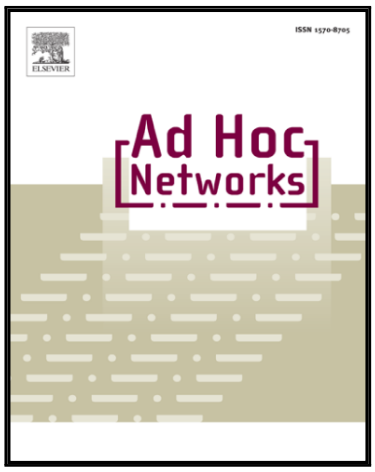

Lightweight and Efficient Privacy-Preserving Data Aggregation Approach for the Smart Grid

Mohamad Badra , Sherali Zeadally

PII: S1570-8705(17)30102-6
DOI: 10.1016/j.adhoc.2017.05.011
Reference: ADHOC 1555

To appear in: *Ad Hoc Networks*

Received date: 10 April 2017
Revised date: 29 May 2017
Accepted date: 30 May 2017

Please cite this article as: Mohamad Badra , Sherali Zeadally , Lightweight and Efficient Privacy-Preserving Data Aggregation Approach for the Smart Grid, *Ad Hoc Networks* (2017), doi: 10.1016/j.adhoc.2017.05.011

Lightweight and Efficient Privacy-Preserving Data Aggregation Approach for the Smart Grid

Mohamad Badra and Sherali Zeadally

***Abstract*-- Over the last few years, we have seen the emergence of a wide range of Smart Grid architectures, technologies, and applications made possible by the significant improvements in hardware, software, and networking technologies. One of the challenges that has emerged in the Smart Grid environment is the privacy of Smart Grid users. Although several privacy-preserving techniques have been proposed recently for the Smart Grid environment, many of them suffer from high computation and communication costs, different types of attacks, and the use of complex key management schemes. To address these drawbacks, we propose an efficient, lightweight privacy-preserving data aggregation approach that makes use of symmetric homomorphic encryption and Diffie-Hellman (DH) or Elliptic Curve Diffie-Hellman (ECDH) key exchange methods. In contrast to previously proposed privacy-preserving schemes for the Smart Grid, we demonstrate the superiority of our proposed approach in terms of its low transmission and message overheads, and resiliency against a wide range of session key attacks, and ability to maintain data integrity against unauthorized modification or data forgery and to ensure authenticity of smart meters' data.**

***Index Terms*-- Cryptography, encryption, key, performance, privacy, Smart Grid.**

I. Introduction

SMART Grid technologies have become increasingly sophisticated over the last few years with a growing shift from the traditional electric power system, which has become inadequate in meeting the challenges and opportunities of the rapidly changing, market-driven ecosystem. Smart Grids have been developed to enhance the traditional electric power grid by integrating state-of-the-art communications and computing technologies, and to efficiently monitor the generation and the usage of energy through two-way communications between the consumer and the Energy Supplier (ES). The bidirectional data flow capability between the consumers and the ES is one of the main facilitators of the Smart Grid (SG). It allows the ES to generate electricity in real-time and to serve its consumers based on their current consumption. Moreover, with Smart Grid technologies, utilities and ESs can notify their consumers of energy pricing in a real-time fashion to: a) minimize the cost for energy generation and distribution, and b) automatically collect data from the energy metering devices for further processing and analysis.

The Advanced Metering Infrastructure (AMI) is used to handle this interaction between ESs and their consumers. AMI defines the interfaces to exchange data between the ES and the smart meter, which is a computing device that is installed in the consumer's house to perform advantageous functions, such as reading real-time energy usage, voltage values, phase angle and the frequency. Smart meters can also communicate with different appliances installed at the consumer's residence. As depicted in Fig. 1, several technologies and applications are integrated together to make up an AMI system. These technologies and applications include: smart meters, Home (local) Area Networks (HANs), Neighborhood Area Network (NAN), wide-area communications infrastructure (WAN), Meter Data Management Systems (MDMS), and operational gateways or concentrators working as main collectors. Interactive messages exchanged via AMI communication networks can be divided into three classes according to the transmission mode [11]: unicast, broadcast, and multicast.

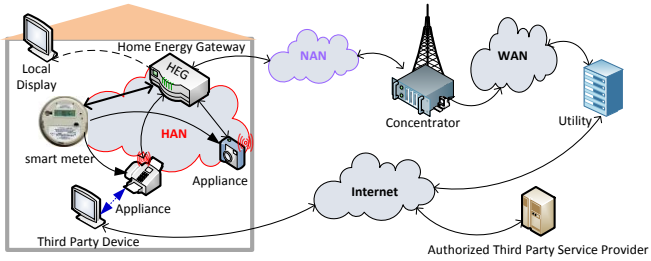

Fig. 1. Smart Grid AMI reference architecture.

Smart Grids, which rely on networking capabilities, face security concerns including vulnerabilities and threats related to IP-based network infrastructures such as denial of services attacks, identity theft and usurpation, cyber-attack and intrusion, passive attacks (e.g., man-in-the-middle and replay attacks), and False Data Injection (FDI) attacks in which the attackers intentionally change the data in a way that the ES will be unable to detect forged or malformed data when collecting energy usage data from consumers. To protect against several of these attacks, security solutions that provide mutual authentication, data integrity, and confidentiality are mandatory in the SG environment. The SG also opens up new threats to privacy and personal habits of consumers [13]. Given the kind of information collected by smart meters (such as electricity consumption of household appliances), privacy

M. Badra is with Zayed University, P.O. Box 19282, Dubai, U.A.E. (e-mail: mohamad.badra@zu.ac.ae, mbadra@gmail.com).

S. Zeadally, College of Communication and Information, University of Kentucky, Lexington, KY, 40506, USA. (e-mail: szeadally@uky.edu).