From Wired to Wireless: Challenges of False Data Injection Attacks against Smart Grid Sensor Networks

Jiachen Liu
Department of Electrical and Computer Engineering
McGill University
Montréal, Canada
jia-chen.liu@mail.mcgill.ca

Fabrice Labeau
Department of Electrical and Computer Engineering
McGill University
Montréal, Canada
fabrice.labeau@mcgill.ca

***Abstract*— Existing studies on False Data Injection Attacks (FDIAs), a type of stealth attacks against power grids aimed at compromising the system cyber-physical security, have primarily been conducted on wired systems in which state estimation is represented by overdetermined DC power flow models. The emerging trend of Smart Grid (SG) assisted by the widespread deployment of Wireless Sensor Networks (WSNs) for various new functionalities, on the other hand, calls for a review of how some certain well-established premises need to be adjusted in the new context. In addition to related studies based on traditional bus-based systems, certain broad changes brought by the use of WSNs in grid systems will be introduced in this paper. Subsequently, differences in terms of bad data detection (BDD), false data injection attack strategy or physical feasibility of attack methods caused by the shift of scenario will be compared and briefly analyzed. A summary of new or previously overlooked requirements for FDIA studies will then be appended. By presenting a comprehensive review of related studies we will shed light on potential future research directions.**

Keywords—Cyber-physical security, false data injection attacks, bad data detection, smart grid, wireless sensor networks.

I. Introduction

Since the proposal of the concept of false data injection attacks (FDIAs) on the state estimation component of power grids several years ago [1], industrial wireless sensor networks (WSNs) in smart grid (SG) are rapidly becoming popular for previously unimaginable consumer-end data collecting and processing needs. Coupled with the utilities' increasing demand for easy-to-deploy monitoring infrastructure especially for substations and non-consumer distribution components [2], this trend is seemingly far from negligible and calls for deeper examination.

In its early stages, the concept of smart grid was nearly equated to the advanced metering infrastructure (AMI). Incorporated with existing wired transmission and distribution networks and focusing on consumer-end data gathering, the "smart" feature has been viewed from perspectives relatively detached from utility automation and management.

However, the more recent trend predicts and calls for greater expansion of the deployment of sensor networks with more resemblance to off-the-shelf WSNs using existing and more mature protocols and components. All kinds of previously unavailable functionalities such as consumer-end pricing are on one hand putting grid automation and management through a transition phase with greater reliance on sensor data, and on the other hand leading to the inevitable scaling of the amount of data transferred, processed and stored throughout the WSNs.

Consequently, sensor node communication and measurement collection in the wireless scenario are more vulnerable and easier to access as they become more wide-spread and standardized. The consequent challenges will only become more severe and threatening as WSNs used in SG become ubiquitous and scaled up.

In this paper, we aim to provide a comprehensive review of the state-of-the-art studies in the field of FDIAs on power grid systems, and to describe up and coming challenges in this field. The remainder of this paper is organized as follows: Section II introduces the state estimation model the originally proposed potential attackers face and the methods they could employ to bypass bad measurement detectors, along with considerations raised by different attack scenarios and constraints. Section III presents the wireless case showing a drastically different picture for attackers compared to previously discussed wired systems. Existing works discussing FDIAs in the wireless scenario are also introduced in this section, followed by proposed directions for future research and the conclusion in Sections IV and V, respectively.

II. Introducing False Data Injection Attacks

The power grid itself consists of transmission and distribution networks across a usually large geographical area that spans all levels from power plants to substations, and, finally, to the customers as illustrated in Fig. 1.

A. The State Estimation Model and Bad Data Detection

Due to the critical nature of the grid infrastructure and the complexity of the system as a whole, the status of the power grid in most practical cases can only be estimated indirectly via the

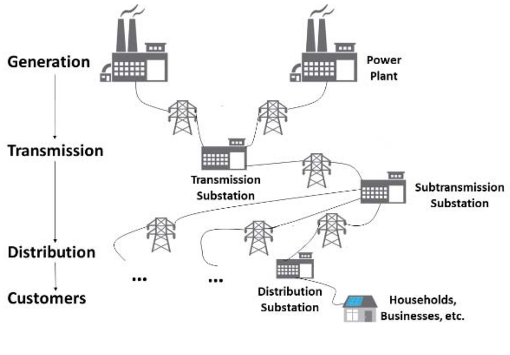

Fig. 1. Simplified illustration of the power grid hierarchy.

This work was supported by Hydro-Quebec, the Natural Sciences and Engineering Research Council of Canada, and McGill University in the framework of the NSERC/Hydro-Quebec Industrial Research Chair in Interactive Information Infrastructure for the Power Grid (IRCPJ406021-14).

readings of meters placed at or near certain components of the grid, as has been pointed out by Pasqualetti et al. [3]. This estimation process is known as state estimation, which takes the aforementioned meter readings (otherwise known as meter measurements or simply measurements) and grid settings such as the network topology as inputs and uses them to optimally approximate the unknown and usually hard-to-measure state variables of the grid. Typical state variables include a minimal but complete set of variables such as bus voltage angles, branch active power flows, and bus active power loads and generations when the DC power flow model is used [4], which we will elaborate on later. In turn, in the control center, to which the measurements are transmitted, the output state variables are used as important criteria maintain, adjust and safeguard the grid in operation. In addition, some of the measurements themselves, depending on the nature of the variables they represent, function as part of the state variable selection.

The state estimation process relies on power flow models. Specifically, the DC power model is usually applied due to its linear form, which has shown to be greatly beneficial to the simplification and regularization of the modeling effort. On the other hand, the AC power flow model takes into account of the effects of both the real and reactive power and is described by nonlinear equations, which can be difficult for the analysis of the state estimation problem and further, the modeling of FDIAs against the state estimation process. The state estimation model using both the AC and the DC power flow model can be respectively represented as follows:

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

$$\mathbf{z} = \mathbf{H}\mathbf{x} + \mathbf{e}, \tag{2}$$

where $\mathbf{z}_{\mathbf{m}\times\mathbf{1}} = (z_1, z_2 \dots, z_m)^T$, $\mathbf{x}_{\mathbf{n}\times\mathbf{1}} = (x_1, x_2 \dots, x_n)^T$, and $\mathbf{e}_{\mathbf{m}\times\mathbf{1}} = (e_1, e_2 \dots, e_m)^T$ are the measurements, state variables and measurement errors, respectively. $\mathbf{h}(\cdot)$ is a nonlinear m-vector function relating measurements to state variables in the AC model, whereas $\mathbf{H}_{m\times n}$ is a full-rank matrix denoting m linear functions linking measurements to state variables in the DC power flow model and corresponding to the network topology, etc. Several key facts vital to the characterization of the measurement problem described in (2) include:

- The DC power flow model, when perceived as a system of linear equations, is overdetermined. In other words, $m > n$ in (1) and (2), which is natural as the state variables are a minimal set.
- The measurement matrix $\mathbf{H}$ is usually sparse in practical networks [4], [5].
- The measurement errors in $\mathbf{e}$ are henceforth regarded to be mutually independent and normally distributed with zero mean.

We will mainly focus on the DC model for the remainder of this paper. Some works taking into account the AC model will be introduced but not elaborated in detail. As has been discussed in [5], [6], given the assumptions on error distributions mentioned above, the maximum likelihood, weighted least-square and minimum variance estimation criteria all converge to the minimum mean squared error (MMSE) estimator:

$$\hat{\mathbf{x}} = (\mathbf{H}^{\mathbf{T}}\mathbf{W}\mathbf{H})^{-1}\mathbf{H}^{\mathbf{T}}\mathbf{W}\mathbf{z}, \tag{3}$$

where $\mathbf{W} = diag(\sigma_1{}^{-2}, \sigma_2{}^{-2}, \dots, \sigma_m{}^{-2})$ and $\sigma_i{}^2$ is the variance of the zero-mean measurement error of the i-th meter.

The concept of bad measurement detection or bad data detection (BDD) comes from the assumption that the estimate of the state variables, such as that given in (3), is supposedly close to the original state variable values. The closer they are, the more accurate the estimate is considered to be. Hence, the 2-Norm of the measurement residual $\|\mathbf{z} - \mathbf{H}\hat{\mathbf{x}}\|$, which should follow a $\chi^2(m-n)$ distribution, was proposed as one of the benchmarks to determine whether or not the estimated state variables $\hat{\mathbf{x}}$ have been affected by bad measurements.

$$\|\mathbf{z} - \mathbf{H}\hat{\mathbf{x}}\| \underset{bad}{\overset{good}{\gtrless}} \tau, \tag{4}$$

where τ is the test threshold determined through a hypothesis test with a significance level of α, which in turn means when $\|\mathbf{z} - \mathbf{H}\hat{\mathbf{x}}\| \geq \tau$, bad measurements exist with a false alarm probability of α. Methodologically, this type of BDD scheme falls into the category of the $\mathrm{J}(\hat{\mathrm{x}})$-tests [7], while there are bad data-coping methods using other criteria. Indirect measures also exist. For instance, after normalization, the largest residuals could be numerically penalized to achieve estimation with bad data suppression [8].

B. Mechanism for False Data Injection Attacks

Such bad data detection schemes work well as long as the state variables are mutually independent, and the measurement errors are normally distributed as described above. However, with a different set of "smart" and carefully designed approaches given the appropriate knowledge of the grid system, attackers would be able to launch attacks bypassing the bad data detector and replacing the original measurements with false ones through compromised meters. The goal of these attacks is to cause errors in the state estimation process, and they are known by the name of false data injection attacks [1]. According to Li et al. [9], FDIAs can essentially be viewed as combinations of data attacks following previous successful device attacks, where the latter take control of the sensor nodes and the former then ensure the injection of malicious data to disrupt or deceive the state estimation of grid networks.

From the physical point of view, what the attackers can compromise in the case of grid state estimation are the meters only. Correspondingly in the mathematical model given in (2), the measurements $\mathbf{z}$ should be viewed as subjected to falsification. The measurement vector under attack can be represented as $\mathbf{z}_{\mathbf{bad}} = \mathbf{z} + \mathbf{a}$, where the non-zero attack vector $\mathbf{a}$ is injected by the attacker via compromised meters. In turn, the estimated state variables $\hat{\mathbf{x}}_{\mathbf{bad}}$ when FDIAs are launched are given as:

$$\begin{aligned}\hat{\mathbf{x}}_{\mathbf{bad}} &= (\mathbf{H}^{\mathbf{T}}\mathbf{W}\mathbf{H})^{-1}\mathbf{H}^{\mathbf{T}}\mathbf{W}\mathbf{z}_{\mathbf{bad}} \\ &= (\mathbf{H}^{\mathbf{T}}\mathbf{W}\mathbf{H})^{-1}\mathbf{H}^{\mathbf{T}}\mathbf{W}(\mathbf{z} + \mathbf{a}) \\ &= \hat{\mathbf{x}} + (\mathbf{H}^{\mathbf{T}}\mathbf{W}\mathbf{H})^{-1}\mathbf{H}^{\mathbf{T}}\mathbf{W}\mathbf{a}.\end{aligned} \tag{5}$$

Let $\mathbf{c} = \hat{\mathbf{x}}_{\mathbf{bad}} - \hat{\mathbf{x}} = (\mathbf{H}^{\mathbf{T}}\mathbf{W}\mathbf{H})^{-1}\mathbf{H}^{\mathbf{T}}\mathbf{W}\mathbf{a}$, then $\mathbf{c}$ should in turn be viewed as the deviation of the estimated state variables caused by the attack, and the 2-Norm of the measurement residual is now:

$$\begin{aligned} &\|\mathbf{z}_{\mathbf{bad}} - \mathbf{H}\hat{\mathbf{x}}_{\mathbf{bad}}\| \\ &= \|\mathbf{z} + \mathbf{a} - \mathbf{H}(\hat{\mathbf{x}} + (\mathbf{H}^{\mathbf{T}}\mathbf{W}\mathbf{H})^{-1}\mathbf{H}^{T}\mathbf{W}\mathbf{a})\| \\ &= \|(\mathbf{z} - \mathbf{H}\hat{\mathbf{x}}) + (\mathbf{a} - \mathbf{H}\mathbf{c})\|. \end{aligned} \quad (6)$$

in which, if $\mathbf{a} = \mathbf{Hc}$, $\|\mathbf{z}_{\mathbf{bad}} - \mathbf{H}\hat{\mathbf{x}}_{\mathbf{bad}}\| = \|\mathbf{z} - \mathbf{H}\hat{\mathbf{x}}\|$ and the bad data detector discussed previously would not be able to detect the existence of injected bad measurements. Such attacks are known as perfect FDIAs.

Alternatively, if $\mathbf{a} \neq \mathbf{Hc}$ but $\|\mathbf{z}_{\mathbf{bad}} - \mathbf{H}\hat{\mathbf{x}}_{\mathbf{bad}}\|$ remains sufficiently small, the attacker can still bypass the bad data detector. In such a scenario, the attack is a generalized FDIA.

While it has been shown that given the required information, it is feasible for the attacker to launch perfect or generalized FDIAs deterministically [5], in practical attack scenarios, the attacker may not have full knowledge nor access to the entire system. Particularly, major constraints for FDIA construction come in the following categories: amount of attacker's resources, in the form of limited numbers of measurements the attack is able to compromise [10]; accessibility of measurements, in the form of a subset of measurements that can potentially be compromised while the rest are not (especially when the network is heterogenous with specially secured nodes) [11]-[13] ; and knowledge of system configuration, in the form of the measurement matrix $\mathbf{H}$ [14]-[16] and implicitly, perhaps also the estimation process and the bad data detection mechanism as illustrated in Fig. 2.

Furthermore, the attacker may wish to minimize the impact of the FDIA launched in order to maximally delay or avoid alert being triggered [17], which is also an important factor to consider in practical attack schemes. This signals the common preference for "constrained" FDIAs, where the attacker is assumed to seek minimal collateral influence it causes to non-targets in the network (typically for economic attacks [18], [19]), over "unconstrained" ones aimed at causing congestion [20] or disruption [21].

On top of the aforementioned, Pasqualetti et al. [22] propose a distributed state estimation plus distributed FDIA detection scheme at the expense of a certain degree of extra hardware cost. Multiple control centers are assumed to be available to form local estimation and detection clusters, while the mathematical model described above is partitioned into smaller but structurally identical parts. Most of the listed works in this section present simulations conducted on IEEE bus systems, however, between the two modes of sensor node communication, i.e. incremental and diffusive, the latter does not assume any particular interconnection structure of the clusters but instead models omnidirectional data broadcasting, which resembles the mechanism of meshed WSNs and may be beneficial to future studies when WSNs in smart grid further scale and proliferate.

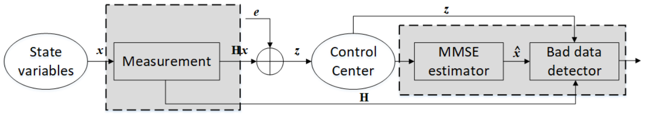

Fig. 2. Block diagram of typical grid static state estimation process with bad data detector, where the parts the attacker needs to know to launch perfect FDIAs are shaded.

III. FDIAs in the Wireless Scenario

The concept of false data injection has long been discussed for applications of wireless sensor networks [23]-[25], but not so much in the specific case of smart grid. Smart grid assisted by the widespread deployment of industrial WSNs for various functionalities is becoming a reality in the near future, and it calls for a review of certain common premises and rules in the past that need to be reconsidered in the new context.

Transmission over potentially noisy wireless channels has to be taken into account as sensor node readings can no longer be assumed to be what the gateway directly receives, contrary to the wired case. In fact, the entire outlook of the system model is changed significantly, in that sensor readings, whether corrupted by FDIAs or not, need to go through an entire layer of management (which usually involves a forwarding or more complex aggregation scheme) and interference to reach the network gateway. Consequently, this offers researchers two applicative domains of WSNs in SG to further explore: the state estimation, only different in that the measurements are wirelessly transmitted, and more or less general-purpose functionalities such as premise monitoring, price report, consumer-end management, etc. [26].

A. FDIAs against Grid State Estimation WSNs

For FDIAs in the context of distributed state estimation WSNs, whether applied in smart grid or not, this means the wireless data gathering process needs to be somehow combined with the state estimation model. A number of works model the state estimation process as discrete-time linear time-invariant (LTI) systems, as described by the equations similar to

$$\mathbf{x}(k+1) = \mathbf{A}\mathbf{x}(k) + \mathbf{B}\mathbf{w}(k) + \mathbf{E}\mathbf{p}(k), \quad (7)$$

$$\mathbf{z}_{i}(k) = \mathbf{C}_{i}\mathbf{x}(k) + \mathbf{v}_{i}(k), \quad (8)$$

where $\mathbf{x}(k)$ is the vector of state variables at time step k, $\mathbf{w}(k)$ is the process noise at time step k, and the initial states are represented as $\mathbf{x}(0)$. $\mathbf{A}$ and $\mathbf{E}$ are matrices determined by the network and the environment the network operates in. At sensor node i, the local measurement vector $\mathbf{z}_{i}(k)$ is generated and updated according to the local measurement matrix, usually determined by the connection topology, and the corresponding state variables, whereas $\mathbf{v}_{i}(k)$ is the local measurement noise.

In many of the works that utilize such models, the essence of the estimation model and bad data detection model remain unchanged when compared to the wired case [27]-[29]. For example, Mo et al. [27], as well as many others, still regard the noise as independent and normally distributed with zero mean, which is identical to the premise given in (2) and (3), although this is hardly true for certain types of WSN applications. For instance, collisions taking place in the MAC layer of sensor networks lead to loss (or potentially corruption) of some data, which clearly cannot be well represented by a Gaussian noise [30]. Factors including data correlation [31], aggregation schemes [32] and operative environment (a moving vehicle in the case of [27]) are all potentially required to be taken into consideration in this regard.

Furthermore, as the discrete LTI system model brings the time dimension into the picture, whereas in the wired case static state estimation can harbor a greater deal of temporal redundancy, many of the related works are confined to only discuss extremely small-scale systems. The work by Mo et al., again, only considers a 2×2 measurement matrix in the speed-acceleration sensing application employing a Kalman filter-based estimation scheme [27]. Lei et al. and Guan and Ge, on the other hand, discussed similarly small systems (5 and 4 sensors, respectively) [28], [29].

B. FDIAs against Other Generic Grid WSN Applications

For more generalized WSN applications, the problem becomes more like a data aggregation problem with the presence of FDIAs. In this case, the low deployment cost will lead to more and more severe scaling of sensor nodes unless the scope of application is determined to be limited to begin with, as has been practiced by Namboodiri et al. [33] where nothing beyond the home-area network (HAN) is considered. When the number of sensors scales up, the cost of most data forwarding schemes would quickly turn prohibitive as these schemes usually simply forward data "as is", while communication could easily cost about 70% of the total network energy consumption [34], [35]. As a result, data aggregation, which employs the idea of in-network processing [36], i.e. combining and compressing while transmitting data appears to be much more desirable as the size of WSNs soars. Nevertheless, at the current stage, new studies are still being produced regarding simpler wireless relay networks, such as [37] (where a one-way, two-hop network is considered).

For this type of studies, higher-level techniques and considerably more complicated network structures are widely used to counter potentially malicious false data injections. Ozdemir and Çam [35], for example, propose to use nodes between any pair of intermediate data aggregator nodes to check encrypted data and aim to guarantee the data integrity of a deterministic number of nodes, instead of trying to statistically minimize the FDIA threat. A three-phase network scheme (initialization, data aggregation, and attestation of compromised nodes) is proposed by Boonsongskrikul et al. [38] in which a hierarchical aggregation tree with considerable sensor node redundancy (for dedicated attestation purposes only) is presented. Wang et al. [39] on the other hand seek to utilize authentication key pairs and message authentication codes (MACs) to detect possible false data injection. It is, however, noteworthy to point out that among existing studies, this one has actually shown simulations on a sufficiently large network with 400 sensors, up to 10 of which are modeled to be compromised.

Lower-level approaches have also been presented. In another work focusing on HAN wireless systems, Islam and Koo [40] proposes that since sensor activity can usually be expected to be sparse in many WSN applications such as premise monitoring, it would be desirable if the sparsity could be exploited in the form of maximizing data compression and minimizing the communication overhead during the data aggregation process. As a result, the idea of compressed sensing [41] is utilized to achieve a significant save on the energy consumption of the data gathering process. However, in terms of scalability, the mere 22-node ZigBee HAN with impractical bipolar (0-1) data input shows clear limitations.

The data aggregation models in many studies of this kind is often similar to $\mathbf{z} = \mathbf{Hx} + \mathbf{e}$ at a given time instant, seemingly similar to that of static state estimation in wired grid systems, However, some significant differences exist:

TABLE I. DIFFERENT IMPLICATIONS OF VARIABLES IN FORMALLY SIMILAR WIRED AND WIRELESS GRID SENSOR NETWORK MODELS

	Wired Scenario	**Wireless Scenario**
$\mathbf{x}$	Grid state variables: voltage angles of all buses, etc.	Sensor readings: varied but largely zero due to energy constraints in many cases
$\mathbf{z}$	Meter measurements: real power projections of all buses, real power flows, etc.	Aggregated and propagated data
$\mathbf{H}_{\mathbf{m}\times\mathbf{n}}$	Determined by grid topology, sparse; $m > n$	Determined by wireless channels and aggregation scheme; $m \ll n$
$\mathbf{e}$	Abstracted normally distributed measurement errors in most cases	Could be irregularly-distributed depending on the situation

IV. FUTURE RESEARCH DIRECTIONS

In this section, we avoid suggesting areas of research in the field of FDIAs against state estimation in wired grid networks, which is readily available in many previous reviews and summaries, particularly a fairly recent one by Liang et al. [17]. Instead, we focus on the specific issues raised by the increasing reliance of smart grid on wireless sensor networks.

First of all, scaling of the network is more and more recognized as the inevitable trend. Coupled with the openness, accessibility and commonality of both the wireless network as a whole and the wireless sensor nodes constituting the network, attackers may now be able to compromise more network components with less difficulty. How to trade-off between keeping large WSNs especially the data aggregation part simple (and hence less costly) and making the networks sufficiently secure (which usually corresponds to the degree of network sophistication) should be a top priority. For instance, in-network processing techniques for data aggregation such as network coding could be utilized to ease the scaling issue by reducing the communication overhead, while the consequent data correlation may be used for locating data inconsistencies caused by FDIAs.

The wireless transmission process in either state estimation or other WSN applications within the scope of smart grid brings yet another layer of complication and difficulties, since in the wired static state estimation model measurements are what the control center directly reads. Channel degradation and interference are issues to be taken into account for practical studies on FDIAs, especially as researchers have to put themselves first in the shoes of potential malicious attackers, who may now have previously non-existent problems such as acquiring accurate information about the effective measurement process (affected by possibly changing wireless channels), to design and analyze patterns and effects of the attacks, and then to switch perspectives to further develop detection and defense schemes for utilities.

Furthermore, certain less frequently discussed features that could be found in smart grid WSN applications can be exploited. For example, sparsity of sensor node activity combined with prominently underdetermined aggregation process leaves room for theories like compressed sensing to operate.

V. Conclusions

In this paper, we have presented a review of existing research on FDIAs against smart grid sensor networks. We have introduced both the case of FDIAs against state estimation in more traditional wired systems and that of the emerging wireless scenario where WSNs are heavily relied on. Challenges as well as opportunities brought by new or previously overlooked issues such as massive scaling, sensor activity sparsity and non-Gaussian error varieties have been presented and briefly analyzed, which to our knowledge has not been done systematically before. Finally, we offered a summary of potential research directions regarding for future studies in this field.

References

[1] Y. Liu, P. Ning, and M. K. Reiter, "False data injection attacks against state estimation in electric power grids," in Proceedings of the 16th ACM Conference on Computer and Communications Security, 2009, pp. 21–32.

[2] G. Liang, S. R. Weller, J. Zhao, F. Luo, and Z. Y. Dong, "The 2015 Ukraine blackout: implications for false data injection attacks," IEEE Trans. Power Syst., vol. 32, no. 4, pp. 3317–3318, 2017.

[3] F. Pasqualetti, F. Dörfler, and F. Bullo, "Attack detection and identification in cyber-physical systems," IEEE Trans. Automat. Contr., vol. 58, no. 11, pp. 2715–2729, 2013.

[4] A. Monticelli, State Estimation in Electric Power Systems: A Generalized Approach. New York, NY: Springer Science & Business Media, 1999.

[5] 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, pp. 13:1--13:33, 2011.

[6] A. J. Wood and B. F. Wollenberg, Power Generation, Operation, and Control. New York, NY: John Wiley & Sons, 1996.

[7] V. H. Quintana, A. Simoes-Costa, and M. Mier, "Bad data detection and identification techniques using estimation orthogonal methods," IEEE Trans. Power Appar. Syst., vol. PAS-101, no. 9, pp. 3356–3364, 1982.

[8] H. M. Merrill and F. C. Schweppe, "Bad data suppression in power system static state estimation," IEEE Trans. Power Appar. Syst., no. 6, pp. 2718–2725, 1971.

[9] X. Li, I. Lille, X. Liang, R. Lu, X. Shen, X. Lin, and H. Zhu, "Securing smart grid: cyber attacks, countermeasure, and challenges," IEEE Commun. Mag., vol. 50, no. 8, pp. 38--45, 2012.

[10] R. Bobba, K. Rogers, Q. Wang, H. Khurana, K. Nahrstedt, and T. Overbye, "Detecting False Data Injection Attacks on DC State Estimation," in 1st Workshop on Secure Control Systems, Stockholm, Sweden, 2010.

[11] J. Chen and A. Abur, "Placement of PMUs to enable bad data detection in state estimation," IEEE Trans. Power Syst., vol. 21, no. 4, pp. 1608–1615, 2006.

[12] S. Cui, Z. Han, S. Kar, T. T. Kim, H. V. Poor, and A. Tajer, "Coordinated data-injection attack and detection in the smart grid: a detailed look at enriching detection solutions," IEEE Signal Process. Mag., vol. 29, no. 5, pp. 106–115, 2012.

[13] H. M. Khalid and J. C. H. Peng, "Immunity toward data-injection attacks using multisensor track fusion-based model prediction," IEEE Trans. Smart Grid, vol. 8, no. 2, pp. 697–707, 2017.

[14] M. Esmalifalak, H. Nguyen, and R. Zheng, "Stealth false data injection using independent component analysis in smart grid," in 2011 IEEE Int. Conf. Smart Grid Commun. (SmartGridComm), Brussels, Belgium, 2011, pp. 244–248.

[15] M. A. Rahman and H. Mohsenian-Rad, "False data injection attacks with incomplete information against smart power grids," in 2012 IEEE Glob. Commun. Conf., Anaheim, CA, 2012, pp. 3153–3158.

[16] V. Kekatos, G. B. Giannakis, and R. Baldick, "Grid topology identification using electricity prices," in Proc. IEEE Power and Energy Society General Meeting, National Harbor, MD, Jul. 2014, pp. 1–5.

[17] G. Liang, J. Zhao, F. Luo, S. R. Weller, and Z. Y. Dong, "A review of false data injection attacks against modern power systems," IEEE Trans. Smart Grid, vol. 8, no. 4, pp. 1630–1638, 2017.

[18] L. Xie, Y. Mo, and B. Sinopoli, "False data injection attacks in electricity markets," in Smart Grid Communications (SmartGridComm), 2010 First IEEE International Conference on, Gaithersburg, MD, 2010, pp. 226–231.

[19] A. Tajer, "False data injection attacks in electricity markets by limited adversaries: stochastic robustness," IEEE Trans. Smart Grid, vol. PP, no. 99, pp. 1-1, 2017.

[20] L. Jia, J. Kim, R. J. Thomas, and L. Tong, "Impact of data quality on real-time locational marginal price," IEEE Trans. Power Syst., vol. 29, no. 2, pp. 624–636, 2014.

[21] Y. Yuan, Z. Li, and K. Ren, "Modeling load redistribution attacks in power systems," IEEE Trans. Smart Grid, vol. 2, no. 2, pp. 382–390, 2011.

[22] F. Pasqualetti, R. Carli, and F. Bullo, "A distributed method for state estimation and false data detection in power networks," in 2011 IEEE Int. Conf. Smart Grid Commun. (SmartGridComm), Brussels, Belgium, 2011, pp. 469–474.

[23] S. Zhu, S. Setia, S. Jajodia, and P. Ning, "An interleaved hop-by-hop authentication scheme for filtering of injected false data in sensor networks," in IEEE Symposium on Security and Privacy, Berkerly, CA, 2004, pp. 259–271.

[24] F. Ye, H. Luo, S. Lu, and L. Zhang, "Statistical en-route filtering of injected false data in sensor networks," in Proc. IEEE INFOCOM 2004, Hong Kong, China, 2004, vol. 4, pp. 2446–2457.

[25] Z. Yu and Y. Guan, "A dynamic en-route scheme for filtering false data injection in wireless sensor networks," Proc. IEEE INFOCOM 2006, Barcelona, Spain, 2006, pp. 1–12.

[26] K. C. Budka, J. G. Deshpande, and M. Thottan, Communication Networks for Smart Grids: Making Smart Grid Real. London, UK: Springer, 2014.

[27] Y. Mo, E. Garone, A. Casavola, and B. Sinopoli, "False data injection attacks against state estimation in wireless sensor networks," in Proceedings of the IEEE Conference on Decision and Control, Atlanta, GA, 2010, pp. 5967–5972.

[28] Y. Guan and X. Ge, "Distributed attack detection and secure estimation of networked cyber-physical systems against false data injection attacks and jamming attacks," IEEE Trans. Signal Inf. Process. over Networks, vol. PP, no. 99, pp. 1–1, 2017.

[29] L. Lei, W. Yang, C. Yang, H. Shi, and H. Yan, "False data injection attack on distributed state estimation over a wireless sensor network," in 35th Chinese Control Conf. (CCC), Chengdu, China, 2016, pp. 8108–8113.

[30] S. Ghazanfari-Rad and F. Labeau, "Diffusion least-mean squares over distributed networks in the presence of MAC errors," in 2012 Conference Record of the Forty Sixth Asilomar Conference on Signals, Systems and Computers (ASILOMAR), Pacific Grove, CA, 2012, pp. 1787–1791.

[31] S. Yoon and C. Shahabi, "Exploiting spatial correlation towards an energy efficient clustered aggregation technique," in IEEE International Conference on Communications, Seoul, S. Korea, 2005, vol. 5, pp. 1–20.

[32] M. Nabaee and F. Labeau, “Restricted isometry property in quantized network coding of sparse messages,” in GLOBECOM - IEEE Global Telecommunications Conference, Anaheim, CA, 2012, pp. 112–117.

[33] V. Namboodiri, V. Aravinthan, and W. Jewell, “Toward a secure wireless-based home area network for metering in smart grids,” IEEE Syst. J., vol. 8, no. 2, pp. 509–520, 2014.

[34] A. Perrig, R. Szewczyk, J. D. Tygar, V. Wen, and D. E. Culler, “SPINS: security protocols for sensor networks,” Wirel. networks, vol. 8, no. 5, pp. 521–534, 2002.

[35] S. Ozdemir and H. Çam, “Integration of false data detection with data aggregation and confidential transmission in wireless sensor networks,” IEEE/ACM Trans. Netw., vol. 18, no. 3, pp. 736–749, 2010.

[36] H. Karl and A. Willig, Protocols and Architectures for Wireless Sensor Networks. Chichester, England: John Wiley & Sons, 2006.

[37] X. Liu, Y. Guan, and S. W. Kim, “Bayesian test for detecting false data injection in wireless relay networks,” IEEE Commun. Lett., vol. PP, no. 99, pp. 1–1, 2017.

[38] A. Boonsongsrikul, K. Lhee, and M. Hong, “Securing data aggregation against false data injection in wireless sensor networks,” in 2010 The 12th International Conference on Advanced Communication Technology (ICACT), Phoenix Park, South Korea, 2010, pp. 29–34.

[39] J. Wang, Z. Liu, S. Zhang, and X. Zhang, “Defending collaborative false data injection attacks in wireless sensor networks,” Inf. Sci. (Ny)., vol. 254, pp. 39–53, 2014.

[40] T. Islam and I. Koo, “Compressed Sensing-based data gathering in wireless Home Area Network for smart grid,” in 2012 Int. Conf. Informatics, Electron. Vis., Dhaka, Bangladesh, 2012, pp. 82–86.

[41] D. L. Donoho, “Compressed sensing,” Inf. Theory, IEEE Trans., vol. 52, no. 4, pp. 1289–1306, 2006.