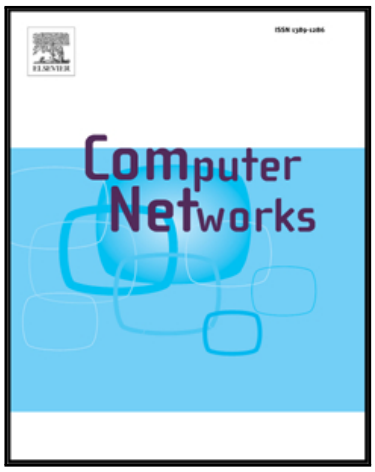

A Privacy-aware Data Dissemination Scheme for Smart Grid with Abnormal Data Traceability

Xu Zhang, Mi Wen, Kejie Lu, Jingsheng Lei

PII: S1389-1286(16)30383-8
DOI: 10.1016/j.comnet.2016.11.009
Reference: COMPNW 6051

To appear in: *Computer Networks*

Received date: 19 August 2016
Revised date: 20 October 2016
Accepted date: 10 November 2016

Please cite this article as: Xu Zhang, Mi Wen, Kejie Lu, Jingsheng Lei, A Privacy-aware Data Dissemination Scheme for Smart Grid with Abnormal Data Traceability, *Computer Networks* (2016), doi: 10.1016/j.comnet.2016.11.009

A Privacy-aware Data Dissemination Scheme for Smart Grid with Abnormal Data Traceability

Xu Zhang[a], Mi Wen[a,*], Kejie Lu[a,b], Jingsheng Lei[a]

[a]*Shanghai University of Electric Power, Yangpu District, Shanghai 200090*
[b]*The Department of Computer Science and Engineering, University of Puerto Rico at Mayagüez, Puerto Rico, USA*

Abstract

In a typical smart grid, a large number of smart meters are deployed at energy consumers' premises, which can report real-time usage data to the control center of energy producer. Although such a communication model can help to improve the efficiency and reliability of electricity delivery, which is crucial to our society, it also leads to several security issues: (1) attackers may peek the privacy of energy consumers, and (2) attackers may tamper the transmitted data for their own benefits or purposes. To deal with these security issues, many researchers have proposed different schemes for privacy preservation or abnormal data detection. However, existing studies usually address them separately. In this paper, we jointly resolve these two major security issues in smart grid. Specifically, we propose a privacy-aware data dissemination scheme for smart grid with abnormal data traceability (PDDS), based on bilinear group theory and non-interactive zero-knowledge proof. In our scheme, we design a novel link function that can verify whether there are different signatures that are signed by the same consumer, which effectively reduces the time and communication overhead for tracing. To evaluate the correctness and performance of the proposed scheme, we first develop solid security analysis, which shows that the proposed scheme can efficiently preserve identity confidentiality and data integrity. We then conduct extensive simulation experiments, which further demonstrate that our scheme can significantly reduce communication costs.

Keywords: smart grid, group signature, privacy, linkability, traceability.
PACS:

1. Introduction

In recent years, smart grid has attracted great attention from governments, industry, and academia all around the world, because it is expected to be more efficient and reliable than the traditional power grid. To achieve these advantages, a smart grid consists of not only the power infrastructure but also a network of smart devices and control centers that can monitor and manage energy usage [1, 2]. With smart grid, stakeholders such as energy producers and energy consumers can all benefit from the advanced infrastructure.

Specifically, smart meters [3] can be installed for energy consumers to monitor and control their energy usage. These smart meters and other data collectors (such as the gateways in a residential community) can form a network that forwards energy consumption data from consumers to the energy producers. The network can also deliver energy information from an energy producer to the consumers, such as the time-varying pricing information, with which a smart meter can further control smart appliances of an energy consumer to reduce the electricity bills.

On the other hand, an energy producer may own a control center. The control center can receive energy consumption data from energy consumers and then generate electricity bills. Moreover, the control center can analyze real-time energy consumption data and then dynamically adjust the generation and distribution of energy, as so to improve the efficiency and reliability of the infrastructure. Finally, the control center may dynamically announce the pricing to further optimize the operation of the grid.

Clearly, the communication capability is essential to the operation of smart grid and can benefit both the energy producers and energy consumers. Nevertheless, the communication channels between the control centers and smart meters are also prone to various security attacks. In particular, many attacks are targeting two security aspects, data privacy and data integrity.

For data privacy, it has been reported that frequent data reporting may expose consumers' habits and behaviors, causing serious privacy problems [4, 5]. For instance, Greveler et al. [6] showed that smart meters' fine-grained data could even be utilized to identify which television channel a consumer is watching. To protect consumers' privacy, there are many different approaches. For instance, the control center can request energy data less frequently, which may reduce the efficiency of smart grid. Consumers can install rechargeable batteries to hide the details of energy consumption [7, 8], which also increases the cost of consumers. Alternatively, smart devices can aggregate energy consumption data [9, 10, 11], or apply anonymity schemes to hide the real identity of consumers [12, 13].

*Corresponding author
Email addresses: xiaoputao178@163.com (Xu Zhang), wenmi2222@gmail.com (Mi Wen), kejie.lu@upr.edu (Kejie Lu)