International Journal of Complex Systems – Computing, Sensing and Control
Vol. 2, No. 1-2, pp. 27-34, 2014

EVOLUTION OF WIRELESS SENSOR NETWORK SECURITY

YANG XIAOMEI[1], MA KE[2,*]
[1]*College of Computer and Information*
Three Gorges University
Yichang, Hubei, China

[2]*College of Materials and Chemical Engineering*
Three Gorges University
Yichang, Hubei, China

ABSTRACT—The wireless sensor network’s nodes are mostly distributed in the wild, and frequently in a state of unattended, therefore, the network vulnerable to various security threats. Under the condition of serious limitations in resources, the traditional network security system which needs to spend a lot of resources is no longer applicable. So, how to ensure the security of wireless sensor network under limited resources has become a key problem. This paper starts from the security features and targets of wireless sensor network, Summarizes the various threats for the wireless sensor network, and the main key management and security routing technologies, then make outlook for the future development.

Key words: wireless sensor network security, attack, key management, secure routing protocol

1. FOREWORD

In recent years, the Internet of Things technology has got rapid development, and as a foundation for the Internet of Things technology, the wireless sensor network (WSN) has got a very wide range of applications, because of the powerful, flexible and low cost in data collection and short distance wireless communication. Wireless sensor network (WSN) usually consists of a large number of sensor nodes which were deployed in the target area, according to different types of sensor, the node can collect various data, and transfer data to the base station after a simple processing, thus realize various functions. Sensor nodes are usually small, low cost and energy limited, only has little storage space, simple processing and wireless communication ability .According to the requirements of data acquisition, nodes can be distributed in the wild or very hostile environment, where the human difficult to reach, then self-organize to structure network, and complete the task. This is the cause of the wireless sensor network is widely used, and also the cause of the wireless sensor networks are more likely to be suffered from more kinds of attacks.

[*] Correspondence author :Ma Ke, E-mail: 24863303@qq.com

2. WIRELESS SENSOR NETWORK (WSN) CONSTRAINTS

The organize and operation mode of Wireless sensor network (WSN) are different from traditional wired network, due to the smaller volume and limited energy of the sensor nodes, the processing power and storage capacity and communication bandwidth of wireless sensor network are very limited. Therefore, when discussing suitable security mechanism for wireless sensor network, we must consider all aspects of the restrictions in the first place, so as to find out security mechanism which is suitable for wireless sensor network characteristics. The constraints of wireless sensor network mainly embodied in the following aspects:

2.1 Limited Energy

Limited energy is one of the major characteristics of wireless sensor network (WSN), under the condition of the limited energy, network nodes need to complete data acquisition, data transmission and simple data processing, and other functions, in all operations, and data transmission is the one who cost most energy. In literature [1], the study found that each bit transmitted in WSN consumes about as much power as executing 800 to 1000instructions. So, in order to prolong the life cycle of sensor nodes, must try to reduce unnecessary data transmission, the security mechanism must be designed to find a balance between cost energy and ensure safety. Not for the sake of higher security, irrespective of the excessive consumption of energy, we should to get good security algorithm on the premise of lower energy.

2.2 Limited Capacity

Sensor nodes are small and the storage capacity is limited, after ensuring the basic functions such as collect data and maintain network, the rest of the storage will be very few, usually only a few kilobytes to a few KB, at present all mature security algorithm cannot be stored and run in such a small storage space.

2.3 Unreliable Communication

In wireless sensor networks, data communication adopts connectionless method, which is usually has less redundant data and better real-time performance, but connectionless method will lead to unreliable of data communication. Unreliable wireless communication mode is easy to produce bad or tampered packets. In addition, even if the communication channel is reliable, because of the characteristic of the wireless signal transmission, still prone to conflicts occur or be attacked.

2.4 Higher Communication Latency

Because of the signal transmission distance of wireless sensor nodes is very short, data usually takes multi-hop to reach destination, when data is passing the intermediate node, it also need to finish necessary data fusion and processing, thus lead to the high transmission delay, and higher communication latency make synchronization of data transmission difficultly, this also led to a part of the security mechanism is not easy to implement

2.5 Unattended Node

The nodes of wireless sensor network are usually in wild field where human difficult to reach, so they are often in a state of neglect, this makes physical attack to node is very easily, It is also one aspect which must be considered when designed security mechanism.

3. SECURITY OBJECTIVES OF WIRELESS SENSOR NETWORK

Based on the above characteristics, in the design of wireless sensor network security mechanism, the researcher need to achieve the following main objectives:

Data confidentiality, integrity, availability and instantaneity: These targets are the basic goals of all network security. Wireless sensor network (WSN) is also need to keep the data from eavesdropping, forging, tampering or replay, and can be successfully transmitted from the sender to the receiver.

Self-organization: Nodes usually in a state of unattended, so when the node is destroyed, or network structure has changes, the nodes need to self-organization and self-repair, which requires the dynamic characteristics of security mechanism, especially for dynamic allocation of key and dynamic maintenance of trust relationship.

Time synchronization: Many applications of wireless sensors require time synchronization, and the corresponding security mechanism should also be time synchronization. In the literature [4], the author describes a safe synchronization mechanism.

4. CLASSIFICATION OF WIRELESS SENSOR NETWORK THREAT

The problem of network security mainly because of the attacks, without attack, there would be no security issues. In wireless sensor network (WSN), due to the limitation of environment and resources, the types and quantity of attacks are more than other types of networks.

4.1 Attack Source

The attacks of wireless sensor network can be divided into two sources: external attack and internal attack.

External attacks come from outside of network, can be divided into passive attacks and active attacks. Passive attacks mainly appear as information eavesdropping, in the wireless sensor network (WSN), a large amount of data can be gained through the remote access, so aggressor can complete information monitoring at very low risk. Aggressor can get some sensitive information by collecting some seemingly harmless information to aggregate and analysis the characteristics of the data flow. This is difficult to be detected, but can use data encryption to protect against it. Active attack has more methods. It mainly performance for various forms of denial of service attacks, such as placing interference sources to interfere with the normal communication, Consume a large amount of network resources on purpose which may lead to resource depletion of network resources, etc. Most of the external attack can prevent through certification, in addition to the network interference. For network interference can prevent by spread spectrum and frequency hopping communication.

Internal attacks are mainly due to hijacked node. Hijacking node has some main types of methods:

Aggressor can capture a sensor node directly and reprogrammed for it. Because sensor nodes are usually unattended, so this method is simple and quick. However, this is not easy to capture automatically, usually requires the attacker to reach the target site to complete it manually, but a lot of sensor nodes are usually located in some place where human difficult or not suitable to reach.

Attackers use some nodes which have more computing resources such as laptop computers to attack sensors, destroy its security mechanism, embed malicious code, using this method, the aggressor can hijack sensor nodes without physical contact and change in the location of node, compared with the former method, this method need to spend more time to destroy the security mechanisms.

The attacker replace original sensor by fake nodes. After the attacker has captured sensor node, he can get some important information such as key and node ID, with the help of these information, the attacker can fake a large number of nodes, and scatter them to sabotage the network.

Compared with the external attack, internal attack is more difficult to detect and prevent. After internal node has be hijacked, the attacker may steal confidential information, report some wrong information, destroy the normal routing or collude with other hijacked node to make all kinds of disruptive behavior.

4.2 A Layered Attack and Defence

The architecture of wireless sensor network is shown in the Table 1, the analysis of the hierarchical network structure is helpful to study the network security. Each layer of network will suffer different kind of attack, some attacks involving multiple layers or even use the link between two different levels. Layered attack and defense is shown in the following Table I.

Table I, Attacks on WSNs and Countermeasures

Layer	Attacks	Defence
Physical	Jamming	Spread-spectrum, priority messages, lower duty cycle, region mapping, mode change
Link	Collision	Error-correction code
	Exhaustion	Rate limitation
	Unfairness	Small frames
Network	Spoofed routing information & selective forwarding	Egress filtering, authentication, monitoring
	Sinkhole	Redundancy checking
	Sybil	Authentication, monitoring, redundancy
	Wormhole	Authentication, probing
	Hello Flood	Authentication, packet leashes by using geographic and temporal info
	Ack. flooding	Authentication, bi-directional link authentication verification
Transport	Flooding De-synchronization	Client puzzles Authentication

Source: Y. Wang, G. Attebury, and B. Ramamurthy, IEEE Communications Surveys and Tutorials, Vol. 8, No. 2, pp. 2-23, 2006

5. WIRELESS SENSOR NETWORK SECURITY RESEARCH STATUS

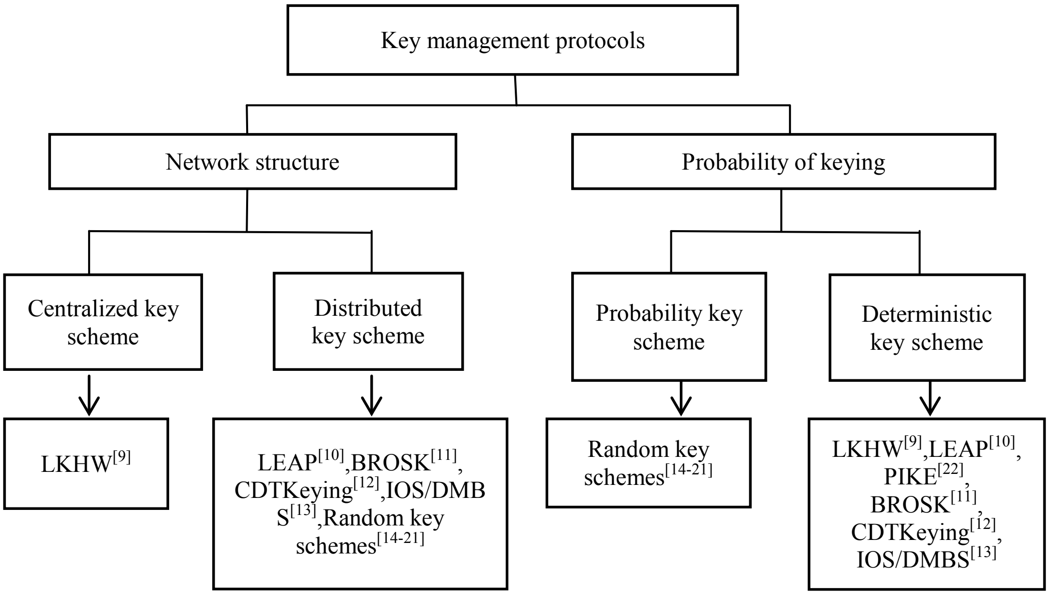
There have been many researchers who were studying the security of wireless sensor network with limited resources under the above background, and have achieved some results.

5.1 Key Management

Key management is the foundation of the realization of wireless sensor network security, also is the kernel mechanisms to ensure security of network services and all kinds of application, WSN resources have serious limitations, public key cryptography algorithm such as RSA is computationally intensive, so it was considered not suitable for wireless sensor network, but in recent years, research has shown that if researcher choose appropriate algorithm and parameters, and optimize and reduce power consumption, public key cryptography algorithms can also be used in wireless sensor networks[6,7,8]. For public key cryptography algorithm in the WSN applications, the literatures at home and abroad mostly focus on the research and improvement of RSA and

ECC algorithm. Relative to the public key cryptography, symmetric cryptography mechanism have obvious advantages in computing speed and energy consumption, so there are many researchers devote themselves to the application of symmetric cryptographic mechanisms in WSN. In symmetrical cryptography mechanism, both communication sides use the same key for encryption and decryption, as a result, the key distribution has always been a challenge in the symmetric encryption. How to design a highly efficient and flexible key distribution scheme is always the key point of research. Each has advantages and disadvantages of two kinds of cryptography, in practical application, choose what kind of cryptographic algorithms depends on the computing and communication ability of sensor nodes, so, in addition to the improvement of cryptographic algorithm, improvement of hardware performance is necessary too. Work along both lines, researcher can better ensure the safety of WSN.

Key management scheme can be divided into randomness and deterministic according to the form of key generation; and it can be divided into centralized and decentralized according to the organization form of network nodes. The classification of key management scheme is shown in figure 1.


Key management protocols
Network structure
Probability of keying
Centralized key scheme
Distributed key scheme
Probability key scheme
Deterministic key scheme
LKHW[9]
LEAP[10],BROSK[11], CDTKeying[12],IOS/DMBS[13],Random key schemes[14-21]
Random key schemes[14-21]
LKHW[9],LEAP[10], PIKE[22], BROSK[11], CDTKeying[12], IOS/DMBS[13]

(Source: Y. Wang, G. Attebury, and B. Ramamurthy, IEEE Communications Surveys and Tutorials, Vol. 8, No. 2, pp. 2-23, 2006)

Figure 1. A taxonomy of key management protocols in WSNs

The LEAP (Localized Encryption and Authentication Protocol) [10] suggested by Zhu is a multi-key management protocol based on the symmetric cryptographic, each node has four keys: one personal key shared with base station, a set of keys shared with all nodes, a pair of keys shared with neighbors, and a cluster key shared with adjacent nodes in the same cluster used to broadcast in cluster. The key management mechanism ensures that a node will not affect the other nodes after being hijacked. In addition to LEAP, researchers also put forward PIKE, BROSK, CDTKeying, E-G key management protocol etc.

5.2 Secure Routing Protocol

Most routing protocols did not consider security problems when design, but there are many attacks on the routing protocol as shown in Table 1, so the security of routing protocol is important to ensure network data transfer smoothly. In the study of security routing protocol, literature [23] put forward the security model of the sensor network routing and security goals for the first time, and it summarized kinds of attacks on routing in wireless sensor network, it also discussed the countermeasures to secure routing and matters need attention during the design, however, this paper haven't suggest any specific security protocols. A.Perriget al proposed a set of security protocol suitable for sensor network: SPINS. SPINS is composed of two parts, the SNEP (Secure Network Encryption Protocol) and μTESLA. SNEP can provide authentication, data confidentiality, integrity and instantaneity. μTESLA can provide verifiable safe broadcasting under the condition of the resource is very limited. We can use the SPINS to build high-level security protocols.

In the literature [24], J. Deng et al proposes a new security routing protocol, namely INSENS (Intrusion tolerant routing in wireless sensor networks), INSENS is a kind of sensor network routing protocol which can tolerate attacks. Literature [25] proposes a security routing protocol suitable for wireless sensor network data aggregation, including authorization mechanism, establishment mechanism of lightweight Shared secret key, safety broadcast mechanism. Some other literatures also have doing research of security aggregation. Such as B.Przydatek put forward a new framework of data fusion security, which is suitable for large sensor network [26]. In addition, there was researcher who puts forward the random routing policy SR (stochastic routing) based on the research of complex system.

6. OUTLOOK

In addition to the above research, there are many studies dedicated to research of safety data fusion technology and localization algorithm, and the research of various kinds of intrusion detection and defense system. Computer network is a typical complex system, and because of highly self-organization and flexibility, the characteristics of the complex system are more obvious in wireless sensor network (WSN). In such a complex system, there are lots of factors which are affecting the safe operation of the network, and they interact with each other, so when researching all kinds of security problems, the researcher can't to do only a single study with a problem divided from the system, they must be studied in its entirety. Now with the rise of the Internet of Things, the application of wireless sensor network is more and more widely, the security problem is getting more and more attention, on the basis of research on individual security, how to building complete security architecture should be working direction for all researchers.

ACKNOWLEDGMENTS

This work was partially supported by National Key laboratory open fund (Grant No. KF2015W001) and Fund of Key Laboratory of Plant Nutrition and Fertilizer, Ministry of Agriculture (Grant No. IARRP-2014-36).

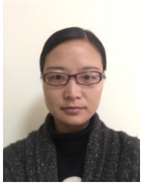
REFERENCES

1. J. Hill, R. Szewczyk, A. Woo, S. Hollar, D.E. Culler, and K. Pister, "System architecture directions for networked sensors", In Proceedings of the 9th International Conference on Architectural Support for Programming Languages and Operating Systems, New York, ACM Press, pp. 93-104, 2000.

2. S. Capkun and J.-P. Hubaux, “Secure positioning in wireless networks”, IEEE Journal on Selected Areas in Communications, Vol. 24, No. 2, pp. 221-232, 2006.
3. L. Lazos and R. Poovendran, “SERLOC: Robust localization for wireless sensor networks”, ACM Transactions on Sensor Networks, Vol. 1, No. 1, pp.73-100, 2005.
4. S. Ganeriwal, S. Capkun, C.-C.Han, and M.B. Srivastava, “Secure time synchronization service for sensor networks”, In Proceedings of the 4th ACM Workshop on Wireless Security, pp. 97-106, New York, NY, USA, ACM Press, 2005.
5. Xiu-li Ren, Wei Yang, Jian-sheng Xue, and Fengjie Yin. Wireless sensor network node copy attack detection based on partitioning method. The electronic journal [J]. (9):2095-2100, 2010.
6. N. Gura, A. Patel, A. Wander, H. Eberle, and S. Shantz, “Comparing elliptic curve cryptography and RSA on 8-bit CPUs”, In Proceedings of Workshop on Cryptographic Hardware and Embedded Systems (CHES ’04), 2004.
7. G. Gaubatz, J.P. Kaps, and B. Sunar, “Public key cryptography in sensor networks-Revisited”, In Proceedings 1st European Workshop on Security in Ad-Hoc and Sensor Networks (ESAS ‘04), 2004.
8. A.S. Wander, N. Gura, H. Eberle, V. Gupta, and S.C. Shantz, “Energy analysis of public-key cryptography for wireless sensor networks”, In Proceedings of the 3rd IEEE International Conference on Pervasive Computing and Communication, 2005.
9. R. Di Pietro, L.V. Mancini, Y.W. Law, S. Etalle, and P. Havinga, “LKHW: A directed diffusion-based secure multi-cast scheme for wireless sensor networks”, In Proceedings of the 32nd International Conference on Parallel Processing Workshops (ICPPW’03), IEEE Computer Society Press, pp. 397- 406, 2003.
10. S. Zhu, S. Setia, and S. Jajodia,“LEAP: Efficient security mechanism for large–scale distributed sensor networks”, In Proceedings of the 10th ACM Conference on Computer and Communications Security, pp. 62-72, New York, NY, USA, ACM Press, 2003.
11. B. Lai, S. Kim, and I. Verbauwhede, “Scalable session key construction protocols for wireless sensor networks”, In IEEE Workshop on Large Scale Real Time and Embedded Systems, 2002.
12. S.A. Cametepe and B. Yener, “Combinatorial design of key distribution mechanisms for wireless sensor networks”, In Proceedings of the 9th European Symposium on Research Computer Security, 2004.
13. J. Lee and D.R. Stinson, “Deterministic key pre-distribution schemes for distributed sensor networks”, In Proceedings of Selected Areas in Cryptography, pp. 294-307, 2004.
14. L. Eschenauer and V.D. Gligor, “A key-management scheme for distributed sensor networks”, In Proceedings of the 9th ACM Conference on Computer and Networking, pp. 41- 47, 2002.
15. W. Du , J. Deng, Y.S. Han, and P.K. Varshney, “A pair-wise key pre-distribution scheme for wireless sensor networks”, In Proceedings of the 10th ACM Conference on Computer and Communications Security, pp. 42-51, New York, NY, USA, ACM Press, 2003.
16. H. Chan, A. Perrig, and D. Song, “Random key pre-distribution schemes for sensor networks”, In Proceedings of the IEEE Symposium on Security and Privacy, pp. 197, IEEE Computer Society, 2003.
17. J. Lee and D.R. Stinson, “A combinatorial approach to key pre-distribution for distributed sensor networks”, In Proceedings of the IEEE Wireless Communications and Networking Conference, 2005.
18. R.D. Pietro, L.V. Mancini, and A. Mei, “Random key-assignment for secure wireless sensor networks”, In Proceedings of the 1st ACM Workshop on Security of Ad hoc and Sensor Networks, New York, ACM Press, pp. 62-71, 2003.

19. W. Du, J. Deng, Y.S. Han, S. Chen, and P.K. Varshney, "A key management scheme for wireless sensor networks using deployment knowledge", In Proceedings of IEEE INFO COM, Hong Kong, pp. 586-597, 2004.
20. D.D. Hwang, B. Lai, and I.Verbauwhede, "Energy-memory security tradeoffs in distributed sensor networks, In Proceedings of the 3rd International Conference on Ad-hoc Networks and Wireless, pp. 70-81, 2004.
21. D. Liu and P. Ning, "Location-based pair-wise key establishments for static sensor networks", In Proceedings of the ACM Workshop on Security in Ad hoc and Sensor Networks, 2003.
22. H. Chan and A. Perrig, "PIKE: Peer intermediaries for key establishment," in Proc. IEEE INFOCOM, 2005.
23. Chris Karlof and David Wagner, Secure routing in wireless sensor networks: attacks and countermeasures. Ad Hoc Networks 1, 293-315, 2003.
24. J. Dang, R. Han, and S. Mishras, Security Support for In-Network Processing in Wireless Sensor Networks http: //www.cs.colorado.edu/~mishras/research/papers/sasn03.pdf, 2003.
25. J. Deng, Richard Han, Shivakant Mishra. INSENS: Intrusion-Tolerant Routing in Wireless Sensor Networks. Technical Report, 2003.
26. B. Przydatek, Song D, and Perrig A., "SIA: Secure Information Aggregation in Sensor Networks", Proc.1st ACM Int. Conf. Embedded Networked Sensor Systems (ACM SenSys 2003), pp. 255-265, 2003.

ABOUT THE AUTHORS



X.M. Yang received the B.Sc. degree in computer science from Central China Normal University, China in 2003; and received master degree in computer application from China Three Gorges University, China in 2011. Yang worked as a teacher in the China Three Gorges University since 2003. Her research interests include computer network, network and information security, wireless sensor network.

Ma Ke received the B.Sc. degree in computer science from South-Central University for Nationalities, China in 2003; and received master degree in electric engineering from China Three Gorges University, China in 2014. Ma has worked in the China Three Gorges University since 2003. His research interests include computer network, complex system and parallel computing.