_i$ u prisustvu napada modeluje kao:

$$\boldsymbol{z}_i^{(\boldsymbol{a})} = \begin{cases} \boldsymbol{z}_i, i \notin m_S \\ \boldsymbol{z}_i + \boldsymbol{a}_i, i \in m_S \end{cases}, \quad (7)$$

gde je $\boldsymbol{a}_i$ $i$-ti element vektora napada $\boldsymbol{a}$.

Pretpostavimo da napadač raspolaže istim merenjima $\boldsymbol{z}_i, i \in m_S$ i istim lokalnim stanjem $\boldsymbol{x}_i$ kao i operator u kontrolnom centru. Ako originalna merenja prolaze tradicionalne testove, tada će i napadnuta merenja $\boldsymbol{z}_i^{(\boldsymbol{a})}$ proći test, pod uslovom da važi:

$$\boldsymbol{a}_i = \boldsymbol{h}(\boldsymbol{x}_i + \boldsymbol{c}_i) - \boldsymbol{h}(\boldsymbol{x}_i), \quad (8)$$

gde $\boldsymbol{c}_i$ predstavlja promenu $i$-te napadnute komponente stanja.

U prilog ovoj tvrdnji postoji i matematički dokaz dat u sledećem delu teksta.

Ako je rezidual originalnog merenja:

$$\boldsymbol{r}_i = \boldsymbol{z}_i - \boldsymbol{h}_i(\boldsymbol{x}_i) \leq \tau, \quad (9)$$

tada je rezidual napadnutog merenja za $i \in M_S$:

$$\boldsymbol{r}_i^{(\boldsymbol{a})} = \boldsymbol{z}_i^{(\boldsymbol{a})} - \boldsymbol{h}_i(\boldsymbol{x}_i + \boldsymbol{c}_i) = \boldsymbol{z}_i + \boldsymbol{a}_i - \boldsymbol{h}_i(\boldsymbol{x}_i + \boldsymbol{c}_i), \quad (10)$$

Dodavanjem i oduzimanjem $\boldsymbol{h}_i(\boldsymbol{x}_i)$ i uzimanjem u obzir jednačine (8) i (9) dobija se jednačina (11):

$$\boldsymbol{r}_i^{(\boldsymbol{a})} = \boldsymbol{z}_i + \boldsymbol{a}_i + \boldsymbol{h}_i(\boldsymbol{x}_i) - \boldsymbol{h}_i(\boldsymbol{x}_i) - \boldsymbol{h}_i(\boldsymbol{x}_i + \boldsymbol{c}_i)$$

$$\boldsymbol{r}_i^{(\boldsymbol{a})} = \boldsymbol{z}_i + \boldsymbol{a}_i - \boldsymbol{a}_i - \boldsymbol{h}_i(\boldsymbol{x}_i) = r_i. \quad (11)$$

Pošto je $\boldsymbol{r}_i \leq \tau$, detektori loših podataka neće reagovati pozitivno. Drugim rečima, ako je originalno merenje konzistentno, napadač može dizajnirati vektor napada tako da i novo merenje ostane „nevidljivo“ za detekciju.

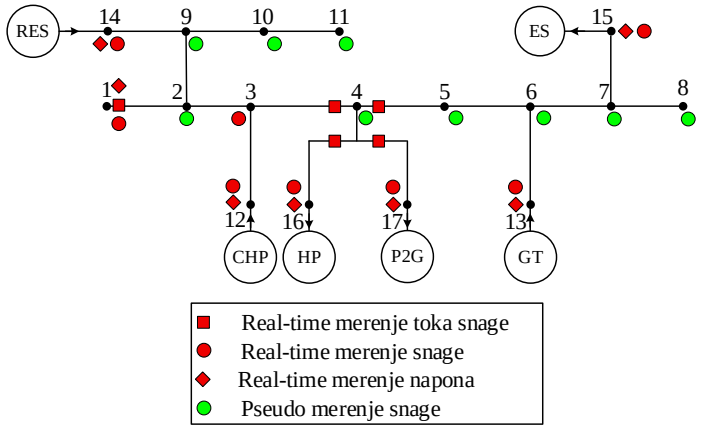
Da bi ovo bilo moguće, u literaturi se pretpostavlja da napadač poseduje dovoljno računarske snage da proceni lokalni vektor stanja $\boldsymbol{x}_i, i \in I_S$. Ova pretpostavka se uglavnom zasniva na činjenici da SCADA merenja nisu sinhronizovana i da se prikupljaju različitim brzinama u različitim delovima sistema. Međutim, prisustvo real-time merenja zasnovanih na μPMU uređajima, koja su vremenski sinhronizovana i poseduju visoku frekvenciju uzorkovanja, značajno ograničavaju mogućnost napadača da blagovremeno proceni stanje sistema i konstruiše pravi vektor $\boldsymbol{a}_i$. Time se dodatno dovodi u pitanje izvodljivost pažljivo dizajniranih FDIA napada u distributivnim mrežama sa real-time merenjima i ograničenom mernom redundansom.

## III Opis sistema i FDIA implementacija

U ovom poglavlju detaljno su opisani korišćeni podaci, model posmatrane mreže i tipovi merenja. Prikazan je način implementacije napada sa ciljem analize ranjivosti tradicionalnih testova loših podataka na FDIA napade u distributivnim mrežama. Zatim je predstavljena procedura formiranja vektora napada i dizajn modifikovanih merenja.

### *III.1 Opis test sistema i merenja*

Za potrebe istraživanja korišćen je test sistem sa 17 čvorova, koji predstavlja deo distributivne mreže. Topologija mreže sa konfiguracijom merenja prikazana je na slici 1. RES (renewable energy source) predstavlja obnovljivi izvor energije koji predaje aktivnu snagu u mrežu, dok je sistem za skladištenje energije (ES) u režimu potrošnje, odnosno preuzima snagu iz mreže. Na sabirnicu 12 priključen je kogenerativni agregat (CHP), koji takođe predaje snagu u mrežu. Na sabirnicu 13 vezana je gasna turbina (GT), čiji je režim rada proizvodnja električne energije. Na sabirnici 16 nalazi se toplotna puma (HP), koja u datom režimu rada preuzima snagu iz mreže. Na sabirnicu 17 priključen je *Power-to-Gas* (P2G) konvertor, koji takođe predstavlja potrošača električne energije. Struktura mreže je odabrana tako da obezbedi realne uslove za primenu SE, ali i da bude dovoljno pregledna za analizu FDIA napada.




**Slika 1.** Topologija mreže i konfiguracija merenja test sistema sa 17 čvorova

Iz posmatranog sistema dobijamo informacije o različitim tipovima merenja, čime se obezbeđuje minimalni stepen redundanse potreban za sprovođenje WLS SE, odnosno postojanje većeg broja međusobno zavisnih merenja u odnosu na broj nepoznatih stanja. Ova merenja uključuju:

- tokove snaga u različitim granama (u realnom vremenu),
- injektiranje snaga (u realnom vremenu),
- napone po čvorovima (u realnom vremenu),
- injektiranje snaga za čvorove bez direktnog merenja (pseudo merenja).

*III.2 Opis izvedenog napada*

Kako bi se ispitala ranjivost sistema napad je konstruisan tako da proveri izvodljivost prikrivenog FDIA napada nad real-time merenjima napona. U tom slučaju razlikujemo dva scenarija:

**Scenario A**, matematički prikaz dat je jednačinom (11). Meta napada je moduo napona $|V|$. Napad je simuliran u svakom čvoru pojedinačno. U okviru svakog slučaja menjano je isključivo jedno merenje, ali su dodatno ispitani i različiti novi perturbacije kako bi se ispitala osetljivost sistema na različite intenzitete napada.

$$\boldsymbol{c}_i = \begin{cases} |\boldsymbol{\Delta V}|_k, i = k \\ 0,\ i \neq \mathrm{k} \end{cases}, \tag{12}$$

**Scenario B**, matematički prikaz dat je jednačinom (12) meta napada ugao napona $\theta$. Napad je ponovo simuliran u svakom čvoru pojedinačno i u okviru svakog slučaja promenjeno je po jedno merenje.

$$\boldsymbol{c}_i = \begin{cases} \boldsymbol{\theta}_k, i = k \\ 0,\ i \neq \mathrm{k} \end{cases}, \tag{13}$$

Izvodljivost ovih scenarija definiše se isključivo na osnovu strukture napadnog vektora $\boldsymbol{a}$ i to na sledeći način:

1. napad se smatra *izvodljivim* samo ako vektor $\boldsymbol{a}$ ne sadrži veličine koje se odnose na pseudo merenja,
2. dok se svaki scenario u kome je za prikrivanje napada neophodno uključiti pseudo merenja u vektor $\boldsymbol{a}$ klasifikuje kao *neizvodljiv*.

## IV Analiza izvodljivosti FDIA napada u uslovima ograničene merne redundanse

Imajući u vidu ograničenu mernu redundansu karakterističnu za distributivne mreže, može se očekivati da prostor za konstruisanje prikrivenog FDIA napada, opisanog u prethodnom delu rada, bude ograničen. U tom smislu, analiza rezultata ima za cilj da ispita u kojoj meri struktura mernog sistema utiče na izvodljivost napada, kao i da li u takvim uslovima tradicionalni BDD algoritmi mogu zadržati svoju efikasnost.

**Tabela 1.** Struktura izvodljivosti napada u Scenariju A **($|\boldsymbol{\Delta V}| = \boldsymbol{0.1}$)**

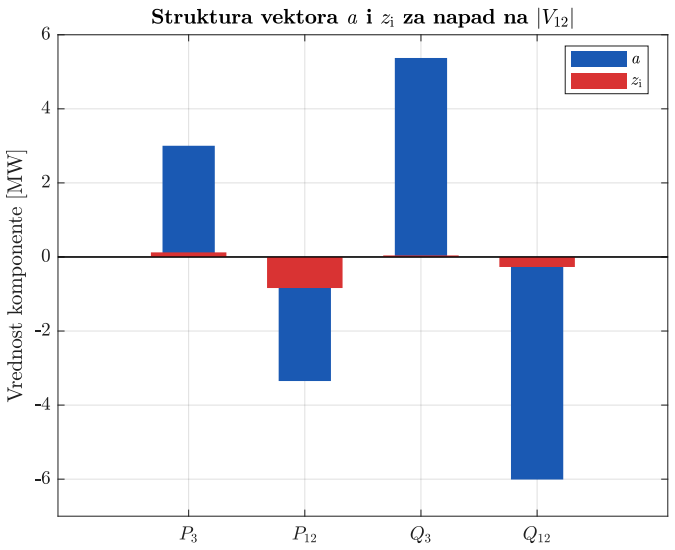
| Meta napada | Pogođena PQ injektiranja | Pogođeni tokovi snaga | Pseudo merenja uključena | Izvodljiv: ■ - DA ■ - NE |
|---|---|---|---|---|
| $\|V_1\|$ | 2 | 2 | Da | |
| $\|V_{12}\|$ | 4 | 0 | Ne | |
| $\|V_{13}\|$ | 4 | 0 | Da | |
| $\|V_{14}\|$ | 4 | 0 | Da | |
| $\|V_{15}\|$ | 4 | 0 | Da | |
| $\|V_{16}\|$ | 4 | 2 | Da | |
| $\|V_{17}\|$ | 4 | 2 | Da | |

U nastavku su detaljno prikazani rezultati po scenarijima, uz diskusiju uloge merne redundanse i rasporeda merenja u mreži na izvodljivost napada. Napadi su simuliran u svakom čvoru pojedinačno i izveden je promenom amplitude napona i faznog ugla napona za vrednosti koje su izabrane kao kompromis između uočljivog poremećaja i pokušaja zadržavanja napada u realističnim granicama rada distributivne mreže.

Analiza strukture vektora $\boldsymbol{a}$ za Scenario A, kada je perturbacija magnitude napona 0.1 r.j, prikazana je u tabeli 1.

Iz tabele vidimo da napad u svakom od posmatranih čvorova izaziva promenu aktivnih i reaktivnih injektiranja, kao i tokova snaga u granama [5]. U samo jednom analiziranom slučaju, čvor 12, uočeno je da je za uspešno izveden napad nepotrebno uključivanje pseudo merenja u vektor $\boldsymbol{a}$. S obzirom na definisani kriterijum izvodljivosti, prema kome se napad smatra neizvodljivim ukoliko zahteva manipulaciju pseudo merenja, može se zaključiti da samo 1 od 7 analiziranih napada zadovoljava uslov izvodljivosti.

Usredsredimo se na napadnuti čvor 12. Na slici 2 prikazane su nenulte komponente vektora $\boldsymbol{a}$ ($\Delta P_3$, $\Delta P_{12}$, $\Delta Q_3$ i $\Delta Q_{12}$) i njima odgovarajuće veličine iz vektora $\boldsymbol{z}_i$ ($P_3$, $P_{12}$, $Q_3$ i $Q_{12}$). Na osnovu legende sa slike 1 se može potvrditi da se korišćene veličine isključivo odnose na real-time merenja aktivnih i reaktivnih injektiranja i tokova snaga, dok nijedna komponenta vektora $\boldsymbol{a}$ ne obuhvata pseudo merenja.

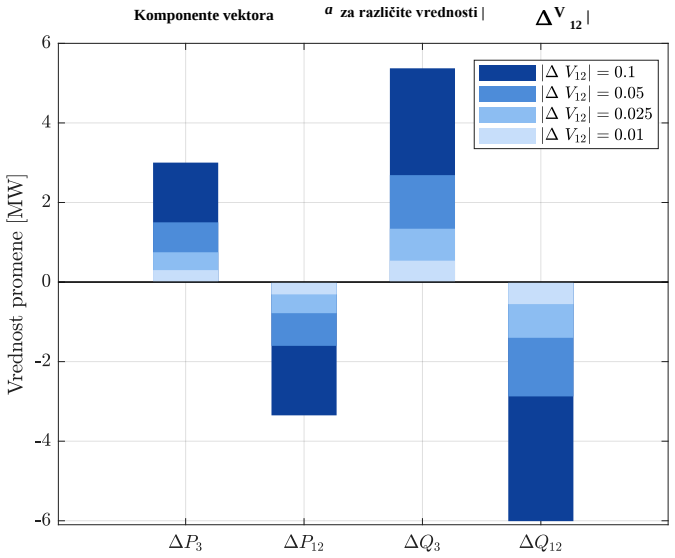



**Slika 2.** Nenulte komponente vektora $\boldsymbol{a}$ i $\boldsymbol{z}_i$ za promenu magnitude napona $|\boldsymbol{V_{12}}|$ od 0.1 r.j.

U cilju provere robusnosti dobijenog rezultata za čvor 12, dodatno su analizirani slučajevi sa manjom perturbacijom magnitude napona – slika 3.

Dobijeni rezultati pokazuju da struktura napadnog vektora ostaje nepromenjena, tj. nenulte komponente su iste kao u prvom slučaju ali proporcionalno manjeg intenziteta.To ukazuje da izvodljivost napada u čvoru 12 ne zavisi od konkretne vrednosti perturbacije, već od topologije mreže i konfiguracije merenja u njegovoj okolini.

Nakon analize napada na magnitudu napona, razmatra se Scenario B, u kome je meta napada fazni ugao napona θ. Kao i u prethodnom scenariju, napad je simuliran pojedinačno u svakom čvoru sa dostupnim real-time merenjem ugla, pri čemu je izvodljivost procenjivana na osnovu strukture napadnog vektora $\boldsymbol{a}$, što je prikazano u tabeli 2.

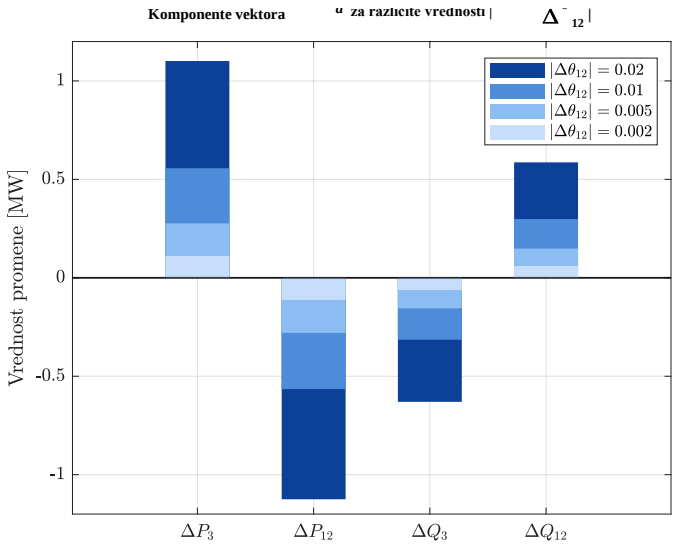



**Slika 3.** Nenulte komponente vektora $\boldsymbol{a}$ za različite vrednosti perturbacije magnitude napona $|\boldsymbol{\Delta V_{12}}|$

**Tabela 2.** Struktura izvodljivosti napada u Scenariju B $(|\boldsymbol{\Delta\theta}| = \boldsymbol{0.01})$

| Meta napada | Pogođena PQ injektiranja | Pogođeni tokovi snaga | Pseudo merenja uključena | Izvodljiv: - DA - NE |
|---|---|---|---|---|
| $\|\theta_{12}\|$ | 4 | 0 | Ne | |
| $\|\theta_{13}\|$ | 4 | 0 | Da | |
| $\|\theta_{14}\|$ | 4 | 0 | Da | |
| $\|\theta_{15}\|$ | 4 | 0 | Da | |
| $\|\theta_{16}\|$ | 4 | 2 | Da | |
| $\|\theta_{17}\|$ | 4 | 2 | Da | |

Uočavamo da je struktura napada ista, kao u prethodnom scenariju. Pogledajmo rezultate na slici 4, pa ćemo izvesti zaključak.




**Slika 4.** Nenulte komponente vektora $\boldsymbol{a}$ za različite vrednosti perturbacije ugla napona $|\boldsymbol{\Delta\theta_{12}}|$

Karakteristične veličine koje se pojavljuju u vektoru napada $\boldsymbol{a}$ su iste bez obzira da li je meta napada magnituda ili fazni ugao napona, što je i očekivano s obzirom na formulaciju jednačina injektiranja i tokova snaga (2). Veličine menjanju svoj intenzitet proporcionalno nivou perturbacije i prate njegovu promenu ali se ne menjaju po poziciji u mreži. Što opet potvrđuje činjenicu da izvodljivost napada u čvoru 12 ne zavisi od konkretne vrednosti perturbacije, već od topologije mreže i konfiguracije merenja u njegovoj okolini. Ovi rezultati sugerišu da ograničena merna redundansa i raspored merenja u mreži, mogu predstavljati faktor koji u većini slučajeva otežava konstrukciju prikrivenog FDIA napada, čak i bez primene sofisticiranih metoda detekcije.

Pored pojedinačnih napada na jednu veličinu ($V$ ili $\theta$), razmotrena je i hipotetička situacija u kojoj bi napadač istovremeno pokušao da kompromituje dve mete, na primer magnitude napona u čvorovima 12 i 13. S obzirom na već uočenu potrebu uključivanja pseudo merenja čak i pri pojedinačnim perturbacijama (osim u čvoru 12), može se zaključiti da bi istovremena promena dve magnitude napona dodatno povećala broj pogođenih merenja u vektoru $\boldsymbol{a}$. U takvom napadu bi manipulacija pseudo merenja bila neizbežna, pa bi napad prema usvojenom kriterijumu izvodljivosti, bio klasifikovan kao neizvodljiv.

## V ZAKLJUČAK

U ovom radu analizirana je izvodljivost FDIA napada u distributivnoj mreži sa ograničenom mernom redundansom, pod pretpostavkom da napadač nema mogućnost manipulacije pseudo merenja. Dobijeni rezultati ukazuju da u većini razmatranih slučajeva promena magnitude ili faznog ugla napona zahteva promenu pseudo merenja, čime se, prema usvojenom kriterijumu, takvi napadi mogu smatrati neizvodljivim.

U 6 od 7 čvorova napada se smatra neizvodljivim. Izuzetak je čvor 12, kod koga je pokazano da je moguće konstruisati napad isključivo kroz real-time merenja. Dodatna analiza različitih nivoa perturbacije pokazala je da struktura vektora $\boldsymbol{a}$ ostaje nepromenjena, dok se njegove komponente menjaju proporcionalno meti napada. Ovakvo ponašanje sugeriše da izvodljivost napada nije posledica intenziteta perturbacije, već prvenstveno topološke pozicije čvora i rasporeda merenja u njegovoj neposrednoj okolini.

Rezultati dobijeni u radu ukazuju da ograničena merna redundansa, koja je karakteristična za distributivne mreže, može značajno suziti prostor za realizaciju prikrivenih FDIA napada. U takvim uslovima tradicionalni BDD algoritmi mogu biti efikasni u velikom broju scenarija. Takođe, analiza pokazuje da otpornost sistema nije podrazumevana i da zavisi od konkretne konfiguracije merenja. Prethodno navedeno može poslužiti kao osnova za procenu ranjivosti distributivne mreže i kao pomoć dispečeru pri odlučivanju o potrebi uvođenja sofisticiranijih tehnika detekcije napada.

## ZAHVALNICA

Istraživanja prezentovana u ovom radu su delimično finansirana sredstvima Ministarstva nauke, tehnološkog razvoja i inovacija RS, ugovor br. 451-03-33/2026-03/200132 čiji je realizator Fakultet tehničkih nauka u Čačku - Univerziteta u Kragujevcu.

LITERATURA

[1] Whitehead, D.E., Owens, K., Gammel, D., Smith, J. Ukraine cyber-induced power outage: Analysis and practical mitigation strategies, in Proc. *70th Annual Conference for Protective Relay Engineers (CPRE)*, College Station, TX, USA, pp. 1-8, 03-06 April 2017. https://doi.org/10.1109/CPRE.2017.8090056

[2] U.S. Department of Energy, *Cyber threat and vulnerability analysis of the U.S. electric sector*, Office of Electricity Delivery and Energy Reliability, 2016. https://www.energy.gov/sites/prod/files/2017/01/f34/Cyber%20Threat%20and%20Vulnerability%20Analysis%20of%20the%20U.S.%20Electric%20Sector.pdf [pristupljeno 23. 02. 2026]

[3] Win, H. Assessing the Vulnerabilities of Europe's Interconnected Power Grid: Lessons from the 2025 Spain-Portugal Blackout, Energy, 2025. https://www.academia.edu/129139254/Assessing_the_Vulnerabilities_of_Europes_Interconnected_Power_Grid_Lessons_from_the_2025_Spain_Portugal_Blackout [pristupljeno 23. 02. 2026]

[4] Mili, L., Van Cutsem, Th., Ribbens-Pavella, M. Bad Data Identification Methods In Power System State Estimation-A Comparative Study, IEEE Transactions on Power Apparatus and Systems, Vol. 104, No. 11, pp. 3037-3049, 1985. https://doi.org/10.1109/TPAS.1985.318945

[5] Abur, A., Exposito, A.G. Power System State Estimation: Theory and Implementation, Marcel Dekker, New York (NY, USA), 2004. https://doi.org/10.1201/9780203913673

[6] 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. 21-32, 2011. https://doi.org/10.1145/1952982.1952995

[7] Hug, G., Giampapa, J. Vulnerability Assessment of AC State Estimation With Respect to False Data Injection Cyber-Attacks, IEEE Transactions on Smart Grid, Vol. 3, No. 3, pp. 1362-1370, 2012. https://doi.org/10.1109/TSG.2012.2195338

[8] Monticelli, A. *State Estimation in Electric Power Systems: A Generalized Approach*, Kluwer Academic Publishers, Boston, 1999. https://doi.org/10.1007/978-1-4615-4999-4

[9] Krsman, V. *Specijalizovani algoritmi za detekciju, identifikaciju i estimaciju loših podataka u elektrodistributivnim mrežama*, Novi Sad, Fakultet tehničkih nauka, 2017. https://hdl.handle.net/21.15107/rcub_nardus_8404 [pristupljeno 23. 02. 2026]

[10] Liang, J., Sankar. L., Kosut, O. Vulnerability analysis and conse quences of false data injection attack on power system state estimation, IEEE Transactions on Power Systems, Vol. 31, No. 5, pp. 3864-3872, 2016. https://doi.org/10.1109/TPWRS.2015.2504950



AUTORI

**Stefan Čubonović** - asistent, Fakultet tehničkih nauka u Čačku, Univerziteta u Kragujevcu, stefan.cubonovic@ftn.kg.ac.rs, ORCID 0000-0002-0240-5349

**Dragan Ćetenović** - vanredni profesor, Fakultet tehničkih nauka u Čačku. Univerziteta u Kragujevcu, dragan.cetenovic@ftn.kg.ac.rs, ORCID 0000-0001-5087-4863

**Nikola Vojnović** – vanredni profesor, Fakultet tehničkih nauka Univerziteta u Novom Sadu, nikola.vojnovic@uns.ac.rs, ORCID 0000-0001-8361-2085

**Aleksandar Ranković** - redovni profesor, Fakultet tehničkih nauka u Čačku, Univerziteta u Kragujevcu, aleksandar.rankovic@ftn.kg.ac.rs, ORCID 0000-0002-7205-9584


# Malicious Attacks on the State Estimator in Distribution Networks: Analysis of Attack Feasibility under Conditions of Low Measurement Redundancy


***Abstract –*** In the last decade, the use of information and communication technologies in distribution networks has intensified. Such technologies are exposed to the risk of malicious cyber-attacks, which poses a threat to the operation of distribution networks. One of the potential targets of such attacks in distribution networks is the state estimator. Classical bad data detection algorithms, most commonly statistical methods such as the $\chi^2$ test and the Largest Normalized Residual test, are unable to detect malicious false data injection attacks (FDIAs) if these attacks are skilfully concealed. However, due to the low measurement redundancy characteristic of distribution networks, attackers face difficulties in concealing the attack, in which case even classical bad data detection algorithms may be able to identify it. This enables the detection of FDIAs without additional financial investments that would be required for the implementation of sophisticated detection solutions. This paper analyzes the feasibility of FDIAs in distribution networks, aiming to relate attack feasibility to measurement redundancy. The results of the analysis can be used to inform distribution system operators whether there is a need for sophisticated FDIA detection techniques, depending on the measurement infrastructure of the network under their control.



***Index Terms –*** BDD, FDIA, Pseudo measurements, WLS



Rad primljen: 12.04.2026., prihvaćen: 05.09.2026.