Overview of Survey on Security of Wireless Sensor Network

Wei Wang
School of Information Science and Engineering
Guilin University of Technology
Guilin, China
E-mail: 65104628@qq.com

Xiang Yang
School of Information Science and Engineering
Guilin University of Technology
Guilin, China
E-mail: 490745953@qq.com

***Abstract*-As a product of the combination of wireless communication technology, intelligent sensor technology and network technology, wireless sensor network has broad development prospects and more and more scholars have been attracted to that study. Moreover, in the military field, national defense field and other special fields, the security research of wireless sensor network has also been put on the agenda. This paper will briefly introduce the basic concept of wireless sensor network first. After that, the existing wireless sensor network security problems will be raised and the research situation of the security of wireless sensor network will be analyzed. The last part of this paper is about the further research tendency for wireless sensor network security.**

Keywords-Wireless sensor network; security; overview; new development

I. INTRODUCTION

WSNs(Wireless sensor networks) refer to the wireless ad-hoc networks that are composed of the micro sensor nodes which are arranged within the monitored region. The micro sensor nodes are low in price, small in volume and they have computation and communication abilities. These sensor nodes are usually composed of sensors, data processing units, wire-less communications units and power supply modules. These highly-integrated nodes will be used in the hostile environment after being specially packed so as to detect all kinds of key data that can not be acquired by human beings directly. Thus, the wireless sensor networks can be widely applied in detection of ecological environment, informatization of industrial manufacturing, intelligent safegu-ard systems, aeronautics and astronautic aerospace, battlefield awareness and other fields.

II. BACKGROUND OF SECURITY PROBLEMS OF WSNS

Recently, more and more wireless sensor networks have been applied to the field of military defense and other key fields, thus, because of the problem of military network intrusion, the hacker attacks and other problems, we have to consider the security problems of WSNs. At the same time, higher security requirements shall also be put forward for WSNs. These security requirements include the confidentiality, integrity, authenticity, availability, higher robustness and the freshness of the collected node data of wireless sensor networks.

Background of security problems of WSNs can be briefly summarized as the following aspects:

(1) The sensor nodes, which are the basic units of wireless sensor networks, can only be powered by the battery and the small volume of nodes. However, capacity of the battery is not large in general and the nodes are deployed in the uninhabited areas or the dangerous zones, which will bring great troubles to replacement of the battery. In addition, the limited calculation and data storage capacity also make it difficult for the nodes in loading that large and complicated network security protocol. It is also hard for the nodes to resist the memory consumption caused by flooding attacks. Besides, communication bandwidth of nodes is also limited.

(2) At present, there is no optimal security protocol for wireless sensor networks. In the previous time, many predecessors have put forward their security algorithms. However, some of those algorithms have their own drawbacks; some have leaks by themselves; some even lack the self-correcting and self-healing ability for network protocol.

(3) As long as the deployment environment and methods are considered, we can see that the environments of network nodes are usually bad. The openness of nodes, the randomness of deployment, the one-off of usage, the impossibility of maintenance, the bad self-supplying capacity and other characteristics make the sensor nodes easily be physically attacked by the enemy.

III. RESEARCH SITUATIONS OF SECURITY PROBLEMS OF WSNS

A. Research Situations of Security Problems of WSNs

Currently speaking, researches of WSNs security are still immature. Most of the security protocols and algorithms about WSNs have great limitations. In addition, it is also hard to build a perfect model for detection and resistance of attacks of different layers and other kinds of combined attacks. At present, the basic research ideas about security protocols of WSNs can be divided into two kinds. The first kind focuses on some specific network attacks, such as the DV-Hop security algorithm for resistance of wormhole attacks. The other is the protocol algorithms which focus on attacks of

Published by Atlantis Press, Paris, France.

certain layer of wireless network protocols, such as the Tinysec protocol, which can discover the false information of data link layer and which can improve integrity, confidentiality and authenticity of information and which can provide the replay protection for the data.

B. Hot Research Fields of Security of WSNs

Researches of security system of WSNs are mainly done in the following aspects: key management, secure routing, secure data aggregation, secure localization and the privacy protection of nodes. The chapter will focus on introduction and analysis of the above aspects.

- Key management

Key management protocol is the core of secure communication protocol of WSNs. Establishment of WSNs network communication can be divided into two stages, which include the initialization stage and formation stage of the network. Formation stage of the WSNs can be divided into two steps, which includes the detection of the shared key and establishment of the key. In the detection stage, two sensors will be used to find the common key so as to maintain the mutual communication between them.

Recently, people have put forward many key management schemes of WSNs. Some people even did the investigation, collection and classification of those key management schemes, for example, they divided the key managements into the pre-assigned key management, the pre-assigned pair-wise key management, the random key distribution and the key distribution which is based on the Key Distribution Center KDC. There are also researchers who divided the popular key management technology into the pre-shared key scheme, the non pre-shared key scheme, the probabilistic scheme and the defined scheme. Zhang and Varadharajan[1]also divided the key management schemes of WSNs into the symmetrical, the asymmetric and the mixed-typed key management schemes. Among them, the symmetrical key management can be divided into eight key management schemes, including the schemes based on entity or arbitration, bare statistics, multiple-term formula, matrix, arborescence, modular design, EBS and the antithesis. The asymmetric key management schemes can be divided into the key management schemes on the basis of RSA, ECC and ID.

Eschenauer and Gligor[2] also put forward a kind of random key distribution technology. In that technology, a key pool which contains many symmetric keys shall be built firstly. After that, some keys shall be taken randomly and be stored in each sensor node. If two neighbor nodes contain at least one common key, a safe link will be established. Through application of this method, neighbor nodes will not need to share keys in advance. Thus, the risks resulting from key attacks will be greatly reduced.

Zhu and Setia[3] also put forward a kind of LEAP key management protocol. According to the LEAP key management scheme, four keys will be established in each sensor node according to different types of data within WSNs. The four keys include the single key which is shared with the base station; the dual key which is shared with other nodes, the cluster key which is shared with many neighbor nodes and the group key which is shared with all nodes in the network.

- Secure routing

Till now, many routing protocols about sensor networks have been proposed. However, they rarely take the secure routing as their design goal. The security problems of nodes, which are communication paths of the sensor network, become more and more important because of the low computation and memory ability of the WSNs nodes. The attackers can take advantage of this point and inject or modify the routing protocols stored in the nodes through occupying certain nodes. The attackers can also tamper the data and information transmitted by the routing or can selectively transmit the communication packets. They can even transmit the data to the intruded nodes.

Karlof and Wagner[4] of Berkeley of University of California put forward a kind of new secure routing protocol according to the current and future attacks to WSNs routing protocols. At the same time, Karlof indicated in his paper that even though the security problems of ad-hoc network are similar with WSNs, our defense mechanisms which are developed for ad-hoc network may not all be applied for WSNs correctly.

Perryig[5] proposed two kinds of security routing models for WSNs, which are the SNEP (Secure Network Encryption Protocol) and the TESLA. SNEP can provide the high confidentiality and integrity of WSNs and the freshness between nodes and sink nodes (base stations or clusters). TESLA can realize the broadcast authentication from nodes to different points.

- Secure data aggregation

Because the environment parameters collected by adjoining sensor nodes of WSNs are similar, there must be a large number of redundant data information that will be transmitted from the sensor nodes to the sink nodes during the course of information collection of sensor. This will not only waste the limited energy of sensor nodes, but also the communication bandwidth. The data fusion technology can efficiently avoid the above drawbacks. However, the ordinary nodes and the sink nodes (especially nodes on single-layered sensor networks) can be captured easily and data of the fusion nodes can be maliciously modified easily, which will cause errors of the date fusion. All of these things have put forward new requirements for security protocols of date fusion.

Ozdemir[6] has done many researches on secure data aggregation of WSNs. He pointed out that security and the data aggregation are two contradictory problems and the security protocols need the encryption and authentication of sensor nodes. On one hand, according to the security protocols, sensor nodes shall have the

ability to encrypt and identify any form of sensor data before the data transmission. At the same time, the data shall be decoded through the base station. On the other hand, in order to maximize energy usage efficiency of the nodes, the primary data shall have the ability to realize the data fusion.

Zhang and Liu[7]proposed a kind of data fusion scheme with authentication support of the digital watermarking technology. This scheme regarded WSNs network as one picture. In that picture, each node can represent each pixel on the picture. Data of the sensor node can be regarded as gray degree of the picture. Through the application of image compression method, which is similar to JPENG, watermarks of the sensor nodes and the transmitted data will be compressed. After that, the base station will compare and confirm the water-marking data so that the secure data aggregation can be realized.

- Secure localization

Location technology is one of the key techniques of WSNs. The event occurrence and the acquisition of location information of nodes are the foundations of application of WSNs. Positioning of these nodes shall rely on the location information of parts of the beacon nodes of WSNs (the nodes with GPS positioning devices or the nodes with the known geographical location information). The other unknown nodes will assume their own position through the specific location algorithms (Range-based and range-free method).

Through analysis of the existing typical secure localization algorithms of WSNs, we can find that the existing secure localization algorithms have their own pros and cons. TABLE I below shows the analysis and comparison of the existing typical secure localization algorithms.

- Privacy protection

Privacy protection means the protection to some features which concern with the interest of WSNs or the users. It mainly includes the privacy protection of data, the privacy protection of localization and the privacy protection of identity.

Privacy protection of data. The sources of data information here can be divided into two parts, one is the perception information collected from nodes of the sensor nodes, the other is the query information the users submitted to the WSNs. As the main information carrier of WSNs, data of the sensor nodes will also be the attacked targets of intruders. According to sources of the attacks, the attacks can be generally divided into outside attacks and internal attacks. The outside attacks can get key information of the node data through monitoring of the data communication between sensor nodes. Relatively speaking, the outside attacks are less threatened and they can be effectively defended through the encryption and authentication method of data. The internal attacks mean that the intruders can acquire the private information of data through capturing the nodes or putting false nodes in the network or through participating in the network data transmission. If this kind of attacks is applied, the alien nodes will not be easy to be found or removed effectively.

Privacy protection of localization. WSNs have certain application areas. If the WSNs are used to monitor the population and distribution of certain endangered species in the natural preservation zone, privacy protection of the location of information source in the WSNs will become very important. As long as the position privacy is captured by the lawless person, the species which are monitored will be threatened. Thus, we can see the urgency and importance of the privacy protection of localization.

Many scholars have put forward their views and their preparedness plans for the privacy protection of localization, including the source-node privacy protection and the sink node privacy protection. The phantom routing based on the directional random walk which is proposed by Pandurang Kamat is the earliest privacy protection research about location of source nodes of WSNs. He considered that the motion of objects can be constantly tested by the static sensor nodes. Attackers may track the data stream from the nodes to the sink nodes. In order to prevent them from applying the data stream to locate the targets, phantom routing can mislead that track through the random walk and then distribute data from the flooding device or the single path routing.

Privacy protection of identity. In the field of battlefield sensation and home life field, the sensor and the information it collected are related to the specific entity, for example, as long as the identity of users of WSNs is exposed, the serious consequences may be triggered. Thus, key technologies of WSNs must be centered on privacy protection of identity.

Identities of nodes or source nodes can be generally hidden through anonymous mechanisms for privacy protection of their identities. According to the anonymous objects, the anonymous mechanisms can be divided into the anonymity of sender, the anonymity of receiver and the anonymity of communication parties. This paper will not do deeper overview about related researches of privacy protection of identity because that research is still in the primary stage.

IV. CONCLUSIONS

With the widespread deployment and application of WSNs, people pay more and more attention to security problems of WSNs. This paper mainly introduces the hot researches of security problems of WSNs, which are the key management, the secure routing, the secure data aggregation, the secure localization and the privacy protection. Through the analysis, we can find that the existing security algorithms all have their specific application backgrounds and they can only be used to

detect and defend certain types of network attacks. This paper holds that according to similarities and differences of different attack types, more researches shall be done to the detection and defense mechanisms of the same-layered or cross-layered light-weighted coordination-resistant attacks.

REFERENCES

[1] Zhang Jun-qi, Vijay V. Wireless sensor network key management survey and taxonomy[J]. Journal of Network and Computer Applications, 2010(33): 63-75.

[2] Eschenauer L, Gligor V. A key management scheme for distributed sensor networks[C]//In: Proceedings of the 9th ACM Conference on Computer and Communications Security , 2002(11): 41-47.

[3] Zhu S, Setia S, Jajodia S. Leap:Efficient security mechanisms for Large-Scale distributed sensor networks[C]//In: Proc. of the 10thACM Conference on Computer and Communications Security , 2003: 62-72.

[4] Karlof C, Wagner D. Secure routing in wireless sensor networks--attacks[J]. AD HOC Networks, 2003(1): 293-315.

[5] Perrig A, Szewczyk R, Tygar D, et al. Spins: security protocols for sensor networks[J]. Wireless Networks, 2002, 8(5): 521-534.

[6] Ozdemir S, Yangxiao. Secure data aggregation in wireless sensor networks[J]. Computer Networks(53): 2022-2037.

[7] Wei Zhang, Liu Yong-he, Das S, et al. Secure data aggregation in wireless sensor networks- A watermark[J]. Pervasive and Mobile Computing, 2008(4): 658-680.

TABLE I. COMPARISON OF THE EXISTING TYPICAL SECURE LOCALIZATION ALGORITHMS

algorithm name	**based on the distance**	**number of beacon nodes**	**cost**	**power dissipation**	**location accuracy**	**tolerance for attacker**
Liu	yes	on request	lower	lower	lower	lower
ROPE	yes	less	higher	higher	higher	higher
SPINE	yes	more	higher	higher	higher	higher
DRBTS	no	less	higher	lower	higher	lower
HiRloc	no	less	lower	lower	higher	higher
SeRloc	no	less	lower	lower	higher	higher