Monitoring Approach for Detection Compromise Attacks in Smart Meter

Mohammad Hossein Yaghmaee
MEEDC – Iran
yaghmaee@ieee.org

Qurban Ali FRUGH
MEEDC – Iran
Qurbanalifru@gmail.com

Malihe BAHEKMAT
MEEDC – Iran
bahekmatm@yahoo.com

ABSTRACT

The smart-metering system measures and manages the consumption of power, gas and water. Smart metering system is controlled by the remote provider of this service. Given that smart meters are installed in unsafe places (outside houses), there are some challenges in the physical security of these devices. In other words, according to the previous studies and our knowledge, one of strongest challenges facing the smart meters is JTAG interface. A potential adversary can reprogram the board through this interface and compromise the key components of this device including keys, privacy of consumers and other information. In this paper, a monitoring scheme for detecting compromise attack has been proposed. In this scheme, at least two smart meters are used for monitoring one smart meter. To ensure security, the ring architecture was designed to provide high security in a hierarchical structure.

INTRODUCTION

Smart Grid (SG) is a new term which has attracted the growing interest of engineers and researchers in the field of electric power and communication[1]. Smart grid is designed to both effectively produce and consume power and manage the consumer and producer. Today, control data, reading power meters and consumers' information are exchanged in real-time between consumer and producer. Thus, in order to break this connection and obtain personal information of people, an adversary seeks to access these systems by any means. The purpose for obtaining access to such information and resources might be financial or economic or disclosing the identity of the consumer and so on. One of these challenges is cyber-attack or simply, software errors which allows the contents of any remotely controlled smart meter to be switched off by pressing a few keys.

Moreover, remote software upgrade and complex functionality, different wireless communication systems or combination of various technologies such as 3G, WiMAX, WiFi, ZigBee and Optical fiber create more complications. However, we need data connection and cheap communication systems with proper security. On the other hand, an adversary tries to access these systems. It intends to break the secure transfer of data and compromise the privacy of consumers and key materials of these systems.

JTAG interface is one of the access schemes which can be reached physically in the absence of required security measures to deny the access of the unauthorized people. Smart meter is the main part of the Advanced Metering Infrastructure (AMI). Smart meters are systems which make daily or monthly reports of power consumption and control the electricity in a two-way communication between the subscriber and the provider. Smart metering, also, can be remotely controlled. It promotes the efficiency of power consumption and exchanges the sensitive data between consumer and producer of the power. Such data include metering and personal information of consumers which are exchanged in a two-way communication. In terms of the security, these devices are installed in unsecure places outside houses[2].

Physical counterfeiting is the first threat facing smart meters. The AMI technology increases the risk of BOBA (Break-One Break-All) and compromise every smart meter in the network[3], [4]. One of these threats is compromise attack launched by JTAG interface. Using open source tools known as KillerBee, JTAG interface could be accesses by an adversary. In addition to physical security level, AMI meters provide real-time alerts too. Moreover, the advanced circuitry of AMI meters allows the detection of complex counterfeiting. In smart power grid, there is a common communication structure known as hierarchical structure which includes LAN, BAN and NAN. It is used to establish communication between smart meters in the gateway.

In this structure, it is essential for each Local Area Network (LAN) to be authorized by Building Area Network (BAN) as each BAN requires to be authorized by Neighborhood Area Network (NAN) [1]. Smart meters can be used in all LAN, BAN and NAN. That is, smart meters act as a gateway between networks. NAN and BAN network are comprised of multi BAN and LAN sub networks, respectively. It is assumed that there are multi LANs in a BAN and each LAN has one smart meter which sends the electricity usage of each subscriber to the control center [5]. It should be noted that attacks might be launched from several smart meters by an adversary. In this case, our proposed model is more reliable in detecting attacks.

SYSTEM MODEL

In this section, we discuss security requirements, network and attack model. We also describe the proposed model.

A. Security Requirements

The security of the proposed model depends upon the security of Rabin encryption system. Due to computation all imitations, we believe that Rabin encryption system is an appropriate encryption scheme for providing security between smart meter and the control center. This scheme is based on public key. Smart meters, as discussed earlier, suffer from limitations in terms of computing capability [1], [6]. Therefore, we should look for encryption schemes which are able to accomplish two goals. First, they should have the necessary security; second, they demand lower computing capability. Rabin encryption system is the variant of RSA encryption which require lower computation capability.

Rabin encryption system requires lower computation capability for encryption, yet it demands higher processing for decryption. This scheme is shown in figure 1 [2]. Alice encrypts a massage using public key and sends it to Bob.

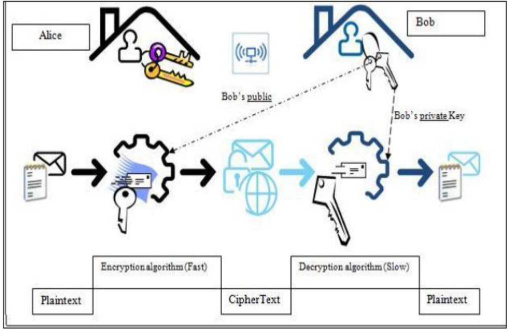

Figure 1. Rabin encryption system

Bob decrypts the text using the provided private key. This process has been shown in the flowing steps:

1. Key generation: Bob generates two keys, one for encryption (public key) and the other for decryption (private key).

a. Two random prime numbers, p and q, which are distinctive in terms of size, are generated.

b. $n = q * p$.is computed.

c. The public key is *n* and the private keys are (p, q).

2. Encryption: Alice receives the public key, i.e. n, from Bob and encrypts M message for Bob.

a. The message expresses the plaintext as a number.

b. The text computes $C \equiv m^2 modn, c\epsilon N$

c. It sends *C* to Bob.

3. Decryption: Bob receives *C* from Alice.

a. 4 messages recover the plain texts, i.e. m1, m2, m3 and m4, then $m_i^2 \equiv cmodn, i1,4$ is computed.

b. The plaintext is distinguished from four messages.

c. The original message recovers m.

Rabin encryption system is faster than its decryption, because the encryption only involves modular squaring. Thus, Rabin system decryption operation is similar to RSA.

B. Network Model

Using the hierarchical structure, it has been assumed that S meters have been installed in BAN network and each smart meter covers a LAN. In the network model we consider S smart meters in the BAN include: $S = (S_0, S_1, S_2, \dots, S_n)$

C. Attack Model

Given that the smart meters are located outside houses, it is assumed that the adversary has physical access to at least one smart meter and is ready to launch a compromising attack through JTAG interface to disclose keys and other information. For example, such attacks are possible by using open sources tools known as KillerBee.

Additionally, the adversary can carry out passive attacks such as eaves dropping by using powerful devices. It has been assumed that this attack model enables the adversary to violate the privacy and identity which decreases the performance of the smart meter.

D. Design Goal

This paper aims to provide security and privacy in smart meters using a monitoring scheme. The results of this research can help identify schemes for detecting compromise attack aimed at smart meters. As a result, each smart meter with a ring will be aware of the adversary's attempts to launch an attack. Thus, it will be able to send an alarm to control center. In this scheme, Robin public key has been used to improve privacy [7].

In this regard, some considerations have been illustrated below.

1. Sending data via low-rate communications: each smart meter can send/receive data from a neighborhood via a secure technique that protects privacy.

2. Cost effectiveness: A large number of smart meters might be purchased for a project, thus the provision of privacy will be of paramount importance. For example, for a promising security infrastructure, we need PKI which may protect the consumer's privacy.

3. Protecting the privacy of consumer in a communication channel: various risks threat the consumer privacy at different levels, such as reviewing online bill or calculating the billing system. As the result, this research focuses on providing privacy for communication channel between the smart meters.

4. Other security goals: Some goals that should be considered in order to protect transmitted information in BAN include confidentiality, accuracy, authentication, and non-repudiation.

PROPOSED *MONITORING* SCHEME FOR COMPROMISE ATTACKS

As mentioned earlier, one of the vulnerabilities of smart meters is JTAG interface. For example, this interface has been built primarily for debugging CS7401xx Microcontroller. It is physically accessible to an adversary in unsecure environment. Thus, due to this vulnerability, an adversary can figure out the all keys in less than a minute[8]. [2],[9] are examples of a strong physical attack on a smart meter to disclose the internal circuitry or compromise attack through JTAG which are normally observable. As shown in figure 2, aimed at detecting the compromise attack, the proposed model is based on the ring. In this scheme, it has been assumed that at least one meter is monitored by two other meters in order to detect compromise attack.

After the detecting an attack, an alarm message is sent to the control center by two neighbor meters. In the proposed structure, each meter has two-way communication with two neighbor meters.

To detect a compromise attack in BAN, four steps are taken:

1. Smart meters initialization
2. Ring building

3. Smart meters compromise detection
4. False alarm clearance

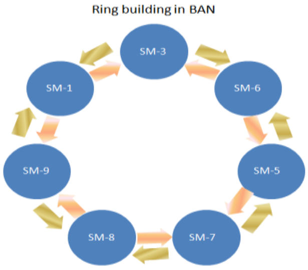

Figure 2- Ring Building in BAN environment

A. Smart meters initialization

The utility collector initializes smart meters by applying Algorithm 1. Utility collector sets up the initialized smart meters in a neighborhood via wireless communication.

Algorithm 1 Smart Meter Initialization

```
1.      Procedure SmartMeterInitialization
    Input un-initialization smart meters $S = (S_o, S_1, S_2, \dots, S_n)$
Output initialization $S = (S_o, S_1, S_2, \dots, S_n)$
2.      for i = 0 to n do
3.      randomly choose a private key $x_i \in [1,1-r]$
4.          Compute the responding public key $Y_i = x_i.G$
5.          Preload smart meter Si with key pair $(x_i, Y_i)$
6.        End for
7.       Return initialized $S = (S_o, S_1, S_2, \dots, S_n)$
8.      End procedure
```

However, the utility provider is responsible for deploying and installing all smart meters. As a result, the utility collector selects an acceptable elliptic curve E and builds Tiny ECC based on G point and R order in E.[2]

The BAN environment is installed. Therefore, $S_i$smart meter may have many neighbors to communicate with [2]. Utility collector initializes smart meters $S = (S_o, S_1, S_2, \dots, S_n)$ by applying the Algorithm 1.

B. Ring building

In the proposed model, all smart meters in BAN monitor each other to detect compromise attack. In this model, meters can launch Ring building by Zigbee mode, after which two meters can monitor one. As a result, the control center responses quickly and run the appropriate command. For example, a pair of smart meters has been installed within a transmission range in a BAN according to figure 3. The Ring architecture in a BAN environment has been shown in Figure 4.

C. Smart meters compromise detection

In this section, four notifications that are sent betweenS_i, S_j and St during each interval time are introduced. The first notification is the normal situation, where S_i computes$K_i = K_i + 1$, then it sends Beaconi = $h(k_i, R_i || S_i || 1)$ to S_j and S_t. The second notification is the detection which computes$K_i = K_i + 1$, and sends Beaconi = $h(k_i, R_i || S_i || 0)$to S_j and S_t. The third notification is the fake or unreserved Beacon, where S_i does not receive any valid beacon from S_i .

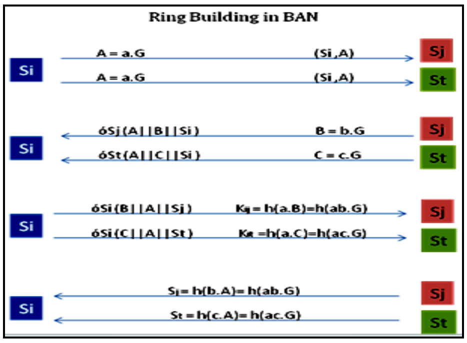

Figure 3- Ring Building in BAN

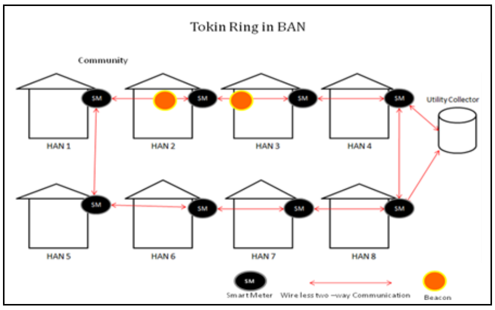

Figure 4- Architecture in a BAN

The last notification is about the maintenance situation, where S_i computes$K_i = K_i + 1$, and then sends Beaconi = $h(ki, R_i || Si || 2)$ to S_j andS_t. Finally, S_j and S_t can analyze the situation according to the Algorithm 2.

Figure 5 shows three situations. When an adversary connects to$S_i$with the aim of disclosure, S_j and S_t will receive$h\ (Ki, R_i || Si || 0)$. As a result, Exception II occurs, i.e., the adversary is connected to S_i. Exception I occurs whenS_t and S_t do not receive any Beaconi, which means the adversary has switched off the S_i.

Exception III occurs when the maintenance device verifies the challenge ofS_i. Thus, S_i predicts the physical connection for programming board duringT_t. Then, Si sends a clear alarm beacon to S_j and S_t. As a result, the utility collector will receive a report about each smart meter in the BAN, and responds accordingly.

SECURITY ANALYSIS

In this section, we assume the adversary is equipped with powerful device with full access to sniffer communication data. In fact, the adversary faces no limitations to access the available computational sources or memory. In our case, we briefly discussed security issues in regard to the proposed Ring monitoring detection scheme.

The shared key $ab.G$ established in Ring building phase is completely secure. As to the key establishment protocol, we embedded the identities of S_i, S_j andS_t using the Naccache-Stern signature to authenticate the validity of $a.G$, $b.G$and $c.G$, which are protected against the man-in-the-middle attack. At the same time, the hardness of elliptic curve and computation of Diffie-Hellman problem is the only shared key recognized byS_i, S_j andS_t which is unknown to the adversary. The Ring monitoring detection scheme can resist the replay attack. Since only the neighborhood nodes S_i, S_j and S_t know the shared key $ab.G$ and given the one-wayness of hash function, it is extremely difficult for an adversary A to get $ab.G$.

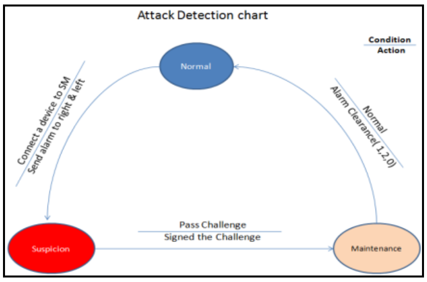

Figure 5- attack detection chart

```
Algorithm 2 Detect Smart Meter Compromise Attack
Procedure DetectSmartmeterCompromiseAttack
 if $S_j$ and $S_t$ receives a valid beacon Beaconi from $S_i$ every a predefined period $T_t$ then
$S_j = S_j + 1 and S_t = S_t + 1$
$if Beaconi = h(K_i, R_i || S_i || 1) then$
            return Normal
$elseif Beaconi = h(K_i, R_i || S_i || 0) then$
            return Exception II
$elseif Beaconi = h(K_i, R_i || S_i || 2) then$
            return Exception III
    End if
else if $S_j$ and $S_t$ doesn't receive a valid beacon Beaconi from $S_i$ every predefined period $T_t$ then
    return Exception I
else
return Exception I
end if
```

If an adversary carries out the relay attack (the physical attack with JTAG interface), it is immediately detected by the meter under attack and Beaconi is sent to neighborhood meters. With the above security guarantees the Ring-based detection and monitoring scheme can be applied to detect the physical connection of the adversary to the smart meter and compromise attack. Furthermore, the dictionary attack is also impossible because the shared key is secure and random number R_i is generated to be added to Beaconi.

The Ring-based monitoring scheme can resist replay beacon attack. In fact, without the proposal scheme, an adversary might attempt to launch a physical attack via$S_i$withS_j or $S_t$being unaware of it. To sum up, the adversary must be able to connect physically and send the beacon message in a normal situation so that it can prevent S_j *and* S_t from sending an alarm to the utility collector. When an adversary connects physically to smart meter, it means that the adversary can simply compromise the smart meter. In this case, two smart meters are monitoring one smart meter to detect compromise attack.

In the simulation, smart meters are deployed within a radius. The parameters of the simulation are:

- There are 20 smart meters
- The information beacon is set at every 2, 4, 8, and 12 seconds.
- The successful compromise of the smart meter by the adversary is T_c, when it has been set in 30 -60 seconds.
- The number of attacks varied from 0 to 18.

In the proposed scheme, we assumed that distributed attack is carried out simultaneously. As a result of the simulation, there are a number of attacks, which vary from 0 to 18. When these attacks are simulated, the percentage of detected attacks is increased from 10% to 100%. The proposed scheme is more reliable than couple base detection. In other words, the proposed scheme is more reliable for simultaneous distributed attacks in a BAN. The result of the simulation has been shown in figure 6.

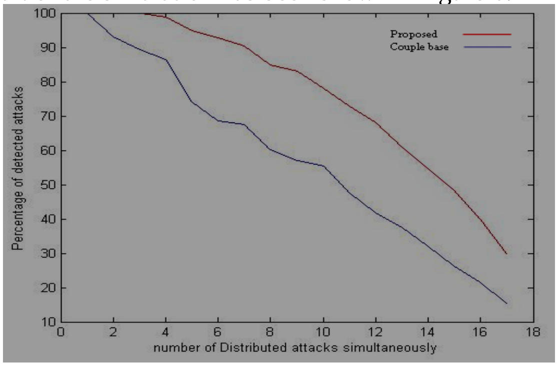

Figure 6- Simulation result

REFERENCES

[1] M. M. Fouda, *et al.*, "A lightweight message authentication scheme for smart grid communications", *Smart Grid, IEEE Transactions on*, pp. 1-1, 2011.

[2] K. Alfaheid, "Secure and compromise-resilient architecture for advanced metering infrastructure", 2011.

[3] CSC, "IDENTIFYING INHERENT SECURITY RISKS AMI and Smart Meters", pp. 1-3, 2009.

[4] C4, "The Dark Side of the Smart Grid - Smart Meters (in)Security", pp. 1-10, 2010.

[5] Z. M. Fadlullah, et al., "An early warning system against malicious activities for smart grid communications", Network, IEEE, vol. 25, pp. 50-55, 2011.

[6] A. Lee and T. Brewer, "Smart grid cyber security strategy and requirements", Draft Interagency Report NISTIR, vol. 7628, 2009.

[7] X. Lin, et al., "TUA: A novel compromise-resilient authentication architecture for wireless mesh networks", Wireless Communications, IEEE Transactions on, vol. 7, pp. 1389-1399, 2008.

[8] X. Lin, "CAT: Building couples to early detect node compromise attack in wireless sensor networks", 2009, pp. 1-6.

[9] T. M. Chen, et al., "Petri Net Modeling of Cyber-Physical Attacks on Smart Grid", Smart Grid, IEEE Transactions on, pp. 1-1, 2011.