Security in Next-Generation Wireless Sensor Networks

Li-jie GAO，Zhi-gang CHEN
School of Software, Central South University
Changsha 410075，China
gaolijiewudi@163.com

Abstract: Wireless Sensor Networks(WSNs) have been widely used in various applications. Recent advances in micro-electro-mechanical systems(MEMS) technology have enabled the development of WSN. Hardware constraints and application scenarios lead to safety problems become important problem that restrict the development of the next generation of WSN. Appropriate security guarantee protocols have been proposed to address various security problems. But, if only cumulate security protocols to sensor nodes will make it increasingly difficult to pay costs to establish and maintain WSN. For existing security problems in network layer, we analyze from the following three aspects: i. Application model classification. Security goals and attack overcome are not same magnitude in different models. ii. Several attacks integrated implementation were adopted by Adversary, to obtain valuable informations. iii. We proposed a security dependence principle presence in WSN , which widely used in object-oriented programming. Extract high-level security abstractions which be depended by specific safety problems, i.e. Clone attack, wormhole attack. We describe relationships and structures of security dependence in several common attacks.

Key words: ***Wireless Sensor Networks; security; attack; application; structure;***

I. INTRODUCTION

Micro-Electro-Mechanism System(MEMS), system on a chip (System on Chip, SoC), wireless communications and the rapid development of low-power embedded technology promote the development of wireless sensor networks (Wireless Sensor Networks, WSN) which consist of plenty of low power, low cost, distributed and self-organization sensor nodes. Wireless Sensor Networks(WSNs) have been widely used in military, environmental, and Internet of Things(IOT). The features of next generation WSN as following. More larger: Accessed terminal type and quantity will be more than before, at the same time, network applications will be more extensive; More faster: Ensured high performance communication; More safer: we have the ability of recognition, authentication and access authorization for network object, implying a trusted network by data encryption and integrity; More timely: making service quality control; More manageable: order management, efficient operations, timely maintenance; More effective: forming the profitable mode that create a significant social and economic benefits.

Different applications scenarios[1] of WSN can be divided into two categories as follow: Environmental mild, characterized by unattended easily, for example, ocean and marsh areas; Environmental harsh, characterized by attended easily, for example, family and plant areas;

For different goals, adversary launched various attacks, such as compromise attacks, clone attack, wormhole attacks and so on. Now cunning adversary not only launched an attack, while several different attacks launched together can reduce costs, get more valuable informations and huge income.

In this paper, we first analysis the two scenarios models in WSN. Different models have different security goals, so, the costs and ways to attack are completely different; Then, we discuss the relationships between several attacks. According to analysis comprehensive attacks, prove they are more dangerous than ordinary attacks, at the same time, they are major security problem in next generation WSN. Finally, we apply security dependence inversion principle in object-oriented to various attacks in WSN, propose security dependence principle which explain the network layer security relies on some high level of abstract safety issues that play a drastic role.

The remainder of this article is organized as follows: Next section reviews related work; Section III shows the security design; Section IV presents conclusion.

II. Related work

In this section, firstly, we describe the existing applications of WSN. Then, we introduce several attacks in network layer and corresponding measures.

The applications of wireless sensor network technology have been classified into four main categories: environmental monitoring, health care, security, and additional applications[2]. The difference is that the application environment is friendly or hostile, such as disaster management and environmental management, in which sensor nodes generally distributed in the ocean, marshes, forests, where are difficult for human to arrive; However,the environment apply to factory equipment and smart home is friendly to humans, of course, also be easily achieved for the adversary.

Compromise attacks involved adversary compromising certain nodes and acquiring their keying materials. Then, they will interrupt the network routing and launch sybil attack[3], where a single node presents multiple identities to other nodes, or clone attack, in which clone one compromised node and put into multiple network places[4]. Yanchao Zhang et al[5] proposed a location-based compromise-tolerant security mechanisms for WSN. Parno et al[6] put forward the clone attack problem, then the researchers proposed various nodes cloning attack detection scheme[7-10]. Perrig et al[11] propose a packet leash mechanism for detecting and thus defending against wormhole attacks. Edith C. H. Ngai et al[12]propose a novel light-weighted algorithm for detecting sinkhole attacks and identifying the intruder in an attack

Existing solutions rarely consider the threats constitute of co-existence several attacks to WSN. Undoubtedly, it will increase the cost of building and maintaining WSN if we just accumulate various protocols of attacks solutions to specific application in WSN. Obviously, this approach is unscientific and undesirable. In this paper, we illustrate the intrinsic relationships of security threats in network layer through above several attacks. We present a security dependence principle of attacks, which describe the possibility of comprehensive attacks. In the future, adversary will be more prefer to launch low-cost comprehensive attacks which will obtain more useful and value informations.

III. Security Design

In this section, Firstly, we analysis the characteristics and security goals of different application models. Then, we study possible comprehensive attacks and their hazards. Lastly, we analysis the architecture constituted by exist attacks through security dependence principle.

3.1 Model research

We assume that the application in WSN is composed of a powerful central base station and many low configuration sensor nodes, most nodes are stationary, their tasks are sensing informations, data processing and data transferring. Application scenarios show in [2]. There are two kinds of application models：

Environment harsh: The deployment of sensor nodes by plane spreading. Adversary unclear the specific location and ID information. The value brought by compromised nodes is much less than the cost of compromising the node(its major responsible is accomplishing perception tasks) through GPS or other sensor nodes located technology. The Applications deploy in environment harsh must:

● Resist natural environmental hazards, such as flood, sunshine, wind, pressure and so on.

● Avoid interfering or shielding channels, such as magnetic interference.

Adversary goals as following:

● Obtain the final data while he is not interested in single sensor node.

● Compromise pivotal sensor node or base station.

Environment mild. The location of sensor nodes is easy to reached for adversary. For example, comparing to marsh areas, we can easily deploy sensor nodes in the factory areas , then, adversary prone to compromise sensor nodes and launch a series of attacks. The Applications deploy in environment mild must:

● Avoiding capture or compromise sensor nodes in WSN by adversary, because it is easy for attacker.

● Avoiding attacker sneap into and launch internal attacks.

Adversary goals as following:

● Compromise or destroy sensor nodes.

● Sneap into WSN, and then, obtain and manipulate informations.

3.2 Comprehensive attacks

Security is one of the major aspects of any application in WSN. In this section, we analysis the influence affected by comprehensive attacks which different traditional. We introduce an example of comprehensive attacks.

Before introducing comprehensive attack, we first introduce a nodes replace attack rely on the action of node capture which is one of the most vexing problems in sensor net work security. [13] pointed out the problem of node capture and explained that its solution majority based on the redundancy which are well suited to sensor networks particularly. Nodes replication attack have been know by us, namely clone attack(Clone attack take advantage of captured normal nodes in a network, acquired node ID and corresponding private informations, and use this to copy arbitrary duplicate nodes, then put those malicious nodes which contain legal informations into critical areas.). [7-10] proposed many solutions for clone attack detection, but few existed clone detection protocols can ensure that the probability of successful detected is 100%, which provided the available conditions to the attack of node replace. Adversary run out of energy of compromise sensor nodes after compromised they by cunning way, or destroy it artificial. And then, replacing the original legitimate sensor nodes by building powerful puppet nodes which have legitimate private informations. In order to hided their identities of puppet, they complied with majority network protocols perfectly, furthermore, they would attached extra functionalities builded by adversary. Using this extra functionalities completed desired tasks for adversary.

Adversary launch the comprehensive attacks consist of compromise attacks, clone attacks, nodes replace attacks, wormhole attacks and sinkhole attacks at the same time. It roughly divided into three steps as following:

Step one: Show like Figure1, adversary sneak into the application of WSN, this situation can easily occur in the environment mild areas, capture or compromise some sensor nodes in it, and then obtain confidential informations through special tricks. Above processes provide helps for next attacks.

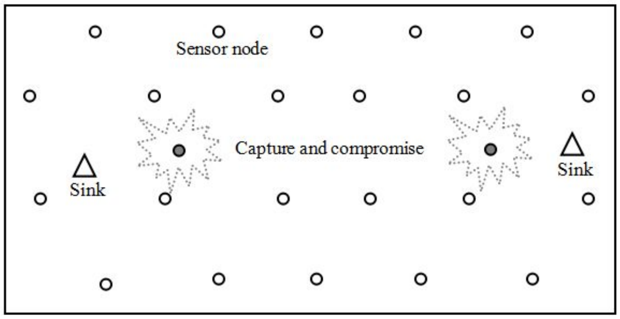

Figure1. Adversary capture and compromise sensor nodes

Step two: Adversary build their own puppet nodes which instead of compromised legal nodes using the confidential informations obtained by the first step. So adversary can evade clone attack detection successfully, because the puppet nodes have legitimate unique ID and replace the original legitimate sensor node(rather than exist with legitimate sensor nodes together in the network), which do not cause the execution of clone attack detection protocols since there does not exist the conflict of different locations but same legal ID. It saves a lot of trouble for adversary. According to above behaviors , adversary has at least two puppet nodes which have plenty of energy, high-profile and high-resistance deployed by adversary. Next, these puppet nodes can jointly launched wormhole attack, and attracted informations traffic between puppet nodes in the network, show in Figure2.

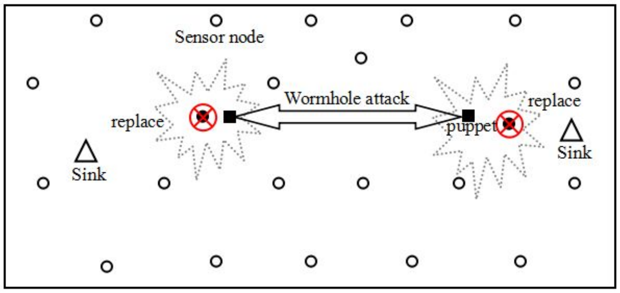

Figure2. Adversary launch wormhole attack

Step three: Since the puppet nodes with powerful function have legitimate identification informations deployed by adversary, it will also have the characteristics of sybil attack. Since puppet nodes have been controlled the flow of information all over the network basically, it can continue to control the flow of informations to sink, then, form sinkhole attack show like Figure3.

The solutions of sensor nodes capture or compromise base on redundancy; Clone attack detection through finding the conflicts of same legitimate ID appear in different locations; There is no related solution to resolve nodes replace attacks; Mostly, wormhole and sinkhole attacks detection use the approach of statistical, they find dramatic changes in the certain statistical patterns and then decide whether there existed corresponding attacks. For each individual attack, people have been proposed multiple routing protocols to solve it. [5] is mainly to solve the capture or compromise attacks, [7-10] can be solved clone attacks, [11] solved the problem of wormhole attack , [12] solve the attack of sinkhole. Recent studies show that more and more scholars began to focus on comprehensive attack , for example, [15] use a secure routing method SEF + LITEWORP detecting false report injections and wormhole attacks in wireless sensor networks. In the future, solving comprehensive attacks with minimum cost will be expected, especially the comprehensive attacks composed by many individual attacks.

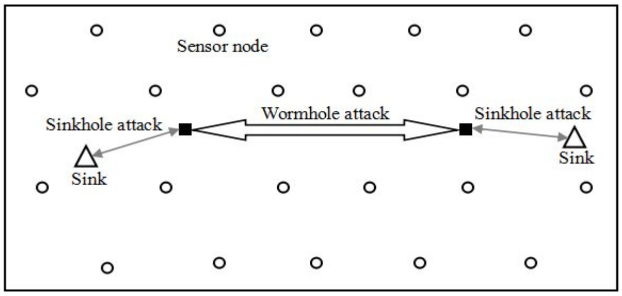

Figure3. Adversary launch sinkhole attack

3.3 Security dependence principle

The so called dependence inversion principle is rely on the abstract, do not depend on the specific in object-oriented programming. Simply, it means that require to program abstractions, not to program instance, thus reducing the coupling degree of models between client and instance. Similarly, for various attacks in WSN, such security dependence principle apply to. A comprehensive attack described in part 3 shows the following dependence relationship:

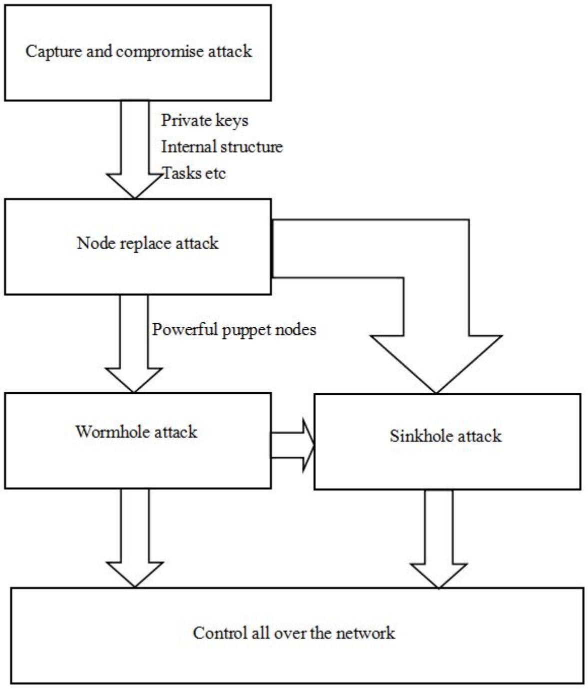

Figure4. Attacks dependence relationship

In the phase of capturing or compromising, adversary prepare for next phase(nodes replace attack) by obtaining legitimate private keys, internal structure and tasks of sensor nodes. Having legal identities, it will construct powerful puppet nodes to replace the legitimate sensor nodes in WSN, forming a sensor nodes replace attack. Further, puppet nodes produced by nodes replace attack do facilitate to wormhole attacks. Puppet nodes(not to be found long time, because of having legitimate identities) with powerful function features attract the majority information flow of the network, then control the flow distribution in the entire WSN. The fact of puppet nodes master basic information all over the network provided by wormhole attacks, adversary can easily launch sinkhole attacks, because the puppet nodes have the characteristics of sybil attack also, so it has a number of legitimate features to communicate with the sink illegal without be discovered. Then, adversary complete control the entire WSN(including ordinary sensor nodes, aggregation nodes and base stations), he can do whatever he wanted.

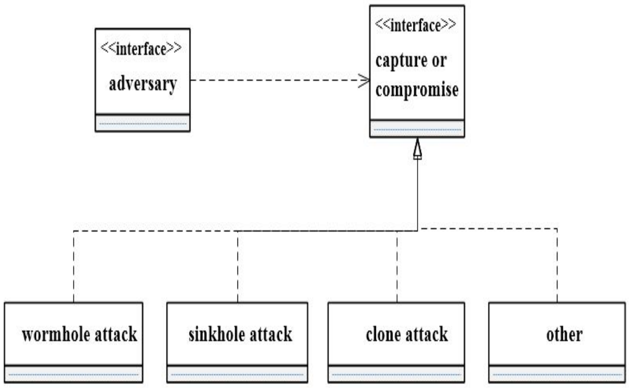

Figure5. Security dependence principle

Figure4 show the dependency relationships between typically attacks in network layer. Capture or compromise attacks are the basis for next series of attacks, nodes replace attack is the key step in the entire complex attacks. Wormhole and sinkhole attacks can be considered as instances of large-scale destruction launched by adversary. Figure5 pointed the security dependence principle apply to comprehensive attacks.

IV. Conclusion

In this paper, firstly, we proposed the application models and the comprehensive attacks based on sensor nodes captured or compromised attacks, clone attacks, nodes replace attacks, wormhole attacks and sinkhole attacks in wireless sensor networks. Furthermore, we analyzed the internal relationships of comprehensive attack, and then pointed out the security dependence principle in this special attack. Lastly, we indicated that comprehensive attack bought huge efficiency and would be the disturbing security problems in WSN.

ACKNOWLEDGEMENTS

This research is supported by:

National Natural Science Foundation of China (No.61379057 and No.61309001),

Projects of International Cooperation and Exchanges NSFC(No.61111140391),

Doctoral Program Foundation of Institutions of Higher Education of China (No. 20120162130008).

REFERENCES

[1] Ana-Belen Garcia-Hernando. WSN application scenarios. Computer communications and networks. 2008: 1-33.

[2] I.F. Akyildiz, W. Su*, Y. Sankarasubramaniam, E. Cayirci. Wireless sensor networks: a survey[J]. Computer Networks, 2002, 38(4): 393-422.

[3] James Newsome, Elaine Shi, Dawn Song, Adrian Perrig. The Sybil Attack in Sensor Networks: Analysis & Defenses. Proceedings of the 3rd international symposium on Information processing in sensor networks. 2004, 259-268.

[4] Z.M. Zheng, A.F. Liu,L.X. Cai. ERCD: An energy-efficient clone detection protocol in WSNs. INFOCOM 2013:2436-24444.

[5] Yanchao Zhang, Wei Liu, Wenjing Lou, Yuauang Fang. Location-based compromise-tolerant security mechanisms for wireless sensor networks[J]. IEEE Journal on Selected Areas in Communications, 2006, 24(2).

[6] B. Parno, A. Perrig, V. Gligor. Distributed Detection of Node Replication Attacks in Sensor Networks. Proc. of 2005 IEEE Symposium on Security and Privacy. 2005:49-63.

[7] M. Conti, R. D. Pietro, L. V. Mancini. Distributed Detection of Clone Attacks in Wireless Sensor Networks. IEEE Transactions on Dependable and Secure Computing. 2011,8(5):685-697.

[8] Y.P. Zeng, J.N. Cao, S.G. Zhang. Random-Walk Based Approach to Detect Clone Attacks in Wireless Sensor Networks. IEEE Journal on Selected Areas in Communications. 2010, 28(5): 677-691.

[9] C. M. Yu, C. S. Lu, S. Y. Kuo. Efficient and Distributed Detection of Node Replication Attacks in Mobile Sensor Networks. Proc. of Vehicular Technology Conference Fall, 2009 IEEE 70th, 2009: 1-5.

[10] K. Xing, F. Liu, X. Z. Cheng. Real-time Detection of Clone Attacks in Wireless Sensor Networks. Proc. of The 28th International Conference on Distributed Computing Systems, 2008:3-10.

[11] Y.-C. Hu, A. Perrig, and D. B. Johnson. Packet Leashes: A Defense against Wormhole Attacks in Wireless Ad Hoc Networks. IEEEINFOCOM 2003, April 2003: 1976-1986.

[12] Edith C.H. Ngai, Jiangchuan Liu, Michael R. Lyu. An efficient intruder detection algorithm against sinkhole attacks in wireless sensor networks[J]. Computer Communications, 2007, 30(11-12): 2353-2364.

[13] Adrian Perrig, John Stankovic, David Wagner. Security In Wireless Sensor Networks. Communications of the ACM - Wireless sensor networks, 2004, 47(6):53-57.

[14] Manpreet Singh,Usvir Kaur. Various Techniques for Wormhole Attack Prevention in Wireless Sensor. International Journal of Agriculture Innovations and Research, 2013, 2(8):2278-7844.

[15] Hyeon Myeong Choi, Su Man Nam, Tae Ho Cho. A Secure Routing Method for Detecting False Reports and Wormhole Attacks in Wireless Sensor Networks. Wireless sensor network, 2013, 5(3):33-40.