Detection of Stealthy False Data Injection Attacks in Unobservable Distribution Networks

James R. K. Rajasekaran, Balasubramaniam Natarajan, Anil Pahwa and Hongyu Wu

***Abstract*—In this paper, a composite scheme is proposed for detecting stealthy data manipulation attacks on distribution system which is unobservable with standard least squares based state estimators. This technique has three stages where the process of data imputation, voltage phasor estimation and the bad data detection are carried out in a systematic manner. The proposed approach is then integrated with moving target defense strategies which perturbs the network parameters to reveal stealthy false data injection attacks. The proposed approach is tested is validated on a three-phase, unbalanced 37-node distribution system and its results are presented. It is shown that the proposed approach has the ability to accurately detect the presence of FDI attacks using limited measurements (i.e., the test system is unobservable).**

***Index Terms*—Bad Data detection, Distribution system, Matrix completion, Moving Target Defence, State Estimation.**

I. Introduction

Cybersecurity aspects of electric grids have gained tremendous attention over the past decade. Traditionally, bad data detection schemes were used to detect arbitrary manipulations of power system measurements but a stealthy approach is proposed in [1] to bypass residual-based detection schemes. Such stealthy false data injection (FDI) attacks satisfy the power balance equations of the network and hence can stay hidden. Stealthy false data can essentially hide an anomaly or persuade the operator to send inappropriate control signals leading to catastrophic consequences. Thus, it is necessary to detect the presence of such stealthy FDI attacks in power systems.A multitude of detection techniques have been developed for conventional power transmission systems. On the other hand, very few attempts have been made to study the effect of FDI attacks and associated detection techniques in the context of distribution systems.

Cybersecurity efforts from the perspective of distribution systems is briefly outlined in [2]. One of the earlier work in the area of cyberattack in distribution system is presented in [3] where the the effect of manipulating the status of overcurrent relay and circuit breaker is studied. A FDI attack methodology for balanced distribution systems is presented in [4] which uses a coarse state estimate to develop the attack vectors. A similar methodology is developed in [5] to execute FDI attacks on unbalanced three phase distribution systems. To detect stealthy FDI attacks in an unbalanced distribution system, the technique given in [6] exploit the transient information in order distinguish legitimate measurements and manipulated values.

Moving target defence (MTD) strategy is one of the popular techniques that can aid in the detection of stealthy FDI attacks on power system measurements [7]. In MTD strategy, the parameters of the given system is perturbed such that the attacker is oblivious to such changes. In the event of an attack, the manipulated measurements will not be in agreement to the system model due to the perturbation in parameters and with such deviations the presence of FDI attack can be detected with conventional bad data detection schemes. The technique given in [8] is one of the early attempts to utilize the MTD strategy for detecting FDI attacks on power system measurements. Such a strategy is adopted for distribution systems in [9] where the network configuration is perturbed to reveal the stealthy FDI attacks and achieve an optimal power flow. The technique given in [10] proposes a MTD strategy where the operating points of the bus injections at predefined nodes are perturbed for the purpose of FDI detection.

Most of the existing studies on the application of MTD in distribution networks consider a fully observable set of measurements for the detection process. But typical distribution systems lack full observability and measurements are not as redundant as compared to its transmission counterparts. As MTD based strategies utilize the residual based schemes for identifying FDI attacks, there is a need to develop bad data detection techniques for unobservable distribution systems which can work in tandem with MTD strategies.

For recovering missing data in PMU measurements, [11] proposed a imputation technique where the low rank property of the measurements is exploited via the matrix completion problem. In [12] and [13], the low rank matrix completion technique is adopted to estimate the state values in distribution systems with low observability. Residual based bad data detection techniques cannot be directly incorporated with the low rank matrix completion approach as the variance of the imputed values would be unavailable. In this paper, a three stage approach is proposed that can analyse the bad data in the unobservable distribution system which can be used to detect FDI attacks using an MTD strategy. This composite scheme uses the matrix completion technique along with the weighted least squares estimator to estimate the bus voltage phasor and its error variance which is later used for detecting bad data using largest normalised residue (LNR) test.

The rest of the paper is organised as follows: Section 2 briefly introduces the FDI attack model adopted in this paper. The proposed approach is detailed in section 3 and its simulation results are presented in section 4. The final section provides the concluding remarks.

II. Attack Model

The objective of the proposed detection framework is to detect any type of data manipulation attack irrespective of

All authors are with Kansas State University, Manhattan, USA.

the attacker's objective. Hence, classical false data injection attack is considered for developing the proposed detection methodology. Let Σ be the set of all the node indices whose cardinally gives the total number of the nodes in a given distribution network. For the purpose of illustrating the FDI attack model, in a no-attack scenario, the amount of complex power injection and complex voltage at phase $m \in \{a, b, c\}$ of bus $j \in \Sigma$ are denoted as $\mathring{\mathbf{s}}_j^m$ and $\mathring{\mathbf{v}}_j^m$ respectively. The attacker aims to manipulate the complex power injection at bus $j \in \Sigma$ to a falsified value $\bullet\mathbf{s}_j^m$. Such a manipulation can hide an anomaly like:

1) inverter overloading from the operators and obstruct them from taking any necessary corrective action; or
2) misrepresenting the system state so that operators can take a wrong control action.

To execute the data manipulation attack in a stealthy manner, the attacker should manipulate the measurements at a set of nodes, $\mathrm{N}_\Sigma(j) \subset \Sigma$, which is the neighbourhood of node j. The set of nodes in which the attacker can manipulate its measurements is defined as region of attaker's influence and it is denoted as $\mathcal{A} = \{j \cup \mathrm{N}_\Sigma(j)\}$. With the premeditated value of $\bullet\mathbf{s}_j^m$ for node j, the attacker can execute a stealthy attack by generating the required amount of data manipulations at the set of nodes, $\mathrm{N}_\Sigma(j) \subset \Sigma$ that satisfies the following condition:

$$\mathring{\mathbf{s}}_j^m - \bullet\mathbf{s}_j^m = \sum_{k \in \mathrm{N}_\Sigma(j)} (\mathring{\mathbf{s}}_k^m - \bullet\mathbf{s}_k^m) \tag{1}$$

The condition given in (1) can be rearranged as:

$$\sum_{k \in \mathcal{A}} \mathring{\mathbf{s}}_k^m = \sum_{k \in \mathcal{A}} \bullet\mathbf{s}_k^m \tag{2}$$

The rearranged condition given in (2) implies that the cumulative complex power flows to the region of attacker's influence from the remaining nodes in the network stay unchanged before and after the attack. Therefore, the complex voltage values outside the region of attacker's influence, $\Sigma \setminus \mathcal{A}$, will also remain unchanged. Since this attack model satisfies the power balance constraint in the network, it will bypass the residual-based bad data detection schemes which typically verifies the given set of data against the system model. Such a false data can be transformed to bad data by employing a hidden MTD strategy which perturbs the network parameters concealed to the attacker. In the next section, a three step methodology is developed to detect the presence of bad data in an unobservable distribution network which can operate in tandem with an MTD strategy for detecting FDI attacks.

III. Proposed Approach

This section is divided into four parts where the first three parts present the three stages of the proposed approach to detect the presence of bad data in an unobservable distribution system. The last part of this section deals with how the MTD strategy can translate FDI attacks into bad data which can be detected using the proposed approach.

A. Imputation of Unavailable Measurements

The first stage of the proposed bad data detection approach imputes the unavailable values at the locations where measurements are not present. To develop the formulation for the imputation method, let Σ be the set of indices of all phase nodes in the given distribution network where the measurements are only available at the nodes given by set ψ. It is considered that the values of voltage magnitude, $|\mathbf{v}|_j$, nodal active power injection, $\mathbf{p}_j$, and reactive power injection, $\mathbf{q}_j$, are measured at node $j \in \psi$. As the equations that relate power and voltages are non-linear, $\mathbf{p}_j$ and $\mathbf{q}_j$ values are transformed to equivalent real part, $\mathbf{c}_j$, and imaginary part, $\mathbf{d}_j$, of current injections at node index j with the a approximate linear formulation as follows:

$$\mathbf{c}_j + \mathrm{i}\mathbf{d}_j \approx \frac{\mathbf{p}_j - \mathrm{i}\mathbf{q}_j}{|\mathbf{v}|_j} \tag{3}$$

$\mathbf{c}$ and $\mathbf{d}$ can be linearly related to the real part, $\mathbf{e}$, and imaginary part, $\mathbf{f}$, of the vector of voltage phasors as:

$$\begin{bmatrix} \mathbf{c} \\ \mathbf{d} \end{bmatrix} = \begin{bmatrix} \mathbf{G} & \mathbf{B} \\ -\mathbf{B} & \mathbf{G} \end{bmatrix} \begin{bmatrix} \mathbf{e} \\ \mathbf{f} \end{bmatrix} \tag{4}$$

where $\mathbf{G}$ and $\mathbf{B}$ are the real and imaginary parts of the bus admittance matrix for the given distribution system. Similarly, the nonlinear relation between the real part, $\mathbf{e}_j$, and imaginary part, $\mathbf{f}_j$, of voltage phasor at node j with voltage magnitude value, $|\mathbf{v}|_j$, can be written in an approximate linear form as:

$$\mathbf{e}_j^0 \cdot \mathbf{e}_j + \mathbf{f}_j^0 \cdot \mathbf{f}_j \approx \mathbf{v}_j^2 \tag{5}$$

where $\mathbf{e}_j^0$ and $\mathbf{f}_j^0$ are the real and imaginary parts of voltage phasor at the previous estimation process. Since the transformed values of $\mathbf{c}$, $\mathbf{d}$, and, $\mathbf{v}^2$ has a linear relationship with $\mathbf{e}$, and, $\mathbf{f}$, the row corresponding to node j in the completed matrix $\mathbf{X} \in \mathbb{R}^{|\Sigma| \times 5}$ which is to be computed is written as:

$$\mathbf{X}_j = \begin{bmatrix} \mathbf{e}_j & \mathbf{f}_j & |\mathbf{v}|_j^2 & \mathbf{c}_j & \mathbf{d}_j \end{bmatrix} \tag{6}$$

The objective of the imputation process is to obtain the completed matrix $\mathbf{X}$ with the values in the partial matrix $\mathbf{M} \in \mathbb{R}^{|\Sigma| \times 5}$ which can be defined as:

$$\mathbf{M}_{j \in \Sigma} = \begin{cases} \begin{bmatrix} \mathbf{0} & \mathbf{0} & |\mathbf{v}|_j^{abc^2} & \mathbf{c}_j^{abc} & \mathbf{d}_j^{abc} \end{bmatrix} & \text{if } j \in \psi \\ \begin{bmatrix} \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} \end{bmatrix} & \text{if } j \notin \psi \end{cases} \tag{7}$$

It is easy to notice that the available measurements enter the partial matrix at its respective positions. On the other hand, the unavailable values are temporarily filled with zeros. To obtain the completed matrix, $\mathbf{X}$, its low rank property is exploited by using its nuclear norm as a part of cost function in the matrix completion problem. Such a formulation for the matrix completion problem should account for the system constraints as previously defined in (4) and (5). Due to the presence of noise in the measurements, these system constraints are enforced in a relaxed approach so that the

problem is feasible. Such a formulation for matrix completion problem corresponds to

$$\arg \min_{\mathbf{X},\boldsymbol{\epsilon},\boldsymbol{\zeta}} \|\mathbf{X}\|_* + \mathbf{w}_1^T\boldsymbol{\epsilon} + \mathbf{w}_2^T\boldsymbol{\zeta} \tag{8a}$$

such that

$$\mathbf{X}_{j,\{3,4,5\}} = \mathbf{M}_{j,\{3,4,5\}}, \forall j \in \psi \tag{8b}$$

$$\begin{bmatrix} \mathbf{e}_j & \mathbf{f}_j & |\mathbf{v}|_j^2 & \mathbf{c}_j & \mathbf{d}_j \end{bmatrix} = \mathbf{X}_{j,*}, \qquad \forall j \in \Sigma \tag{8c}$$

$$\left| \begin{bmatrix} \mathbf{G} & -\mathbf{B} \\ \mathbf{B} & \mathbf{G} \end{bmatrix} \begin{bmatrix} \mathbf{e} \\ \mathbf{f} \end{bmatrix} - \begin{bmatrix} \mathbf{c} \\ \mathbf{d} \end{bmatrix} \right| \leq \boldsymbol{\epsilon} \tag{8d}$$

$$\left| \begin{bmatrix} \mathbf{e}_j^0 & \mathbf{f}_j^0 \end{bmatrix} \begin{bmatrix} \mathbf{e} \\ \mathbf{f} \end{bmatrix} - |\mathbf{v}|^2 \right| \leq \boldsymbol{\zeta}_j \tag{8e}$$

$$\begin{bmatrix} \boldsymbol{\epsilon} \\ \boldsymbol{\zeta} \end{bmatrix} \geq \mathbf{0} \tag{8f}$$

The formulation given in (8) is different from the technique given in [12] as the values of power injection measurements are transformed into equivalent current phasors which are used in the matrix completion process. In this manner, the values of voltage phasors at the nodes without measurement devices can be imputed and can be used in the bad data detection process.

B. Voltage Phasor Estimation

The constraint (8b) in the optimization problem for the imputation process ensures that the values taken at measured locations remains unchanged while solving the low rank matrix completion problem. Hence, the noise content in the measured values are still present along with the pseudo-measurements imputed for the locations where measurements are unavailable.

The second stage involves estimating the bus voltage phasors using the noisy measurements and imputed pseudo-measurements across the network. As (4) and (5) provides a linear relation with the voltage phasors, the measurement model used for the voltage phasor estimation corresponds to

$$\mathbf{z} = \mathbf{H}\tilde{\mathbf{x}} + \boldsymbol{\eta} \tag{9}$$

where

$$\tilde{\mathbf{x}} = \begin{bmatrix} \tilde{\mathbf{e}}^T & \tilde{\mathbf{f}}^T \end{bmatrix}^T \tag{10}$$

$$\mathbf{H} = \begin{bmatrix} \mathbf{I} & \mathbf{0} \\ \mathbf{0} & \mathbf{I} \\ \operatorname{diag}(\mathbf{e}^0) & \operatorname{diag}(\mathbf{f}^0) \\ \mathbf{G} & \mathbf{B} \\ -\mathbf{B} & \mathbf{G} \end{bmatrix} \tag{11}$$

$$\mathbf{z} = \begin{bmatrix} \mathbf{e}^T & \mathbf{f}^T & |\mathbf{v}|^{2^T} & \mathbf{c}^T & \mathbf{d}^T \end{bmatrix}^T \tag{12}$$

$$\eta \sim \mathcal{N}\left(0, \sigma^2\right) \tag{13}$$

In this model, the elements of vector $\mathbf{z}$ can be obtained from the elements of the completed matrix $\mathbf{X}$. To estimate the error variance of pseudo measurements, M sets of old historical measurements, $\mathbf{z}^m$, $m \in [1, \mathrm{M}]$, and its respective state estimates $\tilde{\mathbf{x}}^m$, $m \in [1, \mathrm{M}]$ are considered. With such consideration, error variance at measurement i can be estimated as:

$$\sigma_i^2 = \frac{1}{\mathrm{M}} \sum_{m=1}^{\mathrm{M}} (\mathbf{z}_i^m - \mathbf{H}_i^m \tilde{\mathbf{x}}^m)^2 \tag{14}$$

Since the noise content in the measurements are assumed to have gaussian distribution, the weighted least squares formulation will give the maximum likelihood estimate of voltage phasor which can be written as:

$$\tilde{\mathbf{x}} = \left(\mathbf{H}^T\mathbf{R}^{-1}\mathbf{H}\right)\mathbf{H}^T\mathbf{R}^{-1}\mathbf{z} \tag{15}$$

where the co-variance matrix $\mathbf{R} = \operatorname{diag}(\sigma^2)$. As a considerable amount of noise has been filtered out in the estimate of the state vector, it can be used to analyse the presence of bad data in the consecutive stage of the detection approach.

C. Identification of Bad Data

To identify the presence of bad data in the measured values and the imputed values, largest normalised residue (LNR) test is employed. For LNR test, the residuals are calculated using the voltage phasors estimated in the previous stage as:

$$\mathbf{r} = \mathbf{z} - \mathbf{H}\tilde{\mathbf{x}} \tag{16}$$

To obtain the normalised value of the residuals, the co-variance matrix for all the residuals for measured and imputed values can be given as:

$$\Omega = \mathbf{R} - \mathbf{H}\left(\mathbf{H}^T\mathbf{R}^{-1}\mathbf{H}\right)\mathbf{H}^T \tag{17}$$

With the residual values and its corresponding elements of co-variance matrix, the LNR value, $\mathrm{r}_{\max}^N$, for a given set of measurements can be calculated as

$$\mathrm{r}_{\max}^N = \max_{\{k\}} \frac{|\mathbf{r}_k|}{\sqrt{\Omega_{\{k,k\}}}} \tag{18}$$

Since the measured values are not redundant as compared to the estimated number of variables corresponding to bus voltage phasors, the residuals does not follow the same distribution and hence the thresholds for the LNR test are determined experimentally.

D. Translation of FDI to Bad Data

As presented in the previous section, stealthy FDI attacks have the tendency to evade from the residual based bad data detection techniques like LNR test even if the given set measurements makes the distribution system observable. The proposed three stage approach for identifying bad data enables the detection of stealthy data manipulation attacks in an unobservable distribution network with the help of MTD strategies. Here, consider that special apparatus like D-FACTS devices are placed in the distribution system. These D-FACTS devices can change the values of line reactance typically from 0.8 to 1.2 times its nominal value. The MTD strategy typically involves perturbing the system parameters which in this case are the set points of the D-FACTS devices. These set-points are perturbed in a hidden manner such that attacker is unaware of

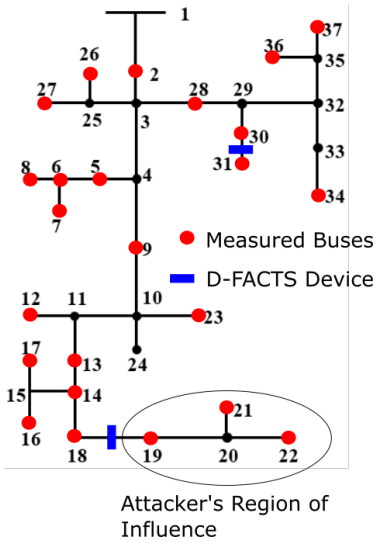

Fig. 1: One-line Diagram of 37-bus test system.

changes and this aids the operator in the detection of stealthy attacks. It is assumed that the attacker does not know the perturbed set-point values of such D-FACTS devices and hence the attacker resorts to using the nominal values of the network parameters. Let $\hat{\mathbf{B}}$ be the imaginary part of bus admittance matrix considered by the attacker whereas the actual value is $\mathbf{B}$. Hence, the system matrix used by the attacker would be $\hat{\mathbf{H}}$ as compared to the actual system matrix $\mathbf{H}$. In such a scenario, when the attacker manipulates the measurement vector as $\hat{\mathbf{z}}$ such that the state vector stays as $\hat{\mathbf{x}}$ by satisfying the following condition of stealthy FDI attack which is:

$$\mathbf{r} = \hat{\mathbf{z}} - \hat{\mathbf{H}}\hat{\mathbf{x}} \tag{19}$$

where $\mathbf{r}$ is the residual in a no-attack scenario. On the other hand, the system matrix that matches with the ground reality is $\mathbf{H}$ and even if the state vector estimated in this condition stays at $\hat{\mathbf{x}}$, the computed residuals will be:

$$\hat{\mathbf{z}} - \mathbf{H}\hat{\mathbf{x}} = \hat{\mathbf{z}} - \hat{\mathbf{H}}\hat{\mathbf{x}} + \left(\hat{\mathbf{H}} - \mathbf{H}\right)\hat{\mathbf{x}} \tag{20}$$

$$= \mathbf{r} + \left(\hat{\mathbf{H}} - \mathbf{H}\right)\hat{\mathbf{x}} \tag{21}$$

With the MTD strategy, the set-points in D-FACTS devices are perturbed, and hence, system matrix perceived by the attacker and the ground reality stays different. In other words, $\hat{\mathbf{H}} \neq \mathbf{H}$, and thus the magnitude of the residuals computed during an attack scenario is higher that that of the residuals in a no-attack scenario as seen in (21). As the rise of residuals can direct increase the LNR values during an attack scenario, the proposed three pronged bad data detection approach with the MTD strategy will be able to detect stealthy FDI attacks effectively.

IV. Simulation Results

The proposed three stage approach for detecting stealthy FDI attacks was tested on the IEEE 37-bus unbalanced distribution system [14] whose line diagram is shown in Fig. 1. The measurements used in the 37-bus test system is injected with

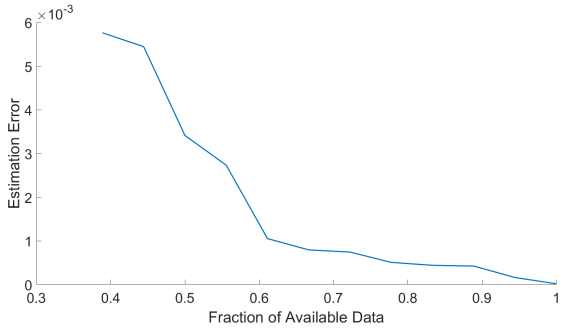

Fig. 2: Estimation error of the proposed approach for different FAD values.

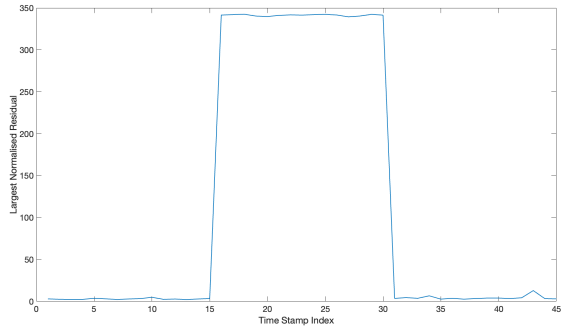

Fig. 3: LNR values during attack and no-attack scenario with 0.65 FAD.

a noise which has zero mean Gaussian distribution and the standard deviation is 1%. The performance of this technique is validated with different values of fraction of available data (FAD) which is the ratio between the number of observable nodes with the total number of nodes in a given network. First the estimation error of the matrix completion-WLS integrated estimation approach is computed for values of FAD from 0.4 to 1 in no-attack scenario and plotted in Fig. 2. It can be noticed that the estimation error seems to stay relatively less and constant for FAD values beyond 0.6 for the given 37-bus test system.

To demonstrate the functionality of the proposed technique, measurements with FAD of 0.65 is considered. Two D-FACTS devices are considered on branches between buses 30 and 31 and between 18 and 19, whose set points are unknown to the attacker. The setpoints of D-FACTS devices are set such that the line reactance has values 0.8 times its nominal value. 45 batches of measurements are considered for this analysis where the attacker executes the FDI attack from the 16th batch until the 30th batch of measurements. We consider that the attacker hijacks the measurements at buses 19, 21 and 22 such that any anomaly inside this region of influence can be concealed in a stealthy manner. Fig. 3 shows the values of LNR for 45 measurement sets which includes both attack and no-attack scenario. It is easy to see that the proposed technique can provide a clear distinction between these two scenarios.

The sensitivity of the LNR values with respect to perturbation of network parameters are analysed by varying the D-

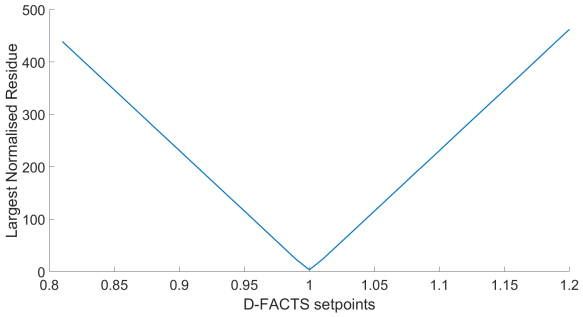

Fig. 4: LNR values with various D-FACTS set-points during attack scenario with 0.68 FAD.

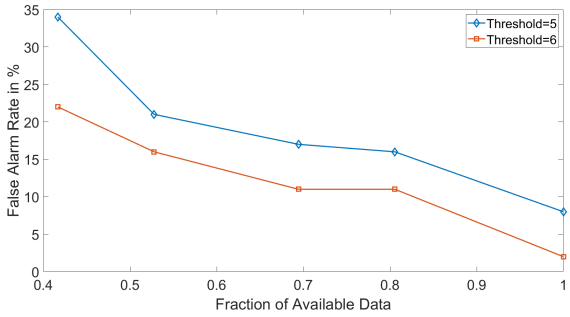

Fig. 5: False alarm rate for for different FAD values under no-attack scenario.

FACTS set-points from 0.8 to 1.2 in steps of 0.05 and plotted in Fig. 4. Since the D-FACTS set-points changes the line reactance in a linear fashion, the increase in LNR values during an attack scenario is directly proportional to the absolute value of the deviation in line parameters relative to its nominal value. Thus, by keeping the set-points at maximum deviation relative to the attacker perceived network parameters, the detection of stealthy FDI attacks becomes effective (as the LNR values under scenario will be noticeably high).

The detection rate under attack scenario and the false alarm rate in the no-attack scenario is evaluated for the proposed technique through 100 Monte Carlo simulations for each bus as target in 37-bus system. It is observed that the detection rate is 100% during attack scenario for FAD values from 0.4 to 1 with threshold values of 5 and 6. This is because the computed LNR values are sensitive to bad data which in this case is a transformed version of the stealthy false data. The false alarm rate of the proposed methodology is obtained for the FAD values from 0.4 to 1 with threshold values of 5 and 6 and plotted in Fig. 5. The false alarm rate tends to decrease as the FAD increases since the error of the integrated estimation approach reduces as the value of FAD increases. Thus the increase in estimation accuracy can eventually reduce the false alarms in the proposed FDI detection scheme.

V. Conclusion

A detection technique is presented in this paper which can identify stealthy FDI attacks in an unobservable distribution network. This technique uses the low rank matrix completion to impute unobserved measurements in the network. The imputed values are used along with the measured values in the weighted least squares based voltage phasor estimator whose results are verified for bad data with LNR test. As the attacker is unaware about the amount of perturbation introduced by the D-FACTS devices, FDI attacks are reflected in the form of bad data. Test results of the proposed approach on the IEEE 37-bus unbalanced distribution system indicate that, during no-attack scenario, the proposed approach provides a moderately accurate estimate of voltage phasors. In the attack case, the proposed approach approach is very adept at detecting FDI with a false alarm rate of less than 15% for FAD values greater than 0.6.

VI. Acknowledgement

This material is based upon work partly supported by the Department of Energy, Office of Energy Efficiency and Renewable Energy (EERE), Solar Energy Technologies Office, under Award # DE-EE0008767 and National Science Foundation under award # 1855216 and award #1929147.

References

[1] Y. Liu, P. Ning, and M. K. Reiter, "False data injection attacks against state estimation in electric power grids," *ACM Trans. Inf. Syst. Secur.*, vol. 14, no. 1, Jun. 2011.

[2] Z. Li, M. Shahidehpour, and F. Aminifar, "Cybersecurity in distributed power systems," *Proceedings of the IEEE*, vol. 105, no. 7, pp. 1367–1388, 2017.

[3] Q. Dai, L. Shi, and Y. Ni, "Risk assessment for cyberattack in active distribution systems considering the role of feeder automation," *IEEE Transactions on Power Systems*, vol. 34, no. 4, pp. 3230–3240, 2019.

[4] R. Deng, P. Zhuang, and H. Liang, "False data injection attacks against state estimation in power distribution systems," *IEEE Transactions on Smart Grid*, vol. 10, no. 3, pp. 2871–2881, 2019.

[5] P. Zhuang, R. Deng, and H. Liang, "False data injection attacks against state estimation in multiphase and unbalanced smart distribution systems," *IEEE Transactions on Smart Grid*, vol. 10, no. 6, pp. 6000–6013, 2019.

[6] J. R. R. Kumar, B. Sikdar, and D. Kundur, "Electromagnetic transients based detection of data manipulation attacks in three phase radial distribution networks," *IEEE Transactions on Industry Applications*, pp. 1–1, 2021.

[7] H. Zhang, B. Liu, and H. Wu, "Smart grid cyber-physical attack and defense: A review," *IEEE Access*, vol. 9, pp. 29 641–29 659, 2021.

[8] K. R. Davis, K. L. Morrow, R. Bobba, and E. Heine, "Power flow cyber attacks and perturbation-based defense," in *2012 IEEE Third International Conference on Smart Grid Communications (SmartGridComm)*, 2012, pp. 342–347.

[9] B. Liu, H. Wu, A. Pahwa, F. Ding, E. Ibrahim, and T. Liu, "Hidden moving target defense against false data injection in distribution network reconfiguration," in *2018 IEEE Power Energy Society General Meeting (PESGM)*, 2018, pp. 1–5.

[10] K. Jhala, P. Pradhan, and B. Natarajan, "Perturbation-based diagnosis of false data injection attack using distributed energy resources," *IEEE Transactions on Smart Grid*, vol. 12, no. 2, pp. 1589–1601, 2021.

[11] P. Gao, M. Wang, S. G. Ghiocel, J. H. Chow, B. Fardanesh, and G. Stefopoulos, "Missing data recovery by exploiting low-dimensionality in power system synchrophasor measurements," *IEEE Transactions on Power Systems*, vol. 31, no. 2, pp. 1006–1013, 2016.

[12] P. L. Donti, Y. Liu, A. J. Schmitt, A. Bernstein, R. Yang, and Y. Zhang, "Matrix completion for low-observability voltage estimation," *IEEE Transactions on Smart Grid*, vol. 11, no. 3, pp. 2520–2530, 2020.

[13] S. Dahale, H. S. Karimi, K. Lai, and B. Natarajan, "Sparsity based approaches for distribution grid state estimation - a comparative study," *IEEE Access*, vol. 8, pp. 198 317–198 327, 2020.

[14] "IEEE PES AMPS DSAS Test Feeder Working Group," https://site.ieee.org/pes-testfeeders/resources/, accessed: 2021-08-10.