Chapter 18
A Key Management Scheme for Secure Communications Based on Smart Grid Requirements (KMS-CL-SG)

Bashar Alohali
Liverpool John Moores University, UK

Kashif Kifayat
Liverpool John Moores University, UK

Qi Shi
Liverpool John Moores University, UK

William Hurst
Liverpool John Moores University, UK

ABSTRACT

Over the last decade, Internet of Things (IoTs) have brought radical changes to the means and forms of communication for monitoring and control of a large number of applications including Smart Grid (SG). Traditional energy networks have been modernized to SGs to boost the energy industry in the context of efficient and effective power management, performance, real-time control and information flow using two-way communication between utility provides and end-users. However, integrating two-way communication in SG comes at the cost of cyber security vulnerabilities and challenges. In the context of SG, node compromise is a severe security threat due to the fact that a compromised node can significantly impact the operations and security of the SG network. Therefore, in this chapter, Key Management Scheme for Communication Layer in the Smart Grid (KMS-CL-SG) has proposed. In order to achieve a secure end-to-end communication we assign a unique key to each node in the group.

DOI: 10.4018/978-1-5225-9866-4.ch018

INTRODUCTION

A SG is a modern electricity supply system. It uses information and communication technology (ICT) to run, monitor and control data between the generation source and the end user. It comprises a set of technologies that uses sensing, embedded processing and digital communications to intelligently control and monitor an electricity grid with improved reliability, security, and efficiency.

SGs are classified as Critical Infrastructures. In the recent past, there have been cyber-attacks on SGs causing substantial damage and loss of services. A recent cyber-attack on Ukraine's SG caused over 2.3 million homes to be without power for around six hours (TOMKIW, 2016). Apart from the loss of services, some portions of the SG are yet to be operational, due to the damage caused. SGs also face security challenges such as confidentiality, availability, fault tolerance, privacy, and other security issues. Communication and networking technologies integrated into the SG require new and existing security vulnerabilities to be thoroughly investigated.

Key management is one of the most important security requirements to achieve data confidentiality and integrity in a SG system. It is not practical to design a single key management scheme/framework for all systems, actors and segments in the SG, since the security requirements of various sub-systems in the SG vary. Two specific sub-systems categorized by the network connectivity layer – the Home Area Network (HAN) and the Neighborhood Area Network (NAN) are addressed. Currently, several security schemes and key management solutions for SGs have been proposed. However, these solutions lack better security for preventing common cyber-attacks such as node capture attack, replay attack and Sybil attack. A cryptographic key management scheme that takes into account the differences in the HAN and NAN segments of the SG with respect to topology, authentication and forwarding of data, is proposed. The scheme complies with the overall performance requirements of the SG.

The proposed scheme uses group key management and group authentication in order to address end-to-end security for the HAN and NAN scenarios in a SG, which fulfils data confidentiality, integrity and scalability requirements. The security scheme is implemented in a multi-hop sensor network using TelosB motes and ZigBee OPNET simulation model. In addition, replay attack, Sybil attack and node capture attack scenarios have been implemented and evaluated in a NAN scenario. Evaluation results show that the scheme is resilient against node capture attacks and replay attacks. Smart Meters in a NAN are able to authenticate themselves in a group rather than authenticating one at a time. This significant improvement over existing schemes is discussed with comparisons with other security schemes.

BACKGROUND

The advancement in information and communication technology (ICT) has not only given the world a smart and high-quality life but also an efficient pr system, energy solutions and intelligent homes to live in. Energy is one of the fundamental requirements to fuel the smart technology and so a 'smart' way of living, and electricity is generally used as the primary source of energy.

According to a report by (BP, 2013), worldwide energy consumption is predicted to increase annually by 1.6% from 2011 to 2030, adding 36% to the global energy consumption by the year 2030. In addition to the continuous growing demand for energy and the environmental concerns, efficient and effective