Authentication Mechanism to Prevent Smart Meter Impersonation in Smart Grid

S. Anbarasan[1]
Pg Scholar,
Dept. Of Information Technology,
Kongunadu College Of Engineering And Technology,
Trichy, Tamil Nadu

R. Karthick[2]
Assistant Professor,
Dept. Of Information Technology,
Kongunadu College Of Engineering And Technology,
Trichy, Tamil Nadu

S. Kalaivanan[3]
Assistant Professor,
Dept. Of Information Technology,
Kongunadu College Of Engineering And Technology,
Trichy, Tamil Nadu

S. Kaarthiga[4],
Pg Scholar,
Dept. Of Information Technology,
Kongunadu College Of Engineering And Technology,
Trichy, Tamil Nadu

***Abstract*—The smart grid has emerged as the significant technology in the power distribution. It integrates information and communication technology with the legacy electrical power systems. It uses wireless data transmission technique for some parts of its communication systems. This will lead the possibility of security vulnerabilities in its communication. Advanced metering infrastructure (AMI) is architecture for automated, Bi-directional communication between a smart meter with an IP address and a utility company. The objective of an AMI is to provide utility companies with real-time data about power consumption and allow customers to make informed choices about energy usage based on the price at the time of use. The smart meter is the significant device in this smart grid environment and it has more security challenges to be considered. This proposed work has addresses one of the security challenges called smart meter impersonation. An intruder impersonates as smart meter and communicates with the gateways (Smart Meter) of different types of hierarchical communication framework in unauthenticated manner. The proposed mechanism provides a novel authentication mechanism and strong key establishment using public key infrastructure with public key certificate and also uses Hash based message Authentication code (HMAC) with digital signature to ensure message integrity.**

***Index Terms*— Advanced metering infrastructure (AMI), communications, Home area network (HAN), security, smart grid (SG), smart meters (SM).**

I. INTRODUCTION

In recent years smart grid has becomes the crucial topic and it makes the attention for the engineers and researchers in the field of both communication and electrical power system. Nowadays the power distribution corporation facing major challenges on the demand and availability because of the growing global population. The smart grid provides the improvement of efficiency and the availability of power system by constantly monitoring, control and managing the demands of customer. The smart grid has composed of millions of devices that connected with each other.

The Advanced Metering Infrastructure (AMI) is the communication infrastructure used for smart grid communication. It consists of different types of intelligent components, such as smart meters, communication networks and data management systems that enable bi-directional communication between utilities and customers to share the power consumption and other information by wired and wireless communication technologies [3]. The smart grid has normally divided into two different layers those are power system layer and communication layer [5]. The power system layer consists of the following bulk power generation, power transmission system, and power distribution system and customer premise [5]. The communication layer consists of wide Area Network (WAN), Neighborhood Area Network (NAN), Building Area Network (BAN) and Home Area Network (HAN) [1][4].

The each communication layer has its own wired and wireless communication network technologies [5]. Ethernets based cable networks are used for wired communication. In wireless technology IEEE 802.11 based WiFi, IEEE 802.15 based ZigBee, GPRS and 3G/4G can be utilized [5]. The communication layers which uses wireless communication faces several security threats that affects security requirements of smart grid communication [1][6]. The each communication layer has its own security threats such as Eavesdropping, Smart meter impersonation, Denial of service and Device impersonation, Gateway (HAN, BAN, and NAN) impersonation, Man-in-the middle and replay attack [1].

The remainder of this paper is organized as follows. In section II has defines related research works on this paper. In section III the system model has explained and the components which are used in the smart grid are discussed, the security requirements and issues are taking into account and packet structure of the smart grid communications has examined. Section IV describes the Proposed Authentication mechanism to prevent the smart meter impersonation followed by conclusion in section V.

II .RELATED WORKS

The smart grid communication technologies, standards and communication requirements are addressed here in [1]. The communication system model is the crucial part of the smart grid communication. There are different kinds of SG

communication layers are studied in [2]. [3] [4] has defines the details of the smart grid communication hierarchies such as Wide Area Network (WAN), Neighborhood Area Network (NAN), Building Area Network (BAN), Home Area Network (HAN). The technologies that has been used by the each tier of the communication network also discussed in [3] [4].

In [2] [3] [5] the security threats that encountered by the smart grid has considered. That detailed the two different types of security threat such as passive and active attack possibly in smart grid communication layer particularly when using wireless transmission medium. These security issues are lead to the need of security requirements that desperately required for secure smart grid communication, those security requirements are thoroughly discussed in [2] [6] [] . In [2] Public Key Infrastructure has proposed for most of the security threats to meet the security requirements. [6] has proposed the framework for solution to secure the Home Area Network (HAN) against all possible security issues in HAN.

In [7] they addressed the privacy challenges in the smart grid communication especially between the customer premise and the utility providers. This paper address the Men-in-the – Middle attack, spoofing and replay attack when transmit the message between smart meter and energy supplier and provide improved privacy solution using Mutual authentication mechanism.

III. SYSTEM MODEL

A. Communication Infrastructure

The communication infrastructure has commonly categorized into different layers such as Home Area Network (HAN), Building Area Network (BAN), Neighborhood Area Network (NAN) those explained as follows.

1) Home Area Network (HAN): In SG consideration a HAN is the lowest end of the hierarchical structure i.e., at the customer end. The HAN manages the on demand power requirements of the customer. This has connects the appliance to a smart meter (HANGW) using the wireless radio communication device Zigbee based on IEEE 802.15.4. The communication range for Zigbee device is 10 to 100m with low power requirement is enough to transmit the data when compared to other wireless solution such as WiFi based on IEEE 802.11, Bluetooth and other electrical home appliance as in Table I. The communication cost is feasible while using Zigbee in the HAN environment.

2) Building Area Network (BAN): The Building Area Network is second tier of the SG communication Infrastructure and it consists of number of Home Area Networks (HANs). This BAN Network has BANGW (smart meter) that installed at the building feeder used to monitor the power requirement and usage of residents of the building. For the BAN to HAN communication we use WiMax that cover more area to facilitate.

3) Neighborhood Area Network (NAN): The neighborhood Area Network is the upper layer in the smart grid communication hierarchy. It consists of a number of Building Area Network (BAN) and it has NANGW (smart meter) used to monitor the power distribution to a particular neighborhood area by the corresponding distribution substation. The WiMax or Broadband wireless technology may be used for the communication between NAN to BAN.

TABLE I. POWER REQUIREMENT OF DIFFERENT APPLIANCE IN A TYPICAL HAN

Electrical Appliance	Power requirement (KW/hr)
Air conditioner	1
Refrigerator	0.2
Microwave oven	0.1
Light bulbs	0.05
Personal computer	0.2

B. Components

1) Smart Meter: The smart meter act as the gateway between Home appliance and other external entities. The each layer in the communication infrastructure has smart meter which is act as the gateway between other communication layers. The each layer has different configured smart meter to process the information [3].

2) Household appliance: In the Home Area Network scenario the smart appliances are the important communication devices that communicate with the smart meter for power requirement and sends the information about power consumption. The legacy Home appliances are not having this communication capability.

3) Electric Utility: The electric utility has used to send the power consumption related details to smart meter and collect the power usage report on hourly manner and also collect error notification using GPRS technologies. Utility has regulates the power consumption, means that utility will instruct the smart meter to limit their usage in on-peak hours by providing incentives.

4) Service Provider: The service provider has the vital role in the smart grid communication. They have register with the electric utility and obtain the digital certificate for their identities and encryption keys. The service provider establish contract with the user and use the smart meter to send the information to internal device and the service provider. The smart meter only communicates with the service provider who has valid certificate.

C. Security Requirements and Threats

In the smart grid communication each communication layer has encountered the security threats according to their specification and configuration of network. These security threats lead to the need of security requirements for securing the SG communication. The followings are the some major security requirements against security issues.

1) Entity Authentication: Each communication layer has the different entities and we have to ensure that the message transmitted between authenticated entities. This requirement has resisted the attacks such as gateway spoofing (HAN, BAN and NAN) and device spoofing in HAN scenario.

2) Confidentiality: In SG environment the confidentiality has ensures that the sensitive information that transmitted between two end points are not disclosed to any other third parties. The data encryption standards are used here to ensure

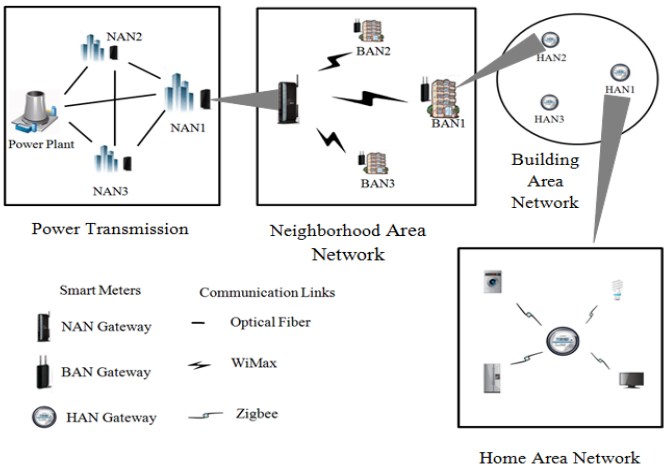

Fig.1. SG Communication Framework

the confidentiality against security attacks such as eavesdropping, traffic analysis.

3) Data Integrity: This requirement is to ensure that the received data between the two entities of smart grid communication environment is not altered or replayed. Different types of information such as power usage, information about electricity charges and control messages are important in SG communication. The alteration in these things leads to the big security issues such as Men-In-The-Middle, Masquerade, modification and replay.

4) Privacy Preservation: The collection and gathering of data by smart grid has increased the privacy related issues. The smart meter has the information about customers, percolation of these information to intruder leads to the serious issues to the consumers. The privacy issue is that the analyzing of network traffic such as frequency patterns, message length lead an adversary to enable the cyber attacks.

TABLE II. ADOPTED PACKET STRUCTURE

Security Header
TCP/IP Header
MSG Header
Raw Message

D. Packet Structure

The data packets send between smart meter and other entities should be follow standard packet format. The packet communication may happen in the form of uni-cast, multicast and broadcast the packet structure has adopted from [3] as shown in Table II. This has four sections such as security header, TCP/IP header, message header and raw message. In this Security Header has security protocols and TCP/IP Header has Meter ID (MAC), Equipment Status and Message type The Message types and Raw message has defined in the Table III.

TABLE III. MESSAGE TYPE

	Type of Message	Description			Size
1	Command/Request	To update meter, to control load, etc.			25 Bytes
2	Meter Periodic Data Read	Real Power (kW)	Reactive Power (kVAr)	Voltage	32 Bytes
3	Confirmation/Notification Message	Failure notification, message			25 Bytes
4	Meter sends Error Report	This report is produced when failure occurs			18 Bytes
5	Meter sends Performance Report	This report is scheduled to determine meter performance			150 Bytes
6	Meter sends Outage Report	Outage report is sent after the supply has been restored			14 Bytes
7	Weekly read submission	Output data after one week			28 Bytes
8	One Month of data	Meter sends one month of data			40320 Bytes
9	Last day import data	Summary of usage on the last day			192 Bytes

IV. SECURE KEY ESTABLISHMENT AND MUTUAL AUTHENTICATION MECHANISM

In the previous section we analysis the security requirements which are essential for secure smart grid communication. The lack of each security requirements leads to serious security issues. This proposed work has addressed the smart meter impersonation and provides the novel multilayer mutual authentication with key establishment mechanism to prevent this security attack. As we discussed earlier in previous section the each communication layer in the smart grid environment has the smart meter and it act as the communication gateway. It also aggregates the information and sends it to next tier of communication layer. In this any intruder impersonate itself as the smart meter and transmit the information to the other smart meter or aggregation gateway. So we need a strong secure authentication mechanism which satisfies security requirements such as authenticity, confidentiality and integrity of information that have transmitted.

In this proposed work we propose a strong key establishment and mutual authentication mechanism using public key Infrastructure. For the secure key exchange we use SSL (Secure Socket Layer) based digital certificate with hash based authentication. Message transmission has used digital signature for message authentication with message that encrypted by previously shared secret session key. The time stamp has used to avoid replay attack. Let we assume that we have two communication end points Smart meter(SM) which is in the Home Area Network(HAN) and HAN Aggregator(HAG) which is collects the information from the smart meters in different Home Area Network(HAN). The each end point has pre-defined Mutual Key (MK) when it is installed.The proposed system has the following procedure to establish the secure communication between SM and HAG.

1. The smart meter (SM) sends the authentication request to the HAN Aggregator (HAG).

2. HAG transmit its Public key certificate, the certificate consists of the following contents:
   $Cert_H = \{id, Pubk_H, E\}$

3. SM verifies the certificate and obtains HAG's Public key.

4. Then, SM generates a symmetric session key (*SSK*) and encrypt it with HAG's Public key and transmits the encrypted Symmetric session key (*SSK*) to HAG.

5. The HAG decrypts the SSK using its own Private Key ($Prvk_H$).

6. HAG generates the random number '*a*' and computes the following hash value I_1:
   $I_1 = H(SSK, MK, a)$ and encrypt this hash value by following way i.e., $J_1 = ESSK(I_1, a)$.

7. HAG transmits J_1 to SM and it decrypts J_1. From that SM obtains I_1 and random number *a*. Then using *SSK*, *MK* and *a*, it calculate I_1 and checks with previously received I_1.

8. If step 7 is satisfied the SM generates random number 'b' and computes the following hash value I_2:
   $I_2 = H(SSK, MK, b)$ and encrypt this hash value by following way i.e., $J_2 = ESSK(I_2, b)$.

9. SM transmits J_2 to HAG it decrypts J_2. From that HAG obtains I_2 and random number *b*. Then using *SSK*, *MK* and *b*, it calculates I_2 and checks with previously received I_2.

10. If step 9 satisfied SM calculates *HMAC* using message with *SSK* and sign this hash value with Symmetric Session Key.
    $SIG_{SSK}\{HMAC(SSK,M)\}$

11. Then SM transmits the message *M* with digital signature and time stamp *T* encrypted with Symmetric Session Key (*SSK*).

    $\{M||T||\ SIG_{SSK}\{HMAC(SSK,M)\}\}$

These all eleven steps are processed in each session of the message transmission between smart meter and HAN Aggregator.

This proposed mechanism has pre-shared Mutual Key and each session the HAG sends public key certificate based on the concept of Secure Socket Layer (SSL) communication to Smart meter. This certificate consist the device *id*, HAG public key ($Pubk_H$) and expiry time of certificate (*E*). Then the smart meter generates Symmetric session key and encrypts it using HAG's Public key and send it to the HAG which has sends the valid certificate to Smart Meter. The legitimate HAG can only decrypt the SSK using its private Key. The Symmetric key cryptographic algorithms such as Data Encryption Standards (DES) and Advanced Encryption Standards (AES) are used for Symmetric key generation. The hash function has generated using Symmetric Session Key, Mutual Key, and random number '*a*'. Based on the hash function the mutual authentication between HAG and Smart meter (SM) has performed for each session. This has ensures the Entity authentication for both communication end point. After securely transmits the session key the message has to be processed. The message transmission has started from step 10 to Step 11.

We can analyze the possible of smart meter impersonation here, when the intruder impersonate him/her self as smart meter and perform the mutual authentication and key exchange and tampers the transmitted message between Smart Meter and HAN Aggregator, the smart meter impersonation has occurs. In the proposed system if an intruder obtains the HAG's public key certificate and replace it with his/her own certificate. Then, from that he/she attempts the attack to obtain the Symmetric Session Key generated by Smart Meter. However, the attacker has known the SSK he/she cannot generate the hash value, since he/she doesn't know the previously shared Mutual Key. So, only the legitimate end points can transmits and receives the messages. During the message transmission we use Hash based Message authentication code with the digital signature to achieve the message integrity with Non-Repudiation. We also used the Time stamp to avoid the replay attack. So, this proposed mechanism has achieves three different types of security requirements such as Entity authentication, confidentiality and message Integrity by this single mechanism.

V. CONCLUSION

In this proposed system, we have analyzed the security requirements such as entity authentication, availability, confidentiality and integrity that need for Smart grid wireless communication and discussed privacy and security threats. This proposed system has addressed the one of the security challenge called smart meter impersonation which needs the strong entity authentication. The proposed system has provides the strong key establishment using public key certificates and Symmetric session key and pre-shared mutual key ensures the mutual authentication and confidentiality. Hash based Message Authentication Code (HMAC) with digital signature has ensures the message integrity. Thus the proposed system can prevent an intruder from transmitting message by impersonate as smart meter through this strong mutual authentication.

REFERENCES

[1]. Daojing He, Sammy chan, Ya Zhang, Mohesen Guizani, Chun chen and Jiajun Bu., "An Enhanced public key Infrastructure to Secure Smart Grid Wireless Communication Networks" IEEE Network January/Februery 2014.

[2]. J. Liu et al., "Cyber Security and Privacy Issues in Smart Grids," IEEE Commun.Surveys Tuts., vol. 14, no. 4, 2012, pp. 981–97.

[3]. Mohamad Badra and Sherali Zeadally., "An Improved Privacy Solution for the Smart Grid" International Journal of Network Security, vol.0, No.0, pp.1.

[4]. Mostafa M.Fouda, Zubair Md. Fadlullah, Neikato, Rongxing Lu, Xuemin (Sherman) Shen., "A Lightweight Message Authentication Scheme for Smart Grid Communications" IEEE Transactions on smart grid, Vol.2, No 4, December 2011.

[5]. Soohyun Oh and Jin Kwak., "Mutual Authentication And Key Establishment Mechanism Using Dcu Certificate In Smart Grid" Appl. Math.inf.Sci.6 No.1s pp. 257S-264S (2012).

[6]. Vinod Namboodiri, Visvakumar Aravinthan, Surya Narayan Mohapatra, Babak Karimi and Ward Jewell., "Toward a Secure Wireless-Based Home Area Network for Metering in Smart Grids" IEEE System journal, Vol.8, No.2, June 2014.

[7]. Zubair A.Baig and Abdul-Raoof Amoudi., "An Analysis of Smart Grid Attacks and Countermeasures" Journal of Communication Vol.8, No.8, August 2013.