

Detekcija False Data Injection napada u pametnim mrežama primenom mašinskog učenja na Big Data setovima

Vladimir Bečejac*, Dobrila Škatarić*, Petar Lukić*

* Univerzitet u Beogradu, Mašinski fakultet, Kraljice Marije 16, Beograd

Rezime – Digitalizacija elektroenergetskog sistema omogućava efikasnije upravljanje, ali otvara prostor za sofisticirane sajber napade, poput ubacivanja lažnih podataka. Tradicionalne metode detekcije loših podataka često nisu u stanju da prepoznaju napade koji su dobro programirani i ostaju unutar granica greške estimacije stanja. Ovaj rad daje pristup detekciji lažnih napada primenom algoritama mašinskog učenja u MATLAB okruženju. Koristeći velike setove podataka razvijen je model koji identifikuje anomalije u korelacijama mrežnih parametara u realnom vremenu. Rezultati simulacija na IEEE test sistemima pokazuju visoku preciznost modela u razlikovanju normalnih promena podataka od zlonamernih manipulacija podacima, čime se direktno unapređuje pouzdanost i odgovorna upotreba digitalne infrastrukture EES.

Ključne reči – FDIA, mašinsko učenje, estimacija stanja, big data

1 UVOD

Digitalizacija elektroenergetskih sistema (EES) i razvoj koncepta pametnih mreža (Smart Grids) značajno su unapredili mogućnosti upravljanja, monitoringa i optimizacije rada sistema u realnom vremenu. Integracija SCADA/EMS sistema, Phasor Measurement Units (PMU), naprednih komunikacionih protokola i distribuiranih izvora energije omogućila je precizniju procenu stanja sistema, bržu reakciju na poremećaje i efikasnije planiranje rada [1]. Međutim, povećana zavisnost od informaciono-komunikacione infrastrukture istovremeno je otvorila prostor za nove bezbednosne izazove, posebno u domenu sajber bezbednosti. Savremeni elektroenergetski sistem više nije isključivo fizički sistem, već kompleksan sajber-fizički sistem u kome kompromitacija podataka može imati ozbiljne operativne posledice [2].

Jedna od najznačajnijih pretnji u tom kontekstu jesu False Data Injection (FDI) napadi, odnosno napadi ubacivanjem lažnih/loših merenja u proces estimacije stanja. Za razliku od klasičnih grešaka u merenju, FDI napadi su namerno konstruisani tako da ostanu neprimećeni od strane tradicionalnih metoda detekcije loših podataka (Bad Data Detection – BDD). U standardnoj formulaciji procene stanja, merni vektor se opisuje linearnim ili nelinearnim modelom oblika

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

gde su $\mathbf{z}$ vektor merenja, $\mathbf{x}$ vektor stanja (naponi i uglovi), a $\mathbf{e}$ šum merenja. Ako napadač konstruiše vektor napada u skladu sa strukturom mernog modela, moguće je generisati takozvani

„stealth“ napad koji ne menja statističke osobine reziduala i prolazi kroz χ^2 test bez detekcije [3]. Takvi napadi mogu prouzrokovati pogrešne operativne odluke, nepravilno dispečersko upravljanje, pa čak i destabilizaciju sistema [4].

U literaturi su FDI napadi detaljno analizirani sa teorijskog stanovišta, pri čemu je pokazano da napadač koji poznaje mernu matricu sistema može konstruisati vektor napada Jacobian matrice tako da ostane nevidljiv standardnim testovima reziduala [5]. Dalja istraživanja proširila su analizu na AC modele, parcijalno kompromitovana merenja te scenarije sa ograničenim znanjem napadača [6,7]. Istovremeno, sve veća dostupnost velikih skupova podataka (Big Data) iz SCADA i PMU sistema podstakla je razvoj metoda zasnovanih na mašinskom učenju za detekciju anomalija u elektroenergetskim mrežama [8]. Primena algoritama kao što su Support Vector Machines, neuronske mreže, ansambl metode i duboko učenje pokazala je da podaci sadrže obrasce koji omogućavaju razlikovanje normalnih operativnih promena od zlonamernih manipulacija [9].

Posebnu pažnju u novijim istraživanjima zaslužno privlače ansambl metode, naročito algoritam Random Forest, zahvaljujući njegovoj robusnosti, otpornosti na prenaučavanje i sposobnosti obrade visoko-dimenzionalnih podataka [10]. Random Forest kombinuje veliki broj stabala odlučivanja koji su trenirani na različitim podskupovima podataka i karakteristika, čime se ostvaruje stabilna i pouzdana klasifikacija čak i u prisustvu šuma i nelinearnosti. U kontekstu detekcije napada na infrastrukturne sisteme, ova karakteristika dobija poseban značaj, jer realni elektroenergetski podaci sadrže prirodne varijacije opterećenja, merni šum i operativne promene koje ne smeju biti pogrešno interpretirane kao napad [11,12].

Motivacija ovog rada proističe iz potrebe da se razvije metodologija koja će moći da detektuje sofisticirane, „stealth-like“ FDI napade u realističnim uslovima rada sistema, uz istovremeno očuvanje niske stope lažnih alarma. Cilj rada je razvoj i testiranje modela zasnovanog na Random Forest algoritmu za detekciju FDI napada na velikom skupu sintetički generisanih podataka dobijenih simulacijom IEEE test sistema sa 14 čvorova u MATPOWER (delu Matlab-a) okruženju. Dataset obuhvata 20.000 uzoraka (10.000 normalnih i 10.000 napadnutih scenarija), generisanih uz varijaciju opterećenja i prisustvo mernog šuma, čime se postiže realističan model operativnih uslova.

Doprinos rada ogleda se u: (i) generisanju Big Data skupa podataka zasnovanog na AC proračunu tokova snaga, (ii)

implementaciji stealth-like FDI napada sa parcijalnim kompromitovanjem merenja, (iii) primeni Random Forest algoritma za klasifikaciju normalnih i abnormalnih stanja i (iv) detaljnoj analizi performansi modela kroz standardne metrike tačnosti, preciznosti, odziva i ROC (Receiver Operating Characteristic) analizu. Rezultati pokazuju da je moguće postići visoku preciznost detekcije uz veoma nisku stopu lažnih alarma, čime se potvrđuje potencijal primene mašinskog učenja u unapređenju sajber bezbednosti pametnih mreža.

II TEORIJSKE OSNOVE

II.1. Model merenja i procena stanja (State Estimation)

Osnovni zadatak procene stanja u elektroenergetskom sistemu jeste određivanje vektora stanja sistema na osnovu raspoloživih merenja. Vektor stanja u AC modelu obično se definiše kao:

$$x = [\theta_1 \quad \theta_2 \quad \dots \quad \theta_n \quad V_1 \quad V_2 \quad \dots \quad V_n]^T,$$

gde su θ_i – naponski ugao u čvoru i , V_i – amplituda napona u čvoru i , n – broj čvorova u mreži.

Merenja u sistemu formiraju vektor merenja:

$$z = [z^1 z^2 \dots z^m]^T,$$

gde je m ukupan broj merenja u sistemu. Opšti nelinearni model merenja može se zapisati u obliku:

$$z = h(x) + e$$

gde su:

- $h(x)$ – nelinearna vektorska funkcija koja povezuje stanje sistema sa merenjima,
- e – vektor mernog šuma, koji se najčešće modeluje kao Gaussova slučajna promenljiva sa kovarijansom R .

Procena stanja se najčešće sprovodi metodom ponderisanih najmanjih kvadrata (WLS – Weighted Least Squares). U tom slučaju procenjeno stanje dobija se minimizacijom funkcije cilja:

$$J(x) = (z - h(x))^T R^{-1} (z - h(x))$$

Ova funkcija predstavlja ponderisanu kvadratnu normu reziduala, pri čemu matrica R^{-1} daje veću težinu pouzdanijim merenjima.

Rešenje se dobija iterativnim postupkom (najčešće Newton–Raphson metodom), pri čemu se koristi Jacobian matrica:

$$H = \partial h / \partial x$$

Jacobian matrica H sadrži parcijalne izvode mernih funkcija po komponentama vektora stanja i predstavlja ključni element u procesu linearizacije modela.

Linearizovani model oko radne tačke može se zapisati kao:

$$\Delta z = H \Delta x + e$$

gde su:

- Δz – inkrement merenja,
- Δx – inkrement stanja,
- H – Jacobian matrica.

Ovaj linearizovani model ima ključnu ulogu kako u evaluaciji detekcije loših podataka, tako i u izgradnji False Data Injection (FDI) napada, jer struktura matrice H određuje prostor u kojem je moguće osmisliti napad koji ostaje neotkriven standardnim

metodama detekcije.

II.2. Problem detekcije loših podataka (BDD)

U realnim elektroenergetskim sistemima merenja su podložna različitim vrstama grešaka: šumu senzora, komunikacionim smetnjama, kvarovima mernih uređaja i privremenim prekidima prenosa podataka. Zbog toga je sastavni deo procesa procene stanja i mehanizam detekcije loših podataka. Nakon dobijanja procenjenog stanja $\hat{x}$, računa se vektor reziduala:

$$r = z - h(\hat{x}),$$

gde su:

- z – vektor merenja,
- $h(\hat{x})$ – procenjene vrednosti merenja na osnovu procenjenog stanja.

Ako su merenja korektna i greške slučajne (Gaussove), rezidual bi trebalo da ima statistička svojstva koja odgovaraju pretpostavljenom šumu. U suprotnom, pretpostavlja se prisustvo loših podataka.

Najčešće korišćen test je χ^2 test, zasnovan na sledećoj statistici:

$$T = r^T R^{-1} r$$

gde je R kovarijaciona matrica šuma merenja. Dobijena vrednost T poredi se sa pragom χ^2 raspodele za odgovarajući broj stepeni slobode $(m - n)$, gde je m broj merenja, a n broj stanja.

Ako je:

$$T > \chi^2 \alpha (m - n)$$

zaključuje se da postoji loš podatak u mernom skupu.

Ovaj pristup je efikasan za detekciju slučajnih grešaka i pojedinačnih odstupanja, ali se zasniva na pretpostavci da su greške nezavisne i da nemaju strukturu koja je povezana sa modelom sistema. Upravo tu leži njegova osnovna slabost u kontekstu sajber napada.

II.3. FDI napadi

False Data Injection (FDI) napadi predstavljaju sofisticirani oblik manipulacije mernim podacima, pri čemu napadač ne ubacuje proizvoljne greške, već pažljivo konstruisane promene koje prate strukturu mernog modela sistema.

Pretpostavimo da napadač modifikuje merni vektor z u:

$$z' = z + a$$

gde je a vektor napada. Ako napadač poznaje (ili dovoljno dobro aproksimira) Jacobian matricu H , može konstruisati napadni vektor u obliku:

$$a = H c$$

gde je c proizvoljan vektor dimenzije broja stanja.

U tom slučaju dobijamo:

$$\begin{aligned} z' &= Hx + e + Hc \\ z' &= H(x + c) + e \end{aligned}$$

što znači da napad dovodi do pogrešnog procenjenog stanja $x' = x + c$, ali rezidual ostaje nepromenjen u odnosu na slučaj bez napada.

Rezidual u prisustvu napada postaje:

$$\begin{aligned} r' &= z' - H x' \\ r' &= (H(x + c) + e) - H(x + c) \\ r' &= e \end{aligned}$$

Dakle, statistika reziduala ostaje ista kao i u normalnim uslovima. Takav napad naziva se stealth napad, jer prolazi kroz standardni χ^2 test bez detekcije.

U realnim uslovima napadač (haker) često nema pristup svim merenjima, već kompromituje samo podskup merenja. U tom slučaju govorimo o parcijalno kompromitovanom FDI napadu. Ipak, čak i tada je moguće konstruisati napade koji značajno utiču na estimirano stanje sistema, naročito ako su kompromitovana strateški važna merenja (npr. tokovi snaga na kritičnim dalekovodima, kao što su interkonektivni, ili uglovi napona u ključnim čvorovima).

Posledice FDI napada mogu biti ozbiljne:

- pogrešna procena opterećenja dalekovoda;
- netačna analiza sigurnosti sistema;
- pogrešne dispečerske odluke;
- povećanje rizika od preopterećenja ili čak kaskadnih ispada.

Zbog toga se tradicionalni BDD pristupi smatraju nedovoljnim u kontekstu sajber bezbednosti, a u poslednje vreme sve veću ulogu imaju metode zasnovane na mašinskom učenju, koje analiziraju obrasce podataka i mogu detektovati anomalije čak i kada su one modelom „nevidljive“.

III RANDOM FOREST ALGORITAM

Random Forest (RF) predstavlja jedan od najmoćnijih i najrasprostranjenijih algoritama mašinskog učenja zasnovanih na ansamblu stabala odlučivanja (Decision Trees). Razvio ga je Leo Breiman 2001. godine, a njegova suština leži u kombinovanju velikog broja pojedinačnih stabala kako bi se dobio model sa znatno većom tačnošću i otpornošću na preprilagođavanje (*overfitting*) u poređenju sa pojedinačnim stablima. Algoritam se oslanja na dve ključne tehnike: Bagging (Bootstrap Aggregating) i nasumični odabir karakteristika (Feature Randomness). Umesto da se celokupan set podataka koristi za svako stablo, RF kreira više podskupova podataka putem nasumičnog uzorkovanja sa ponavljanjem. Ako imamo N primera u trening setu, za svako stablo se bira N uzoraka, pri čemu se neki primeri mogu ponoviti, dok drugi ostaju neiskorišćeni. Ovi neiskorišćeni podaci nazivaju se *Out-of-Bag* (OOB) uzorci i koriste se za internu validaciju modela bez potrebe za posebnim testnim setom.

Prilikom grananja u svakom čvoru pojedinačnog stabla, algoritam ne razmatra sve dostupne ulazne parametre (npr. sve napone i snage u mreži). Umesto toga, bira se nasumični podskup od k karakteristika (obično $k = \sqrt{m}$, gde je m ukupan broj parametara). Ovo osigurava da stabla u "šumi" budu međusobno nekorelisana, što je ključno za detekciju suptilnih FDI napada.

Glavni cilj svakog stabla je da podeli podatke tako da svaki sledeći čvor bude "čistiji" od prethodnog. Najčešće korišćena mera za ovo u klasifikaciji je Gini nečistoća (Gini Impurity).

Za dati čvor, Gini nečistoća se izračunava kao:

$$G = 1 - \sum_{i=1}^c (p_i)^2$$

gde je:

- C : ukupan broj klasa (u ovom radu dve: "Normalno stanje" i "FDI napad").
- p_i : verovatnoća da nasumično odabrani uzorak u tom čvoru pripada klasi i .

Algoritam bira onu karakteristiku i onu tačku podele koja maksimalno smanjuje vrednost G . Time se povećava separabilnost između legalnih podataka i malicioznih injekcija.

Nakon što je "šuma" od T stabala istrenirana, proces klasifikacije novog merenja z odvija se kroz glasanje:

1. Svako pojedinačno stablo $h_t(z)$ daje svoju predikciju (u ovom radu je 0 za normalno stanje, 1 za napad).
2. Konačna odluka $\hat{y}$ donosi se metodom većinskog glasa:

$$\hat{y} = \text{mode}\{h_1(z), h_2(z), \dots, h_T(z)\}$$

Primena RF algoritma u detekciji FDI napada nudi nekoliko ključnih prednosti:

- Pametne mreže generišu veliki broj podataka (Big Data). RF se efikasno nosi tim ulazima bez potrebe za kompleksnom predobradom.
- FDI napadi često koriste nelinearne korelacije između snaga i napona. RF prirodno modeluje ove složene odnose koje linearni BDD testovi ne bi videli.
- Algoritam može rangirati parametre mreže po njihovom značaju. To omogućava dispečerima da identifikuju koje su sabirnice, dalekovodi ili trafostanice najkritičnije tačke (najčešće ciljane) u bezbednosnom smislu.
- Zbog ansambl pristupa, model je otporan na šum u merenjima koji je uobičajen kod senzora na terenu.

U ovom radu za detekciju FDI napada korišćen je Random Forest klasifikator implementiran kroz MATLAB funkciju *TreeBagger*. Model je treniran kao ansambl od 100 stabala odluke, pri čemu svako stablo uči na bootstrap uzorku iz trening skupa, dok se generalizacija poboljšava agregacijom odluka većeg broja stabala. Kao mehanizam regularizacije korišćen je parametar $\text{MinLeafSize} = 5$, koji ograničava dalje grananje stabla kada broj uzoraka u listu postane mali, čime se smanjuje prenaučenosť (*overfitting*) i stabilizuje detekcija u prisustvu šuma i varijacija režima rada. Maksimalna dubina stabla nije eksplicitno zadavana, već je na implicitni način kontrolisana preko MinLeafSize i kriterijuma razdvajanja koji *TreeBagger* koristi pri izgradnji stabala.

Važan hiperparametar u RF metodi je broj karakteristika koje se nasumično razmatraju pri svakom čvoru. U korišćenoj konfiguraciji, pošto nije eksplicitno zadat parametar $\text{NumPredictorsToSample}$, MATLAB koristi podrazumevanu postavku za klasifikaciju, tj. približno $\sqrt{p}$ karakteristika po split-u, gde je p ukupan broj feature-a. U ovom slučaju je vektor karakteristika definisan kao $z = [V_m, V_a, P_f]$, pa je ukupan broj feature-a $p = 2n_b + n_l$. Za IEEE 14 sistem, gde je broj čvorova $n_b = 14$ i broj linija $n_l = 20$, dobijamo $p=48$, pa model na svakom split-u razmatra približno $\sqrt{48} \approx 7$ karakteristika. Pored

toga, u radu je uključena i OOB (out-of-bag) analiza, koja omogućava kvantitativan uvid u to koja merenja najviše doprinose detekciji napada.

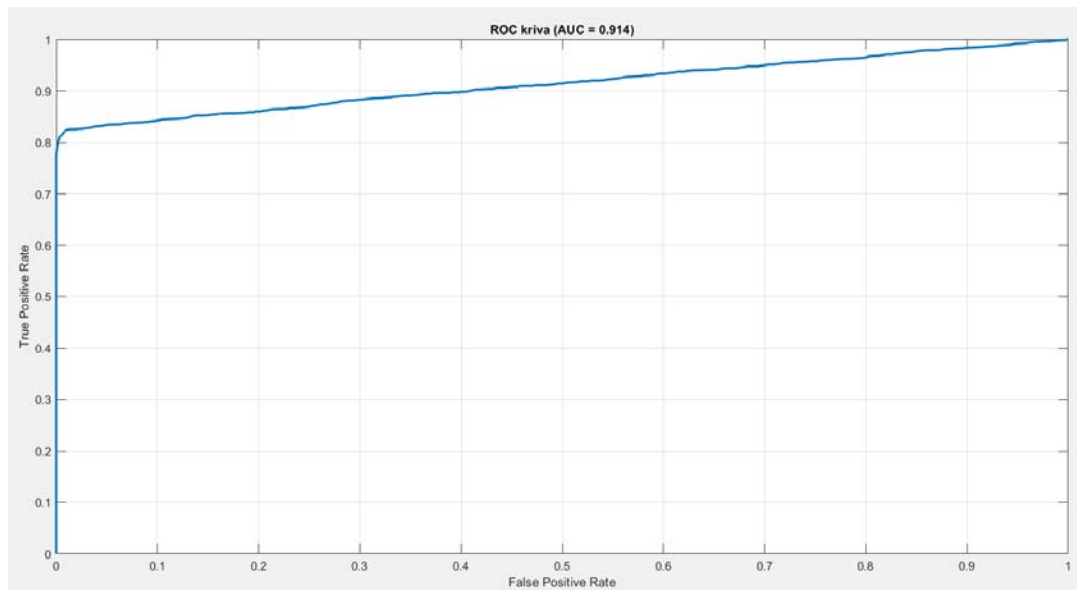
IV ANALIZA REZULTATA I DISKUSIJA

U ovom poglavlju detaljno se analizira efikasnost predloženog Random Forest modela na osnovu simulacija sprovedenih na IEEE test modelu sa 14 čvorova. Fokus je na interpretaciji metrika performansi, robusnosti detekcije u prisustvu šuma i identifikaciji ključnih parametara mreže koji doprinose detekciji.

Test skup je sadržao 6 000 uzoraka što je oko 30% od ukupnog broja uzoraka (20 000). Model je postigao ukupnu tačnost od 90.80%. Međutim, za dublje razumevanje bezbednosnog aspekta, neophodno je analizirati matricu konfuzije iz kojeg se dobijaju parametri *True Negatives* i to 3043. Dakle, model je skoro nepogrešivo prepoznao normalna radna stanja, uprkos varijacijama opterećenja od $\pm 25\%$. Sledeći parametar, *False Positives* i to 24 slučaja ukazuju na izuzetno nizak broj lažnih alarma (svega 0.78% od ukupnih normalnih uzoraka). U realnim sistemima, ovo je ključno jer preveliki broj lažnih alarma vodi ka "zamor operatora" i ignorisanju stvarnih pretnji. Na kraju, *False Negatives* u 528 slučajeva. Ovo su napadi koje je model propustio.

Na slici 1 je prikazana ROC kriva koja prikazuje odnos između stope tačne detekcije napada (True Positive Rate) i stope lažnih alarma (False Positive Rate) pri promeni praga odlučivanja Random Forest modela. Svaka tačka na krivoj odgovara određenoj vrednosti praga verovatnoće na osnovu koje se uzorak klasifikuje kao napad ili normalno stanje. Oblik krive pokazuje da model već pri veoma malim vrednostima lažnih alarma postiže visoku stopu detekcije napada. Ovo se može videti kroz nagli porast krive u početnom delu grafika. To znači da se veliki broj napada može identifikovati bez značajnog povećanja broja pogrešno označenih normalnih stanja. Kako se prag dodatno smanjuje, model postaje osetljiviji, detektuje još više napada, ali istovremeno raste i broj lažnih alarma, što objašnjava postepeno približavanje krive gornjem desnom uglu dijagrama.

Vrednost AUC = 0.914 ukazuje na dobru sposobnost modela da razdvaja napadnute i nenapadnute uzorke; praktično, to znači da model u velikoj većini slučajeva dodeljuje višu verovatnoću napada stvarnim FDI uzorcima nego normalnim operativnim stanjima. Ukupno posmatrano, ROC analiza potvrđuje da Random Forest poseduje visoku separabilnost klasa i omogućava podešavanje kompromisa između stope detekcije i stope lažnih alarma u skladu sa operativnim zahtevima sistema.



Slika 1. ROC kriva

Grafik karakteristika značaja, na slici 2, prikazuje koliko svaka pojedinačna ulazna promenljiva doprinosi odluci RF modela.

Vrednosti su dobijene metodom permutacije nad OOB (out-of-bag) uzorcima. To znači da se meri koliko se povećala greška modela kada se vrednosti određene karakteristike nasumično permutuju. Što je veći porast greške, to je ta karakteristika važnija za klasifikaciju. Na grafiku se jasno vidi da najveći doprinos imaju karakteristike sa višim indeksima, koje u ovom radu odgovaraju tokovima aktivne snage po granama (Pf), dok amplitude napona (Vm) i uglova (Va) imaju manji, ali i dalje merljiv doprinos. Ovakav raspored je očekivan, jer je napad u modelu primarno usmeren na tokove snaga i uglove, pa upravo narušavanje tog odnosa predstavlja ključni signal za detekciju.

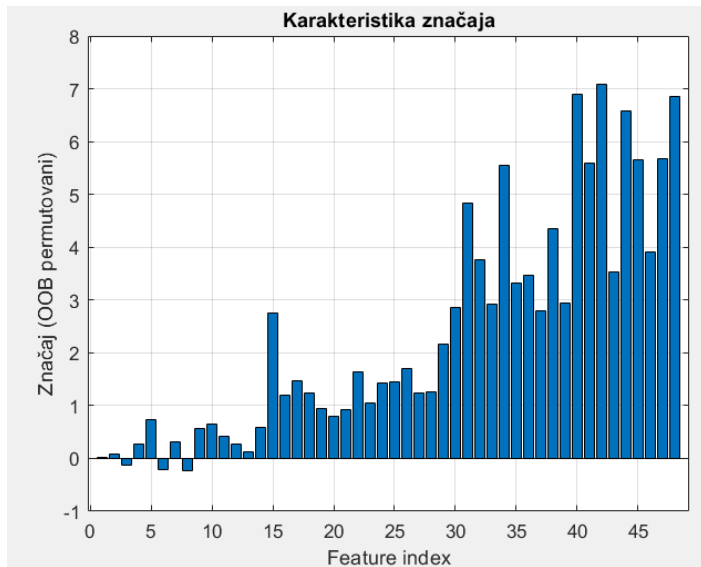
Drugim rečima, model je naučio da prepoznaje nekonzistentnosti u tokovima snaga kao glavni indikator FDI napada, što potvrđuje da detekcija nije slučajna, već zasnovana na fizički smislenim relacijama u mreži.

Na slici 3 su upoređene amplitude napona po sabirnicama za jedno normalno stanje i jedno stanje pod FDI napadom.

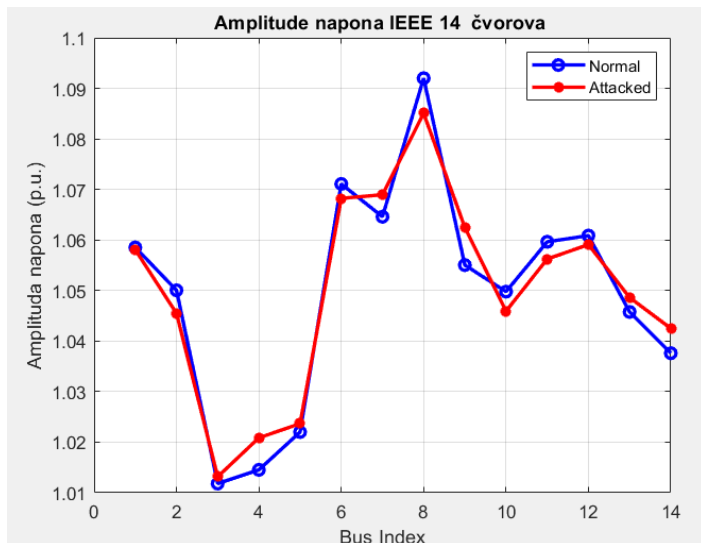
Može se uočiti da su krive gotovo preklopljene i da su odstupanja relativno mala, reda nekoliko hiljaditih delova po jedinici. To znači da napad ne izaziva drastične promene naponskih nivoa, već su razlike suptilne i u okviru opsega koji se može očekivati usled prirodnih varijacija opterećenja i mernog šuma.

Upravo u tome se ogleda karakter stealth-like napada: on ne

proizvodi očigledne fizičke anomalije koje bi se lako uočile prostim praćenjem trenda napona. Umesto toga, napad narušava unutrašnju konzistentnost između više merenja (npr. odnose između uglova i tokova snaga), što nije direktno vidljivo iz samog grafikona napona. Ova slika ilustruje zašto klasični pristupi zasnovani samo na pragovima ili jednostavnoj analizi pojedinačnih veličina mogu da zakažu, dok model mašinskog učenja koristi kompleksnije obrasce u podacima kako bi razlikovao normalna i kompromitovana stanja.



Slika 2. Karakteristika značaja RF metode



Slika 3. Amplitude napona u mreži IEEE sa 14 čvorova

VIII ZAKLJUČAK

U radu je predstavljena metodologija za detekciju False Data Injection (FDI) napada u elektroenergetskim mrežama primenom Random Forest algoritma mašinskog učenja. Na osnovu sintetički generisanog skupa podataka, koji obuhvata 20.000 scenarija (10.000 normalnih i 10.000 napadnutih), model je treniran i testiran u MATLAB/MATPOWER okruženju na IEEE 14 čvorova sistemu. Rezultati su pokazali ukupnu tačnost od

90.80%, uz visoku preciznost od 99.01% i F1 meru od 0.8971. Posebno je značajna niska stopa lažnih alarma, što je od ključnog značaja u realnim operativnim uslovima kako bi se izbegao zamor operatera i degradacija poverenja u sistem za detekciju.

Analiza ROC krive i vrednosti AUC = 0.9142 potvrđuje dobru sposobnost modela da razdvaja normalna i kompromitovana stanja sistema. Dodatno, analiza značaja karakteristika pokazala je da su tokovi aktivne snage po granama najpouzdaniji indikatori napada, zbog fizičke strukture elektroenergetskog sistema i načinom konstrukcije FDI scenarija. Rezultati ukazuju da ansambl metode poput Random Forest-a mogu uspešno detektovati i stealth-like napade koji prolaze kroz tradicionalne BDD mehanizme zasnovane na χ^2 testu.

Iako dobijeni rezultati pokazuju visoku efikasnost predloženog modela, potrebno je naglasiti određena ograničenja ovog istraživanja. Dataset korišćen u radu generisan je sintetički na osnovu Monte Carlo simulacija i AC proračuna tokova snaga, te ne predstavlja realne SCADA/EMS ili PMU podatke iz operativnog sistema. Takođe, analiza je sprovedena na IEEE 14 čvorova test sistemu, koji predstavlja relativno mali i topološki pojednostavljen model u odnosu na realne prenosne mreže. Konstrukcija napada zasnovana je na DC aproksimaciji mernog modela, što predstavlja pojednostavljenje u odnosu na pun nelinearni AC model.

U budućim istraživanjima neophodno je proširiti analizu na veće test sisteme, uključiti realne operativne podatke i razmotriti naprednije scenarije napada sa ograničenim znanjem napadača. Takođe, moguća je integracija vremenskih karakteristika i dubokih neuronskih mreža radi unapređenja stope detekcije slabijih napada. Predloženi pristup predstavlja korak ka implementaciji inteligentnih sistema za sajber bezbednost u pametnim mrežama i potvrđuje potencijal primene mašinskog učenja u unapređenju pouzdanosti i sigurnosti savremenih elektroenergetskih sistema.

ZAHVALNICA

Prikazani rezultati su rezultat istraživanja podržanog od strane Ministarstva nauke, tehnološkog razvoja i inovacija RS po Ugovoru 451-03-34/2026-03/ 200105 od 05.02.2026. god.

LITERATURA

- [1] Fang, Xi, et al. Smart grid - The new and improved power grid: A survey, IEEE communications surveys & tutorials, Vol. 14, No. 4, pp. 944–980, 2011. <https://doi.org/10.1109/SURV.2011.101911.00087>
- [2] Liu, Y., Peng, N., Reiter, M.K. False data injection attacks against state estimation in electric power grids, ACM Transactions on Information and System Security (TISSEC), Vol. 14, No. 1, pp. 1–33, 2009. <http://dx.doi.org/10.1145/1653662.1653666>
- [3] Kosut, O., Jia, L., Thomas, R.J., Tong, L. Malicious data attacks on the smart grid, IEEE Transactions on Smart Grid Vol. 2, No. 4, pp. 645–658, 2011. <https://doi.org/10.1109/TSG.2011.2163807>
- [4] Deng, R., Xiao, G., Lu, R. Defending against false data injection attacks on power system state estimation, IEEE Transactions on Industrial Informatics, Vol. 13, No. 1, pp. 198–207, 2015. <https://doi.org/10.1109/TII.2015.2470218>
- [5] Bećejac, V., Đorđević, M., Jelenić, N., Marković, M., Mosurović, M. Estimacija stanja u elektroenergetskom sistemu sa PMU uređajima i maliciozni napad injektiranjem loših merenja i njegova detekcija, Energija, ekonomija, ekologija, Vol. 26, No. 1, pp. 42–50, 2024. <https://doi.org/10.46793/EEE24-1.42B>

- [6] Hug, G., Giampapa, J.A. 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>
- [7] Liang, G., Zhao, J., Luo, F., Weller, S.R., Dong, Z.Y. A review of false data injection attacks against modern power systems, IEEE Transactions on Smart Grid, Vol. 8, No. 4, pp. 1630–1638, 2017. <https://doi.org/10.1109/TSG.2015.2495133>
- [8] Musleh, A.S., Chen, G., Dong, Z.Y. A survey on the detection algorithms for false data injection attacks in smart grids, IEEE Transactions on Smart Grid, Vol. 11, No. 3, pp. 2218–2234, 2019. <https://doi.org/10.1109/TSG.2019.2949998>
- [9] He, Y., Mendis, G.J., Wei, J. Real-time detection of false data injection attacks in smart grid: A deep learning-based intelligent mechanism, IEEE Transactions on Smart Grid, Vol. 8, No. 5, pp. 2505–2516, 2017. <https://doi.org/10.1109/TSG.2017.2703842>
- [10] Breiman, L. Random forests, Machine learning, Vol. 45, No. 1, pp. 5–32, 2001. <https://doi.org/10.1023/A:1010933404324>
- [11] Ozay, M., Esnaola, I., Vural, F.T.Y., Kulkarni, S.R., Poor, H.V. Machine learning methods for attack detection in the smart grid, IEEE transactions on neural networks and learning systems, Vol. 27, No. 8, pp. 1773–1786, 2015. <https://doi.org/10.1109/TNNLS.2015.2404803>
- [12] Radoglou-Grammatikis, P.I., Sarigiannidis, P.G. Securing the smart grid: A comprehensive compilation of intrusion detection and prevention systems, IEEE Access, Vol. 7, pp. 46595–46620, 2019. <https://doi.org/10.1109/ACCESS.2019.2909807>

AUTORI

Dr Vladimir Bećejac – doktor elektrotehnike i računarstva, Univerzitet u Beogradu: Mašinski fakultet, vbecejac@mas.bg.ac.rs, ORCID [0000-0002-2679-9354](https://orcid.org/0000-0002-2679-9354)

Dr Dobrila Škatarić – doktor elektrotehnike i računarstva, Univerzitet u Beogradu: Mašinski fakultet, dskataric@mas.bg.ac.rs, ORCID [0000-0001-8335-3300](https://orcid.org/0000-0001-8335-3300)

Dr Petar Lukić – doktor elektrotehnike i računarstva, Univerzitet u Beogradu: Mašinski fakultet, plukic@mas.bg.ac.rs, ORCID [0000-0002-4832-1693](https://orcid.org/0000-0002-4832-1693)

Detection of False Data Injection Attacks in Smart Grids Using Machine Learning on Big Data Datasets

Abstract – Digitalization of the electric power system enables more efficient management, but also creates space for sophisticated cyber-attacks, such as false data injection. Traditional bad data detection methods are often unable to recognize attacks that are well-programmed and remain within the error bounds of state estimation. This paper provides an approach to detecting false attacks by applying machine learning algorithms within the MATLAB environment. Using large datasets, a model has been developed that identifies anomalies in the correlations of network parameters in real-time. Simulation results on IEEE test systems demonstrate the model's high precision in distinguishing normal data changes from malicious data manipulations, thereby directly improving the reliability and responsible use of EPS digital infrastructure.

Index Terms – FDIA, Machine learning, State estimation, Big data