International Journal of Security and Its Applications
Vol.8, No.6 (2014), pp.41-50
http://dx.doi.org/10.14257/ijsia.2014.8.6.04

Analysis of Typical Secure Routing Protocols in WSN

Jingsha He[1,2,a], Bo Zhou[1,b] and Ruohong Liu[2,c]

[1]*School of Software Engineering, Beijing University of Technology, Beijing 100124, China*

[2]*Beijing Development Area Co., Ltd., Beijing 100176, China*

[a]*jhe@ bjut.edu.cn,* [b]*yuzhibo@ emails.bjut.edu.cn,* [c]*lrh450820@126.com*

Abstract

This paper will first sum up the typical attacks and countermeasures in the network layer of Wireless Sensor Network (WSN), then it will classify the existing secure routing protocols according to the core secure schemes used by them, and emphatically introduce and analyze the typical ones among them. Finally this paper will propose some problems on secure routing, which requires further studying.

Keywords: *Wireless Sensor Network (WSN), network security, secure scheme, secure routing protocol*

1. Introduction

In many application fields of WSN, such as security guarding and battlefield environment monitoring, data collected and transmitted by the sensor nodes is very sensitive, so it is important to ensure the security of data during the collection and transmission process. Due to the use of multi-hop forwarding data transmission mechanism and self-organization networking mechanism, each node in WSN is required to participate in discovering, establishing and maintaining the routing. These characteristics make the routing protocol in WSN vulnerable to various attacks.

At the same time, in order to save energy by reducing data transmission, the perception data need in-network processing such as data fusion, redundant message deletion and data compression during the transmission to the sink node. Each intermediate node in the transmitting link is required to read, modify and compress the data. The possibility of some intermediate nodes captured by attackers makes it impossible to guarantee the data security in WSN, when only using end to end encryption mechanism. New security mechanism should be introduced into the network layer of WSN, which is called secure routing protocol. Secure routing protocol should not only make effective routing decisions to guarantee that the data is transmitted in an energy saving way, but also ensure the safety of data during the transmission and processing.

There are many restrictions in the WSN security implementation. These include the vulnerability of open wireless channel transmission, easy capturing of cheap sensor nodes with weak protection, vulnerability of physical protection due to the unattended deployment environment, which is not suitable for public key cryptography algorithm because of the limited calculation, storage and energy of the node. All of these restrictions make the secure routing in WSN a challenging research topic, attracting scholars from all over the world to work on it, and they have achieved abundant results.

ISSN: 1738-9976 IJSIA

2. Typical Attacks and Common Countermeasures

2.1. Typical Attacks

In the initial design of many routing protocols, people focused on things like how to improve success ratio of data submission, reduce transmission delay, save battery energy of the nodes and prolong survival time of the network. However, security was not taken into consideration, thus affected many routing protocols to have serious security problems and was used to attack the WSN. The typical attacks are shown in Table 1.

Table 1. Typical Attacks

Name	*Description*
False routing information	The attacker participates in the data transmission process and transmits false routing information to other nodes in the network.
Sinkhole attack	The attacker attracts some or all the neighbor nodes to send the data to him by claiming that he has plenty of energy or optimal path. Then he will drop all of the data he got and send false data to other nodes in the network.
Selective forwarding	This kind of attack is the improvement of sinkhole attack. In sinkhole attack, the attacker will easily get caught because of dropping all the data he got from other nodes, but if using selective forwarding, he can hide much longer because it is normal to lose some data in a network with dynamic topology.
Sybil attack	The attacker has multiple identities in the network. It makes ordinary nodes think that more nodes exist in the network so that they can send the data to the database through them. Otherwise most of the data are sent to the attacker.
HELLO flood	The attacker broadcast routing information in high energy signal so that each node in the network thinks that the attacker is its direct neighbor and tries to send its data to the attacker.
Wormhole attack	The attacker controls a malicious node to get some messages from the network. Then he creates a tunnel by giving statements of low delay link and retransmits the data he received in a totally different way.
Acknowledgement spoofing	The attacker controls a malicious node to eavesdrop some packets, which was sent to a neighbor node and use them to cheat on the link layer so as to a sender will believe that a bad link is good or a dead node is alive. Then all data transmitted in this link will be lost.
DoS	Generally the attacker has enough energy. He can use DoS to create network chaos by consuming network bandwidth or using up energy of the ordinary sensor nodes.

Attackers usually launch a specific type of attack to a specific type of routing protocol. They can also create more threatening attacks by combining the attacks introduced in Table 1. And with the deepening of research, more and more new types of attacks will be discovered.

2.2. Common Countermeasures

In order to deal with the various attacks in WSN, researchers have proposed many countermeasures and the common ones are shown in Table 2.

Table 2. Common Countermeasures

Category	*Description*
Countermeasures for external attack	We can keep most of the external attacks away through simple encryption and authentication in the link layer of WSN.
Countermeasures for sybil attack	We can use symmetric key between nodes and a trusted base station. Where a set of neighbor nodes can use the key they got from the base station to achieve authentication and encrypted connection between them. Even though the attacker can move in the network and establish a shared key with other nodes, the base station can still find him by limiting the number of neighbor nodes that each node could have.
Countermeasures for HELLO flood	We can use bidirectional authentication before two nodes communicating with each other. The transmission power of ordinary nodes is so small that it cannot send the confirmation message to the attacker successfully. Even though the attacker can occasionally achieve the confirmation by using a high power receiver, the base station can still prevent it by limiting the number of neighbor nodes.
Countermeasures for selective forwarding	The best countermeasure for selective forwarding is multi path routing. When there are N mutual independent paths for a source node to send its data to a destination node, we can then prevent N attackers from attacking the network.
Countermeasures for broadcast authentication	Since all of the nodes trust the base station, we cannot allow attackers forge the information of the base station as they wish. We can achieve this goal by using digital signature or adding authentication information.
Countermeasures for wormhole attack and sinkhole attack	These two kinds of attacks are the most difficult to prevent, especially when they are combined with each other. It is hard to detect wormhole attack because attackers use private frequency between them. And it is also hard to prevent sinkhole attack because ordinary nodes are unable to distinguish the authenticity of the information sent by the attacker. So the best countermeasure is focusing on these two kinds of attacks when we design a routing protocol.

When designing a secure routing protocol, we should find out how to prevent different kinds of attacks and create a secure operating environment for the WSN. But the diversity of attacks and the inherent defects of WSN make it very difficult to design a secure routing protocol with comprehensive countermeasures.

3. Typical Secure Protocols

In 2002, Perring proposed the earlier secure routing problem in WSN. The following year, Karlof made a discussion on the typical attacks which secure routing protocols faced and some countermeasures. He also elaborated the importance of secure routing protocols. From then on, many researchers focused on this area and many secure routing protocols have been proposed. According to the core secure schemes used by these secure routing protocols, we can divide them into several categories: feedback information based secure routing protocols, geographical position based secure routing protocols, cipher algorithm based secure routing protocols, multi path transmission based secure routing protocols, and hierarchical structure based secure routing protocols and secure routing protocols response to specific attacks.

3.1. Feedback Information based Secure Routing Protocols

In some routing protocols, nodes make a series of decisions to improve the network security through the feedback information such as delay, trust, geographical position and remaining capacity. These decisions include safe path selection, low energy consumption path selection and trusted neighbor nodes selection.

AE-ARAN [1] is an anonymous and efficient secure routing protocol which is based on ARAN. It introduced the D-S theory of evidence and dealt with the random factors and subjectivity in trust evaluation. This protocol calculates the trust of nodes according to the trust evaluation model, and then selects the trusted nodes to participate in the routing. During the routing building process, the routing table of each node will store a hash routing registration table which contains the anonymous identity of the node. When establishing a new routing, all the node needs to do is calculate whether the hash identity of the destination node is in their own routing table, which can effectively guarantee the anonymity of network and avoid repeated initiated routing. All in all, AE-ARAN can effectively detect and isolate the malicious nodes, resist attacks like modify and black hole attack to improve reliability, robustness and security of the whole network. The advantage is more obvious when facing too many malicious nodes.

Castor secure routing protocol proposed by Galuba [2] can solve the problems of safety, computability and adaptability at the same time. This protocol only uses some simple acknowledgment packets and doesn't need any control information. Each node makes its own routing decision in a local area and it only stops transmitting data after receiving the acknowledgment packet from the destination node. This protocol has good protection not only on a variety of common attacks but also on special attacks against it.

3.2. Geographical Position based Secure Routing Protocols

Geographical position information can be used as important routing decision basis to improve the performance of data transmission. Many geographical position based secure routing protocols have been proposed in the present. This kind of protocol usually needs to exchange coordinate position information between neighbor nodes and this characteristic makes it vulnerable to attacks, especially sybil attack. So we should improve its security by using pertinent security mechanism.

There are many ways to achieve anonymity, such as anonymize information of the source node and destination node and anonymize routing path. Li [3] proposed three ways to achieve geographical position information anonymity of the source node. In the three ways, he chose the minimum distance, angle and quadrant as the basis to select intermediate nodes. By deleting the information of last hop node, the protocol prevents the attacker from going back to find the last hop node. Thus making him unable to determine information of the source node. The protocol requires each node to know the geographical position information of other nodes and transmit data to the sink node unilaterally. In addition, all the three ways have a good energy-saving effect.

Prism routing protocol [4] achieve the protection of security and privacy. The protocol uses group signature mechanism to authenticate nodes; it uses anti-tracking mechanism to prevent tracking by attackers and is required to ensure the integrity of the routing information. Nodes don't have unique ID in the whole network, but you must know the geographical position of nodes. Communication between nodes is based on topological structure or new conditions, when this condition cannot be met, it will be made up by using the way of hit-and-miss.

3.3. Cipher Algorithm based Secure Routing Protocols

We can use encryption mechanism to protect information from being stolen by attackers and use authentication mechanism to prevent attackers from joining the network. Application of the above security mechanisms can effectively enhance the security of WSN.

Misra [5] proposed an end to end protocol algorithm, ETESC. The core idea of this algorithm is that pre configure different keys for each node to strengthen the elastic of some segments. Lever principle is also used in the algorithm. The protocol is comprised of different key management and routing with elastic aware. And we can also get good security effect when combined with geographical position information based routing protocol or data centered routing protocol.

Ariadne is an on-demanded secure routing protocol [6]. It can resist various attacks and also is very effective in reducing the loss caused by captured node. In order to achieve this security, the protocol can only rely on efficient symmetric key encryption operation. On the basis of DSR routing protocol, Ariadne added TES-LA mechanism, but it requires time synchronization and timely certification in this protocol.

3.4. Multi Path Transmission based Secure Routing Protocols

Multi path routing can effectively improve the delivery ratio of data and balance energy consumption to prolong lifetime of the sensor nodes. At the same time, it is also an effective countermeasure for selective forwarding attack.

The basic idea of MSR [7] protocol is the division of an original information into sub datagrams through canceling code. These sub datagrams are then sent out through independent multiple paths and are combined by the destination node. The protocol mainly includes random multi paths, forced passive confirmation and canceling code. Random multi paths are only established when needed. Forced passive confirmation is based on monitoring traffic passively, by analyzing secure behavior of the neighbor nodes in order to reduce the header of the routing datagrams. All in all, MSR has countermeasures for most of the common attacks.

Connectivity is an important concept in multi hop routing protocols. SeMuRa [8] extended K-connectivity and introduced the conception of K-X-connectivity. The protocol also extended DSR algorithm by using ultimate digital signature authentication during the datagram exchanging. In order to guarantee the security of routing, the protocol requires that

a node must be able to authenticate other nodes in the establishment of routing and monitoring the behavior of its neighbor nodes. In addition, forged datagrams must be detected before they reach the destination node. SeMuRa uses watchdog mechanism to detect the situation when node doesn't transfer datagrams and can effectively avoid wormhole attack.

3.5. Hierarchical Structure based Secure Routing Protocols

Sensor nodes are usually powered by battery; it is hard to replenish their energy. So energy saving is an important challenge for WSN. Even though hierarchical network structure has a good characteristic of energy saving, it unfortunately has a serious impact on performance and security of the network once key nodes such as cluster head and tree root are attacked. We need to use specific security protection mechanism.

LEACH is a typical clustering based secure routing protocol, but it didn't properly consider security issues. AC [9] added security considerations on the basis of LEACH. There are three layers of routing in the protocol, a layer for cluster head selecting, a different layer for identity authentication and confidentiality, and another layer for routing. This protocol requires each sensor node to confirm its base station before the deployment through unique ID as well as the formation of clusters and head in each cluster. All of this work is completed by the LEACH protocol.

SHSMRP [10] combined hierarchical network structure and Nano tree. The node can obtain geographical position information of their own and use it as an important condition to join the network. The protocol consists of five parts: nodes information aggregating, Nano trees structuring, sub Nano trees structuring, data transmitting and Nano trees maintaining. Its own local key hierarchy is designed according to LKHW and it guarantees the secrecy and integrity of data by using HMAC. All of these make it possible to effectively avoid sybil attack and wormhole attack.

3.6. Secure Routing Protocols Response to Specific Attacks

Due to a specific routing protocol, it usually just faces several specific types of attacks, so we can design specific countermeasures according to the characteristics of different attacks to improve the security of routing protocols.

DoS attack can be divided into passive attack and active attack. S_LEACH [11] is a secure routing protocol that deals with the passive DoS attack and can strengthen the mutual cooperation ability between nodes. This protocol introduced Bias Game Method on the basis of LEACH routing protocol. Bias Game Method can make the malicious nodes more active and affect the intrusion detection system to run better in the active time of malicious nodes.

The main idea of the protocol proposed by Song [12] is discovering routing according to determined statistics. It improved the judgment on wormhole attack and can even pinpoint the location of the attackers. But if the behavior of a malicious node is normal in the routing process, it will be difficult to detect, especially blackhole attack.

3.7. Comparison of All the Categories of Protocols Above

Through the introduction and analysis on the typical existing protocols, we have a better understanding on theoretical basis, working mechanism and characteristics of each type of protocol. In order to get a more specific understanding of the differences between different categories of protocols, I made a horizontal comparison on all the categories of protocols above in this section, as shown in Table 3.

Table 3. Comparison of Protocols

Category of the protocol	*Attacks that can resist*	*Main defects*	*Resource consumption level*
Feedback information based secure routing protocols	False routing information, Sinkhole attack, Wormhole attack, Replay attack	It's not easy to ensure the authenticity of the feedback information.	Low
Geographical position based secure routing protocols	False routing information, Sinkhole attack, Wormhole attack	The attacker can steal topology information of the network through the geographical position information.	Low
Cipher algorithm based secure routing protocols	False routing information, Sybil attack, Sinkhole attack, Wormhole attack, Replay attack	High-strength encryption algorithm means high resource consumption.	High
Multi path transmission based secure routing protocols	Selective forwarding, False routing information, Sinkhole attack, Wormhole attack, Replay attack	Nodes failure in multi paths will increase network delay.	Low
Hierarchical structure based secure routing protocols	False routing information, Sybil attack, Sinkhole attack, Wormhole attack, HELLO flood, Acknowledgement spoofing	The cluster head nodes become the focus of attack, cluster head nodes reselecting consumes energy and time.	Low
Secure routing protocols response to specific attacks	One protocol can resist one or a few specific types of attacks	The same protocol can just prevent a few specific attacks and it is difficult to transplant and extend the protocol.	General

4. Research Prospects on Secure Routing Protocols in WSN

Domestic and foreign researchers have done a lot of work on secure routing protocols in WSN and achieved abundant research results. Many effective security routing mechanisms have been proposed. But there are still some problems that need further research:

1) In the present, we usually assess the security, computation cost and communication cost of secure routing protocols according to simulative experiment data obtained from specific network settings. There is no effective and unified security analysis and evaluation mechanism for different protocols. Thus we need to establish a unified evaluation model

based on security for the secure routing protocols in WSN and develop the corresponding evaluation mechanism.

2) WSN with immobile nodes has limitations in performance and cost in some realistic applications. Thus emerged the mobile sensor networks in which sensor nodes are carried by moving objects such as people, animal and vehicle. However, the current research is mainly on WSN in which sensor nodes are static; we need pay more attention on the routing security of mobile sensor networks.

3) In the present, we usually assume that sensor nodes in WSN are isomorphic. But in many applications, we have to use heterogeneous WSN which is composed of different types of sensor nodes. There is still a lack of profound research on secure routing mechanism of heterogeneous WSN.

4) In WSN where resource is constrained, the conflict between the security of routing mechanism and the resource consumption has always existed. What we need to do is find the best balance point between them.

5. Conclusion

Security problem is one of the key problems we have to solve before the large-scale promotion and application of WSN [13]. And secure routing is the most important content in the research of WSN security. This paper classified the existing secure routing protocols according to the core secure schemes used by them, and emphatically introduced and analyzed the typical ones among them. Base on that, the paper proposed some research prospects on secure routing protocols in WSN. As WSN continues to enter into practical application, there is an increase focus in security issues. Secure routing will get more attention and the research on it will also continue to develop.

Acknowledgements

The work in this research has been supported by National Natural Science Foundation of China (61272500), Beijing Natural Science Foundation (4142008) and the Pre-launch of Beijing City Government Major Tasks and District Government Emergency Projects (Z131100005613030).

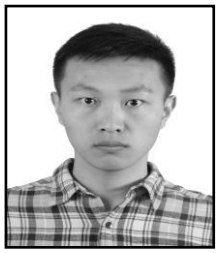
References

[1] L. X. Qing, L. Hui, Y. Kai, *et al.*, "A secure routing protocol of Ad hoc network based on D-S evidence theory", Research and development of computer, vol. 48, no. 8, **(2011),** pp. 1406-1413.
[2] W. Galuba, P. Papadimitratos, M. Poturalski, *et al.*, "Castor: scalable secure routing for Ad hoc networks", Proc of IEEE INFOCOM. Washington DC: IEEE Computer Society, **(2010)**, pp. 1-9.
[3] L. Yun and R. Jian, "Source-location privacy through dynamic routing in wireless sensor networks", Proc of the 29th Conference on Information Communication, Piscataway: IEEE Press, **(2010)**, pp. 1-9.
[4] K. E. Defrawy and G. Tsudik, "Privacy-preserving location-based on-demand routing in MANETs", IEEE Journal on Selected Areas in Communications, vol. 29, no. 10, **(2011),** pp. 1926-1934.
[5] S. Misra, S. Roy, M. D. Obaidat, *et al.*, "A fuzzy logic-based energy efficient packet loss preventive routing proto-col", Pro of the 12th International Symposium on Performance Evaluation of Computer & Telecommunication System. Piscataway: IEEE Press, **(2009)**, pp. 185-192.
[6] Y. Hu, A. Perrig and D. B. Johnson, "Ariadne: a secure on-demand routing protocol for Ad hoc networks", Wireless Networks, vol. 11, no. 12, **(2005),** pp. 21-38.
[7] M. A. Moustafa, M. A. Youssef and M. N. El-Derine, "MSR: a multipath secure reliable routing protocol for WSNs", Proc of the 9th IEEE/ACS International Conference on Computer System and Applications. [S.1.]: IEEE Press, **(2011),** pp. 54-59.
[8] B. Trike, S. Rekhis and N. Boudriga, "A novel secure and multipath routing algorithm in wireless sensor networks", Proc of the International Conference on Data Communication Networking. [S.1.]: IEEE Press, **(2011)**, pp. 1-10.

[9] R. Srinath, A. V. Reddy and D. R. Srinivasan, "AC: cluster based secure routing protocol for WSN", Proc of the 3 rd International Conference on Networking and Services. Washington DC: IEEE Computer Society, **(2007)**, pp. 45.
[10] F. Rong, C. Jian, F. JianQing, *et al.*, "A striner-based secure multicast routing protocol for wireless sensor net-work", Proc of the 2nd IEEE International Conference on Future Networks. Washington DC: IEEE Computer Society, **(2010),** pp. 159-163.
[11] M. Mohi, R. A. Movaghar and P. Zadeh, "A Bayesian game approach for preventing DoS attacks in wireless sensor net-works", Proc of International Conference on Communication and Mobile Computing. [S.1.]: IEEE Press, **(2009),** pp. 507-511.
[12] S. Ning, Q. LiJun and L. XianFang, "Wormhole attacks detection in wireless sensor networks: a statistical analysis approach", Proc of the 19th International IEEE Parallel and Distributed Processing Symposium. Washington DC: IEEE Computer Society, **(2006)**, pp. 26.
[13] W. Yunji, H. Hai-Chao, Y. Y. Jack, L. L. Merry and J. Yufang, "A conceptual cellular interaction model of left ventricular remodeling post-MI: dynamic network with exit-entry competition strategy", BMC Systems Biology, (Suppl 1), vol. 4, **(2010)**.

Authors

Jingsha He, received his B.S. degree from Xi'an Jiaotong University in Xi'an, China and his M.S. and Ph.D. degrees from the University of Maryland at College Park in USA. He is currently a professor in the School of Software Engineering at Beijing University of Technology in Beijing, China and an associate director in the Low Carbon Research Center at Beijing Development Area Co., Ltd. in Beijing, China. Professor He has published over 200 research papers in scholarly journals and international conferences and has received over 40 patents in the United States and in China. His main research interests include information security, network measurement, and wireless ad hoc, mesh and sensor network security.



Bo Zhou, is currently pursuing his ME in software engineering at the College of Software, in Beijing University Of Technology, China. His research interests include information security and network security.