Proceedings of 9th IEEE International Conference
on CYBER Technology in Automation, Control, and Intelligent Systems
July 29- August 2, 2019, Suzhou, China

Residual Saturation Based Kalman Filter for Smart Grid State Estimation Under Cyber Attacks

Md Masud Rana[1*], Rui Bo[1] and Bong Jun Choi[2]
[1]Department of Electrical & Computer Engineering, Missouri University of Science & Technology, USA
[2]School of Computer Science and Eng & School of Electronic Eng, Soongsil University, Seoul, Korea
[1*]Email: mamaraece28@yahoo.com

***Abstract*—Most of the traditional state estimation algorithms are provided false alarm when there is attack. This paper proposes an attack-resilient algorithm where attack is automatically ignored, and the state estimation process is continuing which acts a grid-eye for monitoring whole power systems. After modeling the smart grid incorporating distributed energy resources, the smart sensors are deployed to gather measurement information where sensors are prone to attacks. Based on the noisy and cyber attack measurement information, the optimal state estimation algorithm is designed. When the attack is happened, the measurement residual error dynamic goes high and it can ignore using proposed saturation function. Moreover, the proposed saturation function is automatically computed in a dynamic way considering residual error and deigned parameters. Combing the aforementioned approaches, the Kalman filter algorithm is modified which is applied to the smart grid state estimation. The simulation results show that the proposed algorithm provides high estimation accuracy.**

***Index Terms*—Cyber attacks, dynamic state estimation, distributed energy resources, Kalman filter, state-space power network, residual saturation.**

I. Introduction

Designing a smart energy management system is a significant contribution to realize a reliable and efficient operation of smart grid [1]. Basically, the grid distribution systems are integrated with distributed energy resources (DERs) which are easy to attacks as the distribution systems or microgrid users are less aware of threats [2], [3], [4]. A number of techniques for state estimation of cyber physical systems (CPS) such as smart grid and water treatment plant have been demonstrated [5], [6], [7]. A Kalman filter (KF) algorithm is developed for CPS such as water treatment plant in [8], [9]. Basically, the performance of this algorithm is demonstrated considering different attacks where attackers can provide misleading information to the utility operator.

Moreover, the attack detection and state estimation problem is formulated for random set theory in [10]. Several kinds of cyber-attacks such as sensor/actuator data corruption, extra packet injection and packet substitution are investigated. The different form of KF algorithms and their potential applications are described in [11], [12], [13], [14], [15], [16]. In order to handle reply attacks, the secure estimation scheme is investigated in [17]. Furthermore, the nonlinear state estimation considering cyber attacks is presented in [18], [19]. The evet-based minimum mean square error scheme for smart grid state estimation is proposed in [20]. Additionally, the forecast aided KF algorithm considering cyber attack is explored in [21]. The state-space based observer considering attack is described in [22], [23], [24], [25].

Hackers that destroy information privacy have been studied in the literature. In those researches, hacker normally has whole or incomplete knowledge of grid topology. Based on incomplete grid topology due to limited resources, a false data protection scheme for smart grid is proposed in [26]. For instance, the cyber physical system measurement outputs are coded and encrypted for detecting injection attacks [27]. Considering the coloured Gaussian noise, the generalized likelihood ratio test detector is presented in [28]. An alternating direction method of multipliers scheme is proposed for compensating the cyber attacks [29]. Different optimization algorithms for cyber attack protection are described in [30].

From machine learning point of view, researchers are trying to develop robust estimation algorithms ignoring so much mathematical difficulties or considering unrealistic power system information. In [31], a deep learning algorithm for grid state estimation is proposed, and it provides better results compared with the artificial neural network and support vector machine. It uses a deep belief network to efficiently describe the temporal behavior of the cyber attacks. Moreover, the recurrent neural network to recognize cyber attack in the grid is designed in [32]. The Long Short Term Memory (LSTM) network for anomaly detection scheme is presented in [33], [34], [35]. Basically, LSTM based prediction model is deigned to detect intrusion [36]. The reinforcement learning scheme for smart grid considering cyber attack is described in [37], [38]. A data-driven online attack detection method is presented in [39], [40]. However, all these methods cannot directly reflect the power system operation in real-time. In this paper, we develop a centralised state estimation algorithm for smart grid incorporating multiple DERs. The simulation results show that the proposed algorithm provides high estimation accuracy.

II. State-space Representation of Power Networks

The smart grid provides higher efficiency, reliability, and consumer-centricity in an environment of growing power demand [31]. The state state-space representation of power networks is obtained on the basis of a set of differential equations of DERs, power networks and uncertainties. Using Kirchhoff's laws, a set of differential equations are written and after simplifying them, the state-space compact form is obtained.

Generally speaking, the distributed energy resources (DERs) such as solar cells and wind turbines are connected to the power network. The connecting point are point common coupling (PCC) voltages. The PCC voltages and DER voltages are denoted by $\mathbf{V}_b = [V_{b1}, V_{b2}, \cdots, V_{bn}]'$ and $\mathbf{V}_s = [V_{s1}, V_{s2}, \cdots, V_{sn}]'$, where V_{bi} and V_{si} are the i-th PCC voltages and DER voltages, respectively [41] [42].

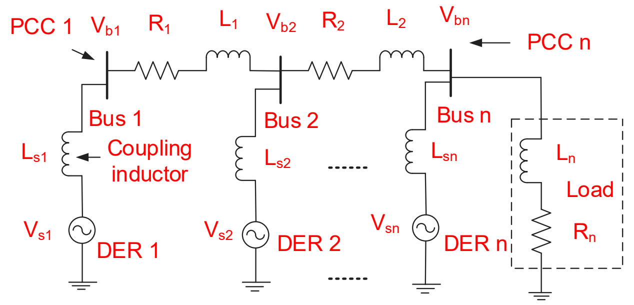

Fig. 1: The n-bus system connected to DERs [41] [42].

Let's applying Kirchhoff's voltage law at bus-1 for s-domain as follows [41] [42]:

$$\frac{V_{b1} - V_{s1}}{sL_{s1}} + \frac{V_{b1} - V_{b2}}{R_1 + sL_1} = 0$$
$$(\frac{L_1}{L_{s1}} + 1)sV_{b1} - sV_{b2} + \frac{R_1}{L_{s1}}V_{b1} - \frac{R_1}{L_{s1}}V_{s1} - \frac{L_1}{L_{s1}}sV_{s1} = 0. \tag{1}$$

It can be written as a time domain expression as follows:

$$(\frac{L_1}{L_{s1}} + 1)\dot{V}_{b1} - \dot{V}_{b2} + \frac{R_1}{L_{s1}}V_{b1} - \frac{R_1}{L_{s1}}V_{s1} - \frac{L_1}{L_{s1}}\dot{V}_{s1} = 0. \tag{2}$$

Here, $(\dot{\bullet})$ is the first order derivative with respect to time. Similarly, all other bus voltages and their corresponding time-domain expressions are obtained.

$$\mathbf{W}\dot{\mathbf{V}}_b = \mathbf{W}_1\mathbf{V}_b + \mathbf{W}_2\mathbf{V}_s + \mathbf{W}_3\dot{\mathbf{V}}_s. \tag{3}$$

Here, $\mathbf{W} =$

$$\begin{bmatrix} \frac{L_1}{L_{s1}}+1 & -1 & 0 & 0 & \cdots & 0 \\ \frac{L_2}{L_{s1}} & \frac{L_2}{L_{s2}}+1 & -1 & 0 & \cdots & 0 \\ \frac{L_3}{L_{s1}} & \frac{L_3}{L_{s2}} & \frac{L_3}{L_{s3}}+1 & -1 & \cdots & 0 \\ \frac{L_4}{L_{s1}} & \frac{L_4}{L_{s2}} & \frac{L_4}{L_{s3}} & \frac{L_4}{L_{s4}}+1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \\ \frac{L_n}{L_{s1}} & \frac{L_n}{L_{s2}} & \frac{L_n}{L_{s3}} & \frac{L_n}{L_{s4}} & \cdots & \frac{L_n}{L_{sn}}+1 \end{bmatrix}$$

$$\mathbf{W}_1 = \begin{bmatrix} -\frac{R_1}{L_{s1}} & 0 & 0 & 0 & \cdots & 0 \\ -\frac{R_2}{L_{s1}} & -\frac{R_2}{L_{s2}} & 0 & 0 & \cdots & 0 \\ -\frac{R_3}{L_{s1}} & -\frac{R_3}{L_{s2}} & -\frac{R_3}{L_{s3}} & 0 & \cdots & 0 \\ -\frac{R_4}{L_{s1}} & -\frac{R_4}{L_{s2}} & -\frac{R_4}{L_{s3}} & -\frac{R_4}{L_{s4}} & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \\ -\frac{R_n}{L_{s1}} & -\frac{R_n}{L_{s2}} & -\frac{R_n}{L_{s3}} & -\frac{R_n}{L_{s3}} & \cdots & -\frac{R_n}{L_{sn}} \end{bmatrix}$$

$\mathbf{W}_2 = -\mathbf{W}_1$.

$$\mathbf{W}_3 = \begin{bmatrix} \frac{L_1}{L_{s1}} & 0 & 0 & 0 & \cdots & 0 \\ \frac{L_2}{L_{s1}} & \frac{R_2}{L_{s2}} & 0 & 0 & \cdots & 0 \\ \frac{L_3}{L_{s1}} & \frac{R_3}{L_{s2}} & \frac{R_3}{L_{s3}} & 0 & \cdots & 0 \\ \frac{L_4}{L_{s1}} & \frac{R_4}{L_{s2}} & \frac{R_4}{L_{s3}} & \frac{R_4}{L_{s4}} & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \\ \frac{R_n}{L_{s1}} & \frac{R_n}{L_{s2}} & -\frac{R_n}{L_{s3}} & -\frac{R_n}{L_{s3}} & \cdots & \frac{R_n}{L_{sn}} \end{bmatrix}$$

The system is linearised around the operating points as follows:

$$\begin{aligned} \mathbf{W}\Delta\dot{\mathbf{V}}_b &= \mathbf{W}_1\Delta\mathbf{V}_b + \mathbf{W}_2\Delta\mathbf{V}_s + \mathbf{W}_3\Delta\dot{\mathbf{V}}_s. \\ \Delta\dot{\mathbf{V}}_b &= \mathbf{A}^c\Delta\mathbf{V}_b + \mathbf{B}^c\Delta\mathbf{V}_s + \mathbf{L}\Delta\dot{\mathbf{V}}_s. \end{aligned} \tag{4}$$

Here, $\Delta\mathbf{V}_b = \mathbf{V}_b - \mathbf{V}_{ref}$, ΔV_s represents the change in DER voltages required for bus voltages to approach $\mathbf{V}_{ref}$, simplified terms $\mathbf{A}^c = \mathbf{W}^{-1}\mathbf{W}_1$, $\mathbf{B}^c = \mathbf{W}^{-1}\mathbf{W}_2$, and $\mathbf{L} = \mathbf{W}^{-1}\mathbf{W}_3$.

$$\begin{aligned} \Delta\dot{\mathbf{V}}_b - \mathbf{L}\Delta\dot{\mathbf{V}}_s &= \mathbf{A}^c\Delta\mathbf{V}_b - \mathbf{A}^c\mathbf{L}\Delta\mathbf{V}_s + \mathbf{A}^c\mathbf{L}\Delta\mathbf{V}_s + \mathbf{B}^c\Delta\mathbf{V}_s \\ \Delta\dot{\mathbf{V}}_b - \mathbf{L}\Delta\dot{\mathbf{V}}_s &= \mathbf{A}^c[\Delta\mathbf{V}_b - \mathbf{L}\Delta\mathbf{V}_s] + [\mathbf{A}^c\mathbf{L} + \mathbf{B}^c]\Delta\mathbf{V}_s \\ \dot{\mathbf{s}} &= \mathbf{A}_c\mathbf{s} + \mathbf{B}_c\mathbf{u}. \end{aligned} \tag{5}$$

Here, $\mathbf{s} = \Delta\mathbf{V}_b - \mathbf{L}\Delta\mathbf{V}_s$ is the PCC volatge deviation from the reference value, $\mathbf{A}_c = \mathbf{A}^c$ for notional consistency, $\mathbf{B}_c = \mathbf{A}^c\mathbf{L} + \mathbf{B}^c$ and $\mathbf{u} = \Delta\mathbf{V}_s$ is the DER input voltage. Based on the step size parameter μ, the continuous-time system is discretise to $\mathbf{A} = \mathbf{I} + \mu\mathbf{A}_c$ and $\mathbf{B} = \mu\mathbf{B}_c$.

The power network and measurement are obtained as follows:

$$\begin{aligned} \mathbf{s}_{t+1} &= \mathbf{A}\mathbf{s}_t + \mathbf{B}\mathbf{u}_t + \mathbf{w}_t. \\ \mathbf{z}_t &= \mathbf{C}\mathbf{s}_t + \mathbf{D}\mathbf{d}_t + \mathbf{v}_t. \end{aligned}$$

Here, $\mathbf{s}_t \in \mathbb{R}^n$ and $\mathbf{z}_t \in \mathbb{R}^p$ are the state and measurement, $\mathbf{v}_t \backsim N(\mathbf{0}, \mathbf{Q})$ and $\mathbf{w}_t \backsim N(\mathbf{0}, \mathbf{R})$, $\mathbf{C}$ is the sensing matrix, $\mathbf{D}$ is the attacker matrix ($\mathbf{D} \neq \mathbf{0}$ with attack and $\mathbf{D} = \mathbf{0}$ without attack), and $\mathbf{d}_k \in \mathbb{R}^p$ is the cyber attack. Based on this noisy and corrupted version of measurement, the cyber attack protection algorithm is designed in the following section.

III. Proposed Attack-Resilient State Estimation Algorithm For Smart Grid

The saturation function is used in different applications and systems as illustrated in [22], [23], [24], [43], [25]. When the attack is happened, the measurement residual error dynamic goes high, and it can ignore using the proposed saturation function. Basically, the Kalman filter operates recursively on streams of noisy input data to produce a statistically optimal estimate of the underlying system state. It has two steps:

- **Prediction Step:** Produces estimates of the current state variables, along with their uncertainties [44], [45].
- **Correction Step:** Updated the estimate of the current state variables using a weighted average, with more weight being given to estimates with higher certainty [46], [47].

The prediction step is given by [48], [47]:

$$\hat{\mathbf{s}}_{t|t-1} = \mathbf{A}\hat{\mathbf{s}}_{t-1|t-1} + \mathbf{B}\mathbf{u}_t. \tag{6}$$

$$\mathbf{P}_{t|t-1} = \mathbf{A}\mathbf{P}_{t-1|t-1}\mathbf{A}' + \mathbf{Q}. \tag{7}$$

Here, $\hat{\mathbf{s}}_{t|t-1}$ and $\mathbf{P}_{t|t-1}$ are the prediction state and error covariance while $\hat{\mathbf{s}}_{t-1|t-1}$ and $\mathbf{P}_{t-1|t-1}$ are their corresponding initial values.

Inspired by different application domain papers in [22], [23], [24], [43], the modified correction step for smart grid state estimation is given by:

$$\hat{\mathbf{s}}_{t|t} = \hat{\mathbf{s}}_{t|t-1} + \mathbf{K}_t[sat_\sigma(\mathbf{z}_t - \mathbf{C}\hat{\mathbf{x}}_{t|t-1})]. \tag{8}$$

$$\mathbf{K}_t = \mathbf{P}_{t|t-1}\mathbf{C}'(\mathbf{C}\mathbf{P}_{t|t-1}\mathbf{C}' + \mathbf{R})^{-1}. \tag{9}$$

$$\mathbf{P}_{t|t} = \mathbf{P}_{t|t-1} - \mathbf{K}_t\mathbf{C}\mathbf{P}_{t|t-1}. \tag{10}$$

Here, $\hat{\mathbf{s}}_{t|t}$ and $\mathbf{P}_{t|t}$ are the updated state and error covariance, $\mathbf{K}_t$ is the estimation gain, and $sat_\sigma(\mathbf{z}_t - \mathbf{C}\hat{\mathbf{x}}_{t|t-1})$ is the residual saturation. The saturation function is define as follows:

$$sat_\sigma(\mathbf{z}_t - \mathbf{C}\hat{\mathbf{x}}_{t|t-1}) = \begin{bmatrix} sat_{\sigma_1}(z_{j,t} - C_j\hat{\mathbf{x}}_{t|t-1}) \\ \vdots \\ sat_{\sigma_p}(z_{p,t} - C_p\hat{\mathbf{x}}_{t|t-1}) \end{bmatrix}. \tag{11}$$

Here, C_j is the j-th row of the original sensing matrix and $sat_{\sigma_j}(z_{j,t} - C_j\hat{\mathbf{x}}_{t|t-1}) = max[-\sigma_j, \; min\{\sigma_j, (z_{j,t} - C_j\hat{\mathbf{x}}_{t|t-1})\}]$ is the standard scalar saturation function [22], [23], [24], [43]. The dynamic adaptation of this saturation function is necessary. It can be computed in an iterative way as follows:

$$\sigma_{j,t+1} = \alpha_j\sigma_{j,t} + \beta_j(z_{j,t} - C_j\hat{\mathbf{x}}_{t|t-1})^2, \quad j = 1, \cdots p.$$

Here, $\sigma_{j,t} > 0$ is the initial saturation value, and $\alpha_j, \beta_j > 0 \; \forall j$. Basically, $\sigma_{j,t+1}$ is changed according to the measurement residual error dynamics. The first term pushes (related to α) the saturation level to almost zero while the last term minimises the estimation error. Combining these two terms, the algorithm can automatically tolerance the cyber attack.

IV. PERFORMANCE ASSESSMENT

We conduct a performance evaluation of the proposed algorithm for smart grid state estimation. All software simulations are conducted in the Matlab 2018a environment. The simulation results are compared with the benchmark results found by a centralised KF method. The cyber attacks happen in 2.6, 4, 5, 5.5, 7 and 8 sec. The considered process and measurements noise covariances are Gaussian distribution and the covariances are shown in Table I. The sampling period is 0.0001 sec.

TABLE I: Simulation parameters with Matlab.

Symbols	Values	Symbols	Values
R_1	0.175 Ω	R_2	0.1667Ω
R_3	0.2187Ω	R_4	0.001 Ω
L_1	0.0005 H	L_2	0.0004 H
L_3	0.0006 H	L_4	0.0148 H
$\mathbf{Q}$	0.001*$\mathbf{I}$	$\mathbf{R}$	0.04*$\mathbf{I}$
μ	0.0001 sec	L_{sn}	0.001 H

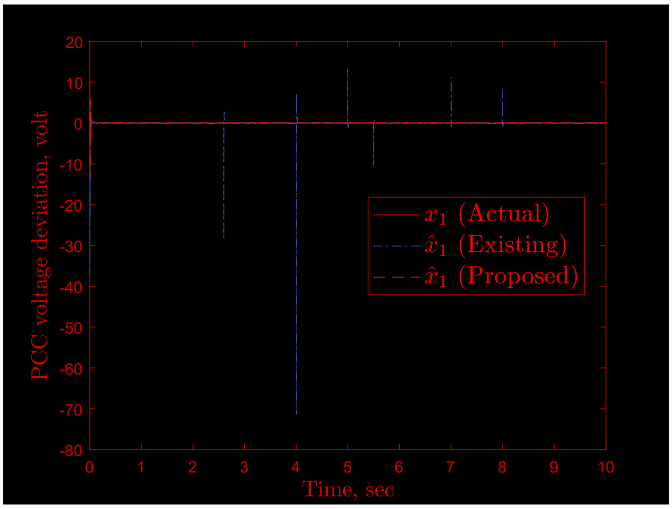

Fig. 2: PCC of DER 1 deviation (x_1) and it estimation.

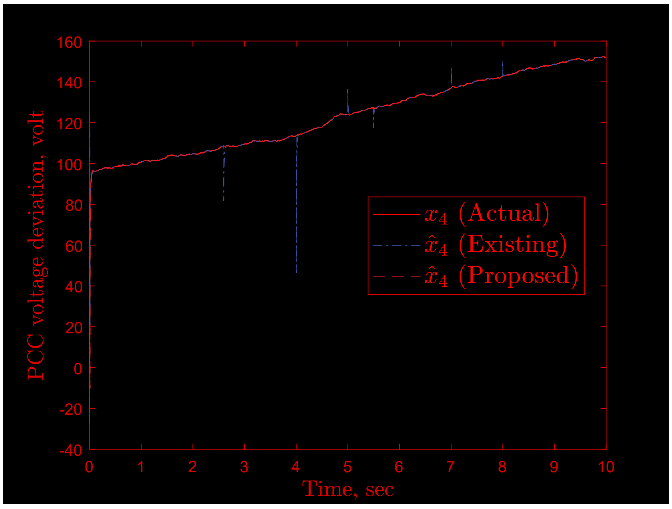

Fig. 3: PCC of DER 4 deviation (x_4) and it estimation.

Figures 2-3 show the dynamic state responses of the system states and estimation results. Figure 2 shows the PCC voltage of DER 1 and it estimation result. It can be seen that the proposed algorithm can able to tolerate the cyber attack while existing method cannot perform well. This is due to the fact that the proposed attack-resilient algorithm can be automatically ignored the cyber attack, and the state estimation process is continuing which acts a grid-eye for monitoring whole power systems. The proposed saturation function is automatically computed in a dynamic way considering residual error and deigned parameters. Similarly other estimated states have similar accuracy.

V. CONCLUSION AND FUTURE WORK

The cyber attack is not only create financial problem but also make our life difficulty to survive. In order to protect grid information, this paper proposes an cyber attack protection algorithm. First, the mathematical model of the power system is described, and measurements are obtained by a set of sensors. The sensing information is polluted by noise and cyber attacks. Based on the received information, the proposed algorithm is developed. The correction step of the Kalman filter is modified using proposed saturation function of the residual error. Moreover, the saturation function is obtained considering weighting factor and residual error dynamics. Numerical results show that developed algorithm can perform well compared with existing method. In the future, we will develop a hieratical estimation algorithm for smart grid state estimation. A potential avenue for further research is to detect the cyber attack in smart grid and to develop a forecast based offline/online protection strategy.

ACKNOWLEDGEMENT

This material is based upon work supported by the National Science Foundation under Grant No. 1837472. Moreover, this research was supported under the NRF, Korea (NRF-2019R1C1C1007277) funded by the MSIT, Korea.

REFERENCES

[1] C. Zhao, J. He, P. Cheng, and J. Chen, "Analysis of consensus-based distributed economic dispatch under stealthy attacks," *IEEE Transactions on Industrial Electronics*, vol. 64, no. 6, pp. 5107–5117, 2017.

[2] M. M. Rana and L. Li, "Renewable microgrid state estimation using the Internet of Things communication network," *ICACT Transactions on Advanced Communications Technology*, vol. 5, no. 3, pp. 823–829, 2016.

[3] J. Pan, R. Jain, S. Paul, T. Vu, A. Saifullah, and M. Sha, "An Internet of things framework for smart energy in buildings: Designs, prototype, and experiments," *IEEE Internet of Things Journal*, vol. 2, no. 6, pp. 527–537, 2015.

[4] M. M. Rana, L. Li, and S. Su, "Internet of things (IoT) in 5G mobile technologies," in *Microgrid State Estimation Using the IoT with 5G Technology*. Springer, 2016, pp. 175–195.

[5] M. M. Rana and L. Li, "Kalman filter based microgrid state estimation using the internet of things communication network," in *Proc. of the International Conference on Information Technology-New Generations*, 2015, pp. 501–505.

[6] ——, "Distributed generation monitoring of smart grid using accuracy dependent Kalman filter with communication systems," in *Proc. of the International Conference on Information Technology-New Generations*, 2015, pp. 496–500.

[7] ——, "An overview of distributed microgrid state estimation and control for smart grids," *Sensors*, vol. 15, no. 2, pp. 4302–4325, 2015.

[8] C. M. Ahmed, S. Adepu, and A. Mathur, "Limitations of state estimation based cyber attack detection schemes in industrial control systems," in *Proc. of the Smart City Security and Privacy Workshop*, 2016, pp. 1–5.

[9] Y. He, S. Li, and Y. Zheng, "Distributed state estimation for leak detection in water supply networks," *IEEE/CAA Journal of Automatica Sinica, to apper in 2019*.

[10] N. Forti, G. Battistelli, L. Chisci, S. Li, B. Wang, and B. Sinopoli, "Distributed joint attack detection and secure state estimation," *IEEE Transactions on Signal and Information Processing over Networks*, vol. 4, no. 1, pp. 96–110, 2018.

[11] C.-Y. Chong, "Forty years of distributed estimation: A review of noteworthy developments," in *Proc. of the Sensor Data Fusion: Trends, Solutions, Applications*, 2017, pp. 1–10.

[12] C.-Y. Chong, K.-C. Chang, and S. Mori, "A review of forty years of distributed estimation," in *Proc. of the International Conference on Information Fusion*, 2018, pp. 1–8.

[13] M. De Sanctis, E. Cianca, G. Araniti, I. Bisio, and R. Prasad, "Satellite communications supporting internet of remote things," *IEEE Internet of Things Journal*, vol. 3, no. 1, pp. 113–123, 2016.

[14] M. M. Rana, W. Xiang, and X. Li, "Position and velocity estimations of mobile device incorporate GNSS," *IEEE Access*, vol. 6, pp. 31 141–31 147, 2018.

[15] L. Lyu, C. Chen, S. Zhu, and X. Guan, "5G enabled codesign of energy-efficient transmission and estimation for industrial IoT systems," *IEEE Transactions on Industrial Informatics*, vol. 14, no. 6, pp. 2690–2704, 2018.

[16] M. Rana, W. Xiang, and B. J. Choi, "Grid state estimation over unreliable channel using IoT networks," in *Proc. of the International Conference on Control, Automation, Robotics and Vision*, 2018, pp. 945–948.

[17] B. Chen, D. W. Ho, G. Hu, and L. Yu, "Secure fusion estimation for bandwidth constrained cyber-physical systems under replay attacks," *IEEE transactions on cybernetics*, vol. 48, no. 6, pp. 1862–1876, 2018.

[18] M. A. Rahman and H. Mohsenian-Rad, "False data injection attacks against nonlinear state estimation in smart power grids," in *Proc. of the Power & Energy Society General Meeting*, 2013, pp. 1–5.

[19] H. Karimipour and V. Dinavahi, "On false data injection attack against dynamic state estimation on smart power grids," in *Proc. of the International Conference on Smart Energy Grid Engineering*, 2017, pp. 388–393.

[20] Y. Qi, P. Cheng, L. Shi, and J. Chen, "Event-based attack against remote state estimation," in *Proc. of the Conference on Decision and Control*, 2015, pp. 6844–6849.

[21] K. Manandhar, X. Cao, F. Hu, and Y. Liu, "Detection of faults and attacks including false data injection attack in smart grid using Kalman filter," *IEEE Transactions on Control of Network Systems*, vol. 1, no. 4, pp. 370–379, 2014.

[22] A. Alessandri and L. Zaccarian, "Results on stubborn luenberger observers for linear time-invariant plants," in *Proc. of the European Control Conference*, 2015, pp. 2920–2925.

[23] ——, "Stubborn state observers for linear time-invariant systems," *Automatica*, vol. 88, pp. 1–9, 2018.

[24] T. Hu, Z. Lin, and B. M. Chen, "An analysis and design method for linear systems subject to actuator saturation and disturbance," *Automatica*, vol. 38, no. 2, pp. 351–359, 2002.

[25] S. Tarbouriech, G. Garcia, J. M. G. da Silva Jr, and I. Queinnec, *Stability and stabilization of linear systems with saturating actuators*. Springer Science & Business Media, 2011.

[26] Y. Li and Y. Wang, "False data injection attacks with incomplete network topology information in smart grid," *IEEE Access*, vol. 7, pp. 3656–3664, 2019.

[27] F. Miao, Q. Zhu, M. Pajic, and G. J. Pappas, "Coding schemes for securing cyber-physical systems against stealthy data injection attacks," *IEEE Transactions on Control of Network Systems*, vol. 4, no. 1, pp. 106–117, 2017.

[28] B. Tang, J. Yan, S. Kay, and H. He, "Detection of false data injection attacks in smart grid under colored Gaussian noise," in *Proc. of the Conference on Communications and Network Security*, 2016, pp. 172–179.

[29] D. Du, X. Li, W. Li, R. Chen, M. Fei, and L. Wu, "ADMM-based distributed state estimation of smart grid under data deception and denial of service attacks," *IEEE Transactions on Systems, Man, and Cybernetics: Systems, to appear in 2019*.

[30] K. Pan, A. Teixeira, M. Cvetkovic, and P. Palensky, "Cyber risk analysis of combined data attacks against power system state estimation," *IEEE Transactions on Smart Grid, to appear in 2019*.

[31] Y. He, G. J. Mendis, and J. Wei, "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.

[32] Q. Deng and J. Sun, "False data injection attack detection in a power grid using RNN," in *Proc. of the Annual Conference of the IEEE Industrial Electronics Society*, 2018, pp. 5983–5988.

[33] R. Vinayakumar, K. Soman, and P. Poornachandran, "Long short-term memory based operation log anomaly detection," in *Proc. of the International Conference on Advances in Computing, Communications and Informatics*, 2017, pp. 236–242.

[34] Y. Cheng, H. Zhu, J. Wu, and X. Shao, "Machine health monitoring using adaptive kernel spectral clustering and deep long short-term memory recurrent neural networks," *IEEE Transactions on Industrial Informatics*, vol. 15, no. 2, pp. 987–997, 2019.

[35] W. Lu, Y. Li, Y. Cheng, D. Meng, B. Liang, and P. Zhou, "Early fault detection approach with deep architectures," *IEEE Transactions on Instrumentation and Measurement*, vol. 67, no. 7, pp. 1679–1689, 2018.

[36] P. Malhotra, A. Ramakrishnan, G. Anand, L. Vig, P. Agarwal, and G. Shroff, "Lstm-based encoder-decoder for multi-sensor anomaly detection," *arXiv preprint arXiv:1607.00148*, 2016.
[37] Z. Ni, S. Paul, X. Zhong, and Q. Wei, "A reinforcement learning approach for sequential decision-making process of attacks in smart grid," in *Proc. of the Symposium Series on Computational Intelligence*, 2017, pp. 1–8.
[38] Z. Ni and S. Paul, "A multistage game in smart grid security: A reinforcement learning solution," *IEEE Transactions on Neural Networks and Learning Systems, to appera in 2019*.
[39] X. Wang, D. Shi, J. Wang, Z. Yu, and Z. Wang, "Online identification and data recovery for pmu data manipulation attack," *IEEE Transactions on Smart Grid, to appear in 2019*.
[40] L. K. Mestha, O. M. Anubi, and M. Abbaszadeh, "Cyber-attack detection and accommodation algorithm for energy delivery systems," in *Proc. of the Conference on Control Technology and Applications*, 2017, pp. 1326–1331.
[41] S. R. Mishra, M. P. Korukonda, L. Behera, and A. Shukla, "Enabling cyber physical demand response in smart grids via conjoint communication and controller design," *IET Cyber-Physical Systems: Theory & Applications, to apper in 2019*.
[42] H. Li, L. Lai, and H. V. Poor, "Multicast routing for decentralized control of cyber physical systems with an application in smart grid," *IEEE Journal on Selected Areas in Communications*, vol. 30, no. 6, pp. 1097–1107, 2012.
[43] H. Fang, M. A. Haile, and Y. Wang, "Robustifying the kalman filter against measurement outliers: An innovation saturation mechanism," in *2018 IEEE Conference on Decision and Control (CDC)*. IEEE, 2018, pp. 6390–6395.
[44] M. M. Rana and W. Xiang, "IoT communications network for wireless power transfer system state estimation and stabilization," *IEEE Internet of Things Journal*, vol. 5, no. 5, pp. 4142–4150, 2018.
[45] M. M. Rana, "Modelling the microgrid and its parameter estimations considering fading channels," *IEEE Access*, vol. 5, pp. 10 953–10 958, 2017.
[46] M. M. Rana, W. Xiang, and E. Wang, "Smart grid state estimation and stabilisation," *International Journal of Electrical Power & Energy Systems*, vol. 102, pp. 152–159, 2018.
[47] M. M. Rana, W. Xiang, E. Wang, and X. Li, "Monitoring the smart grid incorporating turbines and vehicles," *IEEE access*, vol. 6, pp. 45 485–45 492, 2018.
[48] M. M. Rana, L. Li, and S. W. Su, "Controlling the renewable microgrid using semidefinite programming technique," *International Journal of Electrical Power and Energy Systems*, vol. 84, pp. 225–231, 2017.