Ad Hoc Networks 32 (2015) 98–113

Contents lists available at ScienceDirect

Ad Hoc Networks

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

A novel secure aggregation scheme for wireless sensor networks using stateful public key cryptography

Omar Rafik Merad Boudia [a,*], Sidi Mohammed Senouci [b], Mohammed Feham [a]

[a] STIC Laboratory, University of Tlemcen, Algeria
[b] Drive Laboratory, University of Burgundy, Nevers, France

ARTICLE INFO

Article history:
Received 2 May 2014
Received in revised form 3 October 2014
Accepted 2 January 2015
Available online 24 January 2015

Keywords:
Wireless sensor networks
Secure data aggregation
Homomorphic encryption
Simple power analysis

ABSTRACT

Wireless sensor networks (WSNs) are nowadays considered as an important part of the Internet of Things (IoT). In these networks, data aggregation plays an essential role in energy preservation. However, WSNs are usually deployed in hostile and unattended environments (e.g. military applications) in which the confidentiality and integrity security services are widely desired. Recently, homomorphic encryptions have been applied to conceal sensitive information during aggregation such that algebraic operations are done directly on ciphertexts without decryption. The main benefit is that they offer the end-to-end data confidentiality and they do not require expensive computation at aggregator nodes since no encryption and decryption are performed. However, existing solutions either incur a considerable overhead or have limited applicability to certain types of aggregate queries. This paper presents a novel secure data aggregation protocol for WSNs. The scheme employs Stateful Public Key Encryption (StPKE) and some previous techniques in order to provide an efficient end-to-end security. Moreover, our solution does not impose any bound on the aggregation function's nature (Maximum, Minimum, Average, etc.). We present and implement our scheme on TelosB as well as MicaZ sensor network platforms and measure the execution time of our various cryptographic functions. Simulations are also conducted to show how our scheme can achieve a high security level (by providing the above security services) with a low overhead (in terms of computation and communication) in large-scale scenario.

1. Introduction

Wireless sensor networks have received much attention over the last few years, not only in academia, but also in industries for the study and development of a plethora of potential applications in various domains such as military, health, and environmental. Nowadays considered as one of the main elements in the Internet of Things (IoT) [1], WSNs are composed of many sensor nodes where the resource limitation represents the most important feature. In fact, the sensors are constrained in battery power, communication, and computation capability; therefore, every possible solution that aims to conserve these resources is extensively sought [2]. Data aggregation is one of the techniques that is actually considered as an essential paradigm for WSNs since it tends to save both computation and communication resources. With such technique, data are captured by sensor nodes and fused as they flow in the network by intermediate nodes and then transmitted to the sink over the wireless link. In IoT context, the sink node can be considered as an Internet powered device that gathers readings (aggregated data) and sends them to the cloud. In a

* Corresponding author. Tel.: +213 557 884 999.
E-mail address: om_meradboudia@mail.univ-tlemcen.dz (O.R. Merad Boudia).

http://dx.doi.org/10.1016/j.adhoc.2015.01.002
1570-8705/

nutshell, the sink node manages all the interaction between the WSN and the outside world (known as *Front-End solution*, in which the WSN is completely independent from the Internet [3]). Data aggregation allows in-network processing which leads to lesser packet transmissions and reduces redundancy, and therefore, helps in increasing the WSN's overall lifetime [4].

The major problem of data aggregation is when we aim to provide security. On one hand, it should be noted that aggregation and security have opposite goals. While the first attempts to reduce the number of packet transmitted, the second adds a non-negligible cost in order to ensure some security properties. On the other hand, WSNs have some special features that are different from other networks, (i) they are limited in terms of resources, which makes the choice of the adequate security algorithm somewhat difficult. Algorithms that are simple and efficient in terms of resources utilization are the most suitable, or sometimes by sacrificing some security in order to render possible the implementation on a wireless sensor, (ii) they are often deployed in hostile and unattended environments, which makes them subject to several kinds of attacks. In an aggregation process for example, due to the amount of data to be fused, the nodes that perform the aggregation function are the most attractive to an adversary, and (iii) they use a wireless link, which may allow an attacker to monitor the transmitted data and even participate in the communication. To summarize, data aggregation protocols must be designed in conjunction with security protocols in order to reach a good compromise between the overall protocol complexity and the provided security level [5]. Guaranteeing security for data aggregation is therefore an intriguing challenge.

Traditional secure aggregation protocols use hop-by-hop encryption [6–8], in which sensor nodes encrypt the captured data and send the ciphertext to the aggregator node; the aggregator node decrypts, performs the aggregation function, and then sends the encryption of the result to the upper aggregator node. Therefore, while these data aggregation protocols improve the bandwidth and energy utilization of the network, and especially allow a simpler implementation of aggregation functions (`Maximum`, `Minimum`, `Average`, etc.), they incur not only a high computation overhead but also delay (due to encryption/decryption effort). Besides, the aggregator nodes can access to the plaintext data, so the end-to-end confidentiality is not provided which is mandatory, especially for military applications. Therefore, the development of efficient schemes with stronger security becomes primordial.

Recently, several solutions [9–15] that provide data confidentiality without inducing delay have been proposed. Known as *Concealed Data Aggregation* (*CDA*), they are based on a particular cryptographic concept, namely *Privacy Homomorphism*, which enables direct calculations (addition and/or multiplication) on enciphered data. The main benefit of these schemes is that they offer the end-to-end data confidentiality and they do not require expensive computation at aggregator nodes since no encryption and decryption are performed. Conversely, actual privacy homomorphisms increase significantly the energy required for encryption and also have limited applicability to certain types of aggregate queries. In fact, only addition-based and multiplication-based aggregation operations are possible. Schemes based on symmetric encryption have been proposed, but most of them were cryptanalyzed [16]. In [11], the authors study and analyze a selected set of asymmetric algorithms for end-to-end privacy in WSNs. Their results show that the Elliptic Curve El Gamal (ECEG) is the most suitable algorithm for WSNs. In [17], we proposed an efficient implementation of ECEG on MicaZ motes. The encryption takes about 1.29 s. However, for an application where the sink needs to continuously collect information about the target area e.g. every 20 s, such a scheme is impracticable and leads to energy depletion. Furthermore, ECEG is additive homomorphic and hence, supports only a limited number of aggregation functions related to addition operation [18]. Another security service namely, the end-to-end data integrity is an interesting issue that becomes a challenge to the cryptographic community. The hop-by-hop verification does not ensure that the aggregator performs correctly the aggregation function. A compromised aggregator can produce a fake aggregate and authenticate it with its legitimate key. Therefore, the end-to-end integrity is another service that is widely desired. Due to the special characteristics of WSNs, it is very challenging to provide these two security services at the same time [18].

1.1. Paper contributions

In this paper, we propose a secure aggregation scheme for WSNs using Stateful Public Key Cryptography (SASPKC). This novel protocol employs Stateful Public Key Encryption (StPKE) proposed by Bellare et al. [19] and some previous techniques to overcome the above problems. The contributions of the present paper are threefold:

- First, SASPKC adopts StPKE for efficiency in terms of computation and communication costs. Simulation and experimental results show the huge decrease of energy utilization of the network in comparison with related work.
- Second, SASPKC aggregates not only ciphertexts but also signatures, the end-to-end data confidentiality and integrity security services are provided using symmetric homomorphic encryption and aggregate Message Authentication Code (MAC), respectively. In our proposal, the base station is able to extract individual data, verify the integrity of all messages, authenticate the senders and eventually identify the malicious node.
- Finally, our implementation on TelosB and MicaZ motes uses a fast algorithm for elliptic curve scalar multiplication to reduce the execution time of SASPKC, the algorithm is also secure against side channel attacks, in particular Simple Power Analysis.

1.2. Paper organization

The remainder of the paper is organized as follow: Section 2 presents the relevant literature review on secure data aggregation in WSNs. Section 3 presents the