Computer Networks 103 (2016) 207–227

Contents lists available at ScienceDirect

Computer Networks

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

Survey paper

Concealed data aggregation in wireless sensor networks: A comprehensive survey

Keyur Parmar*, Devesh C. Jinwala

S. V. National Institute of Technology, Surat, India

ARTICLE INFO

Article history:
Received 10 October 2015
Revised 1 March 2016
Accepted 16 April 2016
Available online 20 April 2016

Keywords:
Wireless sensor networks
Secure data aggregation
Privacy homomorphism
Privacy
Integrity
Replay Protection

ABSTRACT

The objectives of concealed data aggregation are end-to-end privacy preservation and en route aggregation of reverse multicast traffic in wireless sensor networks. Privacy homomorphism has been used to realize these objectives together. Although privacy homomorphism helps in achieving conflicting objectives, namely, privacy and data aggregation, it negatively affects other security objectives such as integrity and freshness. Privacy homomorphism, which protects sensor readings from passive adversaries, makes sensor readings vulnerable against active adversaries whose aim is to modify or to inject malicious data packets in the network. In this article, we present a comprehensive survey of the state-of-the-art concealed data aggregation protocols in wireless sensor networks. We investigate the need for en route aggregation, encrypted data processing, en route and end-to-end integrity verification, and replay protection. We discuss the challenges and their proposed solutions that achieve the conflicting objectives, such as in-network aggregation, privacy, integrity, and replay protection, together. We comparatively evaluate the performance of concealed data aggregation protocols to measure their respective strengths and weaknesses. In addition, we provide a detailed insight into the open research issues in concealed data aggregation and conclude with possible future research directions.

© 2016 Elsevier B.V. All rights reserved.

1. Introduction

Advances in Micro-Electro-Mechanical Systems (MEMS) technology have facilitated the development of tiny sensor devices. These sensor devices have escalating capabilities to perform sensing, processing, and transmission [1,2]. The multitude of these devices can collaborate to form a network, commonly referred to as the Wireless Sensor Network (WSN) [1–5]. WSNs support a wide variety of applications in military and civilian environments such as battlefield surveillance, traffic regulation, home automation, environment and healthcare monitoring, and wildfire detection [3,4,6,7]. One of the characteristic features that separates WSNs from ad hoc networks is the scarce resources [3]. The tiny sensor devices are equipped with very limited resources such as memory, processor, bandwidth, and energy [8,9]. Amongst these resources, non-replenishable energy has a direct impact on the longevity of WSNs. Therefore, there exists a need to reduce the energy consumption in WSNs. In WSNs, as shown by Hill et al. [10], transmission of a single bit over a meter range consumes the same amount of energy as required to execute a thousand CPU instructions. As the Radio Frequency (RF) operations consume far more energy as compared to the CPU instructions, there exists a need to reduce the communication overhead. The reduction of communication overhead increases the lifetime of WSNs. Although mechanisms, such as radio scheduling, control packet elimination, and topology control, help in reducing energy consumption, one of the widely acknowledged approaches to reduce the energy consumption is in-network data aggregation [11–14]. In-network data aggregation supports en route aggregation of reverse multicast traffic in data-centric networks such as WSNs.

Although in-network data aggregation reduces the redundant communication traffic, it is vulnerable to a wide range of attacks [15,16]. Adversaries can compromise intermediate sensor nodes and access the information stored therein. The compromised intermediate (aggregator) nodes can detriment the quality and accuracy of aggregated sensor readings. In addition, the lack of physical protection makes sensor nodes vulnerable to a wide variety of attacks [17–21]. Therefore, secure data aggregation protocols [15,16,22–62] aim at combining security and data aggregation together. Initial secure data aggregation protocols [15,16,27–29,37,44] provide security in a hop-by-hop manner, where encryption and decryption operations are carried out at intermediate hops. However, in hop-by-hop secure data aggregation, sensor readings become vulnerable at compromised intermediate nodes. Therefore, the need to preserve the privacy of sensor readings at intermediate nodes becomes imperative.

* Corresponding author. Tel.: +0918141133115.
E-mail addresses: keyur.mtech@gmail.com (K. Parmar), dcjinwala@acm.org (D.C. Jinwala).

http://dx.doi.org/10.1016/j.comnet.2016.04.013
1389-1286/© 2016 Elsevier B.V. All rights reserved.

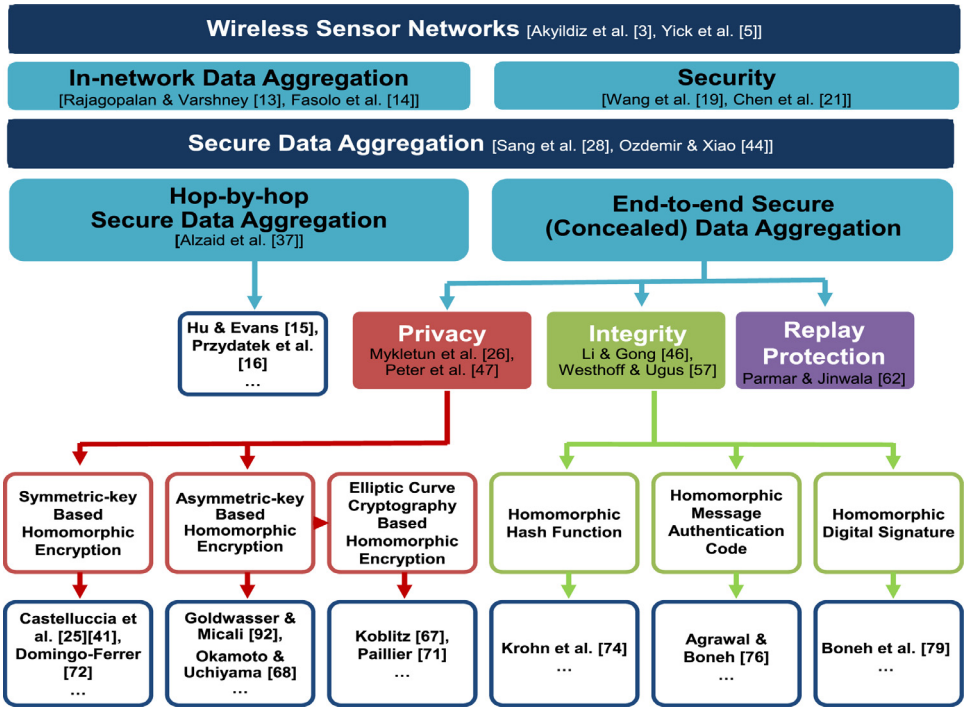

Fig. 1. Taxonomy of secure in-network data aggregation in WSNs.

End-to-end secure data aggregation, also known as concealed data aggregation, provides end-to-end privacy of reverse multicast traffic in WSNs [22,24]. In concealed data aggregation protocols [22,24–26,30–36,38–44,46,47,50–63], data once encrypted can only be decrypted at the base station. In addition, concealed data aggregation protocols support in-network data aggregation at intermediate nodes. Privacy homomorphism, introduced by Rivest et al. [64], enables the processing of encrypted data without decrypting them at intermediate nodes. The ability to process encrypted data helps in preserving the privacy of sensor readings at (compromised) intermediate nodes. In addition, encrypted data processing not only reduces the security vulnerabilities but also reduces the extra computation overhead associated with decryption and re-encryption of sensor readings.

Although privacy homomorphism protects sensor readings from passive adversaries, it makes them susceptible to active adversaries. Privacy homomorphism, used to protect the privacy of sensor readings, is inherently malleable [65,66]. Active adversaries can use the malleability property of privacy homomorphism to modify or to inject malicious data into the network. Hence, the need to preserve the integrity of sensor readings and the need to ensure the freshness of sensor readings become imperative. The conventional security mechanisms assume that encrypted data are not supposed to be altered en route. However, in data-centric networks, data are expected to be altered at intermediate nodes. Therefore, existing security mechanisms used to protect the integrity of data are not viable in data-centric networks [59]. In addition, data freshness becomes another vital security objective for concealed data aggregation protocols of WSNs. Data freshness has an immense impact on the accuracy of collected sensor readings. The conventional security mechanisms used to ensure the end-to-end data freshness are not viable in data-centric networks where data are aggregated en route. In addition, the omnipresent threat of node capture attacks makes data freshness a vital security objective.

The comprehensive taxonomy of secure in-network data aggregation in WSNs is presented in Fig. 1. As shown in Fig. 1, there exist the state-of-the-art surveys that discuss an overview of WSNs [3,5], in-network data aggregation in WSNs [13,14], and security issues in WSNs [19,21]. In addition, there exist a few surveys [26,28,37,44,47] that analyze secure data aggregation protocols in WSNs. Alzaid et al. [37] present a comprehensive survey of the hop-by-hop secure data aggregation protocols in WSNs. The surveys presented by Sang et al. [28] and Ozdemir and Xiao [44] analyze the hop-by-hop and end-to-end secure data aggregation protocols of WSNs. In addition, Mykletun et al. [26] and Peter et al. [47] provide the comprehensive analysis of asymmetric-key based privacy homomorphism techniques in WSNs. However, these surveys only consider homomorphic encryption techniques used for privacy preservation in secure data aggregation protocols of WSNs. Therefore, there is a need to survey the state-of-the-art privacy preserving secure data aggregation protocols along with the integrity and freshness preserving secure data aggregation protocols of WSNs. As per our knowledge, this is the first survey that exclusively explores the state-of-the-art concealed data aggregation protocols in WSNs.

In this article, we investigate the impact of in-network data aggregation on vital security objectives such as confidentiality, privacy, integrity (message authentication), and freshness. We explore privacy homomorphism [64] and its variants such as homomorphic encryption [25,41,66–73], homomorphic hash functions [74,75], homomorphic Message Authentication Codes (MACs) [76,77], and homomorphic digital signatures [78,79]. We classify concealed data aggregation protocols based on their homomorphic features and provide an in-depth analysis of their strengths and weaknesses. We comparatively evaluate the performance of secure data aggregation protocols based on their respective security features. The security strengths of concealed data aggregation protocols have been analyzed to recommend the security protocols that suits the requirements of sensor networks' applications. In addition, we discuss open research issues and provide future research directions relevant to the concealed data aggregation of WSNs.

The organization of the rest of this article is as follows. Section 2 discusses in-network data aggregation and its impact on WSNs. In Section 3, we present the security issues in WSNs. In addition, we present the impact of in-network data aggregation

Download English Version:

https://daneshyari.com/en/article/450657

Download Persian Version:

https://daneshyari.com/article/450657

Daneshyari.com