International Journal of Intelligent Information Technologies
Volume 16 • Issue 1 • January-March 2020

Secure In-Network Aggregation in Wireless Sensor Networks

Radhakrishnan Maivizhi, Anna University, Chennai, India
Palanichamy Yogesh, Anna University, Chennai, India

ABSTRACT

In-network aggregation is a natural approach in wireless sensor networks (WSNs) to collaboratively process data generated by the sensor nodes. Besides processing, in-network aggregation also achieves effective energy consumption and bandwidth utilization. Since the sensing devices of a WSN are prone to a variety of attacks due to wireless communication and limited resources, secure in-network aggregation is a great challenge. This article proposes a secure in-network aggregation (SINA) protocol for additive aggregation functions. This protocol integrates privacy homomorphism (PH) and secret sharing to achieve both data confidentiality and data integrity. Additionally, the proposed protocol ensures message authentication and data freshness. Moreover, it achieves in-network false data screening which considerably saves energy by not transmitting false packets. Security analysis reveals that SINA protects the network from variety of attacks. Performance analysis shows that SINA consumes less energy while achieving end-to-end security, and thereby increases the lifetime of the WSN.

KEYWORDS

Authentication, Confidentiality, Freshness, Integrity, Privacy Homomorphism, Secret Sharing, Secure Data Aggregation, Wireless Sensor Network

INTRODUCTION

Due to the advances in wireless communication technology, wireless sensor networks are becoming more popular in several spheres of life. A WSN is composed of a number of tiny sensor devices and one or more Base Stations (BSs). The widespread deployment of WSNs in applications includes habitat (temperature, fire, light, humidity, smoke, seismic activity) monitoring, law enforcement, health care, ecological and military supervision (Li et al., 2008).

Despite several applications, two significant properties that are common to most of the wireless sensor networks are: 1.They deduces a collective decision or conclusion about the environment and 2. They function under rigid technological conditions: the sensor devices have limited communication, computation, memory and battery (power) capabilities.

These properties along with the deployment (untrusted and hostile) nature of WSNs, pose a series of security concerns, for example, privacy (Ashrafi et al., 2005; Rajalakshmi et al., 2010),

DOI: 10.4018/IJIIT.2020010104

authentication, key management and integrity. Hence there exists a need to scale down all services to minimize the security overhead.

The lifetime of wireless sensor network is maximized by reducing the consumption of energy. Since the energy needed for transmitting a single bit is equivalent to the energy needed for executing 1000 CPU instructions (Hill et al., 2000), much attention have been given to reduce data transmission (Shim et al., 2015).

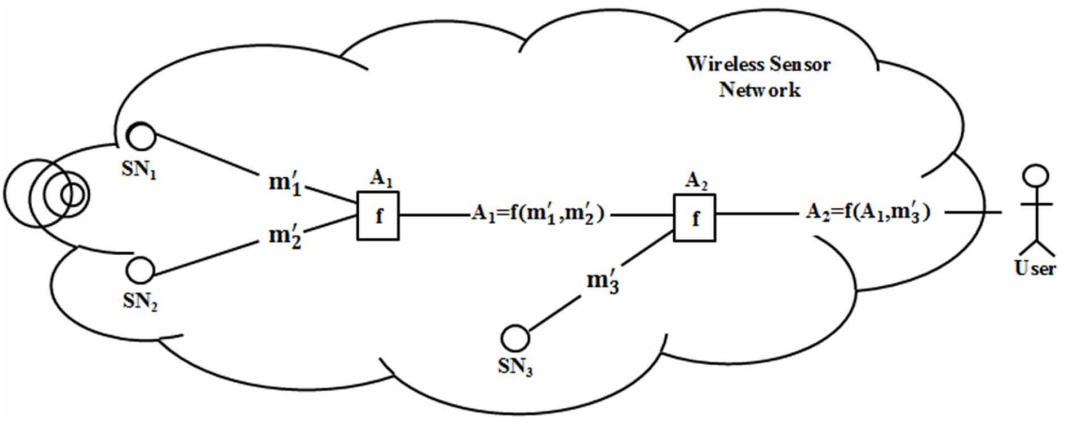
Data aggregation or in-network aggregation (Yao et al., 2002) is a natural approach for reducing data transmission in wireless sensor networks. Aggregation techniques remove redundancy in sensed data. The aim of in-network data processing is to combine the sensed raw data from several sensors using aggregation functions namely MIN, MAX, MEDIAN, MODE, SUM, COUNT, AVERAGE, etc., and forward the aggregated result to its upstream node.

The data aggregation process in WSN has two major goals: 1. To send more meaningful information to the base station so that more appropriate action can be initiated and 2. To increase the lifetime of network by reducing resource consumption of sensor devices. The resource consumption and resource constrained sensors add vulnerability to data aggregation process. For instance, a sensor node that is compromised can reveal the data or alter the data during aggregation. Therefore security becomes an important concern in data aggregation process. Hence several Secure Data Aggregation (SDA) protocols have been proposed. The prominent security requirements of secure data aggregation are: data integrity, data confidentiality, data authentication and data freshness.

Secure data aggregation protocols are classified into two categories. 1. Hop-by-hop secure data aggregation 2. End-to-end or concealed data aggregation (Ozdemir et al., 2009). In hop-by-hop SDA, every intermediate (aggregator) node does the following. (i) share a key with neighbors (ii) decrypt the ciphertexts sent by its children (iii) aggregate the decrypted data, and (iv) encrypt the result and transmit it to its parent node. Even though this approach is feasible, there is a possibility of breaching the security. By compromising privacy (Krishnamoorthy et al., 2017; VidyaBanu et al., 2012) information may be leaked during the decryption process. Also it complicates the key management as it shares a single key with neighbour nodes. In addition, it assumes that all the sensor devices are trusted.

In end-to-end or concealed data aggregation, the intermediate nodes do not need to carry out the costly decryption and encryption and do not need to share the key with neighbors. Instead the encrypted data coming from their child nodes are directly aggregated and are decrypted only at the base station to obtain the result. This is achieved with the help of privacy homomorphism techniques. Figure 1 shows the concealed data aggregation process with privacy homomorphism. The encrypted data m_1' and m_2' from sensors SN_1 and SN_2 are added by the aggregator A_1 and its result and encrypted data m_3' from sensors SN_3 are added by the aggregator A_2 and the result is forwarded to the user.

Figure 1. Data aggregation with PH



Fuzzy Multi-Objective Portfolio Optimization Considering Investment Return and Investment Risk

Shayarath Srizongkhram, Pisacha Suthamanondh, Kittitath Manitayakul, Kunio Shirahadaand Navee Chiadamrong (2022). *International Journal of Fuzzy System Applications (pp. 1-35).*

www.irma-international.org/article/fuzzy-multi-objective-portfolio-optimization-considering-investment-return-and-investment-risk/285552