Inference of Tampered Smart Meters with Validations from Feeder-Level Power Injections

Yachen Tang*, Chee-Wooi Ten†, and Kevin P. Schneider‡
*Global Energy Interconnection Research Institute North America, San Jose, CA 95134 USA
†Michigan Technologial University, Houghton, MI 49931 USA
‡Pacific Northwest National Laboratory, Richland, WA 99352 USA

***Abstract*—Tampering of metering infrastructure of an electrical distribution system can significantly cause customers' billing discrepancy. The large-scale deployment of smart meters may potentially be tampered by malware by propagating their agents to other IP-based meters. Such a possibility is to pivot through the physical perimeters of a smart meter. While this framework may help utilities to accurately energy consumption information on the regular basis, it is challenging to identify malicious meters when there is a large number of users that are exploited to vulnerability and kWh information being altered. This paper presents a reconfiguration switching scheme based on graph theory incorporating the concept of distributed generators to accelerate the anomaly localization process within an electrical distribution network. First, a data form transformation from a visualized grid topology to a graph with vertices and edges is presented. A conversion from the graph representation to machine recognized matrix representation is then performed. The connection of the grid topology is illustrated as an adjacency or incidence matrix for the following analysis. A switching procedure to change elements in the topological matrix is used to detect and localize the tampered node or cluster. The procedure has to meet the electrical and the temporary closed-loop operational constraints. The customer-level anomaly detection is then performed in accordance with probability derived from smart meter anomalies.**

***Index Terms*—Advanced metering infrastructure, tampering detection, switching scheme, distributed generators.**

I. Introduction

ENERGY thieves have been known as the major pitfalls for developing countries as the illegal electricity users are not part of the payment to utilities [1]. Similarly, alteration of individual's electronic energy usage on a smart meter is a covert, fraudulent behavior. Such motivation is to avoid full payment over the course of a long period of time. While smart meters provide the technology to conveniently obtain kWh information to utility billing center, poor physical perimeters may enable individuals to tamper the smart meters. Collectively, such an attack can get more creative that may be propagated through the Intranet of all associated smart meter devices to be enumerated by pivoting through a compromised smart meter [2], [3]. Massive tampering can occur within the home area network (HAN) and neighborhood area network (NAN). Although this may not affect overall reliability of a distribution network, it would implicate the collection of monthly payments from utility's customers, leading to significant lower revenue as part of the financial losses [4], [5]. On the other extreme, the discrepancy may trigger complaints by other customers who do not use usage much but amplified by the malware agents to significantly higher usage.

The metering data has the risk of being tampered during the process of measurement, collection, storage, or transmission while the malware or the worm propagation is usually embedded in the data string of the plausible legitimate metering data. In time-critical communications, the data collection devices usually have access for security, the inquire of data is restricted. Therefore, it is hard to detect the existed malware in these devices. Mike Davis demonstrated the speed of the malware can break a smart meter's safeguard and worms propagation through the loophole in 2009 at Blackhat [6] while the Stuxnet worm attacked the metering units in the power system in 2010 [7], [8]. Different than conventional malicious attacks, several smart meters might share the same identity number or a mechanical unit may generate one or more additional identity number to cause Distributed Denial-of-Service (DDoS) attack. DDoS only affects the unavailability of smart meters. However, this attack can be utilized to reduce the share of resources in the topology and give attackers more information to perform other attacks [9], [10]. A McAfee report warned that an attacker could exploit smart meters easily and takes control of the whole system [11]. Since the system specifications, diverse network protocols, and operational constraints in AMI, the existing defense methods against malicious attacks cannot be applied directly. The main motivation of this work is not to provide a defend method to improve the cybersecurity of the grid network. It proposed a switching operation scheme to detect and localize the occurred attacks or tampering behaviors within a distribution system.

An assumption is that the AMI and SCADA systems have been fully deployed in the test area, however,the SCADA was developed using a comprehensive security policy to protect the system from the cyber attacks or any other threatens, while the validation for smart meters remains in the early stage. The main contribution of this paper is to combine the tamper detection method with the topology reconstruction switching procedure to locate subfeeder or clusters with malicious meters in a distribution system. The distributed generators are considered in this study to reduce the switching combinations. The rest of this paper is structured as follows: Related works are presented in Section II. The switching strategies are formularized in Section III. A case study with a virtual distribution network is discussed in Section IV. The

This work is supported by US National Science Foundation (NSF) projects 1541000 and State Grid Corporation Technology Project 5455HJ180018.

conclusion and the future work are presented in Section V.

II. Related Work

Researchers to prevent anomalous electricity usages have done many existing methods. Artificial intelligence based machine learning and big data analysis [12] have been widely used for intelligent data analysis and data mining to identify normal consumption patterns, thus an obvious deviation between the normal pattern and the measuring data can be considered as an anomaly. Authors in [13] using machine learning techniques on the past data to built models for detecting anomalous meter readings. A distributed intelligent framework using benford's law and stackelberg game to detect electricity theft was proposed in [14]. A technique can identify diverse forms and caused deviations from tampered activities by using artificial neural networks [15] and Kalman filter [16]. The abnormal reports from the load areas with high tampered probabilities can be trained in support vector machine (SVM) [3] for classification. Another main strategy of detecting malicious meters is based on the real-time comparison. In [17], the (feeder) remote terminal unit (RTU/FRTU) provides a strategy to narrow down the search area for energy theft in a smart community. Also, [2] compares the real values with the predicted results to infer the possible tampered activities. The methods to distinguish the legitimate data from metering devices and the malware-carrying data string and using a disassembler to assist mathematical analysis are described in [18]. Different than data based detection approaches, [19] provides the attack and intrusion detection mechanism for a smart grid neighborhood area network (NAN). In addition, some strategies based on graph theory have been developed. In [20], a novel inspection algorithm identifies each meter with a unique binary-coded number to locate the unique malicious meter is proposed. The conversion between the power grid and binary tree or spanning tree is adopted in [3]. Sensors can also be used to detect anomalies in customer levels and even in networks and communication levels. However, the deploy and maintenance fee of a complete sensor system could be expensive and false alarms may occur in the inspection process [21].

The reconfiguration switching scheme in the distribution system is mainly applied for the emergency operation and optimization process [22]. The main purpose to exploit this problem is to achieve optimization. In [23], the authors deal with the problem existed in the radial topology of the distribution network with minimum losses while [24], [25] demonstrated a strategy to optimize the cost for equipment and devices installation and maintenance via changing the states of switching devices. In [26] introduces methods to restore maximum load with minimum steps of switching procedures.

III. Switching Strategies for Tampered Node Localization

The profile-based anomaly detection to detect the irregularity of potentially tampered data by comparing the summation of all smart meters results with the metering result shown in the FRTU at the feeder head [27]. If the offset is quite different (much larger or smaller) than the pre-defined threshold, the reconfiguration switching scheme is utilized to localize the subfeeder, microgrid [28], cluster, or the distribution node with tampered load(s) or malicious meter(s). Since the operational complexity and the cost during the topological reconfiguration, the proposed method is performed once the discrepancy is larger than 20% of the normal power consumption (which will cause massive tampering). All electrical utilities keep the power on during the switching procedures while meeting the closed-loop electrical and operational constraints in the distribution grid [29], [30].

A. Convert the Distribution Network To a Graph

A distribution grid is a radial topology and constructed by different feeders and microgrids. The adjacent feeders are connected with each other through tie switches (normally open and can be closed under emergency situation). The distribution grid can be represented by a graph $G = (V, E)$, which only contains nodes and edges. In G, all distributed power resources and loads are denoted as nodes/vertices V while all nodes are connected by feeder lines with openable tie switches, which are referred to as edges E. The graph is stored in matrix form (adjacency and/or incidence matrix) to straightforward demonstrate the connection relationships between nodes and edges [31].

An example of a distribution network with two feeders and the corresponding adjacency and incidence matrices are shown in Fig. 1. The sparse visualization of the adjacency and incidence matrices for the provided virtual topology is also illustrated in Fig. 1. The $FRTU_1$ is responsible to monitor the consumption states of all customers in the blue area while the $FRTU_2$ metering the green area. The detailed structure of the secondary network (customer level) for each load is shown in the gray block. In other words, the metering results in FRTU should be equal or slightly different than the summation of all smart meters' results under the supervised zone. It should be noted that the order of vertices and edges may change the form of matrices but can not change the topology of the graph. In this example, the order of vertices following the numbering sequence in this figure while the S_1 to S_5 represent edges 2 to 7. The $FRTU_1$ and $FRTU_2$ represent edge 1 and 7, respectively. Two vertices V_3 and V_4 and their connection S_1 (edge 2) is displayed on the visualized sparse matrices. The nonzero elements of these two matrices represent the number of edges in the graph. Since the graph is undirected, each edge is counted twice. This example is used for the case study in this paper.

B. Tampered Node Localization with Switching Strategies

The Algorithm 1 illustrates the iterative process of how the node with tampered load(s) is localized based on the distribution switching procedure. The detailed descriptions of variables are shown as below:

- M_i Topological incidence matrix to represent the connection states between nodes: i is denoted as a node/vertex and j denoted as an edge. If node i is connected

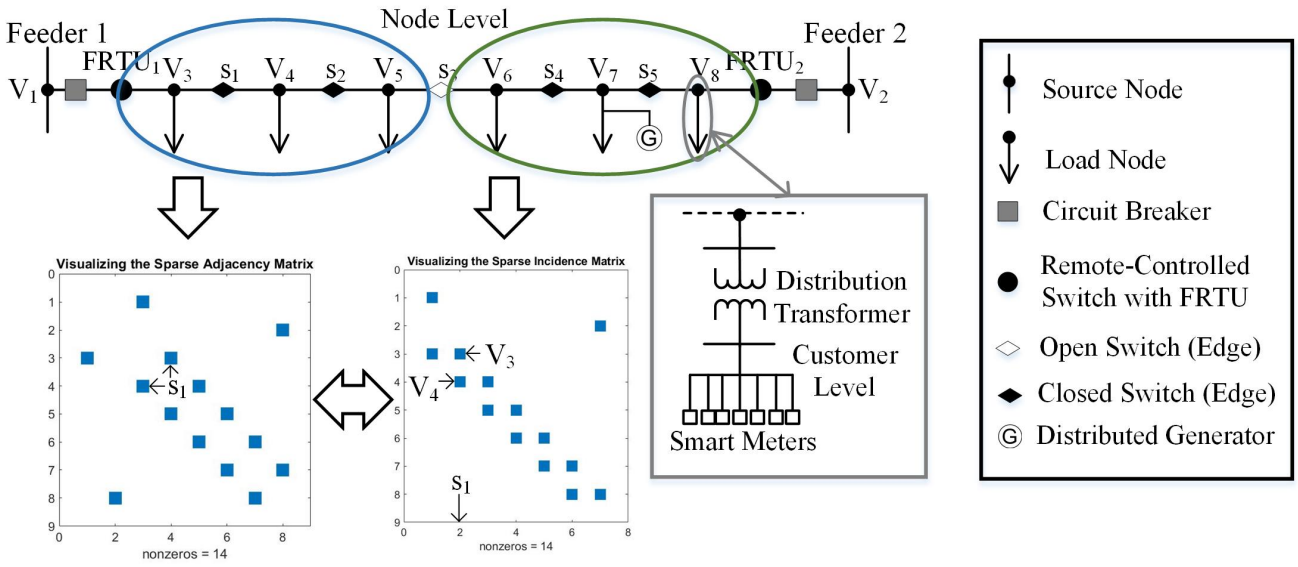

Fig. 1: Sparse visualization of the adjacency and incidence matrices for the provided virtual topology.

by edge j to other node(s), $M_i[i,j] = 1$, otherwise, $M_i[i,j] = 0$.

M_a Topological adjacent matrix to represent the connection states between nodes: both i and j are denoted as nodes/vertices. If node i is connected with node j , $M_a[i,j] = 1$, otherwise, $M_a[i,j] = 0$.

V_r A defined row vector with length $|E|$ to indicate the connection states (open or close) of switches (edges) in the distribution topology. If switch i is open $V_r[i] = 0$, otherwise, $V_r[i] = 1$.

V_s A defined row vector with length $|V|$ to indicate the locations of all distributed power resources in the distribution topology. If node i connected with a power source, $V_s[i] = 1$, otherwise, $V_s[i] = 0$.

I_f Index of RTU/FRTU that indicates there exists tampered load(s).

V_g A defined row vector with length $|V|$ to indicate the location of distributed generators. If vertex i connected with a distributed generators, then $V_g[i] = 1$, otherwise, $V_g[i] = 0$.

The algorithm starts with balancing the benefits of detecting the fraud, only the detected power losses are more than 20%, the process is performed. The algorithm is summarized as follows:

1) Isolate all subfeeders or clusters with distributed generators, if I_f shows no tampered load(s), the tampered load(s) exists in the isolated subfeeders or clusters.
2) Restore the connection of each microgrid sequentially and check I_f to identify which microgrid has the tampered load(s).
3) If the tampered load(s) is not in the isolated area, perform the iteration function to localize the tampered node.
4) Convert the topological incidence matrix to adjacency form and update the current states of all switches for detecting the possible tampered node;
5) Initialize V_f with V_s and set $\widehat{V}_f$ as the previous iteration result of V_f and initialize $\widehat{V}_f$ with 0;
6) Check the status of every node during each iteration by checking $V_f = \widehat{V}_f$;
7) If values of all nodes in the row vector are unchanged in the following iterations, use 1 to replace all nonzero elements in V_f;
8) If there are more than one tampered nodes within a single feeder, update I_f to generate a new V_r and then repeat $F_f\ (M_i, V_r, V_s, I_f)$;
9) Return V_f;
10) 0 element(s) in V_f to represent the location(s) of tampered node(s).

C. Customer-Level Anomaly Detection

In this study, we assume all customers have smart meters. Continue the profile-based tampering detection process in consumers' level by comparing the historical consumption records with the current period report after the localization of tampered node in the load (or lumped load) level. The anomaly score and the attacking probability of smart meters will be considered at the beginning of the customer-level anomaly detection to improve the searching efficiency. The searching process will start from the distribution node covers the smart meters with the highest anomaly index. The anomaly score of the smart meter can be estimated by a statistical approach. The ratio between the recorded number of anomalous readings and the total number of readings over a test period represents the score. The anomaly score can be represented as (1):

$$S_{\mathrm{a}} = \frac{N_{\mathrm{a},t}}{N_{\mathrm{r},t}} \tag{1}$$

where $N_{\mathrm{a},t}$ is number of anomalous readings of a smart meter in a time duration t and $N_{\mathrm{r},t}$ represents the total number of metering results.

Algorithm 1 Tampered Node Localization Algorithm

Input:
M_i, V_r, V_s, I_f
Isolate all subfeeders or clusters with distributed generators.
if I_f shows no tampered load(s) in this system. **then**
  $V_f = V_g$.
  Restore the connection of each subfeeder or cluster sequentially and check I_f.
else
Iteration Fuction: $F_f\ (M_i, V_r, V_s, I_f)$
  $V_r(I_f) = 0$;
  ▷ V_r keeps updating;
  ▷ Convert the topological incidence matrix to adjacency form and update the current states of all switches;
  $M_i \leftarrow M_i \cdot V_r^T$.
  $M_a \leftarrow M_i \cdot M_i^T$.
  Replace all diagonal elements in M_a with 0.
  ▷ Initialization;
  $V_f \leftarrow V_s$.
  $\widehat{V}_f \leftarrow V_f \cdot 0$.
  ▷ Check if the status is same as the previous iteration.
  while $V_f - \widehat{V}_f \neq 0$ **do**
    $\widehat{V}_f \leftarrow V_f$.
    $V_f \leftarrow \widehat{V}_f \cdot M_a + \widehat{V}_f$.
  end while
  Replace all nonzero elements in V_f with 1.
  return V_f.
  ▷ Localize the tampered node.
  Find all 0 elements in V_f.
  while More than one tampered nodes in one feeder, change I_f to generate a new V_r. **do**
    Repeat $F_f\ (M_a, V_r, V_s, I_f)$.
  end while
end if

Assume the alarm system in each smart meter is sensitive, the attacking probability indicates the probability that an alarm occurs during a time duration of t, which can be estimated as (2):

$$P_{\mathrm{a}} = 1 - \prod (1 - Q_m),\ m = 1, 2, 3, \cdots . \tag{2}$$

where Q_m represents the occurrence probability of type m alarm, which can be estimated from the statistics and observations of archived data. There might be more than one tampering on one node.

IV. A Case Study

A test case is utilized to validate the proposed strategy for detecting tampered meters based on the switching procedure. The schemes of changing connection status of switches in the distribution topology have to keep the whole system power on and meet the electrical and operational constraints.

A. Test Case Description

Fig. 2 is the topology of the distribution test network. There are two feeders and six load nodes. The two remote-controlled switches at each feeder head are deployed with a FRTU. An alarm system based on the profile-based tampering detection is also installed in FRTU. The load node with the distributed generator can generate the microgrids. A random generated massive tampering alarm is sent from $FRTU_2$.

The corresponding input incidence matrix can be gathered from the previous section. The input row vectors of the first scenario in Fig. 2 are as $V_s = [1\ 0\ 0\ 0\ 0\ 0\ 0\ 1]$ since V_1 and V_2 are two power sources; $V_r = [1\ 1\ 1\ 0\ 1\ 1\ 1]$ due to the normally open tie switch S_3; $I_f = 7$ for the random fraud alarm and $V_g = 7$ because of the distributed generator. In the second scenario, the V_s, I_f, and V_g remain unchanged while $V_r = [1\ 1\ 1\ 1\ 0\ 0\ 1]$ since the switching procedure.

B. Switching Procedures

Since the topology of the test system keeps unchanged, the input incidence matrix has no changes. The difference between each iteration is the updated connecting status V_r.

1) Step 1: Under the operational constraints, connect the tie switch between these two feeders in order to keep the test system power on during this procedure.

2) Step 2: Isolate the load node V_6 since it connected with a distributed generator which can supply the power for this microgrid.

3) Step 3: Perform the profile-based tampering detection at $FRTU_2$, if $FRTU_2$ shows normally, the tampered loads are not in V_7.

4) Step 4: Perform the profile-based tampering detection at $FRTU_1$, if $FRTU_1$ shows normally, the tampered loads are in V_6; If not, the tampered loads are in V_5.

In this work, a simple virtual distribution network is applied, since the key point of the proposed method is to find out the best sequence of the switching procedure and change the states of openable edges, the different sequence will cause different searching time: the time could be exponential or only spend a linear time in a real distribution network. This is the preliminary work that intends to prove the feasibility of the proposed idea.

V. Conclusion and Future Work

In this paper, a new application is presented to infer tampered node within distribution AMI network using graph-theoretic framework. The data-based tampering detection method is utilized to help indicate the existing of attacks or tampered activities in the system. The consideration of subfeeders, clusters, or microgrids with distributed generators will reduce the number of combinations during the switching procedures that can accelerate the localization of the spot with energy theft. In the process of localizing the tampered load node, the distribution network is converted to a graph only contains vertices and edges. The graph is demonstrated as incidence or adjacency matrix for the analysis. A localization of tampered nodes within a network is introduced.

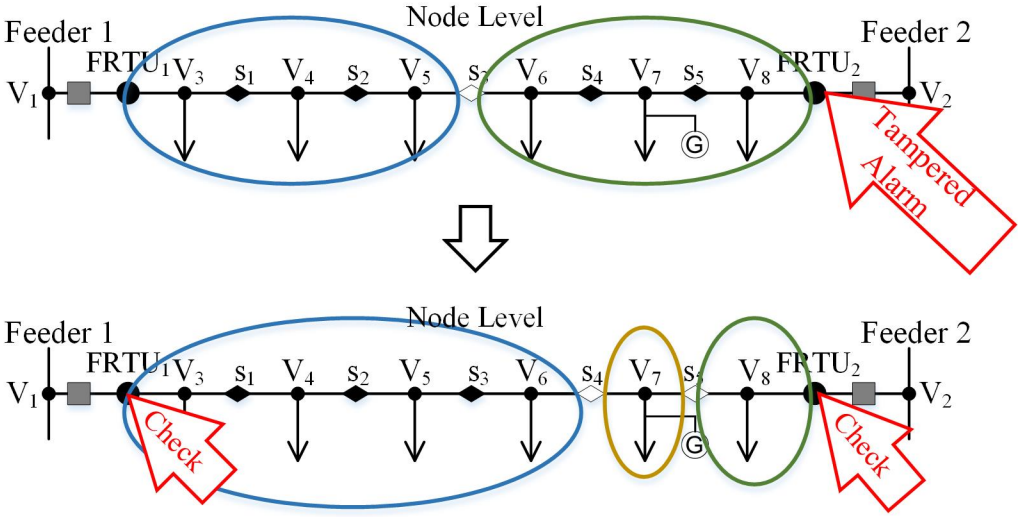

Fig. 2: Switching procedures to localize the tampered load node in the example topology.

Validations can be further extended in the future to study a large-scale distribution framework using the proposed algorithm. The consideration of electrical and operational constraints, corresponding combination strategy, as well as a heuristic search algorithm will be incorporated as part of the future work. The real topology of a distribution system can be drawn based on a real map in the geographic information system (GIS). An agent-based model which can be integrated with multiple modules into a single simulation environment such as the GridLAB-D [32] to generate random tampered nodes and perform the power flow to meet the constraint requirements in the provided network will be conducted.

REFERENCES

[1] J. Nagi, K. S. Yap, S. K. Tiong, S. K. Ahmed, and M. Mohamad, "Nontechnical loss detection for metered customers in power utility using support vector machines," *IEEE Trans. Power Del.*, vol. 25, no. 2, pp. 1162–1171, Apr. 2010.

[2] C. Cody, V. Ford, and A. Siraj, "Decision tree learning for fraud detection in consumer energy consumption," in *Proc. IEEE 14th Intl. Conf. on Machine Learning and Applications*, Dec. 2015, pp. 1175–1179.

[3] P. Jokar, N. Arianpoo, and V. C. M. Leung, "Electricity Theft Detection in AMI Using Customers' Consumption Patterns," *IEEE Trans. Smart Grid*, vol. 7, no. 1, pp. 216–226, Jan. 2016.

[4] P. McDaniel and S. McLaughlin, "Security and privacy challenges in the smart grid," *IEEE Security Privacy*, vol. 7, no. 3, pp. 75–77, Jun. 2009.

[5] J. Smith. (2015) Smart meters take bite out of electricity theft. National Geographic. [Online]. Available: http://news.nationalgeographic.com/news/energy/2011/09/110913-smart-meters-for-electricity-theft/.

[6] M. Davis. (2009) SmartGrid Device Security: Adventures in a new medium. Black Hat. [Online]. Available: http://www.blackhat.com/presentations/bh-usa-09/MDAVIS/BHUSA09-Davis-AMI-SLIDES.pdf.

[7] E. Byres, A. Ginter, and J. Langill. (2010) White Paper: How stuxnet spreads-a study of infection paths in best practice systems. Tofino Security. [Online]. Available: https://www.slideshare.net/YuryChemerkin/how-stuxnet-spreads-a-study-of-infection-paths-in-best-practice-systems.

[8] D. M. Nicol, "Hacking the lights out: The computer virus threat to the electrical grid," *Scientific American*, vol. 305, no. 1, pp. 70–75, Jul. 2011.

[9] K. Cho, M. Jo, T. Kwon, H. Chen, and D. Lee, "Classification and experimental analysis for clone detection approaches in wireless sensor networks," *IEEE Systems Journal*, vol. 7, no. 1, pp. 26–35, 2013.

[10] M. Demirbas and Y. Song, "An rssi-based scheme for sybil attack detection in wireless sensor networks," in *Proc. WoWMoM 2006*, 2006, pp. 566–570.

[11] (2012) smarter protection for the smart grid. McAfee. [Online]. Available: https://www.ccn-cert.cni.es/publico/InfraestructurasCriticaspublico/rp-smarter-protection-smart-grid.pdf.

[12] J. E. Cabral, J. O. P. Pinto, and A. M. A. C. Pinto, "Fraud detection system for high and low voltage electricity consumers based on data mining," in *IEEE Power Energy Society General Meeting*, Jul. 2009, pp. 1–5.

[13] B. Coma-Puig, J. Carmona, R. Gavald, S. Alcoverro, and V. Martin, "Fraud detection in energy consumption: A supervised approach," in *IEEE Intl. Conf. on DSAA*, Oct. 2016, pp. 120–129.

[14] L. Wei, A. Sundararajan, A. I. Sarwat, S. Biswas, and E. Ibrahim, "A distributed intelligent framework for electricity theft detection using benford's law and stackelberg game," in *Resilience Week (RWS)*, Sep. 2017, pp. 5–11.

[15] V. Ford, A. Siraj, and W. Eberle, "Smart grid energy fraud detection using artificial neural networks," in *Proc. IEEE 8th International Symposium on Service Oriented System Engineering*, Dec. 2014, pp. 1–6.

[16] S. A. Salinas and P. Li, "Privacy-preserving energy theft detection in microgrids: A state estimation approach," *IEEE Trans. Power Syst.*, vol. 31, no. 2, pp. 883–894, Mar. 2016.

[17] Y. Zhou, X. Chen, A. Y. Zomaya, L. Wang, and S. Hu, "A dynamic programming algorithm for leveraging probabilistic detection of energy theft in smart home," *IEEE Trans. Emerging Topics in Computing*, vol. 3, no. 4, pp. 502–513, Dec. 2015.

[18] Y. Park, D. M. Nicol, H. Zhu, and C. W. Lee, "Prevention of malware propagation in AMI," in *Proc. IEEE International Conference on Smart Grid Communications (SmartGridComm)*, Oct. 2013, pp. 474–479.

[19] H. Sedjelmaci and S. M. Senouci, "Smart grid security: A new approach to detect intruders in a smart grid neighborhood area network," in *Proc. International Conference on Wireless Networks and Mobile Communications (WINCOM)*, Oct. 2016, pp. 6–11.

[20] X. Xia, W. Liang, Y. Xiao, and M. Zheng, "BCGI: A fast approach to detect malicious meters in neighborhood area smart grid," in *Proc. IEEE International Conference on Communications (ICC)*, Jun. 2015, pp. 7228–7233.

[21] R. Czechowski and A. M. Kosek, "The most frequent energy theft techniques and hazards in present power energy consumption," in *Joint Workshop on CPSR-SG*, Apr. 2016, pp. 1–7.

[22] J. Duan, K. Zhang, and L. Cheng, "A novel method of fault location for single-phase microgrids," *IEEE Trans. Smart Grid*, vol. 7, no. 2, pp. 915–925, Mar. 2016.

[23] A. Augugliaro, L. Dusonchet, M. G. Ippolito, and E. R. Sanseverino, "Minimum losses reconfiguration of mv distribution networks through local control of tie-switches," *IEEE Trans. Power Del.*, vol. 18, no. 3, pp. 762–771, Jul. 2003.

[24] A. Abiri-Jahromi, M. Fotuhi-Firuzabad, M. Parvania, and M. Mosleh, "Optimized sectionalizing switch placement strategy in distribution

systems," *IEEE Trans. Power Del.*, vol. 27, no. 1, pp. 362–369, Jul. 2012.

[25] A. Heidari, V. G. Agelidis, M. Kia, J. Pou, J. Aghaei, M. Shafie-Khah, and J. P. S. Catalo, "Reliability optimization of automated distribution networks with probability customer interruption cost model in the presence of dg units," *IEEE Trans. Smart Grid*, vol. 8, no. 1, pp. 305–315, Jan. 2017.

[26] J. Li, X. Y. Ma, C. C. Liu, and K. P. Schneider, "Distribution system restoration with microgrids using spanning tree search," *IEEE Trans. Power Syst.*, vol. 29, no. 6, pp. 3021–3029, Nov. 2014.

[27] Y. Tang, C. Ten, and L. E. Brown, "Switching reconfiguration of fraud detection within an electrical distribution network," in *Resilience Week (RWS)*, Sept. 2017, pp. 206–212.

[28] L. Wang, C. Cao, and B. Chen, "Model-based micro-grid modeling and optimal pev charging control," in *12th IEEE/ASME International Conf. on Mechatronic and Embedded Systems and Applications (MESA)*, Aug. 2016, pp. 1–6.

[29] L. Wang, S. Feng, and F. Shi, "Risk analysis of closing loop operation based on the main and distribution network integration," in *China Intl. Conf. on Electricity Distribution*, Sept 2012, pp. 1–4.

[30] D. Mao, D. Meyer, and J. Wang, "Evaluating pev's impact on long-term cost of grid assets," in *IEEE Power Energy Society Innovative Smart Grid Technologies Conference (ISGT)*, Apr. 2017, pp. 1–5.

[31] C.-W. Ten and Y. Tang, *Electric Power Distribution Emergency Operation*. Taylor & Francis Group, 2018.

[32] (2012, Dec.) GridLAB-D. U.S. Department of Energy (DOE) at Pacific Northwest National Laboratory (PNNL). [Online]. Available: http://www.gridlabd.org.