Denial of Service Attacks in Wireless Sensor Networks

Chen Li, Yang Xing

Abstract—Wireless sensor network (WSN) is a collection of various micro sensor nodes, which makes communication between nodes and base stations possible. WSN plays an important role in military, health and Internet of things and other information technology fields. With the continuous expansion of WSN application, we find that WSN has a big disadvantage in its application, that is, due to the limitation of memory, processor and battery sensor nodes, there is no built-in security system in sensor equipment. Therefore, WSN is vulnerable to hacker attacks, and because of the particularity of WSN, it is a challenging task to ensure WSN is protected from these attacks. Because the deployment of these networks in dangerous and unattended environments and resource constraints make design and deployment problems more difficult than traditional infrastructure based networks. At present, one of the main attacks on WSN is denial of service (DOS) attack. The purpose of DoS attack is to prevent users from using legal resources and reduce existing resources. The network gradually becomes slow until it is finally closed down. IDS plays an important role in detecting and defending security attacks, but it is not easy to establish intrusion detection and prevention system in WSN to reduce the impact of denial of service attacks. At present, researchers have proposed two ways to solve this problem: one is detection, the other is defense, and the other is complementary. This paper makes a summary of previous research projects, and then puts forward my own thinking. It is believed that the future research on Intrusion Detection Technology of wireless sensor network can make efforts to realize the comprehensive detection of multiple attacks, reduce the consumption of node resources and improve the accuracy of intrusion detection algorithm.

Index Terms—WSN, DOS attack, Intrusion Detection.

1 Introduction

Wireless sensor network is mainly composed of four parts: management node, base station, sensor node and the link between nodes. These four parts work together to complete the monitoring task. Sensor nodes are usually randomly or determinedly deployed in the target area. These nodes sense the data of the monitored objects around them and communicate with each other within a short communication distance. Finally, the information is collected and sent to the base station[1]. The data finally reaches the management node through the network, and the user obtains the data collected by the sensor node at the management node, So as to realize the monitoring of sensor nodes in the region. Internet of things (lots) is known as the third wave of information industry, and WSN has become the core technology of lots with its powerful information collection, processing and transmission capabilities. At present, WSN has been widely used in military, agricultural production, environmental monitoring and so on. It can be predicted that the wide application of WSN is inevitable in the future.

As a deployment device, WSN has been very popular, but because it uses wireless connection, it is very vulnerable to network attacks, resulting in network unavailability. However, compared with the traditional network security, the security problems of WSN have its unique characteristics, such as communication mode, deployment environment, cost constraints, resource constraints and so on, which bring some difficulties and impacts to the solution of the security problems, and even lead to new security problems. In the actual application scenarios, the security threats faced by WSNs are the huge bottleneck of its development. How to solve the security threats faced by WSNs under the special nature of WSNs is an urgent problem, which is of great significance for the development of WSNs.

DOS attack is one of the most common and harmful attacks in WSNs. DOS attack means that the attacker tries to exhaust the network resources in some way, but does not allow the authorized user to access the network resources. This kind of attack can be realized in various ways, such as hardware failure, software error, resource exhaustion, malicious broadcast of high-energy signals, environmental conditions or any complex scenario between these factors [2]. A common example of DoS attack is to saturate the target machine to the extent that it cannot respond to legitimate traffic through external communication requests. If this attack is successful, the communication system may be completely blocked. Many complex denial of service attacks are designed to violate IEEE802.11 MAC protocol and any other layer of WSN, which lead to the legitimate users who pass the authentication can not enter the network, and may even lead to network crash. At present, there are two kinds of solutions to DOS attack, one is defense mechanism, the other is detection mechanism, which complement each other.

2 Research Status of DoS Attack in WSN

DoS attack can occur in every layer of sensor network protocol stack. In all layers, the physical layer attack is difficult to solve, because the built-in sensor node's radio is not a powerful radio and is vulnerable to signal interference attack [3]. The second is the MAC layer. Due to the openness of the channel, the cooperation between sensor based MAC protocols is maliciously manipulated, and the opponent can easily launch collision attacks [4]. In the network layer, attackers can tamper with the entire routing service, such as modifying

packets, copying packets, resulting in communication failure in the network. Wormhole attack [5], gray overall attack and worm overall attack all belong to network layer attack. One of the transport layer attacks is flooding [6], and the other is desynchronization. The attacker frequently sends service requests and occupies the resources of the service node until the node crashes. The application layer is vulnerable to clock sewing, selective data forwarding[7] and data aggregation distortion.

2.1 Detection Mechanism of DoS Attack in WSN

Intrusion detection is a kind of active defense mechanism, which can identify the intrusion that destroys the confidentiality, integrity and availability of the system by monitoring the data, information or behavior. As the second defense line of network security protection, intrusion detection is an effective supplement to the defense mechanism to further enhance the network security. At present, there are three kinds of intrusion detection algorithms in wireless sensor networks. The first one is based on misuse [8]. This method can detect known attacks well, but can't detect new attacks that are not in the intrusion database. The second is based on exception, which is the most common method to detect intrusion by matching business pattern or resource utilization. The third type is based on specification. All the rules in the scheme need to be completed manually, and the workload is relatively large. This section mainly discusses the second kind of intrusion detection algorithm.

In the process of exploring intrusion detection scheme in WSNs, many excellent researchers have contributed their wisdom and proposed a variety of anomaly based detection algorithms. Li et al. [9] proposed an anomaly detection method based on statistical model. This method mainly uses two characteristics of average received power and packet arrival rate for detection. Each node establishes a simple statistical model for its neighbor node behavior to detect node camouflage or energy consumption attack. The node uses the latest n packets sent by neighbor nodes for statistics, and obtains the characteristics of received power and packet arrival rate. Each subsequent packet will be compared with these two characteristics. If it conforms to the statistical characteristics, it is considered normal, otherwise it is considered abnormal.In the current research, some intrusion detection systems are proposed based on machine learning algorithm. For example, maleh et al. [10] proposed an anomaly detection algorithm based on support vector machine (SVM) algorithm and a set of signature rules intrusion detection algorithm. Wang et al. [11] used artificial neural network in each sensor node to provide self-learning ability for the system. Literatures [12-16] are clustering based intrusion detection algorithms, which usually include training and testing stages. In the training stage, a specific clustering algorithm is used to establish a group of clusters in the feature space, and the clusters below a certain threshold are identified as anomalies; In the test phase, each traffic sample will be compared with the clustering set to determine whether it is abnormal or not. This kind of method will consume too much computing resources. In addition to the traditional anomaly detection algorithms mentioned above, some scholars have proposed to apply biological immune algorithm to detect abnormal behaviors in wireless sensor networks, such as DCA algorithm proposed by Kim et al. [17].

2.2 Defense Mechanism of DoS Attack in WSN

When we detect DoS attack in the system, if we take effective mitigation measures immediately, the attack can be stopped, otherwise the system will crash soon. Mokdad and Ben Othman [18] proposed a security policy routing scheme, which takes advantage of the characteristics of multiple paths in sensor networks, divides the initial message into fragments, and the destination node combines the fragments to reconstruct the initial message, so as to disperse the data flow and resist DoS attacks. Similarly, maheswari et al. [19] also proposed a new secure routing scheme, called robust. In this scheme, an improved bidirectional verification scheme is used to correct the Hello flood attack in WSN. Rolla and Kaur [20] propose a request forwarding window technology based on time allocation to detect and prevent DoS attacks. Attackers are detected in the routing request stage and blocked in the routing response stage. If any node drowns the routing request message for more than dynamic time, it will be detected as an attacker, and the detected node will inform others about the ID of the node, and the target node will not choose the path containing the detected node.Gope et al. [21] proposed a method to deal with DoS attack in WSN anonymous authentication protocol. Lyu et al. [22] proposed a geographic opportunistic routing (selgor) based on selective authentication to protect DoS attacks. Selgor can ensure the integrity of data by developing entropy based selective authentication algorithm, and can isolate DOS attackers and reduce the cost of calculation.

3 Thoughts and Suggestions

Although there are intrusion detection and defense algorithms to solve DoS attacks in wireless sensor networks, there are still some problems that need to be solved:

(1) Intrusion detection technology is to analyze the system behavior and log, and then judge the status of the node, that is to say, it occurs after the attack, and the node shows abnormal, IDS can detect it. But the fact is that the attacker will do a series of preparatory work before launching the attack, so how to detect the attacker's intrusion behavior as soon as possible, realize the early detection of the attack, and reduce the damage of the attack to the system, is a problem worthy of our consideration.

(2) Generally, sensor nodes are small and low-cost, so their hardware resources and infrastructure are very limited. The resource consumption of nodes has always been a huge challenge to solve the security problem of WSNs. In the existing intrusion detection algorithms, none of them can achieve high accuracy, and the node overhead (energy, storage) is also considerable, There must be a compromise between accuracy and cost. Therefore, we can consider whether the intrusion detection algorithm can be combined with the routing protocol in WSN and other necessary network functions to achieve the purpose of reducing resource consumption.

(3) At present, most of the intrusion detection methods are aimed at a specific attack, such as DoS attack, rarely considering the situation that multiple attacks occur at the same time. In the real attack, many attackers will use multiple

attack means at the same time, Therefore, how to design an adaptive algorithm that can detect multiple attacks at the same time is also a problem to be considered.

In view of the above three problems, I think that the future research of intrusion detection technology in wireless sensor networks can make efforts to realize the comprehensive detection of multiple attacks, reduce the consumption of node resources and improve the accuracy of intrusion detection algorithm.

4 Conclusion

It can be seen that the wide application of wireless sensor network is an inevitable trend, but the security threat it faces is an unavoidable stumbling block in its development process, especially in the field of high security requirements, such as military. Compared with the traditional wired network, WSN brings great challenges to solve the network security problems with its unique properties, such as power limitation, limited computing power, open environment and radio connection, and even these problems will lead to new security problems. Therefore, how to effectively solve the information security problems under the special working mode and running environment of WSN is a major research hotspot, and it is also the only way for the wide application of WSN, which is of great significance.

Acknowledgments

The authors want to thank all the people who helped with this article and the reviewers.

References

[1] M. A. Alsheikh, S. Lin, D. Niyato and H. Tan, "Machine Learning in Wireless Sensor Networks: Algorithms, Strategies, and Applications," in IEEE Communications Surveys & Tutorials, vol. 16, no. 4, pp. 1996-2018, Fourth quarter 2014.

[2] D. R. Raymond and S. F. Midkiff, "Denial-of-service in wireless sensor networks: Attacks and defenses," IEEE Pervasive Computing, vol. 7, no. 1, 2008.

[3] Cakiroglu M Ozcerit A T. Design and evaluation of a query-based jamming detection algorithm for wireless sensor networks [J].Turkish Journal of Electrical Engineering &Computer Sciences, 2011,19(1): 1-19.

[4] Raymond, David R, Midkiff, et al. Denial-of-service in wireless sensor networks: attacks anddefenses [J].IEEE Pervasive Computing, 2008,7(1): 74-81.

[5] Hu Y C, Perrig A, Johnson D B. Packet leashes: A defense against wormhole attacks in wireless ad hoc networks [A]. // Proc of the Twenty-Second Annual Joint Conference of the IEEE Computer and Communications [C],CA, USA: IEEE Press,2001: 1976-1986.

[6] Bhatnagar R, Shankar U. The proposal of hybrid intrusion detection for defence of sync flood attack in wireless sensor network [J]. International Journal of Computer Science &Engineering Survey, 2012,3(2): 31-38.

[7] Bysani L K, Turuk A K. A survey on selective forwarding attack in wireless sensor networks[A]. //Proc of International Conference on Devices and Communications[C], Mesra, India:IEEE Press, 2011:1-5.

[8] Moon, Soo Young, Ji Won Kim, and Tae Ho Cho. An energy efficient routing method with intrusion detection and prevention for wireless sensor networks. Advanced Communication Technology (ICACT), 16th International Conference on. IEEE, (2014).

[9] Guorui Li, Jingsha He, and Yingfang Fu. Group-based intrusion detection system in wireless sensor networks. Computer Communications 31.1, pp. 4324-4332, (2008).

[10] Maleh, Yassine, et al. A Global Hybrid Intrusion Detection System for Wireless Sensor Networks. Procedia Computer Science 52, pp. 1047- 1052, (2015).

[11] Wang, Shun-Sheng, et al. An integrated intrusion detection system for cluster-based wireless sensor networks. Expert Systems with Applications 38.12, pp. 15234-15243, (2011).

[12] Song J H, Ma C X.Anomaly detection based on data-mining for routing attacks in wireless sensor networks [A].l/ Proc of the second International Conference on Communications and Networking [C], Shanghai, China: IEEE Press,2008: 296-300.

[13] El Mourabit, Yousef, et al. Intrusion detection system in Wireless Sensor Network based on mobile agent. Complex Systems (WCCS), 2014 Second World Conference on. IEEE, (2014).

[14] Shamshirband, Shahaboddin, et al. Co-FAIS: cooperative fuzzy artificial immune system for detecting intrusion in wireless sensor networks. Journal of Network and Computer Applications 42, pp.102-117, (2014).

[15] T. Le, T. Park, D. Cho and H. Kim, "An Effective Classification for DoS Attacks in Wireless Sensor Networks," 2018 Tenth International Conference on Ubiquitous and Future Networks (ICUFN), Prague, 2018, pp. 689-692, doi: 10.1109/ICUFN.2018.8436999.

[16] M. Al-Akhras, A. I. Al-Issa, M. S. Alsahli and M. Alawairdhi, "POSTER: Feature Selection to Optimize DoS Detection in Wireless Sensor Networks," 2020 First International Conference of Smart Systems and Emerging Technologies (SMARTTECH), Riyadh, 2020, pp. 263-265, doi: 10.1109/SMARTTECH49988.2020.00070.

[17] Kim J, Bentley P, Wallenta C, et al. Danger ls Ubiquitous: Detecting Malicious Activities in Sensor Networks Using the Dendritic Cell Algorithm [M]. Springer Berlin Heidelberg,2006.

[18] L. Mokdad and J. Ben-Othman, "Performance evaluation of security routing strategies to avoid DoS attacks in WSN," 2012 IEEE Global Communications Conference (GLOBECOM), Anaheim, CA, 2012, pp. 2859-2863, doi: 10.1109/GLOCOM.2012.6503550.

[19] S. U. Maheswari, N. S. Usha, E. A. M. Anita and K. R. Devi, "A novel robust routing protocol RAEED to avoid DoS attacks in WSN," 2016 International Conference on Information Communication and Embedded Systems (ICICES), Chennai, 2016, pp. 1-5, doi: 10.1109/ICICES.2016.7518942.

[20] P. Rolla and M. Kaur, "Dynamic Forwarding Window Technique against DoS Attack in WSN," 2016 International Conference on Micro-Electronics and Telecommunication Engineering (ICMETE), Ghaziabad, 2016, pp. 212-216, doi: 10.1109/ICMETE.2016.93.

[21] P. Gope, J. Lee and T. Q. S. Quek, "Resilience of DoS Attacks in Designing Anonymous User Authentication Protocol for Wireless Sensor Networks," in IEEE Sensors Journal, vol. 17, no. 2, pp. 498-503, 15 Jan.15, 2017, doi: 10.1109/JSEN.2016.2628413.

[22] C. Lyu, X. Zhang, Z. Liu and C. Chi, "Selective Authentication Based Geographic Opportunistic Routing in Wireless Sensor Networks for Internet of Things Against DoS Attacks," in IEEE Access, vol. 7, pp. 31068-31082, 2019, doi: 10.1109/ACCESS.2019.2902843.

Chen Li received the bachelor's degree majoring information security from the Chongqing University of Posts and Telecommunications. She is studying for a master's degree in Cyberspace Security College of Sichuan University.

Yang Xing received the bachelor's degree majoring information security from the University of Guizhou. She is studying for a master's degree in Cyberspace Security College of Sichuan University.