A Rule-based Attacks Detection Method for Wireless Sensor Networks

http://dx.doi.org/10.3991/ijoe.v10i1.3212

Shen Zihao[1, 2], Liu Shufen[1]
[1] Jilin University, ChangChun, China
[2] Henan Polytechnic University, Jiaozuo, China

***Abstract*—Wireless sensor networks have become an increasingly important area for research and application. Compared to traditional networks, its security faces many unfavorable factors such as severe resource constraints, inability to secure the wireless medium, potentially harsh sensing environment, etc. Attacks detection is an important issue to a wireless sensor network security. In this paper, sensors were classified and different kinds of malicious attacks in a wireless sensor network were analyzed, based on which a rule-based attacks detection method was proposed. The detection rules were given to detect most kinds of malicious attacks.**

***Index Terms*—Malicious attacks, Wireless Sensor Networks (WSNs) , Rule-based Detection.**

I. INTRODUCTION

A wireless sensor network (WSN) is a wireless network with sensing, processing, and communication capabilities. The rapid technology development in MEMS technology and networking has made wireless sensor networks readily available. Today, wireless sensor networks are becoming a feasible solution to various data sensing applications such as automatic monitoring[1, 2], object tracking[3, 4], military applications[5], environmental monitoring[6-10], health monitoring[11-13], home applications[14] etc. In many applications, security of wireless senor networks security is a very critical and challenging issue.

Compared to traditional networks, wireless sensor networks have many unfavorable factors such as severe resource constraints, inability to secure the wireless medium, uncontrollable and potentially harsh sensing environment, and unattended operations to meet desired goals for security and reliability of wireless. It is nearly impossible to implement traditional computer security techniques in wireless sensor networks. Therefore, new security methods including attacks detection should be come up with to specifically cater to the requirements of wireless sensor networks.

In this paper, we analyze the most typical attacks and threats to wireless sensor networks, and focus our work on detecting certain of attacks with a rule-based detection method in wireless sensor networks.

II. SENSORS CLASSIFICATION IN WIRELESS SENSOR NETWORKS

Wireless sensor networks consist of low-cost, low-power sensors with sensing, processing, and communication capabilities. Several hundreds or even thousands of sensors are densely deployed to cooperatively detect and transmit back environmental and physical conditions. During this course, a wireless sensor network may encounter many attacks and some adversary can successfully join the network. In our research, a classification is given to all the sensors in wireless senor networks. Figure 1 shows the sensors classification.

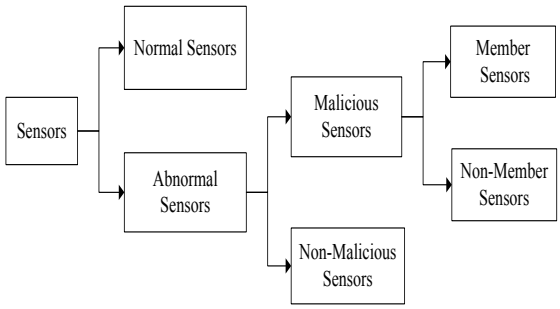

Figure 1. Sensors Classification in Wireless Sensor Networks

Depending on whether the sensors can accomplish their specific task meeting with the advance deployed requirements, all sensors can be divided into two types: normal sensors and abnormal sensors. Normal sensors can accomplish the specific task meeting with the advance deployed requirements, while abnormal sensors cannot accomplish their specific task meeting with the advance deployed requirements or even disrupt other sensors task completion. According to whether the sensors do damage to wireless sensor networks, there are two kinds of abnormal sensors: malicious sensors and non-malicious sensors. Non-malicious sensors are abnormal sensors which die earlier leading to unsuccessful accomplish their specific task, they don't disturb the other sensors. Malicious sensors may interfere with wireless signal, eavesdrop on message, tamer with data, and disrupt route, they will do damage to wireless sensor networks. According to whether the malicious sensor becomes a member of the network during the attack or not, malicious sensors include two kinds: member sensors and non-member sensors. Non-member sensors are not legitimate part of the network and they often filch information from wireless sensor networks through eavesdropping message without disturbing the network norm operation. Member sensors are captured by an adversary. These sensors consume resources and disrupt the normal data-transmission, which bring serious damage to wireless sensor networks.

To solve the security issue in wireless sensor networks, we have to survey how to detect the malicious sensors.

III. MALICIOUS ATTACKS IN WIRELESS SENSOR NETWORKS

In a wireless sensor network, sensors communicate with each other through wireless signal. A wireless sensor network protocol stack consists of five layers: physical layer, data link layer, network layer, transport layer, and application layer. As sensors can be deployed in a variety of environments, wireless sensor networks may encounter many types of attacks. Malicious attacks may occur at any layer in the protocol stack. According to operation mode, the attacks can be passive attacks or active attacks. In a passive attack such as eavesdropping, the attackers usually monitor transmitted data packet without breaking the norm running of network. Messages and conversations are intercepted and read by unintended receivers. Eavesdropping is easier in wireless communications than wired line network. The adversaries through eavesdropping may obtain critical or sensitive information. Moreover, this kind of attack is impossible to detect because passive monitoring will not cause any disruption to the network. Authenticity is critical to defend this attack. On the other hand, active attacks are actively involved in network communications and do serious damage to wireless sensor network These attacks include node replication attacks[15, 16],DoS(Denial of Service) attacks, wormhole attacks[17], black hole attacks[18],selective forwarding attacks, Sybil attacks[19, 20], etc.

A. Node replication attacks

In a node replication attack, an adversary tries to impersonate its identity of other legal node. The attacker then gets the privilege to consume resources of the network or disturb norm network operation or propagate false alarms. To achieve impersonation, the attacker can change its MAC address to one of some other normal nodes.

B. DoS attacks

In a host attack, the adversaries can diminish or nullify a network's capacity to perform its expected functions. DoS attack is a major security problem in security monitoring applications, which deprive sensors of the normally expected services of resources to cause the lacking in sensor communication. Therefore an intruder can prevent the legitimate reports from being passed down to the base station.

C. Wormhole attacks

In a wormhole attack, an adversary that is far away from the base station often convince other sensor nodes that it has the shorter and faster route to the base station, so it is choose as the next hop. It relays packets on an out-of-bound channel and is available only to itself to form a wormhole. Wormhole attacks pose serious threat to WSN since the attacker needn't compromise any sensor nodes and interfere with any message content. This kind attack brings convenience for other type attacks such as sinkhole attacks and selective forwarding attacks.

D. Black hole attacks

When sensor nodes forward data packets to the base station, a routing mechanism based on routing vector selects transmitted path depending on path length. In a black hole attack, an adversary can take advantage of this tactics to cheat other sensor nodes. The attacker makes a zero distance announcement to other nodes to make them believe that it is the best next hop. As a result, all the data packets from the attacker's neighbor nodes are forwarded to the attacker and cannot be transmitted to the proper destination nodes. Therefore a routing black hole is formed. Black hole attacks bring great nodes energy wasted and cause the base station to lose a lot of useful data packets.

E. Selective forwarding attacks

A wireless sensor network adopts different multi-hop routing protocols to forward data packets from the nodes sensing the information to the base station. It is generally assumed that nodes will well cooperate in the forwarding of the received data packets. In a selective forwarding attack, a malicious node on the path towards the base station may determine whether they forward the packets properly to other nodes. Rather than dropping all the received packets, a malicious node can refuse to forward some of the packets that it should forward. Selective forwarding attacks will bring serious damage, but it is hard to detect because the number of data packets being dropped is chosen to reduce the risk of detection to a great extent.

F. Sybil attacks

In a Sybil attack, an adversary uses multiple node identities in its interaction with other sensors. It seems that the sensor is simultaneously located at more than one place. It creates more opportunities to influence the routing mechanism to the attacker's advantage. The result is an adversary can be in different locations at the same time by announcing different locations. Sybil attacks are serious security threats to geography-based routing protocols, fault-tolerant schemes, multi-path routing, and topology maintenance.

IV. A RULE-BASED ATTACKS DETECTION METHOD FOR WIRELESS SENSOR NETWORKS

It is an important issue to determine whether a malicious activity exists in the wireless sensor network. Different attacks bring different consequence to a wireless sensor network. Certain attack such as selective forwarding attack, Sybil attack will cause the data packets loss in a wireless sensor network. Certain attack such as jamming attack, DoS (Denial of Service) attack, wormhole attacks, disguising attack will consumes energy and resource in a wireless sensor network. Certain attack such as wormhole attack will tamper with data in a wireless sensor network. It should take measures against various attacks and identify malicious behavior. In our research, we focus our work on rules-based detection mechanism for wireless sensor network.

We consider a data packet transmission as the following: source node A transmits data packets to destination node D; node A and node B is in the path; node M is the monitoring node within the communication areas of node A and node B. The detection rules can be listed from different types of attacks.

A. Selective forwarding attack detection rule

Rule 1 is for selective forwarding attack detection. It can detect most of this kind of attacks.

Rule 1: when node A transmits data packets to node B, node M gets the each data packet and detects whether its next hop is node B and decides itself next behavior. If yes,

it drops the data packet, if no, it caches the data packet. After a time T, it makes a statistic for the packet loss rate of node B during the time T. Let l express the packet loss rate, L express the threshold of the packet loss. If l>L, a selective forwarding attack is identified.

The normal running packet loss rate as an initialization value assign to L. More over, L can be adjusted with the running of wireless sensor network. Of course, the rule cannot identify the attacker when r is very small, even r is smaller than R.

B. Sybil attack detection rule

Rule2 is for Sybil attack detection. It can detect most of this kind of attacks.

Rule 2: node M monitors node B. After a time T, it receives each data packet and then checks whether the sender's identity is changed. If yes, a Sybil attack is identified.

C. DoS attack detection rule

Rule 3 is for DoS attack detection. It can detect most of this kind of attacks.

Rule 3: when node A transmits data packets to node B, node M gets the each data packet and changes its sending data packets number w with w+1. After a time T, it makes a statistic for the packet sending number of node B during the time T. Let W express the threshold of the sending packet number. If w>W, a DoS attack is identified.

The normal running sending packet number as an initialization value assign to W. More over, W can be adjusted with the running of wireless sensor network.

D. Wormhole attack detection rule

Rule 4 is for wormhole attack detection. It can detect most of this kind of attacks.

Rule 4: node M adopts a chain L to store the destination node of node A. When node A transmits each data packet to its destination node, it adds the destination node Id to L and replaces the associated with counter C with C+1. After a time T, it makes a statistic for the C during the time T. If a certain node B associated with counter C is much larger than others nodes associated with counter and node B is not a sink, a wormhole attack is identified.

Each counter C is assigned an initialization value zero.

E. Node replication attack detection rule

Rule 5 is for node replication attack detection. It can detect most of this kind of attacks.

Rule 5: Before node A transmits data packets to node B, node A makes a shared key negotiation with node B. Node M gets the each data packet and decides whether the negotiation is successful. If yes, node M updates the negotiation number counter n with n+1. Let N express the threshold of the negotiation number. After a time T, node M makes a statistic for the negotiation number during the time T. If n>N, a node replication attack can be identified.

Each counter n is assigned an initialization value zero.

F. Black hole attack detection rule

Rule 6 is for black hole attack detection. It can detect most of this kind of attacks.

Rule 6: when node A transmits any data packet d to node B, node M gets the each data packet and detects whether its next hop is node B. If yes, node M stores the data packets and monitors the retransmitted data packets d' from node B. Node M compares d with d', if they are same in content, node M deletes the data packet p, or else it updates the error number C. After a time T, it makes a statistic for the packet error rate of node B during the time T. Let e express the packet error rate, E express the threshold of the packet loss. If e>E, a worm hole attack is identified.

The normal running packet error rate as an initialization value assign to E. E can also be adjusted with the running of wireless sensor network. With rule 1 similar, the rule cannot identify the attacker when e is very small, even e is smaller than E.

V. CONCLUSION

Unlike traditional networks, a wireless network is designed for specific applications. Because of limited resources and potentially harsh sensing environment, security is an especially important issue for wireless sensor networks. In this paper, the sensors types in wireless sensor networks were discussed. Most kinds of malicious attacks to wireless sensor network were analyzed too. To detect the attacks, a rule-based detection method was proposed. Four detection rules were depicted. The future work might as well focus on designing new rule for other types of attacks.

REFERENCES

[1] Lara Gonzalez-Villanueva, Stefano CagnoniLuca Ascari, "Design of a wearable sensing system for human motion monitoring in physical rehabilitation", Sensors (Switzerland), MDPI AG, vol. 13, no. 6, pp. 7735-7755, 2013-01-01 2013.

[2] Abel C. Lima-Filho, Ruan D. Gomes, Marceu O. Adissi, Tssio Alessandro Borges Da Silva, Francisco A. Belo, Marco A. Spohn, "Embedded system integrated into a wireless sensor network for online dynamic torque and efficiency monitoring in induction motors", IEEE/ASME Transactions on Mechatronics, Institute of Electrical and Electronics Engineers Inc., vol. 17, no. 3, pp. 404-414, 2012-01-01 2012.

[3] Benoit Huyghe, Jan DoutreloigneJan Vanfleteren, "A wireless sensor network protocol for an inertial motion tracking system", Wireless Personal Communications, Springer Netherlands, vol. 71, no. 3, pp. 1961-1975, 2013-01-01 2013.

[4] Zhi-Bo Wang, Zi Wang, Hong-Long Chen, Jian-Feng Li, Hong-Bin Li, Jie Shen, "HierTrack: An energy-efficient cluster-based target tracking system forwireless sensor networks", Journal of Zhejiang University: Science C, Zhejiang University Press, vol. 14, no. 6, pp. 395-406, 2013-01-01 2013.

[5] Hai Liu, Xiaowen Chu, Yiu-Wing Leung, Rui Du, "Minimum-cost sensor placement for required lifetime in wireless sensor-target surveillance networks", IEEE Transactions on Parallel and Distributed Systems, IEEE Computer Society, vol. 24, no. 9, pp. 1783-1796, 2013-01-01 2013.

[6] Danying Gu, "Application of a heterogeneous wireless framework for radiation monitoring in nuclear power plant", Sensors and Transducers, International Frequency Sensor Association, vol. 152, no. 5, pp. 98-104, 2013-01-01 2013.

[7] Othman Sidek, S. A. Quadri, Shahid Kabir, Muhammad Hassan Bin Afzal, "Application of carbon nanotube in wireless sensor network to monitor carbon dioxide", Journal of Experimental Nanoscience, Taylor and Francis Inc., vol. 8, no. 2, pp. 154-161, 2013-01-01 2013.

[8] Xu Xi, Xiaoyao XieZhang Hai, "Application of Theory and Technology of Wireless Sensor Network System for Soil Environmental Monitoring", Sensors and Transducers, International Frequency Sensor Association, vol. 21, no. SPEC.ISS.5, pp. 78-84, 2013-01-01 2013.

[9] Vana Jelicic, Michele Magno, Davide Brunelli, Giacomo Paci, Luca Benini, "Context-adaptive multimodal wireless sensor net-

work for energy-efficient gas monitoring", IEEE Sensors Journal, Institute of Electrical and Electronics Engineers Inc., vol. 13, no. 1, pp. 328-338, 2013-01-01 2013.

[10] Gurkan Tuna, Orhan ArkocKayhan Gulez, "Continuous monitoring of water quality using portable and low-cost approaches", International Journal of Distributed Sensor Networks, Hindawi Publishing Corporation, vol. 2013, 2013-01-01 2013.

[11] Christian Durager, Andreas HeinzelmannDaniela Riederer, "A wireless sensor system for structural health monitoring with guided ultrasonic waves and piezoelectric transducers", Structure and Infrastructure Engineering, Taylor and Francis Ltd., vol. 9, no. 11, pp. 1177-1186, 2013-01-01 2013.

[12] Chang-Kuo Yeh, Hung-Ming ChenJung-Wen Lo, "An authentication protocol for ubiquitous health monitoring systems", Journal of Medical and Biological Engineering, Biomedical Engineering Society, vol. 33, no. 4, pp. 415-419, 2013-01-01 2013.

[13] M. J. Chae, H. S. Yoo, J. Y. Kim, M. Y. Cho, "Development of a wireless sensor network system for suspension bridge health monitoring", Automation in Construction, Elsevier, vol. 21, no. 1, pp. 237-252, 2012-01-01 2012.

[14] Md. Motaharul Islam, Jun Hyuk LeeEui-Nam Huh, "An efficient model for smart home by the virtualization of wireless sensor network", International Journal of Distributed Sensor Networks, Hindawi Publishing Corporation, vol. 2013, 2013-01-01 2013.

[15] Zihao Shen,Shufen Liu, "A routing attack detection method for cluster wireless sensor networks", Journal of Theoretical and Applied Information Technology, Little Lion Scientific, vol. 42, no. 2, pp. 166-170, 2012-01-01 2012.

[16] Shen Zihao,Liu Shufen, "Security threats and security policy in wireless sensor networks", Advances in Information Sciences and Service Sciences, Advanced Institute of Convergence Information Technology, vol. 4, no. 10, pp. 166-173, 2012-01-01 2012.

[17] Nabil Ali Alrajeh, Shafiullah Khan, Jaime Lloret, Jonathan Loo, "Secure routing protocol using cross-layer design and energy harvesting in wireless sensor networks", International Journal of Distributed Sensor Networks, Hindawi Publishing Corporation, vol. 2013, 2013-01-01 2013.

[18] P. S. Ramesh, F. Emily Manoz PriyaB. Santhi, "Review on security protocols in Wireless Sensor Networks", Journal of Theoretical and Applied Information Technology, Little Lion Scientific, vol. 38, no. 1, pp. 79-82, 2012.

[19] Soumyashree Sahoo, Pradipta Kumar MishraRabi Narayan Satpathy, "Secure Routing in Wireless Sensor Networks", International Journal of Computer Science Issues, International Journal of Computer Science Issues (IJCSI), vol. 9, no. 1 1-2, pp. 187-191, 2012-01-01 2012.

[20] Mohammad Sadeghi, Farshad Khosravi, Kayvan Atefi, Mehdi Barati, "Security analysis of routing protocols in wireless sensor networks", International Journal of Computer Science Issues, International Journal of Computer Science Issues (IJCSI), vol. 9, no. 1 1-3, pp. 465-472, 2012-01-01 2012.

AUTHORS

Shen Zihao received his Ph.D. degree in Computer Science and Technology from the Jilin University, China, in 2008. He is currently an associate professor in Henan Polytechnic University, College of Computer Science and Technology, Jiaozuo 454003, China. His research interests include wireless sensor networks and network security. (e-mail: szh@hpu.edu.cn)

Liu Shufen is a professor with the College of Computer Science and Technology, Jilin University, Changchun 130012, China. Her research interests include computer network security and soft architecture.

This research has been supported by the supported by a grant from the Ph.D. Programs Foundation of Ministry of Education of China (No.201241161), Natural Science Foundation of He'nan Educational Committee(No. 13A510325), and by the Doctoral Foundation of Henan Polytechnic University (No.B2010-62). Submitted 28 September 2013. Published as re-submitted by the authors 23 January 2014.