Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 129 (2018) 188–193

Procedia
Computer Science

www.elsevier.com/locate/procedia

2017 International Conference on Identification, Information and Knowledge in the Internet of Things

Energy-efficient adaptive slice-based secure data aggregation scheme in WSN

Pengwei Hua[a], Xiaowu Liu[a,*], Jiguo Yu[a], Na Dang[a], Xiaowei Zhang[a]

[a] *School of Information Science and Engineering, Qufu Normal University, Rizhao, 276826, China*

Abstract

Wireless Sensor Network (WSN) is increasingly involved in many applications. However, security becomes a huge challenge in current research and it must be taken into consideration in the design of communication mechanism in order to expand the practical scene of sensor network. Secure Data aggregation (SDA) is an effective technology to prevent the network from being compromised and improve the lifetime of WSN. In this paper, we propose an energy-efficient Adaptive Slice-based Secure Data Aggregation (ASSDA) scheme which can promote the network performance under the limitation of node resource. Our method can improve the efficiency of data slicing, reduce the energy consumption of nodes, prolong the network life time and maintain a good privacy preservation level in the same time. Theoretical analysis and simulation show that ASSDA has good performances in terms of privacy-preserving, communication overhead, node energy consumption and network lifetime.

Keywords: Wireless Sensor Network; Secure Data Aggregation; Slicing; Mixing;

1. INTRODUCTION

Secure Data aggregation (SDA) is an effective mechanism to deal with redundant data. In a typical SDA process, an tree rooted at Based Station (BS) is usually formed firstly [1]. According to the different roles that the nodes play in the network, they are divided into leaf node and aggregator node. SDA can reduce the amount of network traffic which improves the lifetime of WSN significantly.

As an efficient method, Data Aggregation (DA) can save the bandwidth and improve energy efficiency in a resource-constrained WSN. Recently, DA schemes for different applications have been studied extensively [2] [3] [4] [5] [6]. According to the number of slices in each node, these schemes can be divided into three types: the fixed slicing , the random slicing and the balance slicing .

[*] Corresponding author. Tel: +1-506-559-0631 ; fax: +86-633-398-0462.
E-mail address: Liuxw@mail.qfnu.edu.cn

10.1016/j.procs.2018.03.033

He *et al.* [7] proposed the Slice-Mix-AggRegaTe (SMART) based additive aggregation which is a fixed slicing scheme. SMART includes three steps: slicing, mixing and aggregation. In the slicing step, each sensor node needs to divide its private sensor reading into J pieces, one of them is kept by itself and the remaining $(J-1)$ pieces are encrypted and distributed to $(J-1)$ neighbor sensor nodes. In the mixing step, each node sums up all the data slices including the slices it has received and the one it keeps. In the aggregation step, all nodes aggregate the data and send the result to Base Station (BS) or sink directly which results in high communication overhead and more information collisions. The random slicing demonstrates better performance than the fixed slicing and many proposals are put forward in current researches. Li *et al.* proposed an energy-efficient slice-mix-aggregate (ESMART) [8] based on the technique of data slicing and mixing. Comparison with SMART, ESMART is a random slicing scheme. When the node is an aggregator node in ESMART, it only receives the data pieces from the leaf nodes and does not participate in the slicing operation. The raw data of aggregator will be hided through assembling with the received data pieces in the step of mixing and this also provides the ability of data privacy. The balance slicing is new emerging slicing method. Liu et al. proposed a balance privacy-preserving data aggregation model (BPDA) [9] based on slicing and mixing technique. Comparing with fixed and random slicing, BPDA designs a balance slicing model to ensure that more slices are sent to the nodes which have lower privacy preservation level and enhance the privacy-preserving efficacy from the overall perspective. However, BPDA inherits the weakness of SMART and the large overhead is produced in the process of communication.

In this paper, we present an energy-efficient adaptive slice-based security data aggregation scheme and the adaptive mechanism in the model can decrease the energy consumption of sending data as low as possible. At the same time, our scheme also reduces the traffic, prolongs the lifetime and improves the security level of WSN.

A data aggregation function is defined as $y_{(t)} = f(d_1(t), d_2(t), ..., d_N(t))$, where $d_i(t)$ is the data of node i gathered at time t. In our model, we focus on additive aggregation function. It is a basic aggregation function because plenty of aggregation functions, such as max, min, and average, can be deduced from the additive aggregation function. Moreover, it is worth noting that the use of additive aggregation function is not too restrictive.

2. Energy-efficient ASSDA scheme in WSN

In this section, we present the details of ASSDA. The ASSDA scheme consists of five steps: (1) Construction of aggregation tree; (2) Determination of slicing numbers; (3) Determination of the size of each slicing; (4) Mixing and assembling; (5) Aggregation.

2.1. Construction of aggregation tree

It is necessary to build an aggregation tree rooted at BS for organizing sensor nodes in a network. BS initiates the whole network by issuing $''Hi''$ message to its one-hop neighbors. When a node receives $''Hi''$ message, it replies the $''Join\_Requests''$ message back to BS. According to the intensity of the received $''Join\_Request''$ signal, BS selects several nodes which have strong signal as its own child nodes and replies the $''Join\_Accept''$ message to its child nodes. Let P_a be a predefined value which is the probability that a child node becomes an aggregator node. Take a network with N nodes for example, the number of aggregator nodes is $N * (P_a)$ and the remaining nodes may become leaf nodes, namely there are $N * ((1 - P_a))$ leaf nodes in the entire network. Once the aggregator node is selected, it will continue to broadcast the information of $''Hi''$ to find its own child nodes. If the node received multiple $''Hi''$ messages, it selects the node with the highest signal strength as its parent node. If a node does not receive $''Hi''$ message, it broadcasts $''No\_Parent''$ message to its neighbor nodes in order to search for its parent node. Each aggregator node that receives $''No\_Parent''$ message accepts the isolated node as its child node.

2.2. Determination of slicing numbers

In order to improve the speed of convergence and reduce the traffic in the network, the nodes abide by the following rules when they send their data packets.

- For all nodes, the communication distance is one hop.