Future Generation Computer Systems 88 (2018) 491–500

Contents lists available at ScienceDirect

Future Generation Computer Systems

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

Pairing based anonymous and secure key agreement protocol for smart grid edge computing infrastructure

Khalid Mahmood [a,j], Xiong Li [b,c,*], Shehzad Ashraf Chaudhry [a], Husnain Naqvi [a], Saru Kumari [d], Arun Kumar Sangaiah [e], Joel J.P.C. Rodrigues [f,g,h,i]

[a] Department of Computer Science and Software Engineering, International Islamic University, Islamabad, Pakistan
[b] School of Computer Science and Engineering, Hunan University of Science and Technology, Xiangtan 411201, China
[c] Guangxi Key Laboratory of Trusted Software, Guilin University of Electronic Technology, Guilin 541004, China
[d] Department of Mathematics, Ch. Charan Singh University, Meerut, Uttar Pradesh, India
[e] School of Computing Science and Engineering, VIT University, Vellore, Tamilnadu 632014, India
[f] National Institute of Telecommunications (Inatel), Santa Rita do Sapucaì, MG, Brazil
[g] Instituto de Telecomunicações, Portugal
[h] ITMO University, Saint Petersburg, Russia
[i] University of Fortaleza (UNIFOR), Fortaleza, CE, Brazil
[j] COMSATS University Islamabad, Sahiwal Campus, Pakistan

HIGHLIGHTS

- A paring based key agreement protocol has been introduced for Smart Grid edge computing infrastructure
- It facilitates authentication between the utility control and smart meter without the need of trusted third party
- It offers security and anonymity besides traditional security requirements
- The reliability of the proposed protocol is verified and validated through random oracle model and automated tool ProVerif

ARTICLE INFO

Article history:
Received 21 November 2017
Received in revised form 9 March 2018
Accepted 2 June 2018

Keywords:
Smart grid
Authentication
Anonymity
Smart meter
Edge computing
ProVerif

ABSTRACT

The most vital concern in the realization of the Internet of Things (IoT) is to encounter the disparate communication systems and technologies. Interoperability solutions such as standards can help us to integrate plenty of diverse devices and their applications in an interoperable framework. Since Smart Grid is a non-trivial prevalent application of Edge computing under the umbrella of IoT. The Smart Grid furnishes communication through Internet Protocol to enable interoperability. However, IP-Based communication makes it vulnerable to serious security threats. Therefore, the secure information sharing among diverse communicating agents in the smart grid environments has become a vital concern. Specifically, to enable secure communication between the smart meter and utility, key management prior to authentication is the most critical task to do. Nowadays, several mechanisms have been introduced to establish secure communication within the emerging smart grid environment. Although, these protocols do not support smart meter anonymity and fail to offer reasonable security. In this paper, we use the identity-based signature to present an anonymous key agreement protocol for the Smart Grid infrastructure. This protocol enables the smart meters to get connected with utility control anonymously to avail the services provided by them. The smart meters realize this objective with the private key in the absence of trusted authority. The trusted authority is involved only during the registration phase The proposed protocol is verified and validated through random oracle model and automated tool ProVerif. Moreover, performance analysis is also observed to consolidate the reliability and efficiency of the proposed protocol.

1. Introduction

Internet of things (IoT) has emerged as a prevalent idea in which a huge number of diverse objects are linked up through the Internet to realize a network. It offers a great facility to the

* Corresponding author at: School of Computer Science and Engineering, Hunan University of Science and Technology, Xiangtan 411201, China.
E-mail address: lixiongzhq@163.com (X. Li).

https://doi.org/10.1016/j.future.2018.06.004
0167-739X/

constituents to exchange, monitor and access the intended data with each other [1]. The escalation of the IoT has introduced the cloud infrastructure and its services. Their prosperous implementation has yet introduced another cardinal computing paradigm which is celebrated as edge computing or Edge-of-Things (EoT) computing. This paradigm enables data processing at the edge to promise low latency, low bandwidth utilization, higher scalability, higher energy preservation, higher privacy and security.

However, there are various challenges to realize the concept of Edge computing. Significant research is underway to overcome these challenges so that diverse systems and their application can be integrated to increase the productivity, reliability and scalability of the existing networks. Researchers are focusing to establish such infrastructure that can entertain the compelling requirements like interoperability, security, scalability, reliability, energy efficiency and re-usability. Since Edge computing has a plethora of valuable applications and Smart Grid is one of them, therefore similar challenges hold for it and similar requirements are intended for it [2–4].

Smart Grid is an ameliorated electricity generation and distribution infrastructure with aided features of intelligence and two-way communication [5–7]. This advanced infrastructure has increased the reliability and efficiency of the power grids, which is achieved through enhanced features of automation and artificial intelligence. Moreover, Smart Grid offers the flexibility to inject renewable energy sources and in turn distributed generation, which is proved to be very difficult in conventional grids [8–10].

Smart meters installed at individual homes are considered as the most important entity in the Smart Grid. As they are responsible to monitor and log the power consumption behavior of the consumers. They act as an interface to communicate with utility providers for information and control commands exchange. Each smart meter is equipped with processing module having limited processing power and scarce memory resource to carry out cryptographic operations. These operations are usually carried out on the data observed through sensing modules.

Since Smart Grid brings abundant benefits for both consumers and utility providers. However, facility off wireless communication through Internet Protocol has made it an easy picking for adversaries. Since the security of IoT [11–13] and cloud computing [14–19] have attracted researchers' attention recently. Designing and developing security solutions such as authentication [20–23] and key management for ensuring the reliability of the Smart Grid environment is also considered as an emerging area of research nowadays.

Recently, Wu and Zhou [24] introduced a novel key management technique for the Smart Grid environment. They have utilized a hybrid cryptosystem to enable effortless key management. Their hybrid cryptosystem is developed on the basis of both symmetric and public key cryptosystem. The symmetric key cryptosystem feature is realized using Needham–Schroeder authentication scheme. Whereas, public key cryptosystem feature is realized by ECC. Their hybrid cryptosystem promises to offer reasonable accessibility, fault tolerance, efficiency, scalability and security features. However, their protocol needs to have at least two separate servers for realizing PKI and trusted authority. Moreover, certificate verification by PKI induces greater computing overhead, which is infeasible for smart meter because it is normally equipped with limited resources.

In [25] Xia and Wang identified that Wu and Zhou's protocol is susceptible to a man-in-the-middle attack and come up with enhanced key distribution protocol for the Smart Grid environment. Xia and Wang's protocol presents the idea of Lightweight Directory Access Protocol (LDAP), which is utilized in the replacement of trusted third party. Their protocol can be considered as more useful through lower operating cost due to the use of LDAP. Moreover, they prescribed that single point failure threat can be avoided by deploying multiple LDAP servers.

Xia and Wang's protocol is proved to be susceptible to impersonation and anonymous key share (UKS) attacks by the Park et al. [26]. Moreover, Xia and Wang's protocol does not offer the perfect forward secrecy and anonymity of both smart meters and utility providers. Additionally, it is identified that most of the protocols enforce trusted authority to play an active role during authentication between the communicants. This activity can put the whole system at risk because compromise of trusted authority can enable the adversary to obtain the master key. The obtained master key can be used to engender the private keys of the communicants. Therefore, this issue is resolved by keeping trusted authority away from online authentication sessions and just utilizing it during the registration phase of the communicants.

In [27] Tsai and Lo presented an anonymous key generation and distribution protocol through identity-based signature and encryption. Their protocol initially facilitates mutual authentication between the smart meter and utility control. Later it helps session key establishment between the said communicants to enable invincible communication. However, Odelu et al. [28] identified that Tsai and Lo's protocol is vulnerable to leakage of ephemeral secret keys and offers weak privacy for smart meter's credential. Therefore, Odelu et al. introduced an enhanced key agreement scheme for smart grid infrastructure.

Very recently, various identity-based authenticated key exchange schemes have been introduced [27,29]. These schemes enable communicants to achieve mutual authentication and exchange a common session key at the end of the successful authentication process. Nevertheless, they are proved to be infeasible or impractical due to resource-constrained nature of the Smart Grid communicating entities. Furthermore, these solutions do not offer user anonymity. Later, Wang [30] introduced four protocols for realizing authentication using a smart card. However, none of these solutions promise to offer user anonymity.

In this paper, we use the identity-based signature to present an anonymous key agreement protocol for the Smart Grid infrastructure. This protocol empowers the smart meters for anonymous information exchange with utility. Moreover, the role of trusted authority is minimized as it is only engaged during the registration phase. This feature not only reduces the dependency on the trusted authority but it also reduces the communication overhead and expected delay. The smart meters exploit the concerned private keys to replace the post-registration role of trusted authority. The proposed protocol is verified and validated through random oracle model and automated tool ProVerif. Moreover, performance analysis is also observed to consolidate the reliability and efficiency of the proposed protocol.

The rest of the paper is outlined as follows: Section 2 presents the introduced key agreement protocol. Section 3 elaborates the security strength analysis through random oracle model. Formal security validation through an automated tool ProVerif is delineated in Section 4. Security features and performance comparison is presented in Section 5. In the end, paper is concluded in Section 6.

2. Proposed Key Agreement Protocol

This section presents the proposed protocol. However, some preliminaries in the form of communicating components of the system, utilized notations and system setup are elaborated first.

2.1. Communicating components of the system

The proposed scheme is designed for secure and reliable communication between smart grid's components such as smart meters and utility control at service provider's end. The secure communication is enabled by three entities namely, smart meters, utility control and last but not the least trusted authority. A smart