Chapter 30
A Privacy-Aware Data Aggregation Scheme for Smart Grid Based on Elliptic Curve Cryptography With Provable Security Against Internal Attacks

Ismaila Adeniyi Kamil
https://orcid.org/0000-0002-1939-0219
University of Ibadan, Ibadan, Nigeria

Sunday Oyinlola Ogundoyin
University of Ibadan, Ibadan, Nigeria

ABSTRACT

In smart grids (SGs), smart meters (SMs) are usually deployed to collect and transmit customers' electricity consumption data in real-time to the control center. Due to the open nature of the SG communication, several privacy-preserving data aggregation schemes have been proposed to protect the privacy of customers. However, most of these schemes cannot protect against internal attackers and they are not efficient, since SMs are constrained in processing, memory, and computing capabilities. To address these problems, the authors propose a privacy-aware lightweight data aggregation scheme against internal attackers based on Elliptic Curve Cryptography (ECC). The scheme satisfies all the security requirements of SG, and supports conditional traceability, strong anonymity and autonomy. The authors demonstrate that the proposed scheme provides confidentiality based on the Computational Diffie-Hellman (CDH) assumption and unforgeability in the security model based on the intractability of the Discrete Logarithm (DL) problem. Extensive performance analysis shows that the proposed scheme is very efficient.

DOI: 10.4018/978-1-7998-8954-0.ch030

1. INTRODUCTION

Smart grid (SG) has revolutionized the power grid system by utilizing the information and communication technology to enhance sustainability, improve reliability, and maximize cost of power generation, transmission, and distribution (Gungor, Lu, & Hancke, 2010; Fang et al., 2012; Li et al., 2018). According to National Institute for Standards and Technology (NIST) model (Framework, 2010), smart meters (SMs) are two-way communication devices installed in buildings (residential, industry, or company) to gather and transmit (e.g. every 15 minutes) the real-time electricity consumption data to the Operation Center (OC) and also to receive control data from the OC. Two-way communication is used in the SG system to collect and analyze real-time data for efficient power allocation and prompt response to potential threats and security issues (Fang et al., 2010 & Li et al., 2018). The collected data not only allow the OC to effectively manage and control the power grid, but enhance cost computation, prediction of future situations, power allocation, and monitoring of unforeseen circumstances (Wen et al., 2017). Besides, the electricity usage data can be used for economic purposes such as business advertisement and government policies (Gong et al., 2016; Zhu, Huang & Takagi, 2016; Li et al., 2017; Zhou, Zhu & Castiglione, 2017).

However, if proper measure is not put in place, the information of a single SM may reveal sensitive information about the habits and lifestyles of the residents corresponding to that SM compromising their privacy (Vahedi et al., 2017; Liu et al., 2019). The residents' habits can be monitored by analyzing the relevant SM's data (gas, water, electric consumption) (Karopoulos, Ntantogian & Xenakos, 2018). With these data, it is possible to know the number of people living in an apartment, when they are in or out of home (Karopoulos et al., 2018), which appliances are used at a particular time, even their religion or other habits based on energy usage profiling (Garcia & Jacobs, 2011). An attacker may read the electricity usage profile to determine the activities of the residents in order to commit a crime. For example, if there is low or zero power consumption, the attacker can deduce that the residents are not at home, and can therefore burgle the house.

An attacker may also modify or alter the power consumption data for dubious reasons. For example, since electricity usage data can be used for purpose of energy feedback with dynamic pricing and billing, an attacker can unbalance the load management and dynamic pricing systems if it can succeed in injecting false data. This unbalance in the system can affect the operation of a power grid, increases the cost of power generation, or cause energy blackout in some regions (Braeken, Kumar & Martin, 2018). Besides, the integrity and confidentiality of the information of energy consumption reading is also of utmost importance, because this sensitive information could be used by adversaries for financial gain. A customer with malicious intention may report an erroneous or zero electricity data to the utility company for financial gain. For example if a consumer is a cottage or a small scale enterprise, the attacker can obtain useful information about the company's products and utilize this information for monetary benefits by selling the information to their competitors or blackmailing the company (Abdallah & Shen, 2018). While it is very important to preserve the privacy of customers against external adversaries, it is also imperative to protect their privacy against internal attackers such as disgruntled employees who may be curious to obtain sensitive private information of SMs for malicious intentions.

To address these issues, a privacy-preserving data aggregation scheme is generally used. Basically, there are two requirements of a privacy-preserving data aggregation scheme in SG (Liu et al., 2018); the OC must be able to calculate the sum of power consumption data in a region, and must not be able to extract the electricity usage data of a single SM in a particular region. Some data aggregation schemes