Detection of False Data Injection Attacks in Smart Grid Communication Systems

Danda B. Rawat, *Senior Member, IEEE*, and Chandra Bajracharya, *Member, IEEE*

***Abstract*—The transformation of traditional energy networks to smart grids can assist in revolutionizing the energy industry in terms of reliability, performance and manageability. However, increased connectivity of power grid assets for bidirectional communications presents severe security vulnerabilities. In this letter, we investigate Chi-square detector and cosine similarity matching approaches for attack detection in smart grids where Kalman filter estimation is used to measure any deviation from actual measurements. The cosine similarity matching approach is found to be robust for detecting false data injection attacks as well as other attacks in the smart grids. Once the attack is detected, system can take preventive action and alarm the manager to take preventative action to limit the risk. Numerical results obtained from simulations corroborate our theoretical analysis.**

***Index Terms*—Attack detection, cyber-security, machine learning, power systems security, smart grid security.**

I. Introduction

THE smart grids offer a more efficient way of supplying and consuming energy by providing bi-directional energy flow and communications. Increased connectivity in smart grids and bidirectional communications present severe security challenges. According to Ernest Orlando Lawrence Berkeley National Laboratory [1], power outages cost over $80 billion every year in the U.S. alone. Thus, due to the critical nature of the smart grid services, smart grid systems become a prime target for cyber terrorism [2], [22]. According to a 2014 Washington D.C. based Bipartisan policy center report, more than 150 cyber-attacks targeted energy sector in 2013 alone [3] and 79 attacks in 2014 [4]. Therefore, transformation of traditional energy networks to smart grids requires integrated end-to-end adaptive cyber defense strategy to safeguard smart grid communications, networks and assets used to operate, monitor, and control power flow and measurements.

Recent related studies for smart grid security include [5]–[12]. In [5], a lightweight message authentication method has been used to secure smart grid systems where distributed meters are mutually authenticated using Diffie-Hellman key establishment protocol and hash-based authentication code. In [6], a generalized likelihood ratio detector has been proposed for smart grid security with limited number of meters compromised. Note that the generalized likelihood ratio detector depends on parametric inferences but is not applicable to nonparametric inferences based on function estimation [13]. In [7], smart grid security techniques have been proposed by using supervised learning algorithms. These techniques rely on a training dataset which is used as a reference to detect the attacks in new measurements. This approach could be compromised during training phase and/or the newer attacks including false data injection attacks could go undetected. None of these methods consider security techniques for false-data injection attacks in smart grid systems.

In this letter, we investigate and compare Chi-square detector and cosine similarity matching for attack detection in smart grids where expected values are estimated using Kalman filter [14], [15] that are used to measure deviation from actual measurements. Note that both approaches are capable of detecting random attacks (e.g., reply of denial-of-communication) whereas the cosine similarity approach is also capable of detecting false data injection attacks in the smart grid. Numerical results obtained from simulations corroborate our theoretical analysis presented in this letter.

Throughout this document, the following notation is used. The boldfaced upper-case letter (e.g. $\mathbf{H}$) represents a matrix and boldfaced lower-case letter (e.g. $\mathbf{x}$) represents a vector. The letters (e.g. N and n) denote scalers. The $[.]^{-1}$ and $[.]^T$, respectively, denote the inverse and the transpose of a matrix. The $E(.)$ is the expected operator.

II. State Space Model and Problem Formulation

In a typical power system, there are k buses interconnected by the t transmission lines. The Independent System Operators (ISOs) monitor the power system through Supervisory Control and Data Acquisition (SCADA) measurements using sensors [16]. The received SCADA measurements can be represented in a compact vector-matrix from as

$$\mathbf{z} = \mathbf{H}\mathbf{x} + \mathbf{n}, \tag{1}$$

where $\mathbf{H}$ is the measurement Jacobian matrix, $\mathbf{x}$ is a vector containing state variables and $\mathbf{n}$ is the measurement noise. When the noise has normal distribution with zero mean and σ_i variance (i.e., $\mathbf{n} \sim \mathcal{N}(0, \mathbf{W})$ with $([\mathbf{W}]_{i,i} = \sigma_i)$, then the linear state

Manuscript received March 03, 2015; revised March 30, 2015; accepted April 08, 2015. Date of publication April 10, 2015; date of current version April 20, 2015. This work was supported in part by the U.S. National Science Foundation (NSF) under Grant CNS-1405670. The associate editor coordinating the review of this manuscript and approving it for publication was Prof. Yan Sun.

The authors are with the Department of Electrical Engineering, Georgia Southern University, Statesboro, Georgia, 30460 USA (e-mail: db.rawat@ieee.org; cbajracharya@GeorgiaSouthern.edu)

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/LSP.2015.2421935

vector estimator can be employed [8] to estimate $\mathbf{x}$ including generation outputs and loads which leads to

$$\hat{\mathbf{x}} = (\mathbf{H}^T\mathbf{W}\mathbf{H})^{-1}\mathbf{H}^T\mathbf{W}\mathbf{z}. \tag{2}$$

The goal of the attacker is to insert false data into the measurements (1) as

$$\mathbf{z} = \mathbf{H}\mathbf{x} + \mathbf{n} + \mathbf{a}, \tag{3}$$

where $\mathbf{a}$ is the false data vector inserted by the attacker. Typical attack vector $\mathbf{a}$ is a non-zero vector.

Then the state variable vector $\hat{\mathbf{x}}$ can be estimated using (3) and (2) in stead of (1) and (2) which could be incorrect/wrong due to attacks or random errors in measurements. False data detection could be implemented which compares ℓ_2-norm of the measurement residual [8] against a threshold λ[1]where it determines that there is an attack (or false data) if

$$\|\mathbf{z} - \mathbf{H}\hat{\mathbf{x}}\|_2^2 > \lambda. \tag{4}$$

Note that if the ℓ_2-norm is less than λ, the received measurement is considered as normal.

This approach has problems as the Jacobian matrix $\mathbf{H}$ in smart grid is very sparse, and attackers can insert false data and by pass the test (4) to attack the smart grid when $\mathbf{a} = \mathbf{H}\mathbf{y}$. Here $\mathbf{y}$ is an attack vector [6], [7], [17].

In this letter, our goal is to proposed an alternative approach to detect false data injection attacks in the smart grids.

Attack Model: In this letter, we assumed that an attacker is able to control a subset of the sensor readings in the smart grid system and uses i) DoS attack; ii) random attack; and iii) false data injection attack. In DoS attacks, an attacker floods packets in the network to compromises devices to prevent data transfer and to jam the communication [18]. In random attacks, the attacker simply manipulates the sensor readings by inserting random attack vector generated by the attacker. In false data injection attacks, the attacker is assumed to be familiar to the system and its parameters used in estimation and detection including gain matrix [19].

To detect the attacks in smart grid, an IEEE 9-bus system with sensors to monitor the state parameters and the estimator and detector is shown in Fig. 1. An open-source MATLAB-based power system simulation package MATPOWER [20] is used to simulate the IEEE 9-bus system and detect attacks using Kalman filter based estimation. Kalman filter based estimation and detection is discussed in the following section.

III. Proposed Framework for Attack Detection in Smart Grid

In this section, we present a security framework which can detect various attacks including random attacks, denial-of-communication attacks, replay attacks, and false data injection attacks in the smart grid. The proposed framework uses Kalman Filter techniques to estimate the measurements.

[1]Note that value of the threshold λ should be chosen based on history and trade-off between the detection and false alarm probability.

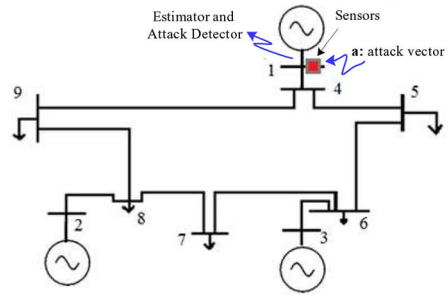

Fig. 1. IEEE 9-bus system with sensors and attacker.

For Kalman Filter technique, we can write (1) in terms of state-space equations with discrete time index n as

$$\begin{aligned}\mathbf{x}_n &= \mathbf{A}_{n,n-1}\mathbf{x}_{n-1} + \mathbf{w}_n,\\ \mathbf{z}_n &= \mathbf{H}_n\mathbf{x}_n + \mathbf{n}_n,\end{aligned} \tag{5}$$

where $\mathbf{A}_{n,n-1}$ state transition matrix (can be initialized with an identity matrix $\mathbf{I}$), $\mathbf{w}_n$ is the state noise vector with covariance matrix $E[\mathbf{w}_n\mathbf{w}_n^T] = \mathbf{Q}_n$.

Then, the Kalman filter equations, for estimation of state variable vector $\mathbf{x}$ based on given initial observations, are as follows. The predicted state or *a priori* estimate is given as

$$\check{\mathbf{x}}_n^- = \mathbf{A}_{n,n-1}\check{\mathbf{x}}_{n-1}^+. \tag{6}$$

Then, the prediction measurement equation can be written as

$$\check{\mathbf{z}}_n = \mathbf{H}_n\check{\mathbf{x}}_n^- \tag{7}$$

The error covariance extrapolation matrix is written as

$$\mathbf{P}_n^- = \mathbf{A}_{n,n-1}\mathbf{P}_{n-1}^+\mathbf{A}_{n,n-1}^T + \mathbf{Q}_{n-1}. \tag{8}$$

Using (8), the Kalman gain matrix equation can be written as

$$\mathbf{G}_n = \mathbf{P}_n^-\mathbf{H}_n^T(\mathbf{H}_n\mathbf{P}_n^-\mathbf{H}_n^T + \mathbf{W}_n)^{-1}. \tag{9}$$

Then the error covariance update equation can be written as

$$\mathbf{P}_n^+ = (\mathbf{I} - \mathbf{G}_n\mathbf{H}_n^T)^{-1}\mathbf{P}_n^-. \tag{10}$$

Finally, the state estimation update (*a posteriori* estimate) is expressed as

$$\check{\mathbf{x}}_n^+ = \check{\mathbf{x}}_n^- + \mathbf{G}_n(\mathbf{z}_n - \check{\mathbf{z}}_n). \tag{11}$$

Then, the estimation error (i.e., the difference between estimated value and the actual measurements) can be written as

$$\mathbf{e}_n = \check{\mathbf{x}}_n^+ - \mathbf{x}_n \Leftrightarrow \check{\mathbf{x}}_n^+ - \mathbf{x}. \tag{12}$$

The estimated values for electrical measurements using Kalman Filter and the actual measured data using sensors are used to detect attacks by finding any deviations between them. Note that we can regenerate the signal using measured data to compare it with expected or estimated values. If a detector finds significant differences between these two values with the

predefined threshold, it triggers an alarm indicating that there is an attack in the systems.

A. Chi-Square Test as an Attack Detector

The deviation in expected/estimated value (by Kalman Filter) and measured value (by sensor measurements) is used to detect malicious attacks in the smart grid. This deviation between there values for a given time index n can be computed as

$$\mathbf{f}_n = \mathbf{z}_n - \check{\mathbf{z}}_n = \mathbf{z} - \mathbf{H}\mathbf{x}_n^+. \tag{13}$$

Then, the scalar value of residue of the difference vector in (13) can be computed as

$$R_{Chi-square} = \mathbf{f}_n^T \mathbf{F}_n \mathbf{f}_n, \tag{14}$$

where $\mathbf{F}_n$ is the covariance matrix of the vector $\mathbf{f}_n$. The Chi-square detector compares the scalar residue value $R_{Chi-square}$ in (14) with a given threshold value which can be obtained by using Chi-square table to detect attacks (e.g., random attacks and replay attacks) in the smart grid. This approach is fast and easy to implement. However, the Chi-square detector can not detect false data injection attacks as shown under the 'Performance Evaluation and Numerical Results' section of this letter. Thus, we propose the cosine similarity matching approach to detect false data injection attacks in smart grids.

B. Cosine Similarity Matching Approach to Detect False-data Injection Attacks

False data injection attacks can be crafted to bypass the statistical detectors such as Chi-square detector. Thus, we propose cosine similarity matching based approach to detect any deviation between measured data (using sensor measurements) and estimated/expected data (using Kalman filter). The cosine similarity matching metric tells how similar the two data vectors are. If both vectors are similar, the value of cosine similarity is one. The cosine similarity metric between the received measurements $\overrightarrow{v}(\hat{\mathbf{x}}) = \hat{\mathbf{x}}$ and estimated observation $\overrightarrow{v}(\check{\mathbf{x}}) = \check{\mathbf{x}}$ can be written as

$$sim(\check{\mathbf{x}}, \hat{\mathbf{x}}) = cos(\theta) = \frac{\overrightarrow{v}(\check{\mathbf{x}}).\overrightarrow{v}(\hat{\mathbf{x}})}{||\overrightarrow{v}(\check{\mathbf{x}})||||\overrightarrow{v}(\hat{\mathbf{x}})||}, \tag{15}$$

where the numerator represents the dot (i.e., inner) product of the vectors $\overrightarrow{v}(\check{\mathbf{x}})$ and $\overrightarrow{v}(\hat{\mathbf{x}})$, and the denominator denotes the product of their Euclidean lengths.

Note that when there is no false data injection attack, two vectors $\overrightarrow{v}(\check{\mathbf{x}})$ and $\overrightarrow{v}(\hat{\mathbf{x}})$ exactly match, and the value of $sim(\check{\mathbf{x}}, \hat{\mathbf{x}})$ is equal to one which represents no attack in the smart grid. However, to compare the performance of the proposed cosine similarity based approach with Chi-square detector, we compute the following

$$R_{cos-sim} = 1 - sim(\check{\mathbf{x}}, \hat{\mathbf{x}}) = 1 - \frac{\overrightarrow{v}(\check{\mathbf{x}}).\overrightarrow{v}(\hat{\mathbf{x}})}{||\overrightarrow{v}(\check{\mathbf{x}})|| \times ||\overrightarrow{v}(\hat{\mathbf{x}})||}, \tag{16}$$

and compare it against a given threshold[2].

[2]Note that the threshold that is used to compare with detector output could be estimated using its history and measurements in the smart grid.

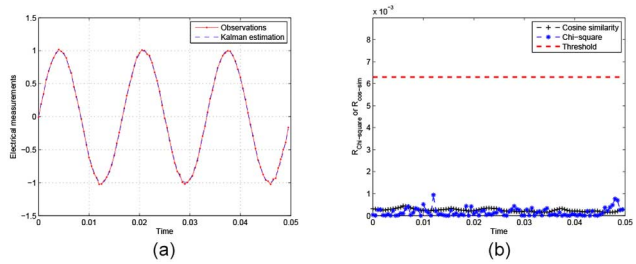

Fig. 2. Variation of electrical measurements and Kalman filter estimations vs. the time when there were no attacks. (a) Measured voltage signal and Kalman Filter estimation. (b) Detectors' outputs along with threshold.

IV. Performance Evaluation and Numerical Results

In this section, we simulate different scenarios by using Matlab to corroborate our theoretical analysis. We consider sinusoidal signal with frequency 60 Hz, amplitude 1 Volt, sampling frequency 2000 Hz, $\mathbf{x}_n^- = 0$, and initial covariance matrix $\mathbf{P}_{n-1}^+ = \mathbf{I}$ i.e., an identity matrix. Then, we generated a sine wave with this configuration and added the additive Gaussian white noise with zero mean to the signal using the Matlab function $randn()$. The input signal and the resulting signal obtained using state estimation are plotted with and without attacks. Based on the Kalman filter estimates, we computed the residue for Chi-square detector using (14) and normalized it to compare with cosine similarity matching criteria. We also computed the cosine similarity matching value using (16) and plotted these values along with a given threshold.

A. Attack/Fault Detection

First, we plotted the variation of signal versus the time for electrical measurements and its Kalman filter estimation when no attacks were introduced as shown in Fig. 2(a). For this setup, we also plotted the residue for Chi-square detector using (14) and cosine similarity matching value using (16) as shown in Fig. 2(b). As there is no attacks in the smart grid, the input signal and estimated signal are close enough and their detection metrics (14) and (16) lie below threshold. This indicates that there is no attacks in the smart grid systems.

Second, we introduced random attacks (replay and/or denial-of-communications attacks) into the smart grid and applied Kalman Filter to estimate the expected values of the measurements. Then, we plotted the variation of observations of electrical measurements and their expected values under random attacks as shown in Fig. 3(a). In this case, the estimated data does not corresponds to the measured one as shown in Fig. 3(a) and thus the residue in (14) exceeds the threshold most of the time in Chi-square detection and the similarity metric in (16) also exceeds the threshold as shown in Fig. 3(b). Thus, the both approaches are able to detect attacks and could trigger an alarm to indicate attacks in the smart grid.

Then, to see the effect of a random attack that starts at different time than from beginning, we introduced the attacks at around middle of the observation period as shown in Fig. 3. Before attacks started, the observations were close enough with estimated values by Kalman filter resulting in lower values of residues than the threshold value for both Chi-square detection and similarity matching as shown in Fig. 4(b). However, after attack started, the estimated signal did not correspond to the

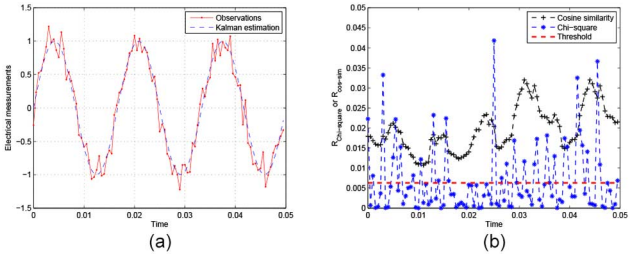

Fig. 3. Variation of electrical measurements and Kalman filter estimations vs. the time when there were random attacks. (a) Measured voltage signal and Kalman Filter estimation. (b) Detectors' outputs along with threshold.

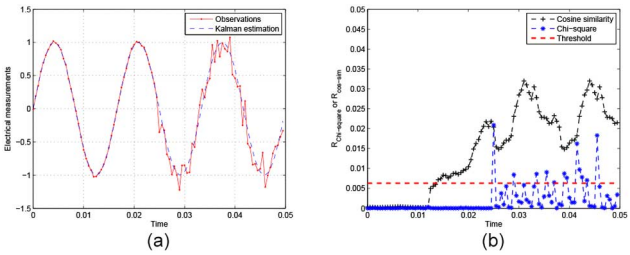

Fig. 4. Variation of electrical measurements and Kalman filter estimations vs. the time when there was random attack in the second half of the observation period. (a) Measured voltage signal and Kalman Filter estimation. (b) Detectors' outputs along with threshold.

measured one as shown in Fig. 4(a) and the detectors resulted in higher values than the threshold indicating that there were attacks in the system. This shows that the attacks could be detected on the fly whenever they start.

B. False Data Injection Attack Detection

In this section, we evaluate the proposed approaches for false data injection attacks in smart grids. We considered that an attacker was attacking the smart grid by inserting false data into measurements using statistics of the measurements [9], [21]. In this scenario, to see the impact of false data injection attacks, we used both Chi-square detector and cosine similarity matching approach using actual measurements and estimated values by the Kalman filter. Again, it is worth noting that both approaches were working perfectly when there were no attacks as shown in Fig. 2. As noted, there was no attack detected since both Chi-square detector and cosine similarity values were not exceeding the given threshold.

Then, we considered that there was false data injection attack in the smart grid where actual measurement observations were not close enough to estimated values by Kalman filter as shown in Fig. 5(a). During this attack, the Chi-square detector resulted in its normalized residue values $R_{Chi-res}$ below its threshold and thus it was not able to detect the attack in the system as shown in Fig. 5(b). However, in the same setup, the cosine similarity matching values ($R_{cos-sim}$ values) were above the given threshold as shown in Fig. 5(b). We performed a couple experiments and observed the same for all cases. Thus, we concluded that the Chi-square detector is incapable of detecting false data injection attacks while the cosine similarity matching approach is capable of detecting false data injection attacks.

Finally, we considered that the false data injection attack was started approximately before the half of an observation time. When there was no attack, the estimated values were close to the actual measurements but they were not close enough after the attack was started as shown in Fig. 6(a). Both detectors

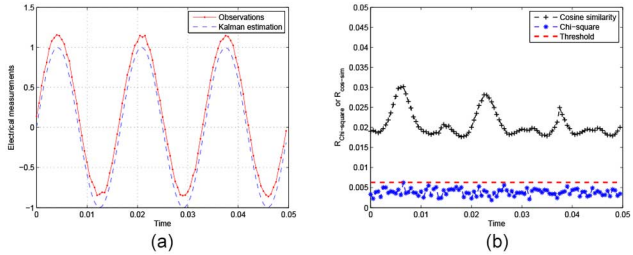

Fig. 5. Variation of electrical measurements and Kalman filter estimations vs. the time when there were false data injection attacks. (a) Measured voltage signal and Kalman Filter estimation. (b) Detectors' outputs along with threshold.

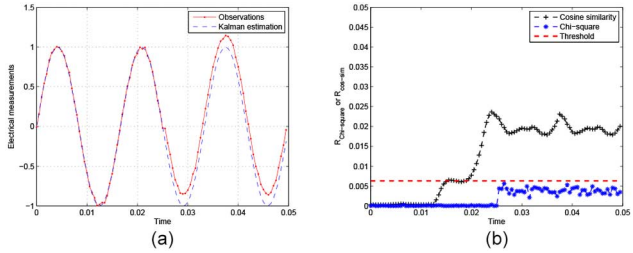

Fig. 6. Variation of electrical measurements and Kalman filter estimations vs. the time when there were false data injection attacks after about half observation period. (a) Measured voltage signal and Kalman Filter estimation. (b) Cosine similarity and Chi-square detector outputs using Kalman Filter against threshold.

were resulting in lower values than the threshold indicating that there was no attack during first half of the experiment. Even after attack was started, the Chi-square detector was unable to detect the attacks as its residue values were below threshold whereas the cosine similarity detector was able to detect the attack as it was giving higher values than the threshold as shown in Fig. 6(b). We performed several experiments and confirmed that the cosine similarity matching approach was capable of detection attacks regardless of the starting time of the false data injection attacks. However, Chi-square detector was unable to detect the false data injection attacks.

We conclude that these results show that the cosine similarity matching approach is capable of detecting all attacks including false data injection attack whereas the Chi-square based detector is incapable of detecting false data injection attacks in the smart grid. It is noted that once the attack is detected, system can take preventive action and/or alarm the manager to take preventative action to limit the risk.

V. Conclusion

In this letter, we have presented the Chi-square detector and cosine similarity matching for attack detection in smart grid systems. We have used Kalman filter estimation to find expected measurements which are used to measure any deviation between actual measurements and estimated values to detect attacks. We have shown that both Chi-square detector and cosine similarity matching are capable of detecting random attacks including denial-of-communication attacks. The Chi-square detector was incapable of detecting false data injection attacks, however, the cosine similarity matching approach was able to detect false data injection attacks. Once the attack is detected, system can take preventive action and alarm the manager to take preventative action to limit the risk. We have presented numerical results obtained from simulations which corroborate our theoretical analysis.

REFERENCES

[1] K. H. LaCommare and J. H. Eto, *Understanding the cost of power interruptions to U.S. electricity consumers*, Sep. 2004 [Online]. Available: http://certs.lbl.gov/pdf/55718.pdf, Accessed Online: Dec. 26, 2014

[2] J. Salmeron, K. Wood, and R. Baldick, "Analysis of electric grid security under terrorist threat," *IEEE Trans. Power Systems*, vol. 19, no. 2, pp. 905–912, 2004.

[3] M. Hayden, C. Hebert, and S. Tierney, *Cyber-security & the north american electric grid: New policy approaches to address an evolving threat*, Feb. 2014 [Online]. Available: http://tinyurl.com/obpqf6r, [Accessed Online: Dec. 26, 2014]

[4] J. Pagliery, *Hackers attacked the united states (U.S.) energy grid 79 times this year*, Nov. 18, 2014 [Online]. Available: http://money.cnn.com/2014/11/18/technology/security/energy-grid-hack, Accessed Online: December 26, 2014

[5] M. M. Fouda, Z. M. Fadlullah, N. Kato, R. Lu, and X. Shen, "A lightweight message authentication scheme for smart grid communications," *IEEE Trans. Smart Grid*, vol. 2, no. 4, pp. 675–685, 2011.

[6] O. Kosut, L. Jia, R. J. Thomas, and L. Tong, "Malicious data attacks on the smart grid," *IEEE Trans. Smart Grid*, vol. 2, no. 4, pp. 645–658, 2011.

[7] M. Ozay, I. Esnaola, F. T. Yarman Vural, S. R. Kulkarni, and H. V. Poor, "Smarter security in the smart grid," in *2012 IEEE Third Int. Conf. Smart Grid Communications (SmartGridComm'12)*, 2012, pp. 312–317.

[8] 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, p. 13, 2011.

[9] Y. Mo, E. Garone, A. Casavola, and B. Sinopoli, "False data injection attacks against state estimation in wireless sensor networks," in *2010 49th IEEE Conf. Decision and Control*, 2010, pp. 5967–5972.

[10] M. Esmalifalak, G. Shi, Z. Han, and L. Song, "Bad data injection attack and defense in electricity market using game theory study," *IEEE Trans. Smart Grid*, vol. 4, no. 1, pp. 160–169, 2012.

[11] Y. Zhu, J. Yan, Y. Sun, and H. He, "Revealing cascading failure vulnerability in power grids using risk-graph," *IEEE Trans. Parallel Distrib. Syst.*, vol. 25, no. 12, pp. 3274–3284, 2014.

[12] Y. Zhu, J. Yan, Y. Tang, and H. He *et al.*, "Resilience analysis of power grids under the sequential attack," *IEEE Trans. Inf. Forensics Secur.*, vol. 9, no. 12, pp. 2340–2354, 2014.

[13] J. Fan, C. Zhang, and J. Zhang, "Generalized likelihood ratio statistics and Wilks phenomenon," *Ann. Statist.*, pp. 153–193, 2001.

[14] R. E. Kalman, "A new approach to linear filtering and prediction problems," *J. Fluids Eng.*, vol. 82, no. 1, pp. 35–45, 1960.

[15] C. K. Chui and G. Chen, *Kalman Filtering: with Real-time Applications*. Berlin, Germany: Springer, 2008.

[16] V. Sood, D. Fischer, J. Eklund, and T. Brown, "Developing a communication infrastructure for the smart grid," in *2009 IEEE Electrical Power & Energy Conf. (EPEC)*, 2009, pp. 1–7.

[17] L. Jia, R. J. Thomas, and L. Tong, "Malicious data attack on real-time electricity market," in *IEEE Int. Conf. Acoustics, Speech and Signal Processing (ICASSP), 2011*, 2011, pp. 5952–5955.

[18] S. Amin, A. A. Cardenas, and S. S. Sastry, "Safe and secure networked control systems under denial-of-service attacks," in *Hybrid Systems: Computation and Control*. Berlin, Germany: Springer, 2009, pp. 31–45.

[19] Y. Mo and B. Sinopoli, "False data injection attacks in control systems," *The First Workshop on Secure Control Systems*, pp. 5967–5972, Apr. 12, 2010, cPSWeek, 2010.

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

[21] S. Bi and Y. J. A. Zhang, "Defending mechanisms against false-data injection attacks in the power system state estimation," in *2011 IEEE GLOBECOM Workshops (GC Wkshps)*, 2011, pp. 1162–1167.

[22] D. B. Rawat and C. Bajracharya, "Cyber security for smart grid systems: Status, challenges and perspectives," in *Proc. IEEE SouthEastCon 2015*, Fort Lauderdale, FL, USA, Apr. 9–12, 2015 , "," , vol. , pp. –, .