Computers and Electrical Engineering 52 (2016) 114–124

Contents lists available at ScienceDirect

Computers and Electrical Engineering

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

A lightweight message authentication scheme for Smart Grid communications in power sector☆

Khalid Mahmood[a], Shehzad Ashraf Chaudhry[a,*], Husnain Naqvi[a], Taeshik Shon[b], Hafiz Farooq Ahmad[c]

[a] Department of Computer Science and Software Engineering, International Islamic University, Islamabad, Pakistan
[b] Division of Information and Computer Engineering, College of Information Technology, Ajou University, San 5, Woncheon-Dong, Yeongtong-Gu, Suwon 443-749, Republic of Korea
[c] College of Computer Sciences and Information Technology (CCSIT), King Faisal University, Al-Ahsa 31982, Kingdom of Saudi Arabia

ARTICLE INFO

Article history:
Received 8 June 2015
Revised 18 February 2016
Accepted 18 February 2016
Available online 8 March 2016

Keywords:
Authentication
Smart meter security
Lightweight cryptography
IoT
Smart Grid
ProVerif

ABSTRACT

The Internet of Things (IoT) has plenty of applications including Smart Grid (SG). IoT enables smooth and efficient utilization of SG. It is assumed as the prevalent illustration of IoT at the moment. IP-based communication technologies are used for setting SG communication network, but they are challenged by huge volume of delay sensitive data and control information between consumers and utility providers. It is also challenged by numerous security attacks due to resource constraints in smart meters. Sundry schemes proposed for addressing these problems are inappropriate due to high communication, computation overhead and latency. In this paper, we propose a hybrid Diffie–Hellman based lightweight authentication scheme using AES and RSA for session key generation. To ensure message integrity, the advantages of hash based message authentication code are exploited. The scheme provides mutual authentication, thwarting replay and man-in-the-middle attacks and achieves message integrity, while reducing overall communication and computation overheads.

1. Introduction

Internet of things (IoT) refers to the emerging concept of computing in which abundant physical objects are connected to the Internet to form a network. This network enables connected objects to access, interpret, exchange and monitor the information of each other. It has brought a revolution in communication technologies by empowering advanced applications such as Smart Grid (SG). Although, IoT has the ability to provide management of energy at home level, but it also has the potential to facilitate the complete advanced electric power grid known as SG. SG is comprised of millions of interconnected and interacting devices that can be considered as the objects present in IoT. Therefore, due to similar nature of both IoT and SG, IoT can easily facilitate the implementation of SG and integrates its feature of collecting and sharing energy related information in SG. This integration will allow SG to carry out its routine tasks in sustainable, efficient, reliable and cost effective manner.

☆ Reviews processed and recommended for publication to the Editor-in-Chief by Guest Editor Dr. J. Kim.

* Corresponding author. Tel.: +92 3335123308; fax: +92 519019766.

http://dx.doi.org/10.1016/j.compeleceng.2016.02.017
0045-7906/

SG is the replacement for conventional power grid because it brings more reliability and efficiency through smart, intelligent and interactive features. SG not only offers distributed control to power suppliers but also satisfies the current and future needs of the consumers [1]. In recent years, SG is seizing the attention from researchers and also from engineers in electric power generation and communication areas [2]. SG is also referred as the future grid. It is an enhancement of the conventional electrical power grid, by integrating digital computation and communication technologies for providing secure, efficient and reliable delivery of electricity and exchange of information between power generators, utility companies and consumers of the electric power [3]. Some important functionalities provided by SG are as under;

1. **Self healing:** SG has the ability to identify, analyze and respond to particular faults swiftly through intelligent and appropriate action in order to recuperate from that fault [4,5].
2. **Motivate and include the consumers:** The SG provides interactive options and information, enabling consumers to select an appropriate available tariff and control their power usage accordingly. In this way, the consumers can make better and cost effective plan for themselves.
3. **Resist attack:** SG can resists against both physical and cyber-attacks.
4. **Increase in power quality:** These days consumer's major demand is constant voltage and therefore SG have the ability to maintain constant voltage which can ultimately increase the power quality and reduces the commercial productivity loss, because sudden fluctuations in voltage can be harmful for electric appliances [4].
5. **Accommodate all sources of generations and storage options:** Conventional power grid doesn't have the ability to integrate renewable energy sources such as green power, wind power and solar power etc. SG on the contrary has the ability to adapt and integrate these renewable resources [4].
6. **Enables electrical markets:** SG supports distributed power sources, which attracts new electric power suppliers and service providers towards the power market, also ensures cost effective power supply to consumer.
7. **Optimizing assets and operate efficiently:** SG automatically assists the equipment conditions, manages its configuration and reduces the maintenance cost as compared to conventional electrical grid.

SG is therefore, an electrical power infrastructure with smart capabilities by allowing power providers, power distributors and power consumers to maintain operating requirements and capabilities in near-real-time [2]. Moreover, SG provides the power to consumers in a stable and reliable way on contrary to conventional power grid [2,6]. The SG sanctions two-way communications among consumers and providers of electrical power, this instinctive feature enable consumers to efficaciously prompt their power requisites to utility providers by which they play an active role and efficiently customize their consumption level [2]. This ability enables the consumers to minimize their energy consumptions by communicating back and forth with the electricity providers. Whereas the conventional grid broadcasts the electricity in one-way fashion and the consumers cannot actively participate, and neither can they customize their consumption level. The demand response capability for the load management can efficiently reduce the load in an emergency situation or in high price situation, so the consumers can reduce their consumption level in these situations accordingly [7]. It was estimated that, the demand response in non-emergency situation can reduce the price from 5% to 15% in peak load.

In SG, a number of sensing devices, smart meters and control-systems lies in the path between providers and consumers of electric power for facilitating the two-way communications [2]. The sensing devices are capable of malfunction detection and the operations that exhibit deviations with respect to normal ranges. It requires a felicitous response from control center, while these responses are converted to control messages and sent to SG segments [2]. For this purpose, the SG communication framework and its functionality must be characterized in order to sanction active consumers participation and facilitate resiliency to sundry security threats. In SG the consumers have smart meters, by which they are capable of identifying their consumption of power in most efficient way as compared to conventional energy meters [2,6].

The smart meters customarily accumulate the electrical consumption information of smart home, which is then amassed by utility company (i.e. for monitoring and billing purposes). Consumers can also access their smart meter for checking their consumption level and adjust the power utilization accordingly (i.e. less utilization of electricity during peak hours for preserving mazuma) [2,6]. For this purpose smart meter sends messages to the utility provider periodically for adjusting their power utilization and participate actively for their power utilization adjustment within SG dynamically. The utility providers can additionally send some special offers by sending messages to smart meters, by which the consumers can preserve mazuma and adjust their utilization accordingly. During peak electrical hours if all the appliances are switched on and the SG are peregrinating to an emergency situation then the utility provider send messages to all consumers by utilizing smart meters to notify about the emergency event and to adjust consumption level accordingly, by which the consumers thwart the situation by shutting down some appliances and participate to the stable environment actively [8]. Whereas the conventional power grid did not have such functionality. The smart meters can efficiently communicate with their appliances and accumulate the energy requisites from all appliances i.e. smart appliances [6].

The SG communication infrastructure consists of homes, buildings and immensely colossal neighborhoods. In order to facilitate SG communication, Internet Protocol (IP) based communications network technologies are the suitable cull for establishing IP-based SG communications. The smart meters and smart appliances (i.e. heater, dishwasher, washing machine, air conditioner, tube light, television etc.) must have a unique IP addresses for supporting SG communication and standards of IETF (Internet Engineering Task Force) for remote management of smart meters located at different places in the hierarchy [2,6].