Information Systems 53 (2015) 213–223

Contents lists available at ScienceDirect

Information Systems

journal homepage: www.elsevier.com/locate/infosys

Scalable end-to-end security for advanced metering infrastructures

Mohamed Nabeel*[,1], Xiaoyu Ding, Seung-Hyun Seo, Elisa Bertino

Purdue University, 305 N University St, West Lafayette, IN 47907, USA

ARTICLE INFO

Article history:
Accepted 14 January 2015
Available online 22 January 2015

Keywords:
Advanced metering infrastructure
End-to-end security
Broadcast messaging
PUF

ABSTRACT

Conventional utility meters are increasingly being replaced with smart meters as Advanced Metering Infrastructures (AMIs) provide many benefits over conventional power infrastructures. However, security issues pertaining to data transmission between smart meters and utility servers are a major concern. In particular, as data travels through several networks, scalable key management schemes are crucial for secure end-to-end communications. In this paper, we propose an approach based on physically unclonable function (PUF) technology for providing strong hardware based authentication of smart meters and efficient key management to assure the confidentiality and integrity of messages exchanged in AMIs. Our approach does not require modifications to the existing smart meter communication. We have developed a proof-of-concept implementation of the proposed approach which is also briefly discussed in the paper.

1. Introduction

End-to-end secure communication between utility servers and smart meters is a key requirement for the overall security of the Advanced Metering Infrastructure (AMI). The messages exchanged between the utility servers and smart meters travel through multiple hops before reaching the destination. In other words, a message between the utility server and a smart meter may travel through one or more collector nodes and other smart meters. Different hops use different communication protocols. For example, the hop between the utility servers and collectors may use a 3G network whereas the hop between the collectors and smart meters may use a radio link. Even though most of these communication protocols provide link level security, this is not sufficient to protect messages traveling between the utility servers and smart meters as compromised/malicious intermediate nodes may not be trusted for the confidentiality and integrity of the messages. Therefore end-to-end message level security is essential to protect messages from attacks carried through the communication channels and intermediate nodes.

In initial AMI deployments, the data formats, security measures, and protocols for smart meter security were proprietary. However, because of the difficulties in achieving secure communication when proprietary methods are adopted and because of interoperability issues, the industry is moving towards a common standard developed by ANSI and known as the ANSI C12 standard [2]. ANSI C12 standard compliant smart meters are required to store a symmetric key used to encrypt and create message authentication codes (MAC), and the passwords used to provide different access privileges. These keys and passwords must in turn be protected by a secure mechanism. Approaches by which data is encrypted with a set of keys which are in turn encrypted with other keys are very common; for example such an approach is used for SQL Server Database Encryption. In the AMI, the application of such an approach requires a scalable, efficient, and robust

* Corresponding author.
E-mail address: nabeel.yoosuf@gmail.com (M. Nabeel).

[1] A preliminary version of this work [1] is published at IEEE SmartGridComm 2012.

http://dx.doi.org/10.1016/j.is.2015.01.004
0306-4379/

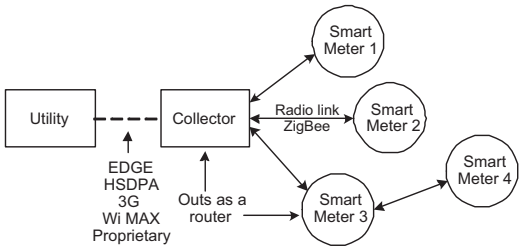

Fig. 1. A simplified AMI.

key management scheme able to support a very large number of smart meters and smart meter authentication. In the absence of a strong authentication mechanism, smart meters are vulnerable to man-in-the-middle attacks. An impostor may persuade the utility server that it is communicating with a valid smart meter and may cause damages.

In this work, we address the problem of designing a key management scheme able to achieve secure end-to-end communication in the AMI. Specifically, our solution provides an efficient approach to manage keys and a strong authentication mechanism. Our solution is based on the use of PUF devices which are inexpensive to manufacture and provide a hardware based strong authentication mechanism resistant to spoofing attacks. We utilize the PUF devices' hardware based one-way function to generate and re-generate the symmetric keys and access level passwords for smart meters. The PUF based secret generation mechanism provides strong protection against key leakage as the master key is never stored in memory. AMIs typically consist of many nodes and utilize both one-to-one (unicast) and one-to-many (multicast) communication patterns to communicate among nodes. The key management scheme should be efficient to such communication patterns among a large number of nodes. Trivial key management schemes do not work. One trivial approach is to assign each node in the AMI network a unique public-private key pair. Another approach is to assign a unique symmetric key at each smart meter. These approaches have one or two limitations: they are either computationally expensive or inefficient to support one-to-many communication pattern. Therefore, we need a different scheme.

We also propose a broadcast group key management (BGKM) scheme [3,4] along with the hardware based secret generation and strong authentication mechanism. The BGKM scheme is a special GKM scheme that allows a subset of nodes to communicate efficiently. BGKM is computationally inexpensive as only symmetric key cryptography is involved. Each smart meter in the network is assigned a unique secret that allows the smart meter to derive the group key. The BGKM scheme is efficient and scalable as it can address any subset of nodes with a single message, and existing smart meters can be revoked or new smart meters can be added without affecting other smart meters.

The rest of the paper is organized as follows. Section 2 provides an overview of the AMI and smart meters. Section 3 describes the key building blocks used in our approach. Sections 4 and 5 describe our scheme for unicast messaging. Section 6 describes our multicast messaging scheme and discusses how to improve the scalability of the proposed scheme. Section 7 briefly discusses the security of the proposed scheme. Section 8 provides an overview of a proof-of-concept implementation we have developed. Section 9 briefly discusses related work, whereas Section 10 outlines a few concluding remarks.

2. Background

In this section we provide a high-level overview of the AMI and smart meters.

2.1. Advanced metering infrastructure

The AMI consists of four main components: the utility company (utility, for short), data collectors, often located in the neighborhood, smart meters, and the home appliances. 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 utility (see Fig. 1). The messages between these two components are transmitted across multiple networks. These messages go through one or more collectors and possibly through other smart meters which act as routing nodes. Long distance communication protocols such as 3G, EDGE or HSPDA are used between the utility and collectors. Short distance communication protocols such as radio links are used between collectors and smart meters. Different network segments use different communication protocols and have their own transport level security.

2.2. Smart meters

An ANSI C12 standard compliant smart meter consists of two internal components (see Fig. 2): the meter board and the communication board connected through a serial port. The meter board contains a set of tables storing various information including keys and passwords used for secure communication and privilege levels. It also performs power consumption measurements. The communication board is responsible for communications with the outside nodes such as collectors, other smart meters, or home appliances, and for performing any required computation. Using an interrupt based mechanism, the communication board fetches data and other necessary information such as keys from the meter board whenever it needs to send data to the utility.

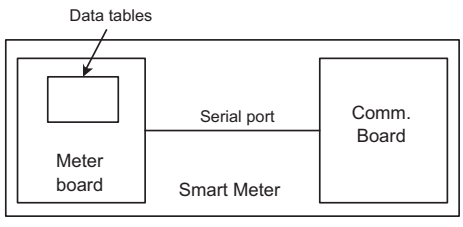

Fig. 2. Two components of a smart meter.