International Journal of Information Security and Privacy
Volume 15 • Issue 1 • January-March 2021

Data Privacy Protection Algorithm Based on Redundant Slice Technology in Wireless Sensor Networks

Peng Li, Nanjing University of Posts and Telecommunications, China

Chao Xu, Nanjing University of Posts and Telecommunications, China

He Xu, Nanjing University of Posts and Telecommunications, China

ABSTRACT

In order to solve the problem that the privacy preserving algorithm based on slicing technology is incapable of dealing with packet loss, this paper presents the redundancy algorithm for privacy preserving. The algorithm guarantees privacy by combining disturbance data and ensures redundancy via carrying hidden data. It also selects the routing tree that is generated by the CTP protocol as the routing path for data transmission. Through division at the source node, the method adds hidden information and disturbance data. This algorithm uses hidden data and adds perturbation data to improve the privacy preserving. Nonetheless, it can restore the original data when data are partly lost. According to the simulation via TOSSIM (TinyOS simulator), in the case of partial packet loss, the algorithm can completely restore the original data. Furthermore, the authors compared accuracy of proposed algorithm, probability of data reduction, data fitting degree, communication overhead, and PLR. As a result, it improves the reliability and privacy of data transmission while ensuring data redundancy.

KEYWORDS

Collection Tree Protocol, Disturbing Data, Network Security, Privacy Protection, Slice Technology

INTRODUCTION

Wireless sensors, as an important carrier within a wireless sensor network, have several shortcomings including a potential for eavesdropping at nodes, limited energy, weak computing capacity, and a high probability of packet loss. The main task of a wireless sensor is to collect and transmit data, and these sensors are often placed in uninhabited areas, proposed by Conti et al. (2013) and Acharya et al. (2005). The data obtained by the sensors may face security threats such as being physically captured, attacked and tampered with by attackers, leading to leaking of private information, proposed by Fan et al. (2012). This is particularly an issue in important areas such as the military or medical field. Because incalculable damage can occur if the attacker obtains a wiretap to intercept sensitive data in the data link layer, and leaks some key information or tampers with the sensitive data through the

DOI: 10.4018/IJISP.20210101.oa1

wiretap. Therefore, it is important that large-scale wireless sensor network applications study and resolve wireless sensor network data privacy concerns, proposed by León et al. (2009).

The wireless sensor network is a randomly distributed network deployed on a large scale, and the data is transmitted by wireless channel. Vinodha and Anita (Vinodha & Anita, 2018) mentions such information transmission methods inevitably occur some security drawbacks. The attacker may perform data interception and stealing on the wireless sensor node through the data link layer. Therefore, the wireless sensor network needs to be protected via privacy technology.

Privacy protection technologies are mainly divided into data privacy protection technology and location information privacy protection technology in the wireless sensor networks. Location privacy protection technology is to prevent attackers from obtaining the target location through communication mode monitoring and analysis. While data privacy protection technology is to prevent attackers from eavesdropping on sensor nodes through the link layer to obtain effective information. This paper mainly concerns on achieving the security protection of the transmission data in the sensor network based on the privacy protection technology.

The current data privacy protection protocols cannot effectively deal with packet loss problem, some of the protocols use retransmission to deal with packet loss, which leads to a negative impact to the sensor networks. Therefore, the original data can be transformed, and some additional data information is increased, so that when it comes to packet loss, the packet can be recovered by using additional data information without retransmission, proposed by Emimanothaya and Babu (Emimanothaya & Babu, 2017).

For some cases where the wireless sensor networks scenario is unstable, such as Hua et al. (2018) the network topology varies. It is necessary for a node to send data to the target node as much as possible, overcoming the probability of data loss. In addition, the privacy protection protocols are effective in confronting monitoring, traffic analysis, data tampering, and replay attacks in wireless sensor networks.

In order to solve the problem that the privacy preserving algorithm based on slicing technology is incapable of dealing with packet loss, this paper presents the linear redundancy algorithm for privacy preserving. A model for a data privacy algorithm is proposed, namely Mixed-Slice private protocol (MS), which is based on slicing technology for the sensitive issue of packets. Under circumstances where the destination node would lose some of the data packets, the entire data can still be restored by a linear redundancy algorithm. The proposed algorithm shows better data accuracy, Data reduction probability and data regression degree compared to the current researches.

The remainder of the paper is organized as follows. Section 2 introduces related work. In Section 3, the system model of data privacy algorithm based on slicing technology is proposed. In Section 4, we detail the key technologies of data privacy protection. Section 5 carries out some comparative experiments and analysis. Section 6 summarizes the paper.

RELATED WORK

Currently, wireless sensor network data privacy protection techniques can be divided into three main classes: Data privacy protection protocol based on segmentation, homomorphic encryption, and disturbance technique. Some typical data privacy protocols will be elaborated on in the following paragraphs.

1. Data privacy protection protocol based on segmentation.

The main idea of data privacy protection protocol based on segmentation is to slice up the original data into separated segments proposed by He et al. (2007) and then choose multiple transmission paths to the destination node for transmitting, in order to achieve