Review and Analysis of Intrusion Detection System for Distribution Networks in Smart Grids

Yuvaraj S. Patil[1], Swati V. Sankpal[2]

[1]*Ph.D. Student, Electronics Engineering, Department of Technology, Shivaji University,*
Kolhapur, MS, India

[2]*Associate Professor, Department of Electronics Engineering, D. Y. Patil College of Engineering and Technology,*
Kolhapur, MS, India

[1]yuvaraj.pat@gmail.com,[2]sankpal16@yahoo.com

Abstract -Most of the countries across the world are transforming their existing electrical grids to Smart Grids. Smart grid provides a bi-directional flow of electricity and information from generation to transmission to distribution. Distribution networks are more exposed to the public and are at increased security risk. Smart meters are the critical elements of power distribution systems. Smart meters provide real-time data such as energy usage, energy utilization pattern, user information to control centres. Vast number of smart meters have been installed in the field in recent years and are more exposed to cyber-physical attacks due to heavy usage of communication infrastructure. False data can be injected in the network by compromising smart meters. This paper provides a review and analysis of recently proposed combination sum of energy profiles attack model and grid sensor placement algorithm used for network observability and detection accuracy.

Keywords - Advance Metering Infrastructure, Networks Communication, Distribution Networks, Cyber Security, False Data Injection (FDI), Grid Sensors, Home Area Networks (HAN), Neighbourhood Area Network (NAN), Smart Grid, Smart Meter.

I. INTRODUCTION

The aim of smart grid is to provide more secure, reliable and very high quality of electrical energy. Smart grids comprises of advanced communication and information infrastructures. Smart grid uses advanced communication and information technology, control systems and computing technologies and helps to modernize and optimize existing electric power systems [1][2][3]. Due to heavy usage of communication infrastructure, smart grids are more exposed to public and causes a number of security risks. Advanced Metering Infrastructure (AMI) is heavily used in distribution networks of smart grids. Distribution networks mainly comprises of Home Area Networks (HAN), Neighbourhood Area Network (NAN) [15] and Grid Sensor Networks. Smart meters are used as endpoints in Home Area Networks. Smart meters provide real time energy usage and end user data to control centers. Control centers uses the information provided by smart meters and performs state estimation and network observability analysis. Without this data, network operators and control centers cannot perform accurate real-time state estimation and analysis of the smart grid system. If the smart meter data is altered by the attackers and false data is injected in the system [11][12][13][14] by compromising smart meters, then it may cause serious problems such as customer information compromise, energy stealing, electricity outage, power equipment damage, malfunctioning of smart grid operations and loss of revenue. To prevent such type of attacks, various cryptographic techniques, secure devices and secure communication networks are used [4] [5]. Few researches have proposed intrusion detection systems (IDS) to detect malicious activities in the power systems [7] [9] [10]. Researchers in [6] have used DC (Direct Current) model for state estimation in power systems [16] and formulated an attack model for false data injection at smart meter level where multiple households are connected using radial tree distribution network. The authors have proposed an intrusion detection system framework to detect anomaly activities at smart meter level and derived an algorithm for grid sensor placement using graph theory. The grid sensors are used for network observability. This paper provides the review and analysis of the combinational sum of energy profile attack model for false data injection at smart meter level and grid sensor placement algorithm proposed by the authors in [6].

II. BACKGROUND AND DC POWER FLOW MODEL

In smart grid systems, measurement data is obtained from smart meters and sensors and based on this data, the control centers perform various activities like data processing, network state estimation and observability analysis. The measured data from the smart meters and sensors may not be always correct because of measurement errors, equipment and network failures, noise signal introduced in communication network and false data injection [13] in the network by attackers. Due to bad measurement data, control centers lead to wrong state estimation and wrong decision making [7].

A. DC Power Flow Model

DC power flow model is usually used for state estimation due to its simple computations and simplicity [8] [16]. The authors in [6] have used a DC power flow model equation as:

$$\mathbf{z} = \mathbf{Hx} + \mathbf{e} \qquad \text{(i)}$$

where

- **H** is a *m*-by-*n* Jacobian matrix (matrix of all first order derivatives) and represents *m* independent networks with *n* state variables related to network topology,
- **x** is the *n*-vector (*n* x 1 matrix) of true states,

- **z** is the *m*-vector of measurements (generator reading and *m* - 1 smart meters energy consumption reading) and
- **e** is the *m*-vector of random errors.

The state estimation $\mathbf{x}^{\wedge}$is obtained by calculating

$$\mathbf{G}^{-1}\mathbf{H}^{T}\mathbf{W}\mathbf{z} \qquad \text{(ii)}$$

where

- $\mathbf{G} = \mathbf{H}^{T}\mathbf{W}\mathbf{H}$ is the state estimation gain matrix and
- **W** is a diagonal matrix representing meter accuracy (reciprocal of measurement errors).

To detect bad measurement data, the measurement residual (residual is the error in a result) $\mathbf{z} - \mathbf{H}\ \mathbf{x}^{\wedge}$is computed and its norm $\| \mathbf{z} - \mathbf{H}\ \mathbf{x}^{\wedge}\|$ is compared with a predetermined threshold δ. When the normalized residual is greater than the predetermined threshold δ, it indicates that the anomalies present in the network i.e.

$$\| \mathbf{z} - \mathbf{H}\ \mathbf{x}^{\wedge}\| > \delta \quad \text{(iii)}$$

Equation (iii) indicates presence of anomalies.

The authors have showed that to inject false data into the system, attackers can derive a attack vector **a** such that

$$\mathbf{z}_{\mathbf{b}} = \mathbf{z} + \mathbf{a} \qquad \text{(iv) and}$$
$$\mathbf{x}^{\wedge}_{\mathbf{b}} = \mathbf{x}^{\wedge} + \mathbf{c} \qquad \text{(v)}$$

where $\mathbf{a} = \mathbf{H}\mathbf{c}$ is an *m* x 1 attack vector.

The authors further showed that the attackers can design the attack vector such that

$$\| \mathbf{z}_{\mathbf{b}} - \mathbf{H}\ \mathbf{x}^{\wedge}_{\mathbf{b}}\| = \| \mathbf{z} - \mathbf{H}\ \mathbf{x}^{\wedge}\| \le \delta \qquad \text{(vi)}$$

The authors have assumed that the attacker has knowledge of network configuration matrix **H**. But in practice, it may be impossible for attacker to gain full knowledge of the entire configuration system.

III.ATTACK MODEL AND FORMULATION

The authors have formulated an attack model where a dishonest customer intentionally tries to steal energy by lowering his smart meter reading and raising his neighbour’s smart meters reading in the a neighbour area network. The authors have also shown that such attacks are not detectable and identifiable at certain time periods. The authors have used a DC power flow model for state estimation and formulation of the attack model [6] [16].

A. Basic Model

The authors have considered a basic DC model that has there state variables as shown in Figure 1.

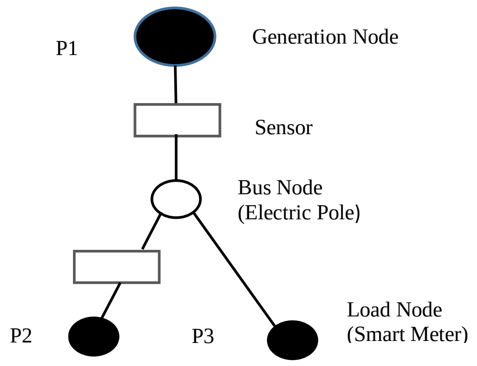

Fig. 1 Basic DC Model

The black node P1 represent generation node, black nodes P2 and P3 represents load nodes (smart meters), white circle represent bus node (electric pole), gray rectangles represents sensors and lines represents power connectivity. For a balanced network,

$$\mathbf{P1 + P2 + P3 = 0} \qquad \text{(vii)}$$

A network is said to be observable if all flows in the network can be observed by obtaining sufficient measurement data. The authors have used this basic DC model and formed a larger neighbourhood distribution network as shown in Figure 2 and proposed an attack model and grid sensor placement algorithm. The authors have made some assumptions such as 1) grid operators have full knowledge of network topologies, 2) the majority of data generated at the nodes are periodic for real-time monitoring and control etc.

B. Attack Model and Formulation

Based on the basic DC model [16], the authors have formed a neighbourhood distribution network using radial tree-like topology as shown in Figure 2. The authors have considered spanning tree topology (a spanning tree does not have loops and cannot be disconnected).

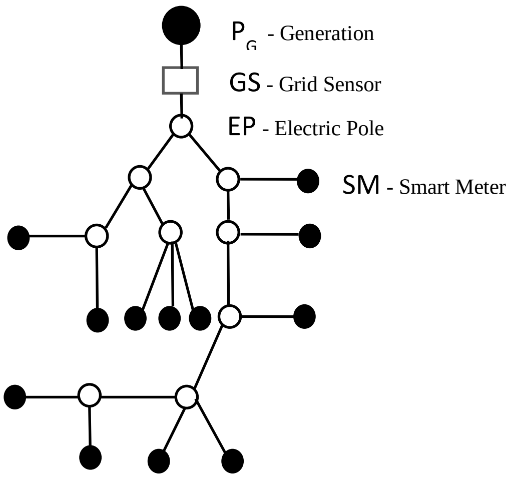

Fig. 2 Neighbour Distribution Network

As shown in the Figure 2, the distribution network consists of four components:

- A root node P_G at which power is generated or delivered from other sources and this node supplies the power P_G to load nodes,
- Grid Sensor (GS) node which measures the generated power $P_{G,}$
- Set of electric poles (EP) or bus nodes N_{EP} = (1, 2, …, n_{EP}), and
- Set of smart meters (SM), N_{SM} = (1, 2, …, $n_{SM)}$

The smart meters have bi-directional communication capability of reporting the household energy consumption to control center and receiving messages from control center in real time. The authors have assumed that the distribution network obeys some properties such that the spanning tree starts with the distribution head node P_G, the EP node cannot be a leaf node, the SM node must be a leaf node and power flow is unidirectional such that the power is delivered from a root node of the tree to the end leaf nodes. For a power balance condition, a summation of individual loads and measurement at GS node must be equal. If this condition is not met, then it indicates that an anomalous activity is present in the network.

The authors have applied False Data Injection (FDI) model to construct the attack scenario at smart meter level in the neighbourhood distribution network [13] [15]. The distribution network shown in Figure 2 is characterized by its network topology and configuration matrix **H** and a set of observed measurements

$$z = [P_G, P_1, P_2,\ldots.., P_i]^T \in \mathbb{Z} \qquad \text{(viii)}$$

where

- $P_G \leq 0$ is the total amount of generated power,
- $P_i \geq 0$, $\square_i \in N_{SM}$ indicates the energy consumption of household *i* and
- $\sum \square_i \in N_{SM}\ P_i = P_G$ for a balanced system.

The authors assumed that the traditional bad measurement detectors does not detect any anomalies [9] [10] i.e. $\| \mathbf{z} - \mathbf{H}\ \mathbf{x}^{\wedge} \| \leq \delta$ under a normal condition and all the smart meters deployed in the network are functioning properly.

It is assumed that the attacker is having a knowledge of configuration matrix **H** and estimation error **e** and is able to construct the attack vector **a** and associated observed measurement vector **ż** such that

$$\| \mathbf{z_b} - \mathbf{H}\ \mathbf{x}^{\wedge}\mathbf{_b} \| = \| \mathbf{z} - \mathbf{H}\ \mathbf{x}^{\wedge} \| \leq \delta \qquad \text{(ix)}$$

where

- $\mathbf{x}^{\wedge}\mathbf{_b} = \mathbf{x}^{\wedge} + \mathbf{c}$ and
- **c** is a non-zero *n* x1 vector designed to derive attack vector **a**.

The above condition in equation (ix) is satisfied in order to bypass the detection.

The attacker launches attack by constructing

$$\mathbf{\dot{z}} = \mathbf{z} + \mathbf{a} = [\mathbf{\dot{P}_G}, \mathbf{\dot{P}_1}, \mathbf{\dot{P}_2}, \ldots..\mathbf{\dot{P}_i}]^{\mathbf{T}} \neq \mathbf{0} \qquad \text{(x)}$$

where

- $\mathbf{a} = [a_G, a_1, a_2,\ldots.., a_i]^T \in \mathbb{Z}$ and
- $\sum \square_i \in N_{SM}\ a_i = a_G = 0$.

The attacker compromises its own smart meter $\boldsymbol{i} \in \mathbf{A}$ for which $\exists \mathbf{a_i} \in \mathbf{a}$, $\mathbf{a_i} < 0$, and victims smart meter $\mathbf{j} \in \mathbf{B}$ for which $\exists \mathbf{a_j} \in \mathbf{a}$, $\mathbf{a_j} > 0$, $\mathbf{j} \neq \mathbf{i}$. This shows that there exists load alteration conditions. The elements of set **A** belongs to attacker's smart meters whereas elements of set **B** belongs to victim's smart meters.

The attack vector **a** is considered such that

$$\mathbf{a} = [\mathbf{a_G}, \mathbf{a_1 x_1}, \mathbf{a_2 x_2}\ldots.., \mathbf{a_i x_i}]^{\mathbf{T}} \qquad \text{(xi)}$$

where

- x_i represents that the smart meter of household $\boldsymbol{i}$ is compromised if $x_i = 1$; else $x_i = 0$.

The main objective of the attacker is to steal energy by lowering the readings of its own smart meters and raise the readings of other's smart meters. The attacker tries to compromise less number of smart meters and minimum energy stealing so that it will not be detectable by bad measurement detectors [11] [12] [14]. The minimization problem for such an attack is represented by below formula.

Min $\sum \mathbf{x_i}$**such that**

$$\sum a_i\, x_i = P_s,\ x_i \in \{0,1\},\ \square_i \in B, \qquad (1)$$

$$a_i \geq P_i^{min}\ (t+1) - P_i(t),\ \square_i \in A \qquad (2)$$

$$a_i \leq P_i^{max}\ (t+1) - P_i(t),\ \square_i \in B \qquad (3)$$

$$P_i(t),\ P_i^{min}\ (t+1),\ P_i^{max}\ (t+1) \geq 0,\ \square_i \in A,\ \in B \qquad (4)$$

where

- $P_s = -\ (\sum \square_i \in A\ a_i) \geq 0$ is the total amount of non-negative power which attacker plans to steal,
- $P_i \in A$ (*t*) is the energy consumption of attacker's smart meter $\boldsymbol{i}$ at time $\boldsymbol{t}$,
- $P_i \in B$ (*t*) is energy consumption of victims smart meter $\boldsymbol{i}$ at time $\boldsymbol{t}$,
- P_i^{min} (*t*+1) is the minimum power value predicted to consume at time *t*+1 and
- P_i^{max} (*t*+1) is the maximum power value predicted to consume at time *t*+1.

The total number of compromised smart meters is

$$k_{SM} = |A| + |B| \leq |N_{SM}| \qquad \text{(xii)}$$

The authors have proved that the attacker can launch successful attack by compromise minimum two smart meters i.e. $k_{SM} \geq 2$ (one smart meter for the attacker and the one for the victim). The Figure 3 shows attack scenario by lowering reading of smart meter 1 (attacker's smart meter) and increasing reading of smart meter 2 (victim's smart meter).

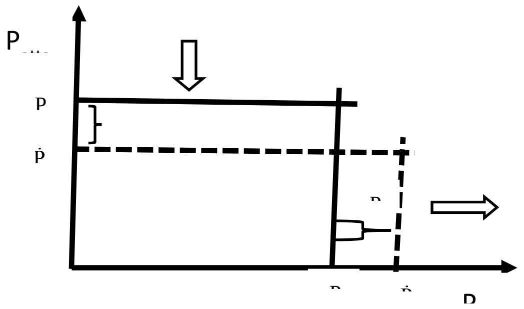

Fig. 3 Attack on smart meter 1 (the attacker) and smart meter 2 (the victim)

IV. GRID SENSOR PLACEMENT ALGORITHM

The authors have proposed a grid sensor placement mechanism and algorithm which is useful for enhanced network observability by deploying sufficient number of grid sensors in distribution network as shown in Figure 4.

It is assumed that all the deployed grid sensors are intrusion resistant (i.e. the sensors cannot be attacked) and the sensors are trustworthy (i.e. the measure data of sensors is accurate) so that their measured data can be compared with smart meter data and identify false data. The proposed grid sensor placement framework provides improved network observability as it deploys sufficient number of grid sensors through the distribution network. The authors have proposed a Grid Placement Sensor algorithm in order to reduce the redundant grid sensors to sufficient number of grid sensors while observability is still maintained

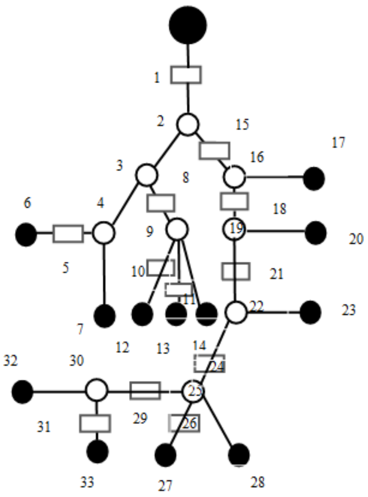

Fig. 4 Neighbourhood distribution network deployed with a number of grid sensors

For a spanning tree shown in Figure 4, the network graph $G(V_T, E_T)$ with depth 1,2,…d ∈ D_T is constructed by a set of EP and SM nodes v_1, v_2, ……., v_n∈ $V_T$and a set of edges E_T, where

$$N_{SM} \subset V_T,\ N_{EP} \subset V_T,\ |V_T| = |N_{SM}| + |N_{EP}| \quad (xiii)$$

The proposed algorithm is as below.

Grid Sensor Placement Algorithm:

Input: Spanning tree graph $G(V_T, E_T)$ and depth D_T.
Output: A *n* x *n* observability indicator matrix I_O that represents observability status of each node.

```
Start
Place a GS node at the edge of root node.
fori = 1 toddo
        Determine the number of child u of v(d), □v∈ V_T
        ifu = 1 then
           No GS node is placed
        else if u > 1 then
            A GS node is placed on any (u-1) of the u edges
            connected to the child and mark 1 for the
            GS placed edges in I_O.
        end if
        Repeat for the other v if having the same d.
end for
```

As shown in the above algorithm, a GS node v_1 is directly placed on the edges between the generation node and bus node v_2. Then start with EP node v_2. EP node v_2 has two children, which can be EP or SM nodes. Either edge $e(v_2, v_3)$ or $e(v_2, v_{16})$ placed with GS node v_{15} in between makes both edges observable. Both edges becoming observable are then marked with 1 in I_O. The process is repeated for the remaining branches till it reaches the leaves with the largest *d*.

The authors have provide a theorem which states that in the spaning tree of a distributed network, the number of GS nodes places on the edges is the same as the number of SM nodes. This theorem helps network operators to find the total number of grid sensors needed for a distribution network to be observable knowing the total number of smart meters deployed in the distribution network.

The authors have assumed that the grid placed sensors are trustworthy and provides accurate results. In reality, the grid placed sensors may not be trustworthy and may malfunction and may provide wrong results. The attackers can also compromise the sensors and can make the sensors unavailable. This can lead to degradation of network observability and functionality.

V. CONCLUSIONS

This paper provides a review and analysis of the combinational sum of energy profile attack model for false data injection at smart meter level and grid sensor placement algorithm for improving network observability of a distribution network. The formulated attack model illustrates that an attacker can lower his smart meter readings and raising other's smart meter readings by compromising the smart meters and thus can steal the energy. The proposed algorithm for placing grid sensors on the edges of spanning-tree distribution network provides sufficient observability and the anomaly detection rate can be improved.

The proposed attack model is limited to single attacker. It is possible that multiple attackers may try to steal energy at same time period by compromising multiple smart meters. Hence the proposed attack model needs to be further explored for multi-player attack.

The grid sensors are considered fully trustworthy. But for practical scenarios, the sensors may not be fully trustworthy. Hence further research is needed to explorer the impact on the network observability if the grid placed sensors gets compromised along with the smart meters.

ACKNOWLEDGMENT

The review and analysis presented in this paper is based on the research work proposed by the authors C H Lo and N Ansari [6].

REFERENCES

[1] Enrique Santacana, Gary Rackliffe, Le Tang and Xiaoming Feng “Getting Smart - With a Clearer Vision of the Intelligent Grid, Control Emerfrom Chaos,” IEEE power and energy magazine, pp. 41-48, Mar/Apr2010.

[2] S. Massoud Amin and Bruce F. Wollenberg, “Towards a Smart Grid, IEEE power and energy magazine, pp. 34-41, Sep/Oct. 2005.

[3] Thomas G. Garrity, “Getting Smart - Innovation and Trends for Future Electric Power System,” IEEE power and energy magazine, pp. 38-45, Mar/Apr. 2008.

[4] Goran N. Ericsson, “Cyber Security and Power System Communication - Essential parts of a Smart Grid Infrastructure,” IEEE trans. Power Delivery, Vol. 25, no. 3, pp. 1501-1507, Jul. 2010.

[5] A. Giani, E. Bitar, M. Garcia, M. McQueen, P. Khargonekar and Poolla “Smart Grid Data Integrity Attacks,” IEEE trans. Smart Grid, 4, no. 3, pp. 1244-1253, Sep. 2013.

[6] C. H. Lo and N. Ansari, “CONSUMER: A Novel Hybrid Intrusion Detection System for Distribution Networks in Smart Grid,” IEEE tr. Emerging Topics in Computing, Vol. 1, no. 1, pp. 33-44, Jun. 2013.

[7] C. W. Ten and C. H. Lu, “Anomaly Detection for Cybersecurity of the Substations,” IEEE trans. Smart Grid, Vol. 2, no. 4, pp. 865-873, Dec. 2011.

[8] Saman Zonouz, Katherine M. Rogers, Robin Berthier, Rakesh B. Bobba,William H. Sanders, and Thomas J. Overbye “SCPSE: Security-Oriented Cyber-Physical State Estimation for Power Grid Critical Infrastructures,” IEEE trans.on Smart Grid, Vol. 3, no. 4, pp. 1790-1799, Dec. 2012.

[9] R. Berthier, W. Sanders, and H. Khurana, "Intrusion detection for advanced metering infrastructures: Requirements and architectural directions," in Proc. 1st IEEE Int. Conf. Smart Grid Commun., Oct. 2010, pp. 350-355.

[10] J. Valenzuela, J. Wang, and N. Bissinger, "Real-time intrusion detection in power system operations," IEEE Trans. Power Syst., vol. 28, no. 2, pp. 1052-1062, May 2013.

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

[12] A. Giani, E. Bitar, M. Garcia, M. McQueen, P. Khargonekar, and K. Poolla, "Smart grid data integrity attacks: Characterizations and countermeasures," in Proc. 2nd IEEE Int. Conf. Smart Grid Commun., Oct. 2011, pp. 232-237.

[13] J. Lin,W.Yu, X.Yang, G. Xu, andW. Zhao, "On false data injection attacks against distributed energy routing in smart grid," in Proc. 3rd IEEE/ACM ICCPS, Apr. 2012, pp. 183-192.

[14] Y. Huang, M. Esmalifalak, H. Nguyen, R. Zheng, Z. Han, H. Li, and L. Song, "Bad data injection in smart grid: Attack and defense mechanisms," IEEE Commun. Mag., vol. 51, no. 1, pp. 27-33.

[15] Z. Xiao, Y. Xiao, and D.-C. Du, "Exploring malicious meter inspection in neighborhood area smart grids," IEEE Trans. Smart Grid, vol. 4, no. 1, pp. 214-226, Mar. 2013.

[16] D. Van Hertem, J. Verboomen, K. Purchala, R. Belmans, and W. Kling, "Usefulness of DC power Flow for active power flow analysis with flow controlling devices," in Proc. 8th IEEE Int. Conf. ACDC, Mar. 2006, pp. 58-62.