Smart FDI Attack Design and Detection with Data Transmutation Framework for Smart Grids

Keerthiraj Nagaraj, Nader Aljohani, Sheng Zou, Tierui Zou, Arturo S. Bretas, Janise McNair, Alina Zare
Department of Electrical and Computer Engineering,
University of Florida, Gainesville, FL
k.nagaraj@ufl.edu, nzjohani@taibahu.edu.sa, shengzou@ufl.edu, tieruizou@ufl.edu,
arturo@ece.ufl.edu, mcnair@ece.ufl.edu, azare@ece.ufl.edu

***Abstract*—Conventional False Data Injection (FDI) attacks yield a distinct change of measurement values which can be easily detected using the state-of-the-art anomaly detection methods. However, if the attackers can learn the statistics of daily load measurement data (e.g., through snooping attacks), then smart FDI attacks can be designed to gradually alter the measurement characteristics over time to avoid detection. In this work, we provide a methodology to protect against smart FDI attacks. First, we create a smart FDI attack that can go undetected when using current state-of-the-art solutions. We then create a novel smart grid cyber defense framework that encrypts measurement data within the power grid and then decrypts data received at the control center to reveal attacked data samples. The proposed framework was validated using the IEEE 118-bus system. Performance was compared between the proposed framework, the Ensemble CorrDet with Adaptive Statistics (ECD-AS) bad data detection methodology and the quasi static model weighted least squares state estimator solution. Results show a mean F1-score of 95% for the proposed technique, 15% for ECD-AS and 18% for the quasi static least square method.**

***Index Terms*—false data injection, machine learning, smart grid, encryption**

I. Introduction

Due to the rapid transition to smart grid (SG), the application of machine learning technology in power systems research has become a growing trend. These techniques help next-generation power systems achieve greater stability, efficiency and robustness of physical processes through integrated control, communication and calculation. However, along with the transition towards the SG paradigm and advanced technology implementation, the power system becomes vulnerable to cyber threats, especially the serious threats on infrastructures. Cyber-attacks, if not detected, can yield misinformation to system operators and potentially cause a collapse of the power system [1], [2]. While much research has been done to address this concern [3]–[5], methods to employ encryption in SG data security are still developing and can be more thoroughly explored. In network security of the SG monitoring system, the core process is State Estimation (SE), the cornerstone of real-time monitoring used by utility companies. SE analyzes the measurement results of the entire system to estimate the voltage and phase of each bus. SE results can be used in many applications, including bad data analysis, which can be used to detect and identify various potential cyber-attacks on SG. Currently, Machine Learning (ML) technology is used to obtain more accurate results through statistical data analysis or to assist in the detection process by considering previous measurement data information [6]. In the authors' previous work [7], an adaptive data-driven anomaly detection framework, Ensemble CorrDet with Adaptive Statistics (ECD-AS), is presented to detect FDI cyber-attacks under a constantly changing system state. ECD-AS uses the mean and covariance matrices of normal samples in the measurement data to adapt its model parameters to changing state of the power system. However, its heavy reliance on measurement statistics might cause its downfall when attackers have either full or partial system knowledge and use this knowledge to gradually inject false data over time, thereby causing ill effects on the functionality of the grid [8].

In this paper, we provide a methodology to protect against smart FDI attacks. First, we design a smart FDI attack to compromise the data integrity of power system measurements based on an attacker gaining knowledge about measurement data and devising attacks that can fool data driven ML-based bad data detection techniques. Next, we present a new encryption/decryption framework to enhance real-time analysis and secure the transmission of power system measurement data. The proposed framework intentionally manipulates data to alter their statistics prior to sending it to the control center. These intentional changes are reverted at the control center to reveal which data samples are the original measurements and which, if any, are attacked/invalid measurements before using the data for various grid functionalities. Therefore, the contributions of this work are twofold:

1) Design of smart FDI attacks that alter measurement statistics gradually over time resulting in harder to detect FDI attacks;
2) An encryption/decryption framework for measurement data to tackle smart FDI attacks;

The remainder of the paper is organized as follows. Section II provides background information on SE and ECD-AS. Section III presents the adversary model and the encryption/decryption framework. A case study is shown in Section IV. Finally, Section V presents conclusions.

This material is based upon work partially supported by the National Science Foundation under Grant Number 1809739.

II. Background Information

A. State Estimation

In modern Energy Management Systems (EMS), the detection of bad data is a typical application of the SE process. The common approach to SE is using the classical Weighted Least Squares (WLS) method described in [9]. In this approach, the system is modeled as a set of non-linear equations based on the physics of the system:

$$\mathbf{z} = h(\mathbf{x}) + \mathbf{e} \tag{1}$$

where $\mathbf{z} \in \mathbb{R}^{1\times d}$ is the measurement vector, $\mathbf{x} \in \mathbb{R}^{1\times N}$ is the vector of state variables, $h : \mathbb{R}^{1\times N} \rightarrow \mathbb{R}^{1\times d}$ is a continuously non-linear differentiable function, and $\mathbf{e} \in \mathbb{R}^{1\times d}$ is the measurement error vector. Each measurement error, e_i is assumed to have zero mean, standard deviation σ_i and Gaussian probability distribution. d is the number of measurements and N is the number of states. In the classical WLS approach, the best estimate of the state vector in (1) is found by minimizing the cost function $J(\mathbf{x})$:

$$J(\mathbf{x}) = \|\mathbf{z} - h(\mathbf{x})\|^2_{R^{-1}} = [\mathbf{z} - h(\mathbf{x})]^T R^{-1}[\mathbf{z} - h(\mathbf{x})] \tag{2}$$

where R is the covariance matrix of the measurements. In this paper, we consider the standard deviation of each measurement to be equal to 1% of the measurement magnitude. The solution to the aforementioned minimization problem is obtained through the linearization of (1) at a certain point x^*. The closed form solution of the linearized model is

$$\Delta\hat{\mathbf{x}} = (H^T R^{-1} H)^{-1} H^T R^{-1} \Delta\mathbf{z}. \tag{3}$$

where $H = \frac{\partial h}{\partial \mathbf{x}}$ is the Jacobian matrix of h at the current state estimate $\mathbf{x}^*$, $\Delta\mathbf{z} = \mathbf{z} - h(\mathbf{x}^*)$ is the correction of the measurement vector. Hence, at each iteration, a new incumbent solution $\mathbf{x}^*_{new}$ is found and updated following $\mathbf{x}^*_{new} = \mathbf{x}^* + \Delta\hat{\mathbf{x}}$ until $\Delta\hat{\mathbf{x}}$ is sufficiently claimed to be small. Using the Innovation Index (II) [10], [11], which quantifies the undetectable error, the Composed Measurement Error (CME) for each measurement i can be expressed as follow:

$$CME_i = r_i \left(\sqrt{1 + \frac{1}{II_i{}^2}} \right). \tag{4}$$

where r_i is the residual and II_i is Innovation Index of the i^{th} measurement. The II_i is strictly positive given that measurement is not critical [10]. The CME values for the set of measurements can then be used in Bad Data Analysis [12]. In particular, the CME based objective function value in (5) is compared to a chi-squared threshold test. If the value of J_{CME} is greater than the chi-squared threshold (with probability p and the degrees of freedom d), then an error is detected in the measurement set.

$$J_{CME}(\hat{\mathbf{x}}) = \sum_{i=1}^{d} \left[\frac{CME_i}{\sigma_i} \right]^2 > \chi^2_{d,p} \tag{5}$$

B. Ensemble CorrDet with adaptive statistics

ECD-AS [7] is an extended work of CorrDet algorithm used for anomaly detection. The CorrDet algorithm updates the statistics of normal samples distribution including mean value and covariance matrix using the Woodbury Matrix Identity [13] in an online fashion when a new sample is detected as normal (if its squared Mahalanobis distanceis less than a threshold). The adaptive threshold introduced in ECD-AS shown in (6) is updated according to statistics of squared Mahalanobis distances of the most recent β normal samples with respect to the distribution of normal samples.

$$\tau = \mu_{thr,-\beta} + \eta * \sigma_{thr,-\beta}. \tag{6}$$

where $\sigma_{thr,-\beta}$ is the standard deviation , $\mu_{thr,-\beta}$ is the mean of squared Mahalanobis distances of most recent β normal samples and value of η decides how many standard deviations the threshold should be from the mean. ECD-AS estimates a set of local CorrDet detectors i.e., $\phi_m(\mu_m,\mathbf{\Sigma}_m,\tau_m)$ for each bus m where μ_m is mean, $\mathbf{\Sigma}_m$ is covariance matrix and τ_m is adaptive threshold for normal samples associated with measurements at bus m. By design, ECD-AS avoids to learn on the very high dimensional data (measurement data in the SG) but can still capture the information in the higher dimensional data for better anomaly detection.

III. Methodology

A. Adversary Models

The three different FDI attack models (random, scaling and ramp) [14] for the value of the injected FDI attack at time t, can be represented by $\mathbf{y}^*[\mathbf{t}]$, as shown in (7),

$$\mathbf{y}^*[\mathbf{t}] = \begin{cases} \mathbf{y}[\mathbf{t}], & t \notin \tau_a \\ \mathbf{y}[\mathbf{t}] + rand(p,q), & t \in \tau_a - - - Random \\ \mathbf{y}[\mathbf{t}](1+\lambda_\mathbf{s}), & t \in \tau_a - - - Scaling \\ \mathbf{y}[\mathbf{t}](1+\lambda_\mathbf{r}), & t \in \tau_a - - - Ramp \end{cases} \tag{7}$$

where $y[t]$ is the original value of measurement y at time t, $rand(p,q)$ is a random number generated using a uniform random function in the interval $[p,q]$, λ_s is a constant value termed as scaling attack factor, λ_r derives values from a ramp function that gradually increases or decreases with time, and τ_a corresponds to the attack time period.

In this paper, we develop four different attack models based on Ramp FDI (RFDI) attacks, as they are shown to have large impact and are harder to detect among various FDI attacks [14]. RFDI attacks change the measurement values gradually with time, altering the measurement statistics such as mean and standard deviation, slowly away from their true values. Data driven and ML based FDI attack detection frameworks in the literature [7] often use these measurement statistics to train their detection models. Hence, a smart RFDI attack would be particularly challenging for such data driven FDI attack detection frameworks. The ramp function used in RFDI attacks can either have linearly or smoothly changing values

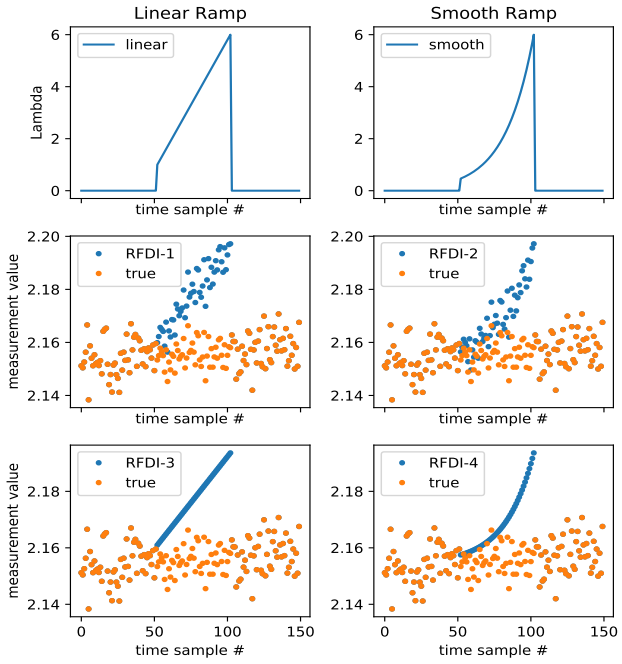

Fig. 1. Examples of smart RFDI attacks

as shown in Fig. 1 for *Linear Ramp* and *Smooth Ramp* which impacts the rate at which inserted false data changes measurement statistics. In Fig. 1, we illustrate the variation in measurement values for normal (orange dots) and attacked (blue dots) samples for various RFDI attack models. We show examples of 4 RFDI attack models for 150 samples where 50 samples (blue dots) are under attack.

In our adversary model, we focus on attacks where the attacker intercepts and alter measurement data in the communication channel to compromise various grid functionality [15] as shown in Fig. 2. We assume collected measurements not to be compromised before being encrypted and sent to the control center. In order to devise smart attacks that are harder to detect, attackers first need to orchestrate snooping attacks to learn about the measurement statistics. Passive snooping attacks (only listening) are harder to detect than spoofing (listening + altering packet content) [16]. We consider Modbus RTU over TCP/IP networking technology, which is commonly used in SG environments to facilitate communication between power grid and control center. The attacker would advertise false information using Address Resolution Protocol (ARP) messages or by directly hijacking the router associated with a bus to read the content (measurement values) of the packets or to manipulate it [17]. Attacks are orchestrated in two phases: Attack Preparation (passive snooping) and Attack Insertion (spoofing). In the attack preparation phase, the attacker performs passive snooping for an attack preparation time period (τ_{ap}) sufficient to estimate target measurement statistics. During the attack insertion (spoofing) phase, attacker inserts malicious data for attack insertion time period τ_{ai} obtained from a ramp function considering following options:

- Option-1 : waits for the packet containing measurement value at current time sample t to alter it and then reroute the same packet to control center, OR
- Option-2 : sends a new packet with false measurement value developed based on learned measurement statistics for time sample t directly to the control center before intercepting original packet, and either use it to update measurement statistics or discard it when it is intercepted.

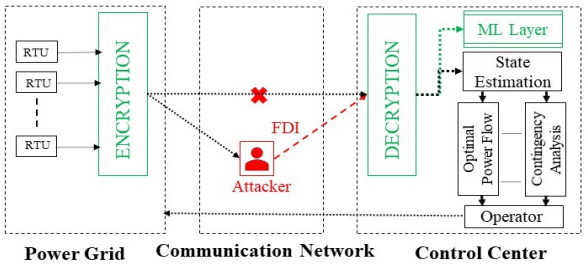

Fig. 2. System architecture of the proposed encryption/decryption framework

Option-2 results in less average time delay in the network as the attacker does not have to wait until the original packet is intercepted to send false data to control center, thereby making it slightly harder to detect compared to Option-1. Based on a linear or smooth ramp function variation, and the above two options for the second phase of the attacks, we design four RFDI attack models, where examples are shown in Fig 1 (the orange dots are the true values and the blue represents RFDI attacks). Note that, in all of the aforementioned RFDI attacks, measurements statistics are taken into account.

1) RFDI-1: In this attack model, the attacker chooses Option-1 during attack insertion phase and the ramp function varies linearly with time. This attack model is given in (8).

$$y^*[t] = \begin{cases} y[t], & t \notin \tau_{ai} \\ y[t] + \lambda_{linear} * \sigma(y[t - \tau_{ap} : t]), & t \in \tau_{ai} \end{cases} \quad (8)$$

2) RFDI-2: In this attack model, equation for RFDI-1 is used, but the ramp function varies smoothly with time. Hence, λ_{smooth} is used instead of λ_{linear} in (8).

3) RFDI-3: In this attack model, attacker chooses Option-2 during attack insertion phase and the ramp function varies linearly with time. The model of this attack is given in (9).

$$y^*[t] = \begin{cases} y[t], & t \notin \tau_{ai} \\ \mu(y[t - \tau_{ap} - 1 : t - 1]) + & \\ \lambda_{linear} * \sigma(y[t - \tau_{ap} - 1 : t - 1]), & t \in \tau_{ai} \end{cases} \quad (9)$$

4) RFDI-4: In this attack model, equation for RFDI-3 is used, but the ramp function varies smoothly with time. Hence, λ_{smooth} is used instead of λ_{linear} in (9).

In (8) and (9), τ_{ap} is attack preparation time period, τ_{ai} is attack insertion time period, λ_{linear} & λ_{smooth} are linear and smooth ramp functions, μ is mean, and σ standard deviation.

B. Encryption and Decryption

In Fig. 2, we show encryption and decryption layers added to the SG along with a ML layer for further data anal-

Procedure 1 Encryption, Attack insertion, Decryption

Encryption

Input: $\mathbf{Z}, \mathbf{Z}_{train}, N, N_c, \mathbf{S}, M$

for $\mathbf{z}_i$ where $i = 1 : M$ **do**
  for $j = 1 : (N/N_c)$ **do**
    Set random.seed = $i \times \mathbf{S}[j]$ using $\mathbf{S}$ from Eq. 10
    $\mathbf{T}_t$ = genRandInt($(j-1) \times N_c + 1$, $j \times N_c$, N_t)
    $\mathbf{T}_v$ = genRandVal($T_{sd} \times \sigma(\mathbf{Z}_{i,train})$, N_t)
    $\mathbf{z}[t]_i^* = \mathbf{z}[t]_i + \mathbf{T}_v ... \forall t \in \mathbf{T}_t$
    $\mathbf{z}[t]_i^* = \mathbf{z}[t]_i ... \forall t \notin \mathbf{T}_t$
  end for
end for

Output: $\mathbf{Z}^*$

Attack Insertion

Input: $\mathbf{Z}^*, \tau_{ap}, \tau_{ai}, \lambda$

Select attack model among RFDI-1,.., RFDI-4

Insert attacks using corresponding Eq. of the chosen model

Output: $\mathbf{Z}^{**}$

Decryption + Detection

Input: $\mathbf{Z}^{**}, \mathbf{Z}_{train}, N, N_c, \mathbf{S}, M$

for $\mathbf{z}_i^{**}$ where $i = 1 : M$ **do**
  for $j = 1 : (N/N_c)$ **do**
    Set random.seed = $i \times \mathbf{S}[j]$ using $\mathbf{S}$ from Eq. 10
    $\mathbf{T}_t$ = genRandInt($(j-1) \times N_c + 1$, $j \times N_c$, N_t)
    $\mathbf{T}_v$ = genRandVal($T_{sd} \times \sigma(\mathbf{Z}_{i,train})$, N_t)
    $\mathbf{z}[t]_i = \mathbf{z}^{**}[t]_i - \mathbf{T}_v ... \forall t \in \mathbf{T}_t$
    $\mathbf{z}[t]_i = \mathbf{z}^{**}[t]_i ... \forall t \notin \mathbf{T}_t$
  end for
end for

Output: $\mathbf{Z}$

Use ECD-AS method [7] to detect attacks in $\mathbf{Z}$ using $\mathbf{Z}_{train}$ as training set.

ysis and attack detection in control center. The proposed encryption process intentionally transmutes a subset of pseudo randomly selected measurement samples by adding pseudo random values. Any attacker intercepting measurement data in the communication network will only have access to these transmuted data. Since only a subset of measurement samples are transmuted, it will be more challenging for the attacker to understand the true measurement statistics needed to successfully devise the smart FDI attacks discussed in Sec III-A. The transmutation methodology is designed in a way to allow decryption of added pseudo random elements to obtain the true measurement values at control center. These measurement values are further analyzed by the state estimator/ML layer to support various grid functionalities. A part of original measurement data that is kept aside for training of attack detection framework is also used to generate pseudo random values needed for measurement transmutation. Let $\mathbf{Z}_{train} \in \mathbf{R}^{N_{train} \times M}$ represent training measurement data, where N_{train} is the number of training samples and M is the total number of measurements. Let $\mathbf{Z}_{i,train} \in \mathbf{R}^{N_{train} \times 1}$ be the ith measurement of training data, where $i = 1 : M$. During transmutation of measurement data, there are 2 important factors to consider, one is which time samples to transmute $\mathbf{T}_t$ and the second is what values $\mathbf{T}_v$ to add. We use the concept of generating pseudo random numbers using fixed random seed values as a starting point to our transmutation process, as a pseudo random number generator with same random seed and other input parameters always return same set of numbers. In our experiments, for illustration purposes we use values from Lazy Carter Sequence $\mathbf{S}$ defined in (10) for setting random seed during measurement transmutation. Any similar fixed integer sequence can be used to define $\mathbf{S}$.

$$\mathbf{S}[j] = (j^2 + j + 2)/2 \tag{10}$$

The proposed framework is implemented considering chunks of measurement data. We present data encryption, attack insertion, measurement data decryption and attack detection processes in Procedure 1. Let the total number of time samples in the measurement data be N, number of time samples in each data chunk be N_c, set of time samples to be used for measurement transmutation be $\mathbf{T}_t$ and have N_t elements for a given a data chunk, T_{sd} be a multiplying factor to vary scale of pseudo random values added during transmutation, the true measurement data to be encrypted and sent to the control center be $\mathbf{Z} \in \mathbf{R}^{N \times M}$, let the encrypted data be $\mathbf{Z}^* \in \mathbf{R}^{N \times M}$, genRandInt$(a, b, c)$ be a function that returns a set of c random integer values in the interval $[a, b]$, genRandVal(p, q) be a function that returns q values from a zero-mean Gaussian distribution function with standard deviation p, and the data which might have attacks be $\mathbf{Z}^{**}$.

IV. Case Study

The proposed framework for detection of smart FDI attacks was validated using the IEEE 118-bus system. Using the MATLAB package MATPOWER [18], 21,600 samples (i.e. one day's worth) of measurements were generated with Gaussian noise based on a common daily load profile that contains temporal information of a power system's changing state. The measurement set includes real and reactive power flows, power injections, and all voltage magnitudes, resulting in 691 measurements with Global Redundancy Level (GRL = d/N) of 2.69, which relates the number of measurements (d) to the number of states (N) to be estimated.

A. Numerical results and discussions

The proposed framework is evaluated for Smart FDI attacks using Precision, Recall and F1-score metrics [19]. Precision and Recall provides information about False Positives and False Negatives respectively. Five different sets of training and testing data are used to report mean values of performance metrics. The number of attacked samples is maintained to be around 5% of total number of samples. We use training data (10% of original data) to design encryption parameters and train ECD-AS detection models. The ECD-AS [7] algorithm has several hyper-parameters that are optimized based on

TABLE I
PERFORMANCE COMPARISON OF THE PROPOSED FRAMEWORK (PREC: MEAN PRECISION, REC: MEAN RECALL, F1: MEAN F1-SCORE)

Model	SE [12]			ECD-AS [7]			Proposed		
	Prec	*Rec*	*F1*	*Prec*	*Rec*	*F1*	*Prec*	*Rec*	*F1*
RFDI-1	1.0	0.13	0.23	0.09	0.58	0.16	0.99	0.97	0.98
RFDI-2	1.0	0.05	0.09	0.08	0.52	0.14	0.97	0.93	0.95
RFDI-3	1.0	0.15	0.27	0.08	0.57	0.16	0.97	0.96	0.97
RFDI-4	1.0	0.06	0.11	0.08	0.53	0.14	0.97	0.86	0.91

cross validation experiments detailed in [7]. The optimized parameters for ECD-AS method are $\alpha = 8e-5$, $\beta = 450$, $\eta = 4$ while for the proposed method are $\alpha = 8e-5$, $\beta = 450$ and $\eta = 9$. Other parameters defined in section III are chosen as follows: $T_{sd} = 2$, $N_t = 75$, $N_c = 100$, $\tau_{ap} = 50$, $\tau_{ai} = 50$, and the ramp function λ varies from 1 to 6 gradually. The λ controls the level of deviation in measurement statistics during smart RFDI attacks. Our experiments revealed that high value of λ increase F1-score since the change in the data statistics is drastic. In contrast, low λ reduces F1-score but the impact on grid functionality is little to negligible.

Numerical results are shown in Table I for the physics based state-of-the-art quasi static model (SE) [12], the ECD-AS model without encryption/decryption (ECD-AS) [7] and the proposed model. In [7], ECD-AS has been demonstrated to perform better than many other random FDI detection algorithms. However, ECD-AS fails to detect smart RFDI attacks due to gradual shift in data statistics. This paper addresses this drawback by enhancing the ECD-AS with encryption/decryption scheme to be able to detect such smart RFDI attacks with high F1-score. The data statistic plays a role in differentiating normal and attacked samples in ML based detection schemes such as ECD-AS. As shown in Table I, proposed framework is able to detect most attacked samples for the listed RFDI attack models. Smart RFDI attacks based on the smooth ramp function (RFDI-2 and RFDI-4) result in a lower F1-score, implying attacks that are harder to detect. The physics based SE results in high mean precision only and ECD-AS results in comparatively high mean recall only, but the proposed framework results in much higher mean F1-score.

V. CONCLUSIONS

This paper presents a smart False Data Injection (FDI) attack design and an easy to implement but effective encryption/decryption mechanism for measurement data. The smart RFDI (Ramp FDI) attack alters measurements gradually over time considering measurement statistics. The proposed encryption/decryption framework improves FDI detection by changing the underlying statistics of the real measurements that might be accessed by attackers in the communication network, which makes the harder to detect smart RFDI attack to be detected easily. The simulation results show that the proposed framework results in much higher F1-scores for attack detection in comparison with state-of-the-art quasi static model weighted least squares state estimator solution and a data driven FDI detection technique. The smart RFDI attacks designed in this paper using a combination of snooping and spoofing techniques can be used as baseline for future studies related to data integrity attacks in smart grids.

ACKNOWLEDGMENT

This material is based upon work partially supported by the National Science Foundation under Grant No. 1809739.

REFERENCES

[1] A. Ashok and M. Govindarasu, "Cyber attacks on power system state estimation through topology errors," in *Power and Energy Society General Meeting, 2012 IEEE*. IEEE, 2012, pp. 1–8.

[2] H. Margossian, M. A. Sayed, W. Fawaz, and Z. Nakad, "Partial grid false data injection attacks against state estimation," *International Journal of Electrical Power & Energy Systems*, vol. 110, pp. 623–629, 2019.

[3] P. Chen, S. Yang, J. A. McCann, J. Lin, and X. Yang, "Detection of false data injection attacks in smart-grid systems," *IEEE Communications Magazine*, vol. 53, no. 2, pp. 206–213, 2015.

[4] A. S. Bretas, N. G. Bretas, B. Carvalho, E. Baeyens, and P. P. Khargonekar, "Smart grids cyber-physical security as a malicious data attack: An innovation approach," *Electric Power Systems Research*, vol. 149, pp. 210–219, 2017.

[5] T. Zou, A. S. Bretas, C. Ruben, S. C. Dhulipala, and N. Bretas, "Smart grids cyber-physical security: Parameter correction model against unbalanced false data injection attacks," *Electric Power Systems Research*, vol. 187, p. 106490, 2020.

[6] J. Cao, D. Wang, Z. Qu, M. Cui, P. Xu, K. Xue, and K. Hu, "A novel false data injection attack detection model of the cyber-physical power system," *IEEE Access*, vol. 8, pp. 95 109–95 125, 2020.

[7] K. Nagaraj, S. Zou, C. Ruben, S. Dhulipala, A. Starke, A. Bretas, A. Zare, and J. McNair, "Ensemble corrdet with adaptive statistics for bad data detection," *IET Smart Grid*, 2020.

[8] A. Sayghe, "Survey of machine learning methods for detecting false data injection attacks in power systems," *IET Smart Grid*, vol. 3, pp. 581–595(14), October 2020.

[9] A. Monticelli, *State estimation in electric power systems: a generalized approach*. Springer Science & Business Media, 1999, vol. 507.

[10] N. Bretas, A. Bretas, and S. Piereti, "Innovation concept for measurement gross error detection and identification in power system state estimation," *IET generation, transmission & distribution*, vol. 5, no. 6, pp. 603–608, 2011.

[11] N. G. Bretas, A. S. Bretas, and A. C. P. Martins, "Convergence property of the measurement gross error correction in power system state estimation, using geometrical background," *IEEE Transactions on Power Systems*, vol. 28, no. 4, pp. 3729–3736, 2013.

[12] N. G. Bretas and A. S. Bretas, "A two steps procedure in state estimation gross error detection, identification, and correction," *International Journal of Electrical Power & Energy Systems*, vol. 73, pp. 484–490, 2015.

[13] B. Alvey, A. Zare, M. Cook, and D. K. Ho, "Adaptive coherence estimator (ace) for explosive hazard detection using wideband electromagnetic induction (wemi)," in *Detection and Sensing of Mines, Explosive Objects, and Obscured Targets XXI*, vol. 9823. International Society for Optics and Photonics, 2016, p. 982309.

[14] S. Sridhar and M. Govindarasu, "Model-based attack detection and mitigation for automatic generation control," *IEEE Transactions on Smart Grid*, vol. 5, no. 2, pp. 580–591, 2014.

[15] X. Li and K. W. Hedman, "Enhancing power system cyber-security with systematic two-stage detection strategy," *IEEE Transactions on Power Systems*, vol. 35, no. 2, pp. 1549–1561, 2020.

[16] P. Anu and S. Vimala, "A survey on sniffing attacks on computer networks," *2017 International Conference on Intelligent Computing and Control (I2C2)*, pp. 1–5, 2017.

[17] G. Sanchez, "Man-in-the-middle attack against modbus tcp illustrated with wireshark," 2020.

[18] R. D. Zimmerman, C. E. Murillo-Sanchez, and R. J. Thomas, "Matpower: Steady-state operations, planning, and analysis tools for power systems research and education," *IEEE Trans. Power Syst.*, vol. 26, no. 1, pp. 12–19, Feb 2011.

[19] E. VALUATIONS, "A review on evaluation metrics for data classification evaluations," 2015.