A Key Management Scheme for Secure Communications of Advanced Metering Infrastructure in Smart Grid

Nian Liu, *Member, IEEE*, Jinshan Chen, Lin Zhu, Jianhua Zhang, *Member, IEEE*, and Yanling He

***Abstract*—Advanced metering infrastructure (AMI) is an important component of the smart grid. The cyber security should be considered prior to the AMI system applications. To ensure confidentiality and integrality, a key management scheme (KMS) for a large amount of smart meters (SMs) and devices is required, which is not a properly solved problem until now. Compared with other systems, there are three specific features of AMI that should be carefully considered, including hybrid transmission modes of messages, storage and computation constraints of SMs, and unfixed participators in demand response (DR) projects. In order to deal with security requirements and considering the distinctive features, a novel KMS is proposed. First, the key management framework of an AMI system is constructed based on the key graph. Furthermore, three different key management processes are designed to deal with the hybrid transmission modes, including key management for unicast, broadcast, and multicast modes. Relatively simple cryptographic algorithms are chosen for key generation and refreshing policies due to the storage and computation constraints of SMs. Specific key refreshing policies are designed since the participators in a certain DR project are not fixed. Finally, the security and performance of the KMS are analyzed. According to the results, the proposed scheme is a possible solution for AMI systems.**

***Index Terms*—Advanced metering infrastructure (AMI), key management scheme (KMS), smart grid, transmission mode.**

I. Introduction

As A NEW emerging technology for smart grid, advanced metering infrastructure (AMI) [1] is the system and network used to measure, collect, store, analyze, and use energy usage data, which provides a convenient bridge between consumers and electric power utilities. In order to provide the broadest possible platform for delivering a wide range of applications in the future, open network and information techniques have been introduced to the smart grid [2], [3], which increases the probability of cyber security threats [4], [5].

In general, the cyber security requirements of AMI include confidentiality, integrality, and availability [6]. Before AMI can be deployed, the confidentiality for customer privacy and customer behavior, as well as message authentication for meter reading, demand response (DR), and load control messages, is the major security requirement to be provided. The confidentiality and integrality can be solved by encryption and authentication protocols, which depend on the security of cryptograph keys. To ensure the security, the key management for large amounts of devices in AMI systems is very important.

The key management scheme (KMS) is always composed of a key organizational framework, key generating, refreshing, distribution, storage policies, etc. Recently, there have been several studies related to the key management of AMI systems. An integrated scheme with confidentiality and authentication for secure AMI communications is proposed in [7], which can provide trust services, data privacy, and integrity by mutual authentications. Several typical application protocols are analyzed and compared for AMI customer applications in [8], which use security mechanisms such as Advanced Encryption Standard (AES) encryption and public-key infrastructure authentication. These research results have relations with key management, but the focus is on the encryption and authentication mechanisms for AMI applications, including device authentication, data confidentiality, and message integrity. How to manage the keys for a large number of smart devices in AMI systems is an issue still lacking in complete solution. Supposing that the AMI network is based on the *ad hoc* wireless sensor network, a key establishment and security algorithm based on public-key cryptography is proposed in [9]. According to the development of smart grid in different countries, the types of AMI networks are various [10], [11]. As a result, the applications of this algorithm are restricted. In [12], the importance of key management has been pointed out, but there is not any specific scheme provided. Furthermore, there have been some KMSs proposed for secure communications of power control systems, such as SCADA systems and wide-area protection systems [13]–[15]. However, these KMSs, along with those used in general IT systems, have difficulties in being directly applied to an AMI system, in that these systems are different in system structures, message characteristics, and requirements.

From the existing research results, we can find that the proposed KMSs are mostly for a specific AMI system. The KMS may be not applicable when the application functions, communications, and information technologies are changed.

Manuscript received January 10, 2012; revised May 7, 2012 and July 1, 2012; accepted August 2, 2012. Date of publication September 4, 2012; date of current version May 16, 2013. This work was supported in part by the National Natural Science Foundation of China under Grant 51007022 and in part by the Chinese Universities Scientific Fund under Grant 12MS32.

N. Liu and J. Zhang are with the School of Electrical and Electronic Engineering, North China Electric Power University, Beijing 102206, China (e-mail: nian_liu@163.com; jhzhang001@163.com).

J. Chen is with the Electric Power Research Institute of Fujian Electric Power Company Ltd., Fuzhou 350007, China (e-mail: 333a3@163.com).

L. Zhu is with the College of Politics and Public Administration, Tianjin Normal University, Tianjin 300384, China (e-mail: linzhu16@126.com).

Y. He is with Fujian Shuikou Hydropower Generation Company, Ltd., Fuzhou 350800, China (e-mail: heyanling86@126.com).

Digital Object Identifier 10.1109/TIE.2012.2216237

However, until recently, most of the AMI systems were in the pilot phase; there is still some degree of uncertainty in the future. In addition, the construction and development of an AMI system are not consistent in different countries and areas. From the perspective of the application requirements, the functions which need to be deployed are also different. Some applications are very simple, such as metering, measuring, and monitoring; some are relatively complex, and they take more into consideration the applications of DR and load control. Similarly, there are also various communication modes depending on the application requirements and user preference.

For the aforementioned reasons, we are trying to propose a more common KMS for AMI systems. To summarize AMI characteristics and trends, we believe that the structure and components of AMI are relatively fixed. In other words, the main object of the key management is the smart meters (SMs), which is constant. Therefore, a key management framework based on key graph is proposed to manage the keys of a large amount of SMs. The functions of AMI are not fixed, but we can design a KMS for the collection of possible functions. In actual condition, the users can choose part of the KMS for specific applications. The communications are not fixed either, but the features of messages transmitted in the communication channels can be decided by the function requirements. In response to this situation, three types of key management processes are designed for unicast, broadcast, and multicast communications depending on function requirements and message types. Considering time requirements of functions, computation, and storage limitations of SMs, specific key regeneration and refreshing policies are designed in each process.

The rest of the contents of this paper will be organized as follows. Section II studies the structure and messages of an AMI system and then summarizes the main features relating to key management. According to these features, the difficulties in designing KMS for AMI are analyzed, and corresponding possible solutions are proposed. From Sections III to VI, a novel KMS is proposed. In Section III, the framework and initialization of the KMS are described. Sections IV–VI present the key management processes for unicast, broadcast, and multicast communications, respectively. Furthermore, the security and performance of the KMS will be analyzed in Sections VII and VIII, respectively. Finally, a conclusion will be presented in Section IX.

II. AMI System Features and Difficulties for a KMS Design

A. Structure of AMI System

An AMI system does comprise a number of technologies and applications that have been integrated to perform as one (see Fig. 1):

1) SMs;
2) user gateways (UGs);
3) home (local) area networks (HANs);
4) wide-area communications infrastructure;
5) meter data management systems (MDMSs).

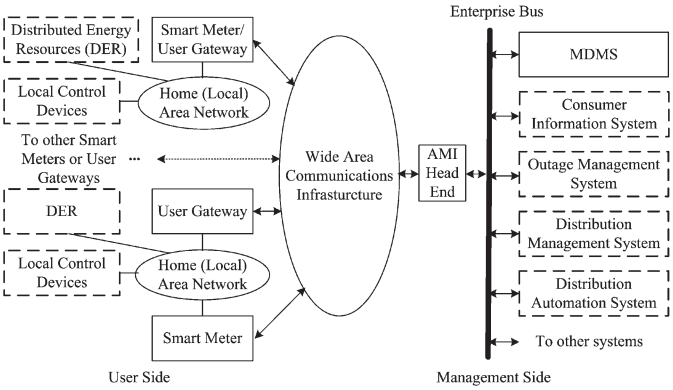
Distributed Energy Resources (DER)
Smart Meter/ User Gateway
Local Control Devices
Home (Local) Area Network
To other Smart Meters or User Gateways
DER
User Gateway
Local Control Devices
Home (Local) Area Network
Smart Meter
Wide Area Communications Infrastructure
AMI Head End
Enterprise Bus
MDMS
Consumer Information System
Outage Management System
Distribution Management System
Distribution Automation System
To other systems
User Side
Management Side

Fig. 1. AMI system structure.

1) SMs: Generally, SMs are solid-state programmable devices that perform a lot of functions, such as bidirectional metering and measuring (not only for electricity consumption but also for real-time electricity load, maximum demand, voltage, current, frequency, power factor, etc.), time-based pricing, consumption data for consumer and utility, net metering, loss or restoration of power notification, power quality monitoring, and remote turn-on or turn-off operations. Moreover, they enable the DR to achieve [16], so as to facilitate greater energy efficiency since information feedback has been shown to reduce consumers' usage [17].

2) UGs: The UG, which is always performed in other devices such as SMs or personal computers, implements protocol conversion and communications between two heterogeneous networks, like the in-home network and wide area network.

3) HANs: A HAN is a kind of local area network, which interfaces with SM, UG, distributed energy resources, and local control devices [17], [18].

4) Wide-Area Communication Infrastructure: The wide-area communication infrastructure supports continuous interaction between the utility, the consumer, and the controllable electrical load. It must employ open bidirectional communication standards, yet requiring high security. Various architectures can be employed [19], with one of the most common being local concentrators that collect data from groups of meters and transmit those data to a central server. Various media can be considered to provide part or all of this architecture, such as optical fiber, power line carrier, copper, radio frequency, Internet, and so on.

5) MDMS: An MDMS, with an AMI head end in contact with the user side, is a database of meter data with analytical tools. Through enterprise bus, it interacts with other systems of the electric power utilities, including consumer information system, outage management system, distribution management system, and so on.

B. Messages in AMI System

Interactive messages are exchanged via AMI communication networks. The messages include meter data, loss or restoration of power notification, publishing of DR projects, subscription or quit of DR projects, electrical pricing information, and remote load control.