MATEC Web of Conferences **44**, 01053 (2016)
DOI: 10.1051/matecconf/20164401053

Research on Wireless Sensor Network Intrusion Detection Technology

Qing Gang Fan[1,a], Li Wang[2] , Yun Jie Zhu[1], Yan Ning Cai[1] and Yong Qiang Li[1]

[1] *Computer Staff Room, Xi'an Research Institute of High Technology, 710025 Xi'an, China*
[2] *Library, Xi'an Research Institute of High Technology, 710025 Xi'an, China*

Abstract. With the development of science and technology, wireless sensor network (WSN) has been widely used in all walks of life. The security problem of WSN has become a research hotspot. Intrusion detection technology has an important position in the network security. In this Paper, firstly, the intrusion and intrusion detection are introduced, secondly, the WSN intrusion detection system and its classification are analyzed. The main study is to analyze the current WSN intrusion detection technology and their respective advantages and disadvantages. The development direction of WSN intrusion detection technology is put forward finally.

The related research on Wireless sensor network (WSN) has become research hotspot at home and abroad at present stage [1-4]. Compared with the common wireless network, WSN has the following characteristics: the self-organizing network, the dynamic change of network topology, the distributed control, multiple wireless network, the node functional limitations, the limitations of wireless network, poor safety, quantity, size, data redundancy and the convergence and so on.

Studies and history suggests that no matter how advanced security measures in the network, the attacker always could find weaknesses in the network system, to carry out attacks. Used alone prevention technology (such as encryption, authentication, etc.) is difficult to achieve the desired security objectives, these technologies can reduce the possibility of network attack, but can't completely put an end to attacks. therefore, the security defensive measures is also indispensable, intrusion Detection System (IDS) is a new network security technology in recent years, it made up for the inadequacy of the preventive measures, can provide real-time intrusion Detection for network security and take appropriate protection.

In this paper, the intrusion detection systems and intrusion detection technology are introduced and analyzed at present stage mainly, then compared their respective advantages and disadvantages, finally put forward his prospect to the development of wireless sensor network intrusion detection technology.

1 Intrusion and intrusion detection

Intrusion detection system in WSN, through collecting and analyzing information of sensor nodes, check the illegal behavior of security policy and the signs of being attacked, and timely report to system administrator. In order to achieve this goal, the WSN intrusion detection system model should be build, the model should include the following three necessary function modules: information collection module, detection engine module, response module, as shown in Figure 1.

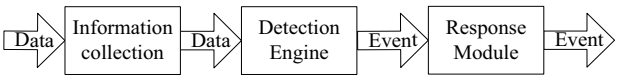

Figure 1. WSN intrusion detection system structure

2 The classification of the intrusion detection system

2.1 According to the distribution system running way

Centralized intrusion detection: the model has a center computer, which is in charge of monitoring, detection and response. It is suitable for the relatively simple network.

Distributed intrusion detection: the model monitor and test the network with a mobile agent, each node has the response analysis ability.

2.2 According to the response way

Active response IDS: if detected after the invasion, to take the initiative to reconfigure the firewall, close the appropriate service or against invaders, then known as the active response.

Passive response IDS: if given only after detected intrusion alarm or log, is a passive response.

[a] Qinggang Fan: fangang3232@126.com

Article available at http://www.matec-conferences.org or http://dx.doi.org/10.1051/matecconf/20164401053

2.3 According to the data sources

Host-based IDS: to test the attack in operating systems, applications, or kernel level. System to get the data on the basis of the system is running to the host, the protection of the target host lies the system running, through monitoring and analysis of host audit records and log files to intrusion detection.

Network-based IDS: the system data source is the original packet of network transmission, NIDS placed in key areas of the network infrastructure, usually using a network adapter running in random mode to real-time monitor and analyze all communication through the network business, in order to protect the network operation.

Hybrid IDS: it is combination system based on the host and the intrusion detection based on network, in the network NIDS is established to detect the network security situation, at the same time HIDS is established on those key host. Better secure protection can be provided than using a single intrusion detection scheme.

2.4 According to analysis method

Anomaly intrusion detection: the method sums up the characteristics of normal operation firstly, then to monitor the subsequent operations. If the normal operating modes of deviation statistical significance are found, the model report to the police immediately.

Misuse intrusion detection: the method collect abnormal operation behavior characteristics firstly, to establish related the feature library, in the subsequent detection process, the collected data and features will be compared to the library code, then come to the conclusion that whether the invasion.

Hybrid intrusion detection: the combination with anomaly detection and misuse detection, intrusion detection based on anomaly can find some unknown attacks, the dependence of specific system is relatively lower, but rate of false positives is high, configuration and implementation is relatively difficult. Intrusion detection based on misuse can detect more accurately identified intrusion behavior, but the dependence of specific system is relatively higher, portability is poor, and can't detect new attack types. Therefore, only combine the two sides, to achieve the best performance of the system.

3 INTRUSION DETECTION TECHNOLOG -Y

The resource limitations and applications correlation characteristics of sensor networks indicate, the study of intrusion detection is a challenging task. An effective sensor network intrusion detection system must have three features, simplicity, accuracy and real-time. Next the wireless sensor network intrusion detection methods and their respective advantages and disadvantages are mainly introduced:

3.1 Intrusion detection based on multi-agent.

Wang Pei in the literature [5] proposed intrusion detection method based on multi-agent for clustering type wireless sensor network, and its system structure is shown in Figure 2.

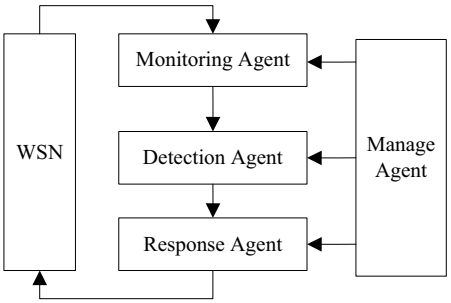

Figure 2. Intrusion detection system based on multi-agent

By having the nodes and the cluster head respectively carry out different detection tasks, combine with the local inspection and joint inspection, use the multiple agent module respectively to realize data collection, analysis, detection and intrusion response and agents management tasks, in order to make the system has simple operation, easy to expand, reduce energy consumption, to enhance the security features. But each node in the scenario, which needs to be equipped with monitoring Agent, inspection Agent, Agent and management Agent, will take up a large amount of storage space of the node, also increase the energy consumption of nodes.

This method can reduce the network load and overcome network latency and good scalability, high security, but each node has more than one proxy function, large energy consumption, in the process of testing activities overlap, the accuracy will be much lower.

3.2 Intrusion detection based on SVM.

In literature [6], anomaly detection based on immune genetic algorithm is put forward, eavesdropping on beacon node from its neighbor node package and extract known as antigens, the key parameters of the number of antigen in if the match is in the life of a probe predefined threshold value is high, the probe will fail and generate a new detector. On the other hand, if the amount of antigen matching threshold, than the life of the detector probe will trigger the intrusion alarm, update mechanism for the detector, make suggestion of IDS more robust. In literature [7], anomaly detection based on support vector machine (SVM) was proposed for selective forwarding attack, using the SVM for intrusion data of robust classification method.

SVM overcome the defects of large sample traditional machine learning methods, based on limited sample

information, in the complexity and the ability to learn of the model, find the best compromise, can obtain the best Fan Hua ability.

Intrusion detection system based on SVM as shown in Figure 3.

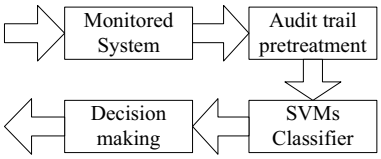

Figure 3. Intrusion detection system based on SVM

This approach to anomaly detection for classification or clustering problems, using machine learning effective learning ability, establish anomaly detection model having certain accuracy. The model has high accuracy, but the disadvantage is too large sample size and too long training time.

3.3 Intrusion detection based on network traffic analysis

The basic structure of intrusion detection model based on flow analysis as shown in Figure 4.

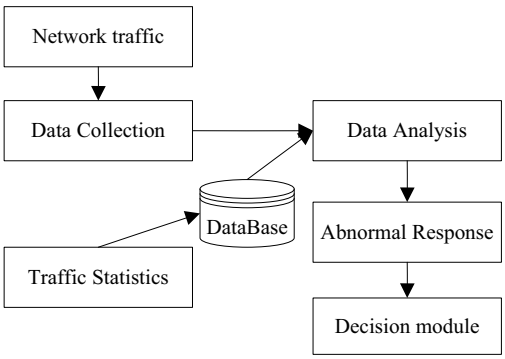

Figure 4. Intrusion detection model structure based on flow analysis

In literature [8], a denial service attack detection scheme based on traffic prediction – MPDD, is designed using Markov linear prediction model for wireless sensor network. In the scenario, each node judgment and detect abnormal network flow based on traffic, without special hardware support and cooperation between nodes. A warning assessment mechanism is put forward, effectively improve the detection accuracy of solutions. Reduce the prediction error or channel error caused by the false positives.

Literature [9], such as intrusion detection scheme based on flow analysis was proposed, based on the statistical analysis of the behavior of the neighbor node threshold technical analysis, and then applied to the selected parameters, namely, under a certain length of time window of the number of packets received and the time interval between packets, it does not require any additional hardware installation and additional communication cost, its computational cost is low.

This method is relatively simple, intuitive, high real-time performance, but requires traffic input to have certain statistical properties, therefore does not have versatility, high rate of false positives.

3.4 Intrusion detection based on the game theory model.

The basic model of intrusion detection system based on game theory is shown in figure 6. Intrusion detector distributed in the network audit network data in some detection methods, detecting intrusion, and submit the test results. Then the game model to simulate the attack and defense both sides of the interactive behavior, and weigh from intrusion detector test results and the test efficiency, reach Nash equilibrium to the secondary IDS make response strategies.

Mohsen Estiri and others in the literature [10] puts forward the theory of repeated game model for intrusion detection for wireless sensor network packet loss against intrusion detection scheme. In this model, the attacker in wireless sensor networks and intrusion detection system as a collaboration, not zero-sum game of both sides, and the average discount factor income is used to display the node at the current stage of game, more valuable than the next phase of. And eventually the system will reach the Nash equilibrium, the formation of wireless sensor network defense strategy.

This method can help managers to weigh the detection efficiency and network resources, but the detection of human intervention is necessary, and has a poor system adaptability.

3.5 Intrusion detection based on the trust mechanism.

Min Lin [11] and put forward the dynamic intrusion detection scheme based on trust model, using the node with higher credibility to alternately testing within the cluster nodes, non-parametric CUSUM detection algorithm was proposed, alarm response also differentiate with the aid of the trust level of trust model, effectively reduce the node energy consumption, reduce the computational overhead of node. Long Ju [12], such as intrusion detection method was proposed based on weighted trust mechanism, at the beginning of the system is assigned to each sensor node weights, each cycle when the node to send with other different report is updated, so that when the node weight below a certain threshold is detected is malicious act.

The advantages of this method has low power consumption, high safety, but when the cluster head nodes invasion, or meet with Sybil attack detection accuracy is reduced, and the threshold setting will affect the precision of the algorithm, and how to find a suitable threshold is a thorny problem.

4 CONCLUSION

From what has been discussed above，the accuracy and real-time performance of intrusion detection technology is not enough to detect all kinds of intrusion behavior.The main challenge of wireless sensor network (WSN) in intrusion detection has the following several aspects. (1) The new type of attack emerge in endlessly. How to improve the ability of intrusion detection system to detect the unknown attack is the need to solve the problem. (2) The resources, which include storage, computing power, energy and bandwidth, are poor. The intrusion detection system based on knowledge learning is not only required to store large amounts of intrusion pattern characteristics, but also with the increase of intrusion type, of the storage space. Limited computing power and energy means that nodes can't run complex intrusion detection algorithm. The algorithm of lightweight should be studied in terms of WSN intrusion detection, in order to adapt to the characteristics of the wireless sensor network (WSN), prolong the life cycle of the network.

References

1. F. Ian, Akyildiz, S. Weilian, S. Yogesh, Computer Net-works, **38**:393-442, 2002.
2. C.C. Mai, Computer knowledge and Technology, 11:29-33, 2015
3. L.X. Chen, Wireless sensor network technology and application, 12-13,2009.
4. I. Onat, A. Miri, Proceedings of the IEEE Internatio-nal Conference on Wireless and Mobile Computing, Networking and Communications253-259, 2005.
5. P. Wang, X.W. Zhou, CHINESE JOURNAL OF SENSORS AND ACTUATORS, **20**, 677-681, 2007.
6. Y. Liu, F.Q. Yu, Proc Int Jt Conf Neural Networks, 439-444, 2008.
7. J.W. Tian, M.J. Gao,S.R. Zhou, Proceedings of the 2009 IEEE International Conference on Information and Automation, 1217-1221,2009.
8. Z.J. Han,W.W. Zhang, Z.G. Chen, Engineering and computer science, **32**,27-29,2010.
9. Y. Ponomarchuk, D.W. Seo, 19th nnual Wireless and Optical Communications Conference, 2010.
10. M. Estiri, A. Khademzadeh, A, Electrical and Computer Engineering (CCECE), 2010 23rd Canadian Conference on, 1-5, 2010.
11. L. Min, N. Shi, Internet Technology and Applications, 2010 International Conference on, 1-4, 2010.
12. L. Ju, H.J. Li, Ubiquitous Information Technologies and Applications (CUTE), 2010 Proceedings of the 5th International Conference on, 1-6, 2010.