International Journal of Applied Engineering Research ISSN 0973-4562 Volume 14, Number 7 (2019) pp. 1488-1492

Multi-Player Attack Detection Model for Smart Meter Security in Smart Grid Systems

Yuvaraj S Patil
Department of Electronics Engineering
D Y Patil College of Engg. and Technology,
Affiliated to Shivaji University,
Kolhapur, India

Swati V Sankpal
Department of Electronics Engineering
D Y Patil College of Engg. and Technology,
Affilited to Shivaji University,
Kolhapur, India

Abstract

Smart meters are one of the critical elements of smart grid systems. Electric utilities deploy smart meters at consumer facilities. Centralized control center owned by electrical utilities monitors and controls smart meters. Smart meters provide real-time energy usage of consumers to control center. Control center leverages the state of the art wired and wireless technologies to check and control consumer energy usage in real-time. Smart meters are more exposed to cyber-attacks due to heavy usage of communication infrastructure in smart grid systems. Attackers can compromise smart meters and can change meter reading to steal energy. Energy theft is one of the critical problem faced by electric utilities because electric utilities lose lots of revenue every year due to energy theft. This paper proposes a model to detect multiple player cyber-attacks on smart meters. The proposed model helps to improve energy theft detection and find the compromised smart meters.

Keywords: Advance Metering Infrastructure, Distribution Networks, Energy Theft, False Data Injection, Smart Grid

I. INTRODUCTION

An electric grid consists of three main subsystems: generation; transmission and distribution; and end consumers. The purpose of transforming existing power grids into a smart grid is to give reliable, high quality electric energy in an efficient way [8]. Smart grid involves a transformation to an information enabled and highly connected network between electricity consumers and electric utilities [9]. Smart grid is an advanced electrical grid in which power generation, transmission, distribution and consumers are connected using advanced communication and information technologies. Smart grid provides reliable, secure and efficient usage of electrical energy. The evolution to smart grids brings significant changes to energy management functions and control systems. Most of the smart grid systems have considered utilizing the existing wired and wireless networks for communication. Due to heavy usage of communication infrastructure, smart grids are more exposed to cyber-attacks and are at increased security risks. Secure communication infrastructure plays a critical role in a smart grid system [8] [9] [11].

An important link between the electricity consumer and the electric utility to enable demand response functionality is to deploy smart meters capable of two-way communication which will measure and quantify the end customers energy consumption at real-time [9]. Advanced metering infrastructure is heavily used in distribution networks to deploy smart meters in the field. Smart meters act as endpoints in distribution networks. Smart meters provide real-time energy usage and consumer information to control centers. Smart meters are capable of bi-directional communication to report the household energy consumption to control center and receive messages from control center in real-time. Control center applies various mathematical and analysis techniques and computational intelligence on the received data and finds energy usage of consumers. Without real-time data, control centers and network operators cannot do accurate real-time estimation, analysis and control of the smart grid system. Smart meters use advanced communication technologies to give real-time information to control centers. Smart meters are more exposed to public due to heavy usage of communication technologies and hence are at increased risk of cyber-attacks.

Energy theft is one of the critical problem faced by electric utilities. Electric energy theft is dishonest or illegal use of electricity equipment [1] and service with the intention to lower energy consumption to lower billing charges [2]. Some unethical consumer/attacker might intend to steal energy by compromising some of the smart meters installed in the field. The attacker can compromise some of the smart meters and alter the smart meter data and inject false data in the system. The attacker intends to steal energy by lowering the reading of its own smart meter/s and raise the readings of victim's smart meter/s. Electrical utilities lose lots of revenue every year because of energy theft [2] [3]. For control centers and electric utilities, it is difficult to distinguish between honest and dishonest customers [1]. It is hard to distinguish between (unintentionally) anomaly and (intentionally) malicious activities [9]. Practically, electric utilities will never be able to get rid of energy theft completely, but can lower and prevent energy theft by using proper security mechanisms.

Compromise of smart meters might lead to serious problems such as electricity outage, malfunctioning of the power equipment's, malfunctioning of the smart grid operations and compromise of the confidential information of consumers. It could lead to unreliable operations, instability, damage to infrastructure and devices if proper and sufficient security mechanism are not used. Hence cyber security of smart meters plays an important role in smart grid systems. Researchers are working to offer various security techniques and secure devices to prevent such type of attacks. Researchers [4] have proposed frameworks and intrusion detection systems to detect malicious

activities and cyber-attacks at smart meter level. Grid sensors detect malicious activities at smart meter level [6] [7]. Electric utilities deploy grid sensors in distribution networks to control and monitor smart meters installed in the field. Grid sensors get smart meter data and give it to control center. The data obtained from smart meters and grid sensors may not always be correct because of measurement errors, equipment and network failures, noise signal introduced in communication network and false data injection [5][6] in the network by attackers. Due to bad measurement data, control center lead to wrong estimation and wrong decision-making.

Researchers [6] have proposed an attack model and intrusion detection framework to detect malicious activities [4] at smart meter level. The attack has limitation of detecting single player attack and cannot detect multi player attacks where more than one attacker tries to steal electricity at the same time period. In this paper, we propose a Multi-Player Attack Detection Model to detect multi player attacks at smart meter level. The proposed multi-player attack detection model helps to improve energy theft detection. The deployed grid sensors and their measurement data considered as secure and trustworthy. Comparison of measurement data of smart meters and grid sensors helps to detect energy theft and find compromised smart meters.

II. BASIC DC MODEL

Generally AC and DC power flow models helps to study electric grid systems. This study uses DC power flow model because of its simple computations and cost effectiveness [10]. Another reason for considering a DC power flow model is that the future distribution networks will make use of power systems based on solar energy and other natural resources which supplies DC power. Fig 1 shows a basic DC Model.

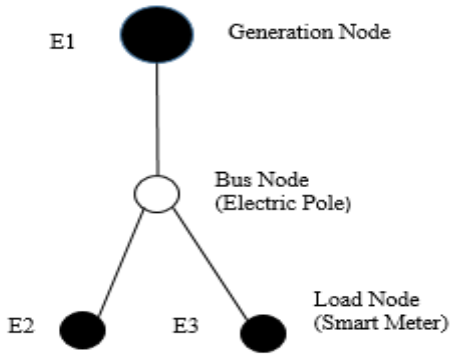


Fig. 1 Basic DC Model

As shown in Fig 1, the bigger black node represents Generation Node (GN) which acts as source node, the other two black nodes represents load nodes which acts as endpoint sink nodes, the white circle represents bus node, and the lines represents power connectivity. The basic DC model has three state variables E_1, E_2 and E_3 where E_1 denotes energy generated by GN node, E_2 and E_3 denotes energy consumed by load nodes. Ideally the sum of energy consumed by all the load nodes connected to the network equals the energy generated by the generation node. The network is a balanced network if the generated energy is equal to total consumed energy. For a balanced network [6],

$$E_1 = (E_2 + E_3) \quad (1)$$

If $E_1 \neq (E_2 + E_3)$, then the network is not a balanced network. If the sum of energy consumed by all the smart meters is not matching with the energy generated by generation node, then it indicates that the network is not balanced and there is energy loss due to various reasons like faulty meters, losses in the transmission and distribution network, communication errors and energy stealing.

The basic DC model shown in Fig. 1 depicts a typical binary tree. This model assumes that it does not contain any loops and the power flow is unidirectional such that power gets delivered from the Generation node and consumed by load nodes. The basic DC model shown in Fig. 1 acts as a building block for developing a distribution network for the study and analysis of the proposed multi-player attack detection model in this paper.

III. DISTRIBUTION NETWORK MODEL

Smart grid system is a feedback loop control system [6]. It relies on the measurement data obtained from smart meters and grid sensors. Electric utilities strategically deploy Grid sensors in Distribution network. The grid sensors monitors smart meters deployed in the distribution network and sends real-time data of the smart meters to the control center periodically. Similarly smart meters too send consumer's energy usage details and other related information to control center periodically. Control center performs various computational and mathematical operations on the received data, determines energy usage of the consumers and performs network state analysis to make sure network stability and security. Fig. 2 shows overall system architectural block diagram of a smart grid system.

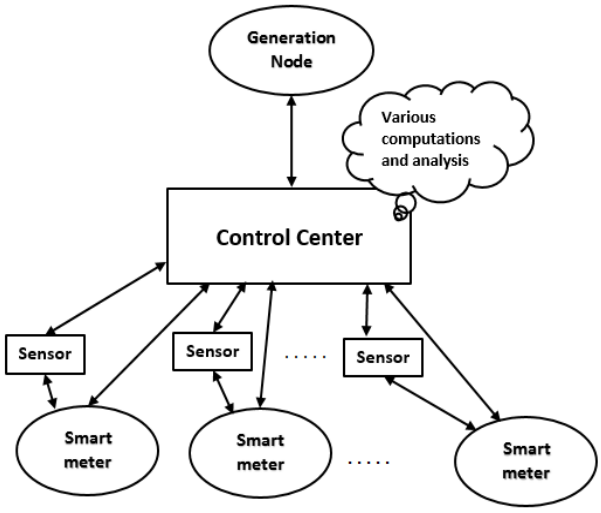


Fig. 2 Overall Architectural Block Diagram of Smart Grid System

A more complex and larger distribution network shown in Fig 3 is developed to study and analysis of the proposed multi-

player attack detection model. This model is based on the basic DC model and uses tree topology. The model consists of one Generation Node (GN), eight Electric Pole (EP) nodes, seven Distribution Pole (DP) nodes and twelve Smart Meter (SM) nodes. The Generation Node acts as a source node. Smart Meters (SM) acts as load nodes and Electric Poles (EP) acts as bus nodes. Smart meters get connected as endpoint nodes. The relationship between the EP nodes needed and the DP nodes needed to form the distribution network is given by equation 2 where n_{DP} denotes the total number of distribution poles and n_{EP} denotes the total number of electric poles. The number of Distribution Pole nodes needed is always one less than the number of Electric Pole nodes needed to form the distribution network. The relationship between the number of EP nodes needed and number of SM nodes needed is given by equation 3 where n_{SM} denotes the number of smart meter nodes and n_{EP} denotes the total number of electric pole nodes. The number of EP nodes needed varies between half the number of SM nodes to equal the number of SM nodes depending on the place of the SM nodes in the distribution network.

$$n_{DP} = (n_{EP} - 1) \quad (2)$$

$$(n_{SM} / 2) <= n_{EP} <= n_{SM} \quad (3)$$

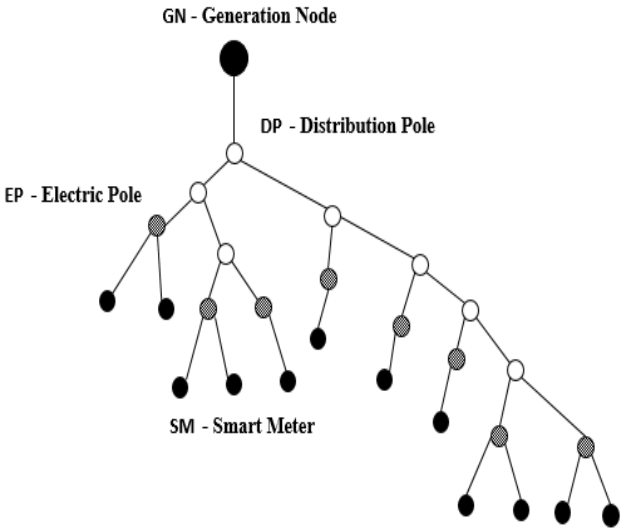


Fig. 3 Distribution Network Model

This study assumes that the distribution network model shown in Fig 3 have the following properties.

- The distribution network does not contain loops and disconnection.
- The control center and electric utilities will have full knowledge of the topologies used in the network.
- The control center and electric utilities will have full knowledge of the smart meters and grid sensors deployed in the distribution network.
- The control center and electric utilities have complete details of the geographical locations of the smart meters and grid sensors deployed in the distribution network.
- Smart meters and grid sensors send real-time information to the control center periodically. The real-time information represents the energy consumption of the consumers.

IV. MULTI PLAYER ATTACK DETECTION SIMULATION MODEL

A. Multi-player Attack Detection Simulation Model

Fig 4 shows a simulation model of distribution network developed using network simulator. We use this model to study and analyse the proposed multi player attack detection model.

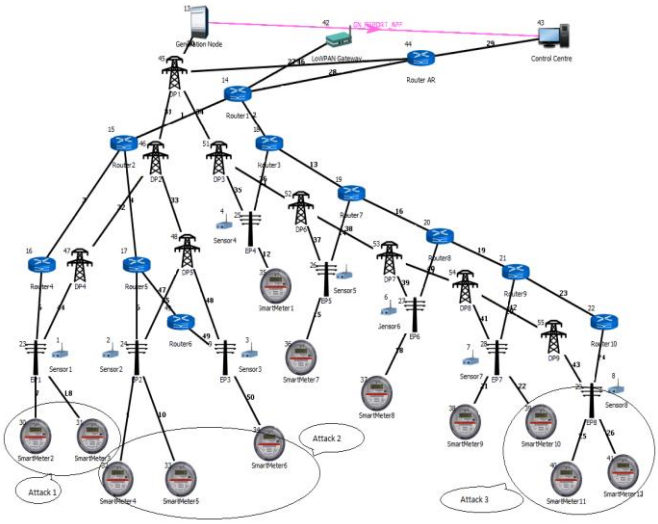


Fig. 4 Multi-player Attack Detection Simulation Model

The multi-player attack detection simulation model consists of four major components 1) Generation Node, 2) Distribution Poles and Electric Poles, 3) Smart Meters and 4) Grid Sensors. Generation node acts as a source node. The Generation Node generates electrical energy E_G. Distribution Network is formed using Distribution Poles and Electric Poles. The generated energy gets supplied to consumers through distribution network. Distribution network use tree topology. Fig 4 illustrates a typical spanning tree. The spanning tree starts with the Generation Node as a root node. It does not have loops and disconnection. Electric Poles connect Smart Meters to the distribution network. The Electric Pole node cannot be a leaf node and the Smart Meter node must be a leaf node [6].

Equation 4 and equation 5 represents a set of Distribution Poles and Electric Poles deployed in the distribution network where n_{DP} denotes the total number of distribution poles, n_{EP} denotes the total number of electric poles, N_{DP} represents a set of distribution poles and N_{EP} represents a set of electric poles.

$$N_{DP} = (1, 2, 3, \ldots n_{DP}) \quad (4)$$

$$N_{EP} = (1, 2, 3, \ldots n_{EP}) \quad (5)$$

Smart Meters deployed at consumers place acts as sink nodes. Equation 6 represents a set of Smart Meters deployed in the distribution network where n_{SM} denotes the total number of smart meter and N_{SM} represents a set of smart meters.

$$N_{SM} = (1, 2, 3, \ldots n_{SM}) \quad (6)$$

Grid sensors get deployed in the distribution network. Equation 7 represents a set of grid sensors deployed in the distribution network where n_{GS} denotes the total number of smart meter and N_{GS} represents a set of smart meters.

$$N_{GS} = (1, 2, 3, \ldots n_{GS}) \quad (7)$$

No smart meter is directly connected to distribution pole. Smart meters are always connected to electric poles. Smart meters are capable of two-way communication. Smart meter keeps track of energy usage of a consumer and reports the household energy consumption to control center. To make the design of distribution network simple and maintainable, one or two smart meter be connected per electric pole.

Control center performs monitoring and controlling of the smart meters deployed in the network. Smart meters send the real-time energy usage report along with other relevant information to control center periodically. Similarly generation node too sends its total energy generation report to control center. Control center keeps record of measurements received from smart meters and generation node. A set of measurement record is given by equation 8 where E_{GN} denotes the total amount of energy generated at generation node, E_{SMn} denotes the energy consumption of smart meter $n \in N_{SM}$ and E represents a set of measurements received at control center.

$$E = (E_{GN}, E_{SM1}, E_{SM2}, \ldots, E_{SMn}) \quad (8)$$

For a balanced network, the sum of energy consumption recorded by all the smart meters must be equal to the energy generated at generation node as shown by equation 9.

$$E_{GN} = \sum E_{SMn} \quad (9)$$

Control center applies various computational and mathematical operations on the received data and performs analysis of the network state, analysis of the energy consumption by the consumers and to make sure network stability and security.

In order to analyze the multi-player attack detection model, we simulated a three player attack scenario as shown in Fig 4. Attack case 1 comprises of smart meter 2 and 3. Attack case 2 comprises of smart meter 4, 5 and 6. Attack case 3 comprises of smart meter 10, 11 and 12. In attack case 1, smart meter 2 belongs to attacker 1 and smart meter 3 belongs to immediate neighboring victim connected to same electric pole. Attacker 1 plans to steal 5% energy from his neighbor. To meet the goal, attacker 1 compromises his own smart meter 2 data and neighbors smart meter 3 data and lowers his meter reading data by 5% and raises his neighbors meter reading data by 5 %. In attack case 2, smart meter 4 belongs to attacker 2, smart meter 5 belongs to immediate neighboring victim connected to same electric pole and smart meter 6 belongs to neighboring victim connected to neighboring electric pole. Attacker 2 plans to steal 10% energy from his neighbors. To meet the goal, attacker 2 compromises his own smart meter 4 data and neighbors smart meter 5 and 6 data and lowers his meter reading data by 10% and raises his neighbors meter reading data by 5 % each. In attack case 3, smart meter 10 belongs to attacker 3, smart meter 11 and 12 belongs to neighboring victims connected to neighboring electric pole. Attacker 3 plans to steal 10% energy from his neighbors. To meet the goal, attacker 3 compromises his own smart meter 10 data and neighbors smart meter 11 and 12 data and lowers his meter reading data by 10% and raises his neighbors meter reading data by 5 % each. We assumes that the attackers hack the smart meter data sent over the network and injects the false data. We assumed that the smart meter sends its report to control center once in a day at configured time.

Grid sensors installed on the electric pole monitors smart meters connected to that electric pole, captures smart meter data and sends the captured information to control center at configured time. We assumed that the grid sensor captured data cannot be compromised and is fully trustworthy.

B. Results and Analysis

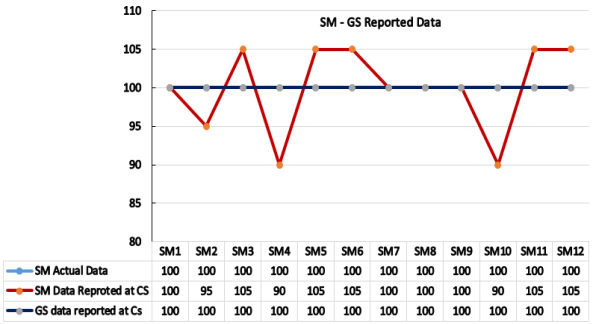
Table 1 shows the real energy consumption data of all the smart meters, smart meters data reported at control center, grid sensors data reported at control center and variation of smart meter data w.r.t to grid sensor reported data.

TABLE I. SMART METER AND GRID SENSOR DATA REPORTED AT CONTROL CENTER AND VARIATION IN REPORTED DATA

SM Number	SM actual data	SM data reported at CS	GS Reported data	SM Data variation w.r.t GS data in %
SM1	100	100	100	0
SM2	100	95	100	5
SM3	100	105	100	5
SM4	100	90	100	10
SM5	100	105	100	5
SM6	100	105	100	5
SM7	100	100	100	0
SM8	100	100	100	0
SM9	100	100	100	0
SM10	100	90	100	10
SM11	100	105	100	5
SM12	100	105	100	5

Fig. 5 shows a graphical representation of the smart meter real data, smart meter data reported at control center and grid sensor data reported at control center. Fig 6 shows variation in smart

meter reported data w.r.t grid sensor reported data at control center.



	SM1	SM2	SM3	SM4	SM5	SM6	SM7	SM8	SM9	SM10	SM11	SM12
SM Actual Data	100	100	100	100	100	100	100	100	100	100	100	100
SM Data Reproted at CS	100	95	105	90	105	105	100	100	100	90	105	105
GS data reported at Cs	100	100	100	100	100	100	100	100	100	100	100	100

Fig. 5 Graphical representation of Smart meter – Grid sensor data reported at Control Center

Control center performs mathematical computations and analysis on the received data and verifies whether the GN node reported data matches with the sum of the SM node reported data. Similarly it verifies whether the smart meter reported data matches with the grid sensor reported data. Control center alerts if it finds any variation in the received data.

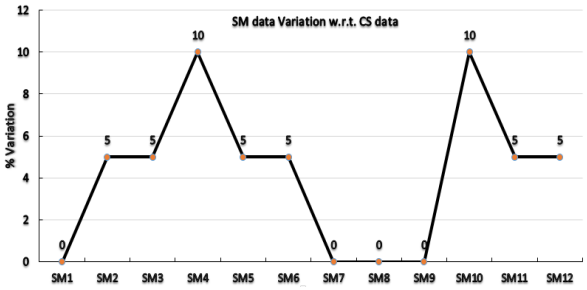


Fig. 6 Variation in Smart meter reported data w.r.t. Grid sensor reported data

In the simulated example scenario shown in Fig 4, even though the smart meter 2, 3, 4, 5, 6, 10, 11 & 12 reading data gets altered by attackers, the sum of all the smart meter reported data matches with the GN node reported data. Hence it is hard for control center to find compromised smart meters and detect energy theft without grid sensors. Control center detects energy theft and identifies compromised smart meters by multiple attackers with the help of grid sensor data. We assumed that the grid sensor data is trustworthy and grid sensors are fully secure and cannot be attacked.

V. CONCLUSION

This paper proposes a Multi-player Attack Detection Model for Smart Meter Security. The proposed multi-player attack detection model is capable of detecting and identifying multi-player attacks on smart meters. The simulation model developed shows a three player attack scenario. The simulation results shows that the control center can detect multi-player attacks on the smart meters and can find the compromised smart meters. Hence control center is capable of detecting multi-player attacks and identifying the compromised smart meters.

REFERENCES

[1] Harsha Khandel, Suchitra Pandey, D. Reynolds "Internet of Things Based Power Theft Detection System" International Journal of Advanced in Management, Technology and Engineering Sciences, Volume 8, Issue III, March 2018

[2] Harsha Khandel, Suchitra Pandey, D. Reynolds "A Review on IOT Based Power Theft Detection and Control Systems" International Journal of Innovative Research in Electrical, Electronics, Instrumentation and Control Engineering, Vol. 5, Issue 9, September 2017

[3] S. Visalatchi and K. K. Sandeep, "Smart energy metering and power theft control using arduino & GSM," 2017 2nd International Conference for Convergence in Technology (I2CT), Mumbai, 2017, pp. 858-961

[4] A. Thomas Paul Roy, Dr.K.Balsubadra "DRPGAC: Detecting And Preventing Malicious Activities In Wireless Sensor Networks" Journal of Theoretical and Applied Information Technology 10th November 2014 -- Vol. 69. No. 1 – 2014

[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] 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

[8] 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.

[9] Thomas G. Garrity, "Getting Smart - Innovation and Trends for Future Electric Power Sys-tem," IEEE power and energy magazine, pp. 38-45, Mar/Apr. 2008.

[10] 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.

S. Massoud Amin and Bruce F. Wollenberg, "Towards a Smart Grid, IEEE power and en-ergy magazine, pp. 34-41, Sep/Oct. 2005