2014

Development Of Water Meter For Secure Communication In The Advanced Metering Infrastructure

Sugwon Hong

Hyung Mo Park

DEVELOPMENT OF WATER METER FOR SECURE COMMUNICATION IN THE ADVANCED METERING INFRASTRUCTURE

SUGWON HONG (1), HYUNG MO PARK(2)
(1): Department of Computer Engineering, Myongji University, Yongin, Gyeonggi-do 449-728 , S. Korea
(2): Passtech, #1305, Kranz techno, 5442-1, Sangdaewon-dong, Jungwon-gu, Seongnam-si, Gyeonggi-do, S. Korea

The Advanced Metering Infrastructure (AMI) is an essential part of the smart water grid. One of the daunting challenges in realizing the services in the AMI system is the security issue. In this paper first we investigate the AMI communication system, and then address security requirements for the AMI system. Especially we point out the different features of the water meter and how these differences might affect developing security mechanisms. Second, we address the implementation issues of the water meter in three aspects: key distribution, deployment and implementation. Then, we propose possible approaches we take to develop water meters briefly.

INTRODUCTION

The Advanced Metering Infrastructure (AMI) is one of the integral components of the smart water grid where water consumption data is collected, stored, and transferred to the utility Meter Data Management System (MDMS). The organizations which are directly involved in promoting and developing the smart water grid have tried to figure out the operating scenarios in the overall domain from water meters up to MDMS, and logical/physical components that should be expected to exist to perform those operations in the full extent. However, how such domain will take shape is still up in the air and requires some time until the actual implementation are in full swing [1].

One of the difficult tasks in realizing the services in this domain is the security issue. While the utility operation system, which is intrinsically the SCADA system, can be almost completely isolated from the outside world from the communication point, the AMI system will lie in the open domain. Since water meters are located in an open area, any cyber attack that is excruciating service providers and users in the current network could take a toll on the services in the smart water grid at the same level [2].

In this paper we consider AMI communication systems, and then address security requirements for the AMI system. Although the requirements are very similar to the ones in the power AMI system, water meters have different features from power meters. We will point out

these differences and how these different characteristics might influence developing security mechanisms.

Second, we address development issues of the smart water meter in three aspects: key distribution, deployment issues, and implementation. And then, we show briefly possible approaches we take with consideration of unique characteristics of water meters.

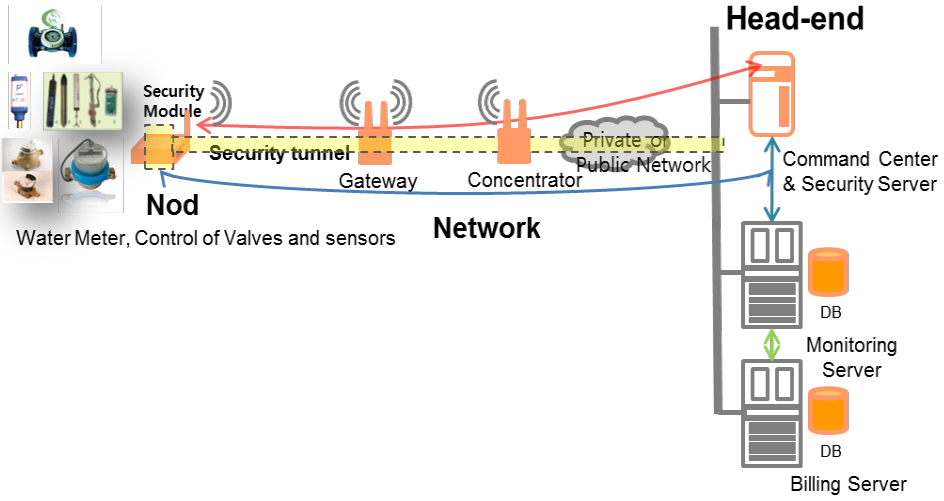

Figure 1. AMI communication system

COMMUNICATION SYSTEM

A typical network architecture of the water AMI communication system is shown in figure 1. Meter Data Management System(MDMS) at the utility operating center collects all data from smart meters at the consumer areas. Meters send data to the nearest concentrator which is called a gateway in this figure and which may be placed on utility's pole tops. Since they are likely to use wireless communication, one single gateway can cover a very limited range within which there are approximately no more than several hundreds of water meters. Gateways send data to next level concentrators, making up several stages of traffic concentration until reaching the head-end of a utility operating center, depending on its coverage. Servers placed in the utility side behind the head-end perform various functions based on the collected data. If necessary, they send control/management commands to meters. All the data and command are traversing back and forth through the network.

In the smart grid, three distinct network domains are considered because they have different characteristics and consequently require different communication technologies and network topologies. First, the network domain which consists of in-premise devices and a smart meter is called home area network(HAN). Next, the domain from the smart meters up to gateways or the higher level of concentrators is called neighborhood area network(NAN). The last domain from the concentrators and the utility head-end corresponds to wide area network(WAN) in which typical optical fiber SDH or cellular communication technologies are commonly used.

In the smart water grid, HAN is unnecessary part since we consider only one device, a water meter in the customer premise's domain. NAN is contentious part since there is no

standard solution until now. For this likely multi-hop wireless network, different proprietary approaches have been proposed and tried. But in order to deploy smart meters and construct network in compatible way, utility companies and meter vendors realized the standard solution. They worked together in the IEEE 802.15 working group and published IEEE 802.15.4g PHY specification recently for the utility neighborhood area network which they also call is smart utility networks(SUN) [3]. Even though they still have much work ahead, this effort laid foundation for the deployment of interoperable AMI communication system.

SECURITY REQUIREMENTS

The primary goal of the AMI security is to guarantee secure channels between water meters and utility head-end. So far, cyber security requirements for the smart grid have been widely studied and several survey papers have been published [4][5]. These works are very comprehensive, and not AMI-specific even though they include AMI security as a part of their endeavor, Here, we summarize the essential security requirements constrained to achieving secure communication between water meters and the head-end., centering around fundamental network security terminologies.

Meter authentication: the identity and authenticity of water meters and associated customers should be verified before joining the network and receiving proper services.

Message confidentiality: Meters need to send usage and state information to the head-end securely, and by the same token the head-ends also send commands or other critical information to the meters safely. In other words, message contents should be secured not to be read by illegitimate nodes.

Message authentication: Receivers need to verify that messages are sent from legitimate senders. Adversaries can inject malicious messages to the either party, consequently causing malfunctions. Meters require strong authentication of the operating servers when they receive any command. On the contrary the server's authentication requirement might be relatively modest. In any case to verify the owner of messages is one of the most important security requirements in many applications which will take place in the AMI system.

Message Integrity and freshness: Receivers need to make sure that the messages they receive are not altered on the way by adversaries. It is also required that messages be recent, and old messages not be reused by any adversary.

Message non-repudiation: Once sending a message, the sender of the message should not deny sending it. This requirement might be necessary for proper billing.

These security requirements are almost the same as in the meters in the smart grid [4][5]. But from the point of practical deployment, water meters differ from meters in the power system. The most salient point is that power will be supplied to water meters not by power lines but by batteries. Thus, security protocols to meet these requirements for water meters should be energy-sensitive, and for this reason the same protocols which can be applied to the power system might not be feasible in water meters. Another point noteworthy is that water meters are

more likely to be installed in unprotected places than their peers in the power system, which implies that they are more vulnerable to physical tampering.

CHALLENGES

Here, we consider three aspects of security challenges briefly for developing water meters to meet the security requirements: key distribution, deployment, and implementation.

Key distribution: The building blocks of the security protocols are the cryptographic algorithms. Every security protocol is based on the underlying encryption/decryption or hash function keys. Thus, the key management including key establishment is an integral part of the security mechanism. The big picture of the key management in the SCADA security mechanism may be helpful to understand the nature of this challenge [6][7].

The public key algorithm is generally used as a convenient way in establishing a secure channel for distributing a session key between two network nodes and in authenticating nodes. However, the public key cryptography places computationally heavy burden on the resource-constrained meters. Another approach is to use the symmetric key algorithm for distributing a session key.

In addition to computational complexity, another important issue to choose the key distribution scheme is scalability. Any key distribution method to be applied to the AMI network should be operated in a large number of meters which have very restricted computing power.

As described in the previous section the fact that a water meter is powered by a built-in battery should be considered when we find the optimum security protocol including key distribution. In this regard a security protocol for smart meters might not be appropriate to apply to smart water meters although both have similar functions and the same security requirements.

Deployment: Another big challenge in a practical sense is a deployment issue. The AMI in the smart water grid will be built for an extended time and is not able to be installed overnight. As mentioned before, one concentrator will cover approximately hundreds of household meters, and the concentrator will be connected to the ultimate head-end through multiple stage of integration. This tree-like topology can have various forms of network architecture including ad-hoc multi-hop network. In addition to network topology, we will wait to see which communication technology will be dominant.

There might be discrepancy in space domain as well as time domain. There will be two different space domains which might have incongruous characteristics: residential areas and non-residential areas such as reservoir or water control centers. The latter might be dependent on different communication technology.

Considering this diverse deployment scenarios, we might need dual mode of the key distribution and subsequent data exchange schemes. One is a negotiation-based method. In this scheme either the public key or the pre-installed master keys in the devices can be used at the every handshake stage to setup a session key. The other is free of any negotiation process to setup a session key. Here, pre-defined key or keys embedded in the device is used as a session key without any handshake process between a meter and a server. This scheme can obviate any negotiating time, consequently reducing energy consumption because it can send data only

when it wants and receive data when it is awake from a server, otherwise it can stay in a sleep mode.

Implementation: Current water meters basically have two functions: measurement and one-way communication function. For secure communication each meter is also required to have security function on top of them. And they will also have to accommodate some control function depending on the extent of services that will be provided in the future water grid. Moreover, the meters will be deployed in unmanned and unprotected location. So they have to be equipped with a certain degree of tamper-proof mechanism. These requirements will restrict the options which we can choose for the security protocol in overall, the key distribution method in particular. To develop meters with those functions with reasonable cost will be one of major practical issues in realizing the smart water AMI system.

SECURITY MEASURES

Due to the importance of security, some commercial meters equipped with security function are already shown in the market, based on the public key management scheme [8]. Here, we explain briefly the approaches we take to implement security measures for developing smart water meters.

We assume that the security server at the utility operating center is a trusted base, and all meters trust the server at the initial setup. At the creating time the server is given a key table which consists of two master keys and terminal IDs. One key is a master encryption key used for encrypting a session key. The other is a master authentication key used to verify the origin and integrity of messages. Each meter is also given two master keys which are shared with the server at the installation time, and can be identified by the meter ID. Session keys are distributed from the server whenever necessary. And we assume that each meter can keep its master keys without any harm.

At the initial registration stage, the server verifies authenticity and legality of meters using their meter IDs and corresponding master keys. So, the security protocol is based on end-to-end model which means that security responsibility lies on the server and meters, and any security functions are transparent to nodes in the middle. This approach is based on the communication technology in which routing is implemented independently of security function. A different approach is also possible, in which case hop-by-hop authentication is implemented in nodes of network [9].

The server and meters use a session key to set up a secure channel between them, and this key is refreshed on a regular base or on request using the master key. And message integrity and freshness can be provided by the message authentication code(MAC) computed from the message concatenated with a nonce, the ID, and the master authentication key they share with. The message authentication code (MAC) also verifies the authenticity of the sender. In order to avoid computational overhead of any encryption technique, ether symmetric or asymmetric, we choose Keyed-Hashing for Message Authentication (HMAC) as an authentication algorithm.

CONCLUSION

In this paper we explain the security aspects for developing smart water meters. And also we point out slight different features of water meters compared to power meters. And we show security measures, taking practical implication into consideration. This is a typical approach for

encryption and authentication [10]. But this protocol can be easily expanded to several variants that can be applied to the setup of secure channel between a meter and a server when we find an optimum security protocol including key distribution.

REFERENCES

[1] Cornish K., "Addressing the challenges of deploying water AMI", WaterWorld, Vol. 28, Issue 6 (2012).

[2] Hong S., "Security Challenges for Customer Domain in the Smart Grid", Special Session 1: Smart Grid, APAP 2011, Beijing (2011).

[3] Chang K.-H., "The IEEE 802.15.4g Standard for Smart Metering Utility Networks", IEEE SmartGridComm 2012 Symposium, (2012), pp476-480.

[4] The Smart Grid Interoperability Panel – Cyber Security Working Group, "Guidelines for smart grid cyber security", NISTIR 7628 (2010), pp1–597.

[5] Wang W. and Zhou L., "Cyber Security in the Smart Grid: Survey and Challenges". Computer Networks, Vol. 57 (2013), pp1344-1371.

[6] Pietre-Cambacedes L., Sitbon P., "Cryptographic key management for SCADA systems – issues and perspectives", International Conference on Information Security and Assurance, (2008).

[7] Choi D., et. al, "Advanced Key-Management Architecture for Secure SCADA Communications", IEEE TRANSACTIONS ON POWER DELIVERY, Vol. 24, No. 3(2009), pp1154-1163.

[8] Certicom, Critical Infrastructure Protection for AMI using a Comprehensive Security Platform.

[9] Yan, Y., Hu R., Das S. Sharif H. and Qian Yi, "An Efficient Security Protocol for Advanced Metering Infrastructure in Smart Grid", IEEE Network, July/August (2013), pp64-71.

[10] Lim L. et. al , "Security Protocols Against Cyber Attacks in the Distribution Automation System", IEEE TRANSACTIONS ON POWER DELIVERY, Vol. 25, NO. 1(2010), pp448-455.