Communications on Applied Electronics (CAE) – ISSN : 2394-4714
Foundation of Computer Science FCS, New York, USA
Volume 3– No.7, November 2015 – www.caeaccess.org

A Novel Non-cryptographic Security Services for Advanced Metering Infrastructure in Smart Grid

Ali M. Allam
Assistant Professor
Department of Electronic, Communication and Computer Engineering, Faculty of Engineering, Helwan University, PO box 11792, Cairo, Egypt.
Department of Applied Natural Sciences, UCC, Qassim University, Unaizah, 51911, PO box 4394, Saudi Arabia.

ABSTRACT

Advanced metering infrastructure (AMI) is an architecture for automated, two-way communication between a smart utility meter and a utility company. It is responsible for collecting all the data and information from the loads and consumers. These data and information are critical as it threats the reliability of electrical energy delivery and consumers' privacy. Traditional security solution rely on public key infrastructure may not suitable due to the scalability of the electric grid. In this paper, the author presents a non-cryptographic approach for providing confidentiality, integrity, and authentication (CIA) for AMI. The methods presented in this paper based on the hardware and physical layer approach. A basic idea of the integrity and authentication techniques is to use physical unclonable function (PUF), while the confidentiality technique is based on channel status information of wireless channel between the AMI subsystems. Our approach is secure and efficient for large scale network.

General Terms

Security, Protocols.

Keywords

Advance Metering Infrastructure; Hardware intrinsic security; physical-layer security.

1. INTRODUCTION

Advance Metering Infrastructure (AMI) is one of the vital functional blocks of the Smart Grid. It is responsible for collecting all the data and information from the loads and consumers, besides that it is responsible for implementing control signals and commands to perform necessary control actions.

AMI is not a single technology; rather, it is a configured infrastructure that integrates a number of technologies to achieve its goals. The infrastructure includes smart meters, communication networks in different levels of the infrastructure hierarchy, Meter Data Management Systems (MDMS), and means to integrate the collected data into a software application platforms and interfaces [1].

However, increasing usage in Smart Grid services bears huge risks at various points and AMI is one such area that can be broken by beginning malicious attacks that could threaten the mission of the smart grid services [2]. In the AMI, a scalable and robust key management system is needed to support a large number of smart meters and support its authentication. Many attacks like man-in-the-middle attack and impersonation attack can be successful in the absence of a strong authentication mechanism.

Our contribution is providing confidentiality, integrity, and authentication (CIA) light weighted, provable secure and efficient scheme for the communication link between subsystems in the AMI. The proposed scheme is based on the use of PUF devices that are low-cost to manufacture and provide hardware based authentication and integrity mechanism resistant to impersonation attacks. Finally, the wireless channel characteristics based encryption mechanism is proposed to provide protection against data interception without using pre-shared or stored master key.

The organization of the paper is as follows. The related works in section 2. Section 3 presents the key building blocks used in our protocol. Section 4 describes the system model. Our protocol introduces in section 5. Section 6, introduces security analysis of the suggested scheme, before the conclusions in Section 7.

2. RELATED WORKS

For providing an interoperability solution for security services in AMI, a common standard was established by ANSI and known as the ANSI C12 standard [3]. ANSI C12 standard, using a symmetric algorithm with pre-stored keys and a message authentication algorithm, is used for providing privacy and integrity. The stored keys used in these algorithms should be protected by a secure mechanism.

In [4], the authors suggested to use PUF with the ANSI standard, which provide the security and integrality for link between smart meter and utility. They used the PUF challenge response technique in authenticated the smart meter to the utility before exchange the data. Unfortunately, their protocol did not resist the impersonation attack because the message 1 and 3 in the protocol holds the challenge and response in plain text that make the attacker easily build the CRP database and impersonate any smart meter in the network.

There have been several people working in the area of AMI data privacy. McDaniel and McLaughlin worked on smart grid security in [5]. There has also been related work of the National Institute of Standards and Technology (NIST) that focused more on the data instead of the system in [6]. The motivation for both works was to provide a review of possible privacy risks that could be created by the smart grid. The contribution of the work in [5] was a review of possible data privacy risks from a viewpoint of the smart grid design. The contribution from [6] was identifying what data could be collected from the smart grid, how it could be exploited, and risk mitigation measures. Efthymiou and Kalogridis did some work with a method to anonymize the bulk of the data coming from smart meters in [7]. The concept is to associate the frequent smart meter readings with a larger group of users, so that the identity of individuals can be masked. This does not include smart meter readings that must be associated with a specific user such as readings used for billing purposes. As discussed in [8], the method of anonymizing smart meter data in [7] does protect a user's identity. However, the smart meter readings can still be data-mined for electrical usage patterns since the anonymous readings still have an identifier. This information can then be mapped to groups of people to determine average behaviors. In addition, the size of the group that a user is being masked in can affect the level of anonymity provided.

Kalogridis, Efthymiou, Denic, Lewis, and Cepeda did work with the privacy of smart meter data in [9]. Instead of achieving privacy through the network traffic between the smart meter and the electrical power supplier, their work focuses on transforming the smart meter readings. Each customer produces an electrical energy signature that can describe their electric power usage behavior. The work in [9] provided a method that transforms a customer's electrical energy signature to hide behavioral patterns.

As shown from above literature survey, the information transmitted through AMI subsystems carry very sensitive data about residential consumption of energy; if this information compromised it will lead to very seductive damage. So the solution is to apply CIA service to this information. The traditional method is to do that by cryptographic methods, but there is two major obstacles for applying this method. First, the device at the end user, such as smart meter does not have a high computation power to perform algorithms and protocols, which provide this service with efficient and secure manner. Second, smart grid is very large scalable network with different technologies and vendors that make key management by using PKI is problem. To avoid these two basic obstacles and provide a security service for transmitting information, we suggest a non-cryptographic approach that needs no key management and uses low computation power. The proposed approach can be summarized into two main solutions, first, using hardware authentication and integrity technique based on PUF. Second, using the wireless channel characteristics to provide confidentiality based on its channel status information (CSI).

3. PRELIMINARIES

In this section, we give an overview for the key hardware building blocks used in our suggested protocol.

3.1 Physically Unclonable Function

Physically unclonable functions or PUFs are innovative physical security primitives which produce unclonable and inherent instance-specific measurements of physical objects. PUFs are one-way functions that are embodied in, a physical structure [10]. The main security properties of PUFs are uncloneability and unpredictability. A PUF feeds with an input challenge $C_i \in C$, where C the set of all possible challenges is, and its output is a response $R_i \in R$, where R is the set of all possible responses. A PUF depends on the random variations during the fabrication of its corresponding circuit, even two PUFs with the same design results in two different functions. In other words, it is physically difficult to make two PUFs perform identically.

3.2 Channel Randomization based Privacy Preserving

Channel state information (CSI) has been used to identify wireless users and provide privacy for transmitted data from eavesdropper [11]. The CSI commonly indicates the channel impulse response. The foundation behind this scheme is that the CSI location-specific and privacy-preserving due to path loss and channel fading. An attacker, who is at a different location from the genuine user, will incur different CSI profile as observed by monitors/access points.

In this paper, we propose a real-time confidentiality method in physical layer based on instantaneous CSI. Our method differs with the existed methods on that we estimate the CSI, and then modulate the transmitted signal with it to compensate the effect of the channel between transmitter and receiver.

We can show the usage of CSI in privacy preserving service as follows. The mathematical model used is following the Shannon's communication theory [12] and assuming the reciprocal property of the Single input single output slow flat fading channel characteristics.

The low pass equivalent model (baseband model) of the received data symbols $r(t)$ at the receiver can be written as:

$$r(t) = s_D(t) * h(t) + n(t) \tag{1}$$

where $s_D(t)$ is the transmitted information bearing complex symbol, $h(t)$ is a complex random variable representing channel attenuation a_{ch} and phase φ_{ch}, and $n(t)$ is some complex additive noise at the receiver. So the impulse response $h(t)$ is:

$$h(t) = a_{ch}\delta(t - \tau_{ch}) \tag{2}$$

Then the transfer function $H(\omega)$ of this channel is:

$$H(\omega) = a_{ch}\, e^{-j\omega\,\tau_{ch}} \tag{3}$$

where the phase-shift due to the delay τ_{ch} in the channel can be represented as:

$$\varphi_{ch} = \omega\tau_{ch} \tag{4}$$

The attenuation and phase-shift of the path between transmitter and receiver is the channel status information (CSI) for the path between the transmitted and the receiver. This CSI is unique for each path, even if with the transmitter and the eavesdropper. It is commonly accepted that a distance of a few wavelengths of carrier frequency is enough to have practically no correlation at all between paths CSI's. For example, for wireless systems working in the frequency range of a few GHz this translates to a distance of a few centimeters. The eavesdropper and receiver are reasonably much farther apart than that.

So the CSI of path can be used as a symmetric secret key between transmitter and receiver and it is updated for each coherent period. So the data signal is compensated by the reciprocal of the transfer function of signal as shown in Fig. 1, then transmitted.

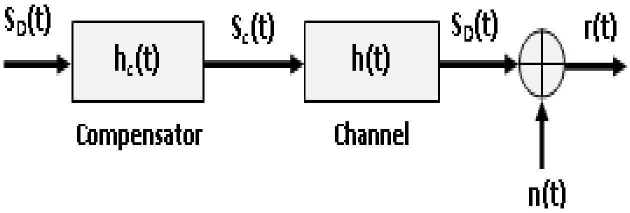

Fig. 1. Communication system model.

The transfer function of the compensator is:

$$H_c(\omega) = \frac{1}{a_{ch}}\, e^{j\omega\tau_{ch}} \quad (5)$$

and its impulse response is:

$$h_c(t) = \frac{1}{a_{ch}}\, \delta(t+\tau_{ch}) \quad (6)$$

So that the cascaded network of compensator and the channel to be:

$$h_c(t) * h(t) = \delta(t) \quad (7)$$

Therefore the transmitted signal at the output of this cascaded network will be:

$$s_D(t) * \delta(t) = s_D(t) \quad (8)$$

and the received signal at the authenticated receiver will be:

$$r(t) = s_D(t) + n(t) \quad (9)$$

Of course, if the eavesdropper received this signal, he will have other impulse response channel $h^{'}(t)$. Therefore the received signal by eavesdropper will be:

$$r(t) = s'_D(t) + n(t) \quad (10)$$

where

$$s'_D(t) = s_D(t) * h_c(t) * h'(t) \quad (11)$$

This discussed technique was proved its security as shift encryption in [13]. The idea of CSI is to compensate the data before its transmission with channel characteristics detected from the pilot signal.

4. SYSTEM MODEL

The Advanced Metering Infrastructure (AMI) consists of four main components: the utility provider end or metering data management system, aggregation point or concentrator, often located in the neighborhood, smart meters, and the home or Home Area Network (HAN). The communication between smart meters and appliances can use several communication protocols such as ZigBee, Wi-Fi, and Ethernet. In this work, we focus only on the communication between smart meters and the concentrator (see Fig. 2). As shown in Fig. 2, the system main components:

- **Smart meter**: equipment that measures the power consumption by the user and sends it to concentrator via secured wireless channel.
- **Concentrator**: equipment that aggregates the data of multiple smart meters and sends it to the metering data management system.
- **Metering data management system (MDMS)**: The MDMS is responsible for aggregating, validating and permitting editing of meter data. It stores the data before it goes to the dedicated storage facilities.

5. PROPOSED PROTOCOL

Figure 3 shows the message flow between smart meter and concentrator in our protocol. As shown in the figure, there is:

- Meter module responsible for measuring the consumption energy.
- PUF used for both hardware authentication of the device with concentrator and message integrity.
- Communication model used to estimate the channel status information of wireless channel between the meter and concentrator that used in modifying the reading data from meter module before transmitting.

5.1 Protocol Procedures

Our protocol undergoes the following procedures in order to provide link security between smart meter and the concentrator in AMI.

- **Enrollment.** The smart meter vendor initializes the system by implementing a data base at concentrator side contain all selected challenge response pairs provided by PUFs integrated into the meter.
- **Registration.** In this step, the device vendor establishes the bond between the owner of the meter and the CRP of PUFs embedded in this meter. We assume that the vendor is in physical contact with customer in this step, so that any transaction by this meter will be appended with the identity of the meter owner (e.g. tariff).
- **Authentication.** Now we explain how the concentrator authenticates smart meter before initiating any further communication. The concentrator sends pre-agreed pilot so the meter can estimate the channel status information (CSI) of the link between them. As shown in Fig. 3, the concentrator sends the challenge to the smart meter. Smart meter uses the embody PUF1 to generate the response to this challenge and send it after signal compensation by CSI to concentrator through the communication module. Upon receiving the response, concentrator compares it with the one in the database related to this device and accepts if equal.

Secure link Messaging. Whenever the concentrator wants to communicate with a smart meter to pick-up the reading, it fetches the record corresponding to smart meter and executes the authentication procedure described earlier. We use another designed PUF2 in meter to provide message integrity of reading data from smart meter. Smart meter sends frame which consists of n bits of energy consumed, which is appended with k bits as message code generated from the PUF2 whose input is the least significant k bits of reading data. At the concentrator side, the received signal decompensate due to channel characterizes, the concentrator checks the integrity of receiving data by taking the least significant k bits of data and compare the corresponding response from database with response appended to the data and accept if equal.

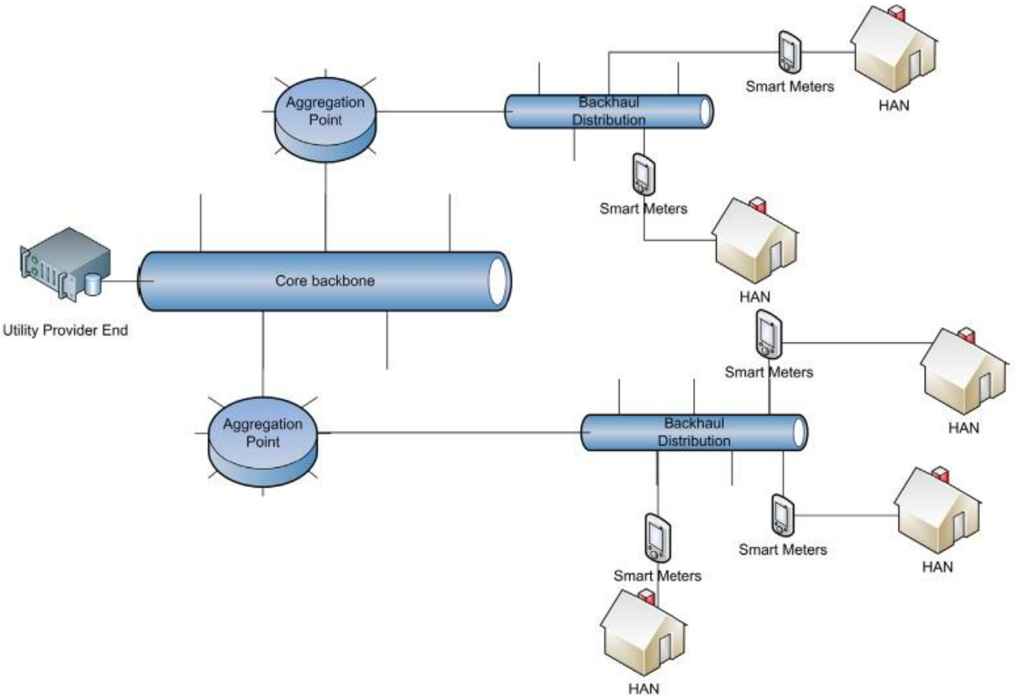

Fig 2: System components.

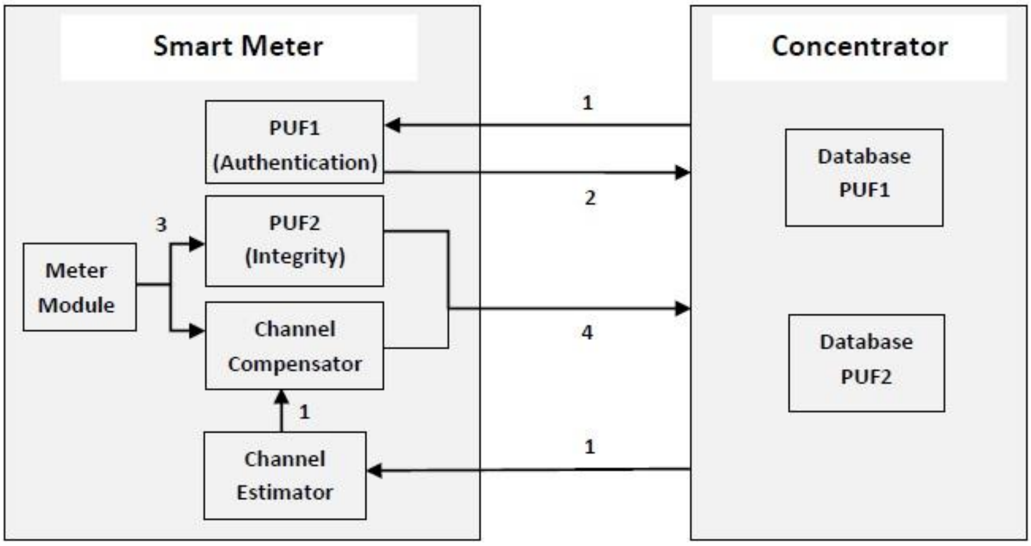

Fig 3: Protocol procedures

5.2 Suggested Protocol

We can summarize the procedures in the following steps:

1. Concentrator sends two messages to meter; the first is a pilot channel to aid the meter to estimate the CSI of channel between them. Second, it selects randomly a challenge from PUF1 database.
2. The meter received the two massages, from pilot through estimator module it detects CSI and sends it to compensator module. Then pick challenge bits and operates embody PUF1 and sends it response to concentrator after signal compensation.
3. Meter module forms the data frame represent the energy consumption, which composed of n bits reading and k bits response from PUF2. The meter sends the data after signal compensation.

The compensated signal will be received by concentrator as measured data while the k LSB of it will get the response corresponding to it from PUF2 database, accept the data if it is equal to the received appended k bits.

6. SECURITY ANALYSIS

As shown above that all the security services depend on the unique instant CSI and the uncloneability of PUF in addition to its unpredictability. In [13], they proved that CSI is similar to shift encryption that provides data secrecy with adequate probability.

The known plaintext attack in [14], is depending on challenge –response exchange in plaintext form which make the attack success. However, our suggested protocol resists this attack by encrypting the response related to the challenge transmitted from the concentrator.

The analysis in [15] presented how the difficulty of random duplication of PUF is**.** To create a forged PUF, an attacker can attempt to fabricate a clone containing a PUF with the exact same type as in the original product. Assume that the attacker also has the design plans of the product, including masks of the IC and the specification of the PUF. The statistical variation in PUF fabrication ensures that for an attacker to successfully create an identical PUF, depending on the PUF's entropy, a large number of ICs need to be fabricated in order to discover a suitable counterfeit.

Assume that the entropy in bits *b*. This means there are potentially 2^b numbers of different PUFs possible. Assume that all the possibilities occur with equal probability. Assume that *k* is the number of valid genuine PUFs the attacker knows, so if a fabricated clone matches one of these *k* PUFs, the attacker can successfully create a counterfeit product with this clone.

Let *a* as the number of PUFs the attacker produces (at random), it is possible to bound the number of successfully created cloned PUFs as (based on the birthday collision attack):

$$s = \frac{a\,.\,k}{2^b}$$

If the cost of creating a PUF is expressed as *c* and the profit of a successful counterfeit product as *p*, it is straightforward to calculate when cloning is profitable:

$$p\,.\,s\ > a\,.\,c\ =$$

$$\frac{p\,.\,k}{2^b} > c$$

Which means the required entropy to make the attack unprofitable is:

$$b > \log k\,.\,\frac{p}{c}$$

This attack model illustrates the importance of entropy in PUF responses; the larger this entropy the higher the cost for an adversary to find a successful clone.

7. CONCLUSION

In this paper, the security approach for AMI that integrates remote meter functions with CIA services has been presented. We have proposed a new approach to secure link communication in an AMI by integrating PUF technology and CSI estimation methodology with a smart meter. Our approach protects the confidentiality and the integrity of the transmitted messages in addition to strongly authenticate smart meters. Furthermore, by exploiting the intrinsic characteristics of PUF devices, we prevent the bandwidth overhead for key management utilized by smart meters.

8. REFERENCES

[1] National Energy Technology Laboratory for the U.S. Department of Energy, "Advanced metering infrastructure, NETL modern grid strategy," 2008.

[2] D.G. Hart, "Using AMI to realize the Smart Grid", in Proceedings of the Conference on Power and Energy Society General Meeting - Conversion and Delivery of Electrical Energy in the 21st Century, Pittsburgh, PA, July 20-24, 2008.

[3] "ANSI C12 smart grid meter package," [Available at] http://goo.gl/PQxkW.

[4] M. Nabeel, S. Kerr, X. Ding, and E. Bertino, "Authentication and key management for advanced metering infrastructures utilizing physically unclonable functions," in Proc. of the Conference on Smart Grid Communications (SmartGridComm), 2012.

[5] P. McDaniel and S. McLaughlin, "Security and Privacy Challenges in the Smart Grid," IEEE Security Privacy Magazine, vol. 7, no. 3, pp. 75-77, 2009.

[6] NIST, "Guidelines for Smart Grid Cyber Security: Vol. 2, Privacy and the Smart Grid," 2010.

[7] C. Efthymiou and G. Kalogridis, "Smart Grid Privacy via Anonymization of Smart Metering Data," in 2010 First IEEE International Conference on Smart Grid Communications, pp. 238-243, 2010.

[8] Todd Baumeister, "Literature Review on Smart Grid Cyber Security ", Todd Baumeister, Tech. report December 2010. [Available at] http://csdl.ics.hawaii.edu/techreports/10-11/10-11.pdf.

[9] G. Kalogridis, C. Efthymiou, S. Z. Denic, T. A. Lewis, and R. Cepeda, "Privacy for Smart Meters: Towards Undetectable Appliance Load Signatures," in 2010 First IEEE International Conference on Smart Grid Communications, pp. 232-237, 2010.

[10] B. Gassend, D. Clarke, M. van Dijk, and S. Devadas, "Silicon physical random functions," in CCS '02. New York, NY, USA: ACM, pp. 148–160, 2002.

[11] IEEE 802.15.4, "Wireless medium access control (MAC) and physical layer (PHY) specifications for low-rate wireless personal area networks (LR-WPANs)," 2003.

[12] C. E. Shannon, "Communication theory of secrecy systems," Bell Systems Technical Journal, vol. 28, pp. 656-715, Oct. 1949.

[13] M. M. Abutaleb and A. M. Allam, " FPGA-based Authenticated Key Exchange Scheme Utilizing PUF and CSI for Wireless Networks," *10th System of Systems Engineering Conference (SoSE)*, pp. 170-175, San Antonio, Texas, USA, 17-20 May 2015.

[14] M. Schulz, A. Loch, and M. Hollick, "Practical known-plaintext attacks against physical layer security in wireless MIMO systems," In Proc. Network and Distributed System Security Symp. (NDSS'14), February 2014.

[15] Ali M. Allam," An Authenticated Key Agreement Protocol Based on Physically Unclonable Function", *International Journal of advanced research in computer science and software engineering*, vol. 3, no. 9, pp. 714 - 719, Sept. 2013.