

## Secured GreenNet: Future Trends of Cyber Security in Smart Metering Infrastructure

Ayesha Afzaal, Mohsin Nazir

Lahore College for Women University, Lahore, ayesha.afzaal@lcwu.edu.pk

**Abstract:** One of the widely used components in the smart grid (SG) is an advanced metering infrastructure (AMI). The AMI is a process of two-way communication between the utility and customer through the information exchange. Some of these kinds of applications are real-time pricing and electricity consumption information by using wireless communication network. However, security is crucial since messages are broad casted via wireless channels through which hackers can capture the messages and then know the contents of the messages. Encrypting messages to cipher text is one of the methods to solve this problem but it already has many open issues regarding keys management. In this paper, a new algorithm of attack detection and avoidance is proposed by paring of smart meters and coupon passing mechanism. Simulation result shows that proposed solution not only increase the attack detection rate but also reduce the effect of attacks on a network.

[Ayesha Afzaal, Mohsin Nazir. **Secured GreenNet: Future Trends of Cyber Security in Smart Metering Infrastructure.** *Life Sci J* 2014;11(6s):62-67]. (ISSN:1097-8135). <http://www.lifesciencesite.com>. 10

**Keywords:** smart grid protocols, meter data management, advanced metering infrastructure, utility collector.

### I. Introduction

Smart grid uses digital technology to provide electricity from suppliers to consumers. It not only let the electricity provider to vaguely examine consumer usage as well as it also allows them to implement erratic rates that can increase or decrease depending load demand in peak hours. Furthermore, customers will also be able to examine their energy consumption information in real time, through which they can save money by reducing their usage during peak/ off peak energy time [1]. The power generation and consumption are physically connected through grid, which distributes electricity economically depending on the limitation of capacity, reliability and security of power equipment's through power lines. The power grid system consists of two parts, transmission and distribution; Bulk transfer of electricity is processed through transmission, which maneuver at a high voltage to transfer electricity from power plants to closest substations. Distribution means the deliverance of electricity from substations to consumers; it steps down the power from medium to low voltage level [2].

To handle the transfer of information in both parts of the smart grid, advance-metering infrastructure (AMI) is used. It covers a whole electricity information network, which includes Smart Meters (SM), communications to and from a utility provider, and also communication between smart devices. With the help of this two-way communication between a utility and customer information, such as real time pricing and usage information can be easily exchanged on periodic bases. The advance meters enable customers to examine and control of energy use in their homes. AMI has three basic elements; 1) Smart meters at consumers home side, 2) Metering communication infrastructure between the consumers

homes and utilities 3) Meter Data Management system (MDM). A migration from energy meter system to AMI system requires multiple enabling technologies. One of the main technologies is

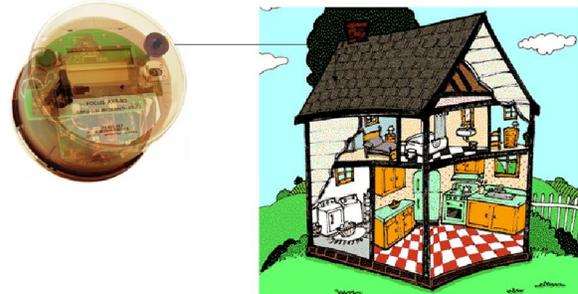


Figure 1: Smart meter inside the house

Smart meter, which is an electrical device attached to houses to collect consumer energy usages information that send to the utility company, including the usage for each electrical device as well as to calculate the bills based on energy utilization [3]. Smart Meters also have the following qualities:

- Interval measurement and storage of consumption data.
- Display of consumption data to consumer.
- Remote connection/disconnection.
- Support for variable energy tariffs.
- Support for demand control.

It's a challenging task to secure such an important component and grid from attacks. As we know that outbreaks can be physical or cyber attacks, the grid must resist against two different attack strategies 1: Attacks on the physical infrastructure of power system. 2: Attacks through the power system, in which the attackers take advantage of power system

communication network for example change his/her billing information by hacking network address [4] etc. According to security point of view, the Smart Grid will resist imbalances in the grid, subject to deliberate IP attack. The Smart Grid will demonstrate resilience to some attacks but all systems operating today have proven vulnerable to determined and well-equipped attackers. Cyber attacks on smart grid can be classified into three categories; component-wise, protocol-wise, topology-wise [5].

The problem is we tackle the security of electricity usage information of consumers particularly in HAN. As privacy is concerned, the scope of the paper focused on two areas (1) Secure Smart Meter from attack (2) Secure data communication between smart meter and utility collector, smart meter is low end device which can be easily misled by attacker, and the communication between smart meter and utility collector in the phase of usage data transformation should also be secured because attacker can easily attack and observe the content of data packets that are being send from smart meter to utility collector during communication. A novel wireless security protocol is proposed for smart meter and advanced metering infrastructure; by introducing a new pair-based scheme to identify the smart meter attacks is also proposed. The Paper will present a coupon usage data protocol to secure threats in information transmission between the smart meters and the utility collector.

The remaining of the paper is structured as follows, section

2 will explain the related work, section 3 will describe the proposed methodology to make the smart grid metering infrastructure more secure and protected from unauthorized access then section 4 will discuss how our proposed solution make the system secure as compare to current unprotected state and finally section 5 will conclude the whole work and discuss some future work that can make the system more efficient and reliable.

## II. Related Work

Marek Jawurek et al. describe that Smart Meter rollouts have begun all over the world. However, real-time monitoring of energy consumption raises many privacy issues. The author focus on the privacy risks of smart metering and discuss the types of data the Smart Grid utilizes and what level of access the different roles of the Smart Grid need for their legitimate business and also provide some scenarios for how this data could be abused by stakeholders of the Smart Grid as well as external attackers [7]. According to Todd Baumeister current electrical power grid is out of date and the Smart Grid is an upgrade that will add many new technologies to meet customers requirements. The

work is separated into different categories; Process Control System (PCS) Security, Smart Meter Security, and Smart Grid Communication Protocol Security [8]. ZigBee Standard is ideal for a low wireless network since it meets all of the requirements of security and businesses. In addition, it supports security in different layers. However, Blaser identifies the security issues in ZigBee related to Symmetric Key Exchanges (SKE) [9]. Depeng Li illustrate validation schemes relying on packet signature and verification introduces heavy cost for computation and communication. Due to its constraint related to resources, smart grids authentication requirement cannot be satisfied by this scheme. Most importantly, it is must to underscore smart grids demand for high availability. He presents an efficient approach to validate data aggregation in smart grid via deploying signature aggregation. Corresponding fault analysis algorithms are contributed to identify forged or error signatures [4]. Both experimental result and performance evaluation demonstrate computational and communication gains [10] Secure Information aggregation for Smart Grids using homo-morphic Encryption deals with the data aggregation usage with homo-morphic encryption passing through a tree when the smart meter transfers the data to the utility collector. This means that each smart meter sends the usage data to neighborhoods smart meter, and then transfers the resultant data to the next smart meter, until the data reaches the collector [11]. Kalogridis proposes a solution to protect data that is stored in the smart meter, so they obfuscate the energy usage. They achieve the goal of protecting privacy by avoiding the identity of the consumption of each electrical device; as a result, the data that is stored in the smart meter cannot determine the habits of consumers. This contribution applies the load signature moderation that combines the consumption of energy from the utility with a rechargeable battery [10].

## III. Proposed Solution

Our proposed security solution has two main parts; smart meter attack detection and passing data coupon between authorized users, to protect the smart meter communication against hackers. There is a utility collector (UC) between a smart meter and utility provider (can be any source of electricity provider i.e. Grid, renewable resources etc.) UC can manage predefined number of clusters of smart meters (CSM) [12].

### A. 1st Component: Smart Meters Attack Detection

It provides a security mechanism to prevent attacker from attacking any smart meter in a cluster controlled by UC. It has four parts 1) Smart meters operation initialization 2) Pair Construction 3) Smart meters Attack detection Process and 4) Detecting

wrong alerts. In all the below steps we consider two smart meters where  $i=1, 2$  forming a smart meters  $s_1$  and  $s_2$  respectively [4].

**1) Phase 1: Smart Meters Operation Initialization:** The utility collector initializes the set of smart meters  $S = S_0, S_1, S_2, S_3 \dots S_n$  to form clusters [13]. Each cluster has a limited number of smart meters defined by utility collector. These Smart meters in a neighborhood clusters can communicate through the utility collector using wireless communication. However, the utility provider also knows about the deployment and initialization for all Smart meter clusters but utility collector manages them all. Phase 1 consists of following steps [14]

- Input: set of un-initialized smart meters  $S^* = S_0^*, S_1^*, S_2^*, S_3^* \dots S_n^*$ . Randomly choose a private key  $X_i$  for each smart meter  $i$ .
- Compute the corresponding public key  $J_i = X_i \cdot G$  here  $G$  is the base of any area provided by UC.
- For smart meter where  $i=1$ ; Preload smart meter  $S_1$  with key pair  $(X_1, J_1)$  and continue in loop until all smart meters are initialized in a specified cluster.
- Output: set of initialized Smart Meter  $S = S_0, S_1, S_2, S_3 \dots S_n$

These steps are shown in figure named Phase 1.

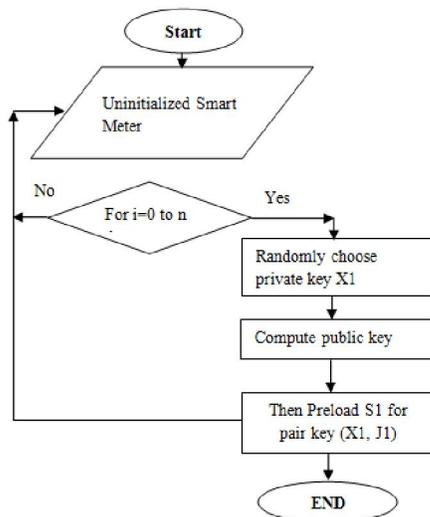


Figure 2: Phase 1; Smart Meters Operation Initialization

**2) Phase 2 (Pairs Construction):** This phase will construct the pair of smart meters; the paired smart meters can send notification to each other for exchanging of information regarding attacks/data [15]. This can be achieved as explained in following steps. The flow chart of these steps is also shown in figure Phase 2.

- Selects a random number  $a$  for any smart meter  $S_1$  to be paired, computes  $A = a \cdot G$ , and get  $(S_1, A)$ .
- After receiving  $(S_1, A)$ , choose one more random number  $b$  and calculates  $B = b \cdot G$  and get  $(S_2, B)$ .
- Then both parties Smart meter  $S_1$ , and  $S_2$  exchange their  $(S_1, A)$  to  $S_2$  and  $(S_2, B)$  to  $S_1$ .
- Next, applies the signature verification process with the help of signature identifier through which they can know that both parties  $S_2$  and  $S_2$  are the real authenticated parties by using signature verification identifier  $A||B||S_1$  as IDA  $(A||B||S_1)$ . In the end, sends  $(S_2, B, IDB(A||B||S_1))$  to  $S_2$ .
- $S_2$  verifies  $IDB(A||B||S_1)$ . If it is valid, creates a signature on  $B||A||S_1$  as IDA  $(B||A||S_2)$  and sends the signature to smart meter  $S_2$ .
- As well in last, they also computes the shared key  $h(a \cdot B) = h(ab \cdot G)$ .
- When verifies the validity of IDA  $(B||A||S_2)$ , also computes the shared key  $h(b \cdot A) = h(ab \cdot G)$ . As  $A = a \cdot G$   $B = b \cdot G$   
 $S_1 = h(a \cdot B) = h(a \cdot b \cdot G) = h(ab \cdot G)$   $S_2 = h(b \cdot A) = h(b \cdot a \cdot G) = h(ab \cdot G)$   $S_1 = S_2$  (same keys so build pair)

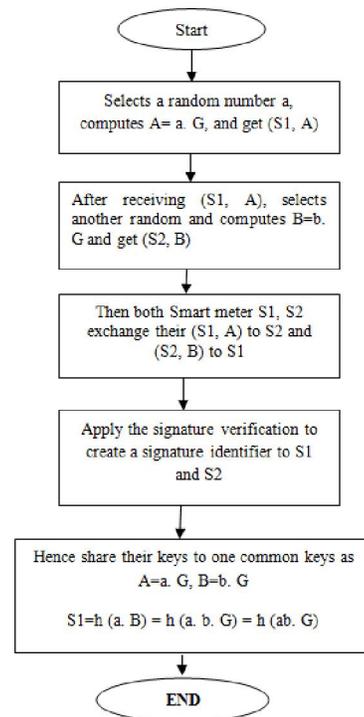


Figure3: Phase 2; Pair Construction

**3) Phase 3 (Smart Meter Attack Detection Process)**

There are four types of Alerts in attack detection process that can be sent between the couples. Suppose  $S_1$  sends 4 types of Alerts to  $S_2$  [13] which is explained in the below steps while the alert format is (key||specifiedsmartmeteraddress||alertnumber). Figure phase 3 also shows these steps.

- Normal Situation Alert means no Attack When  $S_1$  send
- Alert = (KI ||  $S_1$  || 1) to  $S_2$ .
- Attack Situation Alert means  $S_1$  is under Attack When  $S_1$  send Alert = (KI ||  $S_1$  || 0) to  $S_2$ .
- Undefined Attack Alert means where  $S_2$  will not receive valid alert from  $S_1$ .
- Maintenance situation alert, When  $S_1$  sends Alert = (KI ||  $S_1$  || 2) to  $S_2$ .

At Last, the utility collector will get a usage report about each smart meter in the Neighborhood area network (NAN), and will initiate an action according to alert type.

**4) Phase 4 (Wrong Alert Approval)**

In some conditions, a smart meter can be under maintenance process performed by utility company [16]. We need to differentiate it from other possible unusual conditions. In this phase there is a communication between Maintenance device M and Smart Meter.

- Maintenance device M connects with Smart meter  $S_1$ .
- $S_1$  Generate random number R1 with time stamps  $TS_1$  as ( $TS_1$  || R1) and sent to M.
- M device sign challenge with  $X_m$ ; private key of M and send challenge as  $RS_x(TS_1 || R1)$  to  $S_1$ .
- $S_1$  Verify the challenge then  $S_1$  send exception III to  $S_2$  to clear false alarm c.

There are four types of Alerts in attack detection process that can be sent between the couples. Suppose  $S_1$  sends 4 types of Alerts to  $S_2$  [17] which are explained in the below steps while the alert format is (key||specifiedsmartmeteraddress||alertnumber).

**B. 2nd Component: Coupon Usage Data Protocol**

Coupon passing technique helps to improve the security of communication between the smart meter and utility collector and prevents attacker from identifying each household's energy usage information sending by smart meter to UC.

**1) Phase 1: Coupon Operation Initialization: Utility providers generate the public and private keys for each**

utility collector UC; each utility collector has a pair of keys as private and public key. The utility collector UC encrypts the coupon with the private key and sends it to smart meters at the network.

- Input: un-initialized utility collectors.  
UC = UC0, UC1, UC2, UC3...UCn
- Randomly generate two large prime numbers (a and b); a private key xi (a, b)
- Compute the corresponding public key  $Y_i = a \cdot b$
- Preload smart meter UC with key pair (xi,  $Y_i$ ) and then again loop start for more initialization.
- Output: initialized Smart Meter UC = UC0, UC1, UC2, UC3...UCn

**2) Phase 2: Attaching information (electricity usage information) to Coupon:**

To enhance the security of AMI, and to protect the communication between the utility collector and the smart meter all the smart meters will attach their electricity consumption details in the encrypted form to the coupon on their turn it's the responsibility of the coupon to transfer information without any interruption to UC. Following are the steps when Coupon circulates in any cluster [14].

- $S_1$  having ID1 give the Current electricity consumption Data D1 with time stamps  $TS_1$  and random number R1. As ( $ID_1 || U_1 || TS_1 || R_1$ )
- $S_1$  Also obtains Utility Collector public key  $Y_c$ .
- $S_1$  encrypts the Data D1 with obtains Utility Collector public key  $Y_c$ .
- Then  $S_1$  attached the encrypted data to the coupon.s

Figure shows how coupon passed between the utility collector and the smart meter. There are three basic essentials in securing information (data usage) Firstly the UC public key can only encrypt the Coupon; only UC can decrypt the data. Attacker cannot establish own coupon, and then send it to the smart meters since the smart meters report only to a valid coupon, which is sent by the utility collector [13]. Secondly When S encrypts the data with  $Y_c$ , this resist an attacker from observing the data also adding R1, D1 and  $TS_1$  will avoid an attacker from attack, because the utility collectors public key could be hacked but it is rear to hack the whole combination.

Finally all smart meters must report encrypted data to coupon and also must wait for authorized coupon even if SM has is no data to be sent [17].

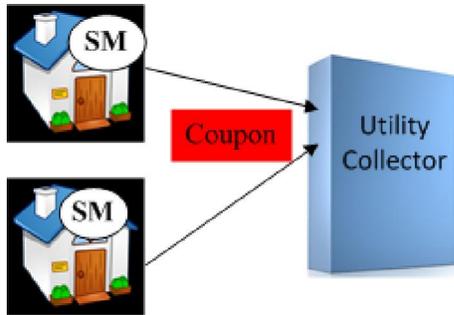


Figure 4: Utility collector and smart meter

**IV. Simulation Environment**

Consider n smart meters randomly deployed in an area of 60m. The parameters used are given as follows [18]:

- The number of smart meter n, which varies from 12 to 24.
- The alert information alert is set as 2, 4, 8 and 12 seconds respectively.
- The threshold value Th of exception detection is in the range of  $1 \leq Th \leq 3$ .
- The time Tc when an attacker A attacks on smart meter, varied in the range of 30 to 60 seconds.

Network tested with different parameters. In each case, 1000 networks are established, the average detection rate all of these networks examined. Here

$$DRS = \frac{DAS + NAS}{TAS}$$

DRS= Detection rate on smart grid.

DAS= number of detected attacks on SM.

NAS=number of new detected attacks on SM.

TAS= number of attacks in the Test Data Base of SM.

FR= False rate.

FA= Number of false alarms.

FS= Number of alert in detection.

$$FR = \frac{FA}{FS}$$

Detection Score (DS)

$$= DR + \left[ \frac{DAS}{NAS + DAS} * \frac{DRS}{DRS + FRS} \right] - \left[ \frac{1}{FS} * \frac{FRS}{DRS + FRS} \right]$$

After calculating the results with the help of above equations; it can be seen in graph that our proposed Solution improves the attack detection rate as compare to existing smart meter security system. Proposed solution will improve the security performance by 60 percent [19].

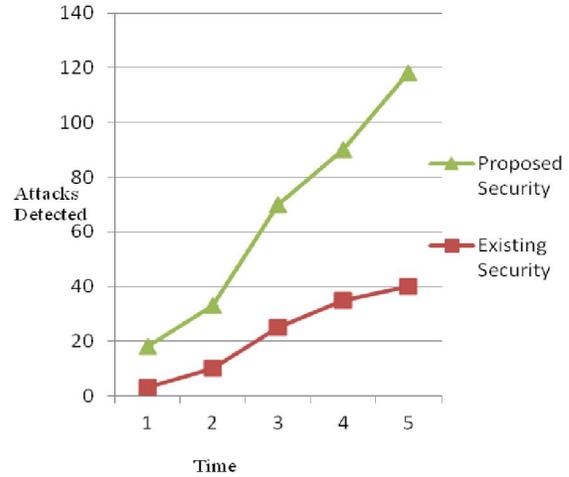


Fig. 5: Attack detection rate comparison

**V. Conclusion And Future Work**

There is advancement in current electric power grid by smart grid, which offer users a flexible, adaptable, real time and secure environment. A security protocol is required to achieve the objective of this secure communication network. In this paper a security solution is provided to detect the attacks on smart metering infrastructure as well as on the communication network its not only enhance the attack detection rate but also overcome the effects of attacks by communicating with utility collector and neighboring clusters of smart meters. Proposed solution has two main components meter attack detection and using coupon technique to reduce the chances of attacks. From the simulation results it shown that our proposed solution makes the smart grid 60 percent more secure as compare to existing security mechanism. There are still many open issues in smart grid security; communication protocols should consider grid characteristics, adaptive security and network scalability before applying any security technique. A cooperative game theoretic approach can be used in smart meter pair construction phase to achieve authentic results.

**References**

1. T. Flick, "Hacking the smart grid," FYRM Associates, Tech. Rep., 2009.
2. Verbauwheide and P. Schaumont, "Smart grid, security and eda," 2011.
3. M. Jawurek and F. C. Freiling, "Privacy threat analysis of smart metering," 2010.
4. S. Spoonamore and R. L. Krutz, "Smart grid and cyber challenges," National Security Risks and Concerns of Smart Grid, March 2007.
5. M. Jawurek and F. C. Freiling, "Privacy threat analysis of smart metering," 2012.

6. B. J. Murrill, E. C. Liu, and R. M. T. II, "Smart meter data: Privacy and cyber security," CRS Report for Congress, February 3, 2012.
7. T. Baumeister, "Literature review on smart grid cyber security," Decem- ber 2010.
8. D. Wei, Y. Lu, M. Jafari, and P. M. Skare, "Protecting smart grid automation systems against cyber attacks," IEEE TRANSACTIONS ON SMART GRID, vol. VOL. 2, NO. 4, DECEMBER 2011.
9. X. W. S. M. IEEE and P. Yi, "Security framework for wireless communications in," IEEE TRANSACTIONS ON SMART GRID, vol. VOL. 2, NO. 4, 2011.
10. S. McLaughlin, D. Podkuiko, and P. McDaniel, "Energy theft in the advanced metering."
11. Kosut, L. Jia, R. J. Thomas, and L. Fellow, "Malicious data attacks on the smart grid," IEEE TRANSACTIONS ON SMART GRID, vol. VOL. 2, NO. 4, DECEMBER 2011.
12. Building Couples to Early Detect Node Compromise Attack in Wireless Sensor Networks, 2009.
13. S. R. Rajagopalan, L. Sankar, S. Mohajer, and H. V. Poor, Smart Meter Privacy: A Utility-Privacy Framework, August 6, 2011.
14. C. Bekara, T. Luckenbach, and K. Bekara, "A privacy preserving and secure authentication protocol for the advanced metering infrastructure with non-repudiation service," The Second International Conference on Smart Grids, Green Communications and IT Energy-aware Technologies, 2012.
15. S. Gerasimenko, "The evolution of wireless home networking."
16. J.-S. Lee, Y.-W. Su, and C.-C. Shen, "A comparative study of wireless protocols: Bluetooth, uwb, zigbee, and wi-fi," The 33rd Annual Confer- ence of the IEEE Industrial Electronics Society (IECON), 2007.
17. D. Niyato, L. Xiao, and P. Wang, "Machine-to-machine communications for home energy management system in smart grid."
18. N. E. Sanchez, "The rabin cryptosystem," 2010.
19. Rial and G. Danezis, "Privacy-preserving smart metering," October 17, 2011.

4/8/2014