Enhancement of Sensor Node Anonymity in WSN-A Survey

Divya K V
Department of ECE, SNGCE Kadyirippu, Ernakulam, Kerala, India.

Shiji Abraham
Assistant Professor, Department of ECE, SNGCE Kadyirippu, Ernakulam, Kerala, India.

Abstract – The advancements in communication technologies enabled the use of wireless sensor network (WSN) s in a wide range of applications. But as range of applications increased, it became necessary to meet the requirements of high performance together with meeting network constraints. As the performance improved, the aspect of network privacy arose as a challenge. The data authenticity and location privacy preservation became important in any network. A number of discussions on privacy preservation of sensor nodes of network by increasing the anonymity were done. Sensor anonymity deals with methods that hide the real identity of the nodes in the wireless sensor network. This paper surveys the different methods used for increasing the anonymity of nodes in the system.

Index Terms–sensor nodes, anonymity, pseudonym, and authentication.

1. INTRODUCTION

Wireless Sensor Networks (WSNs) have been widely considered as one of the most important technologies for the twenty - first century. Enabled by recent advances in microelectronic mechanical systems (MEMS) and wireless communication technologies, tiny, cheap, and smart sensors deployed in a physical area and networked through wireless links and the Internet provide unprecedented opportunities for a variety of civilian and military applications, for example, environmental monitoring, battle field surveillance, and industry process control. Distinguished from traditional wireless communication networks, for example, cellular systems and mobile ad hoc networks (MANET), WSNs have unique characteristics, for example, denser level of node deployment, higher unreliability of sensor nodes, and severe energy, computation, and storage constraints, which present many new challenges in the development and application of WSNs.

A Wireless Sensor Network consists of a number of sensor nodes that are deployed in an environment to perform the function of sensing data and reporting it. A simple architecture of a WSN can be shown as in figure 1. It mainly consists of three units that are the sensing unit, the processing unit and the communication unit.

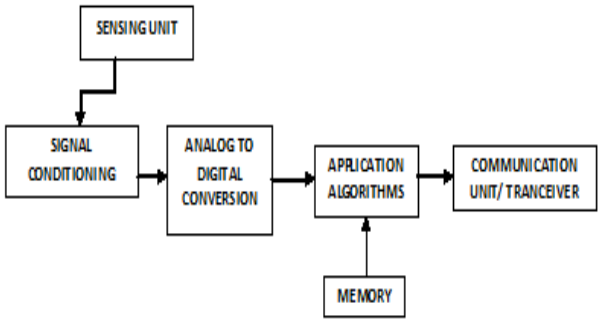

Figure 1: Architecture of WSN

The sensing unit in the system senses the data from the surrounding environments of the WSN. The sensed data is transferred to the processing unit where it is converted to electrical signals using the signal conditioning circuitry. Now, the electrical signal is converted to digital domain using the analog to digital converter. Then this digital signal is fed to the application algorithm which processes it. Memory unit helps the processing of data. The communication unit is the transceiver which communicates the data to other sensors of network or to the base station sink.

However, due to inherent resource and computing constraints, security in sensor networks poses different challenges than traditional network security. First, unlike traditional networks, sensor nodes are often deployed in large accessible areas, presenting the added risk of physical attack. Second, sensor networks interact closely with their physical environments and with people, posing new security problems. And third, most of the early proposed network techniques assumed that all nodes are cooperative and trustworthy.

A distributed sensor network is a heterogeneous system consisting of hundreds or thousands of low-cost and low-power tiny sensors that are interconnected by a communication network. The sensors are embedded devices that are networked via wireless media, integrated with a physical environment and are capable of acquiring signals, processing the signals, communicating and performing simple computational tasks. Common functionalities of WSNs are

broadcasting and multicasting, routing, forwarding, and route maintenance. By correlating sensor output of multiple nodes, the WSN as a whole can provide such functionalities that an individual node cannot. There is no central computer that performs the coordination tasks; instead, the network itself is a computer and users interact with it directly.

The extreme resource limitation of sensor devices poses considerable challenges to resource-hungry security mechanisms. In order to implement effective approaches, a certain amount of data memory, code space, and energy is required. However, these resources are very limited in a tiny wireless sensor and the trend has been to increase the lifetime of such devices by decreasing their memory, CPU, and radio bandwidth.

2. PRIVACY ENHANCEMENT

2.1. Privacy requirements in WSN

Communication security is essential to the success of WSN applications, especially for those mission-critical applications working in unattended and even hostile environments. To ensure that the network functions correctly and safely as purposed, the following are four major security requirements for WSNs:

I. Authenticity: Authenticity enables a sensor to make sure the identities of its communicating entities so that no adversary could masquerade another entity, and disseminate forged messages.

II. Integrity: Integrity ensures that a message being transferred is never corrupted or modified by an adversary without being detected.

III. Confidentiality: Confidentiality ensures that the content of the message being transferred is never disclosed to unauthorized entities. Network transmission of sensitive information, such as military information, requires confidentiality

IV. Availability: Availability ensures the survivability of network services despite denial of service (DoS) attacks.

Existing approaches in privacy protection of WSN can be given in Figure 2.

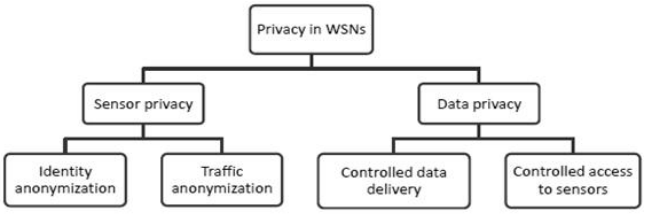

Figure 2: Existing privacy protection approaches

The sensor privacy is involved with the node security whereas the data privacy is based on the message being sent from the sensor nodes.

2.2. Node Anonymity

The sensor node privacy is considered when we need to keep the identity of the nodes unknown from any entity outside the network. The anonymity can be enhanced by the assignment of the location details in some way that the identities are only available for the nodes in the network. There are many methods that can be applied. Some of the available methods that can be considered without compromising the performance are discussed briefly below.

3. METHODS FOR SENSOR NODE ANONYMITY ENHANCEMENT

The methods for improvement of location privacy can be discussed here. There are a number of methods by which the anonymity can be preserved.

3.1. Source anonymity scheme

Network formal model: Model use a generic asset monitoring application, which is called the Panda- Hunter Game, as well as refer to a formal model for asset monitoring applications that can benefit from source-location privacy protection. In the Panda-Hunter Game, a large array of panda-detection sensor nodes has been deployed by the Save-The-Panda Organization to monitor a vast habitat for pandas [9]. As soon as a panda is observed, the corresponding source node will make observations, and report data periodically to the sink via multi hop routing techniques. The game also features a hunter in the role of the adversary, who tries to capture the panda by back tracing the routing path until it reaches the source. As a result, a privacy-cautious routing technique should prevent the hunter from locating the source, while delivering the data to the sink. In the Panda-Hunter Game, we assume there is only a single panda, thus a single source, and this source can be either stationary or mobile. During the lifetime of the network, the sensor nodes will continually send data, and the hunter may use this to his advantage to track and hunt the panda. We assume that the source includes its ID in the encrypted messages, but only the sink can tell a node's location from its ID. As a result, even if the hunter is able to break the encryption in a reasonably short time frame, it cannot tell the source's location.

This formal model for the source-location privacy problem is modified in sensor networks and is proposed in [1]. It examines the privacy characteristics of different sensor routing protocols. It examines two popular classes of routing protocols: the class of flooding protocols, and the class of routing protocols involving only a single path from the source to the sink. In order to provide efficient and private sensor communications, method devises a new technique to enhance

source-location privacy that augments these routing protocols. The routing of information is done by considering a fake source and from that, to the real sink.

Another traditional approach for hiding source in WSN is to let all nodes generate dummy data packets even if they have no event to report. However, this kind of approach introduces large overhead. In order to reduce the large overhead of sending dummy data packets, a method is proposed in [2] using a much shorter control packet to achieve source anonymity. The short control packets are used to coordinate the transmissions of dummy data packets, which prevent revealing the source node and hence provide source anonymity in WSN.

3.2. Pseudonym based anonymisation

Another method is increasing Pseudonimity for achieving communication anonymity in networks that apply geographic-routing algorithms [4]. An Anonymous Receiver-Contention Positioning (ARCPO) routing algorithm is proposed. Node identities (IDs) are kept anonymous. Pseudonyms, i.e., the positions of destinations, are used for data-packet delivery. The anonymity for a destination relies on the difficulty of matching its position to its ID by any observer. Position servers that provide node position information act as trusted third parties and handle identity management. Node mobility makes the use of the pseudonym momentary, and therefore can further improve privacy. The anonymity for the source and intermediate nodes in the path is also achieved because they are not required to reveal any identity information. A receiver-contention mechanism is proposed so that a next hop can be generated without local position information exchange, which otherwise may lead to severe privacy degradation.

Another method is the simple anonymity scheme [8]. In this method, we assign a pseudonym to each node of the network. This pseudonym is used as the identity of nodes during communication of sensed data in the network. A modification is done in this system in paper [5]. Here, a pseudonym is assigned to all nodes in the network. Sensor node anonymity is improved by the anonymous sender and receiver IDs. The method is designed such that a sensor anonymity enhancement scheme based on pseudonym for clustered WSN is proposed. The scheme includes two phases. Both the sensor nodes within a cluster and the cluster heads using fake identities to communicate with each other. It can protect the privacy both of the cluster members and the cluster head nodes.

4. CONCLUSION

In this paper we have done a survey on the works done by various researches for enhancing the anonymity of sensor nodes in network. It is essential to keep the privacy of nodes of a network from any adversary outside the network. Many works pointed out the ways to obtain anonymity in the system. Through this paper, we are recommending various methods available from the works done in the process of improving the anonymity of a sensor node in the network.

REFERENCES

[1] KAMAT P, ZHA NG Yanyong, T RAPPE W, et al. Enhancing source location privacy in sensor network routing. Distributed Computin Systems, 2005. ICDCS 2005, Proceedings,25th IEEE International Conference on. IEEE, 2005:599- 608.

[2] Reindal P , D U Xiaojiang , Nygard K, et.al ."Lightweight Source Anonymity in Wireless Sensor Networks[C];Global Telecommunications Conference(GLOBECOM 2011) 2011 IEEE.2011:1-5

[3] Xiaoxin Wu. "Applying Pseudonimity for Anonymous Data Delivery in Location-Aware Mobile Ad Hoc Networks".., IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY, VOL. 55, NO. 3, MAY 2006.

[4] SHI LeyP, FU Wenjingl, JIA Congl, LIU Xinl, JIA Chunfu, "A Sensor Anonymity Enhancement Scheme Based on Pseudonym for Clustered Wireless Sensor Network" College of Computer & Communication Engineering, China University of Petroleum,Qingdao, Shandong, P.R.China ,College of Computer & Control Engineering, Nankai University, Tianjin, P.R.China,.

[5] Ting Li, Yong Feng, Feng Wang, Xiaodong Fu., "A Dynamic Pseudonyms Based Anonymous Routing Protocol for Wireless Ad Hoc Networks "..,Yunnan Key Lab of Computer Technology Applications, School of Information Engineering and Automation, Kunming University of Science and Technology.

[6] GURJAR A, PATIL A. Cluster based Anonymization for Source Location Privacy in Wireless Sensor Network[J]. IEEE Communication Systems and Network Technologies (CSNT), 2013:248-251.

[7] Jaydip Sen, "A Survey On Wireless Sensor Network Security" ,International Journal of Communication Networks and Information Security Vol.1 No:2 , Aug 2009

[8] Satyajayant Misra and Guoliang Xue*,"Efficient anonymity schemes for clustered wireless sensor networks"., Department of Computer Science and Engineering, Arizona State University, Tempe, Arizona, USA.

[9] "WWWF - the conservation organization," http://www.panda.org/.

Authors

Divya K.V. received her B.Tech degree in Electronics and Communication Engineering from Calicut University, Kerala in 2013.She is currently pursuing her M.Tech degree in Communication Engineering at Sree Narayana Gurukulam College of Engineering, Kadayirippu under Mahatma Gandhi University, Kottayam, Kerala, India.

Shiji Abraham is working as Assistant Professor in Department of Electronics and Communication Engineering at Sree Narayana Gurukulam College of Engineering, Kadayirippu, Kerala. She secured her B.Tech degree from Mar Athanasius College, Kothamangalam, Kerala and her M.Tech degree from University College, Muttam under Mahatma Gandhi University, Kottayam , Kerala, India.