Intrusion Detection Technology of Layered Wireless Sensor Network based on Agent

Genjian Yu*[1,3], Kunpeng Weng[2]
[1]Department of Computer Science, Minjiang University, Fuzhou, 350108, China,
Ph./Fax: +86-15880008991/83760607
[2]Institute of Communications Technology, Fuchun Comminucations, Co., Ltd, Fuzhou, 350108, China,
Ph./Fax: +86-13706968020/83992011
[3]Key Lab of Broadband Wireless Communication and Sensor Network Technology (Nanjing University of Posts and Telecommunications), Ministry of Education, 210003, China, Ph./Fax: 086-15880008991
Corresponding author, e-mail: genjianyu@126.com[1], 282799432@qq.com[2]

Abstract

The intrusion detection system and technology of classified layered-wireless sensor network was able to meet the high safety requirements of wireless sensor network, it is urgent for us to improve the identification and generalization of detection system about characters of intrusion. In this paper, we design an intelligent intrusion detection system which realizes intelligence, the effective and direct way was to add the methods, and it was used for identification and generalization of intrusion characters to the Agent function of intrusion detection. It could obtain credible judgment by updating and examining the database for the actions which the general misuse detection or anomaly detection was not sure if the intrusion was formed.

Keywords: *intrusion detection, agent, wireless sensor network*

1. Introduction

The wireless sensor network was dynamic topology networks. Owning to achieve the rapid and effective communication by nothing basic infrastructure, the wireless sensor network was paid abroad attention in recent years. However, the wireless sensor network was easy to be attacked because of its opening and mobility [1], and the traditional intrusion prevention skill had been unable to effectively deal with the attack, in order to greatly reduce the loss, enough evidence should be collect in the early stages of attack for taking the corresponding defenses, therefore, it is necessary to introduce the intrusion detection technology (IDS). But the application of IDS made for wired structure in the wireless sensor network was not accomplished in on stage, it was affected by many factors [2]. In this paper, we discuss the application of Agent and the intrusion detection system and technology in wireless sensor network, and introduce an intrusion detection system and technology of layered-wireless sensor network based on Agent, and its structure, working principle and performance were deeply analyzed and discussed.

IDS were a network security tools, which dynamically monitored the events in some network environment and decided these events, were represented an attack or normal work. There are many different kinds of IDS [3]. According to the different detection methods of attack, IDS could be divided into IDS based on model and IDS based on exception; According to the different data type of tracking, IDS could be divided into IDS based on host and IDS based on network; According to the different package number of data analysis and the different location, IDS could be divided into centralized IDS and distributed IDS; According to the different response mode of invading, IDS could be divided into active IDS and passive IDS. In which, the distributed active IDS based on network was the trend of Intrusion detection system. As new initiative securities protect technology, Intrusion detection technology provided real time protection against inner or outer attacks and mis-operations, and the ability to detect and respond just before the subject network was damaged. From the angle of network security of 3D depth and multi-level defense, peoples were paying more and more attention to the intrusion detection technology, we could see from the booming product market of the intrusion detection

Received March 14, 2013; Revised May 9, 2013; Accepted May 17, 2013

technology. With the increase of key department and the key business in domestic, what we need badly was the product of intrusion detection technology that had own copyright for wireless environment. But now, the intrusion detection technology was most limited to wire network and remained at the research and sample level, or integrated into the primary module of intrusion detection technology in firewall [4]. Thus, the product of intrusion detection technology had greater room for development under the wireless environment.

Nowadays, the modern Agent was a research field of vitality and influence. Agent might be regarded as an entity existed in some environment, which could sense the environment and receive the information of the environment, then reacted to the information, so reaction in the environment, Agent could be software or hardware controlled by software [5]. Multi-Agent System was related to coordinate the intelligent behavior of a set of autonomous or semiautonomous Agent, the research focused on these Agent how to coordinate each knowledge, objective and strategic planning for taking joint action or solving their own problems. But mobile Agent, in short, the Agent had mobility, it moved between each node of network, had the freedom to choose the operating room and time for representing other entities, according to the specific situation, interrupted the current own execution, moved to another device and resumed operation, then returned to the relational results timely. The purpose of moving was to make the execution of program as close as possible to the data source, reduce the spending of network communication, save bandwidth, balance load, and speed up the execution of task, thus, the processing efficiency of the distributed system was be improved [6].

Because of the virtues of, such as autonomy, initiative, reactivity, mobility, sociality and intellectuality and so on, mobile Agent could be successfully applied in the fields of mobile business processing, intrusion detection, information retrieval, network management and distance learning, then some unresolved key problems of these fields could be solved. According to the development of Agent technology and the propulsion of standardization, many excellent mobile Agent system, tool or platform were sprung up in recent years, such as Aglet [7], Grasshopper [8], and Voyager [9], etc. But the mobile Agent system, tool or platform above were not suit to support the current wireless sensor network because of the high requirement of running resource. Boulis at the University of California, Los Angeles solved the facing question of wireless sensor network by using the framework similar to mobile Agent, the framework defined and supported that the calculation, communication and sensor source in network node could be used by LMCS in the way of particular application. The dynamic deployment of distributed algorithm in network was realized by copying and moving of LMCS, the multi-user supports were gave to wireless sensor network, so, it was good to deploy and update the algorithm and realize the dynamic programming model. But in practice, LMCS was lack of flexibility and durative in coordination and control of whole wireless sensor network, compared with Agent, LMCS was lack of autonomy and responsibility. Agilla was a middleware of mobile Agent for wireless sensor network, which was used to rapidly deploy the application of auto-adapted wireless sensor network. Agilla allowed the user to embed mobile Agent in network node, these Agent coordinated work through tuplespace, and transfered intellectually to accomplish a certain task in network. Wireless sensor network would be a shared and universal computing platform because of the mobility of the code and situation, which could run the autonomous application routine each time, as a result, the proficiency of wireless sensor network was full displayed. The feasibility and advantage of Agent, which was applied to wireless sensor network, was proved by Agilla [10], but the application of Agent in the field of data security of wireless sensor network was still lack of the exactly understanding [11, 12].

This paper presents a intrusion detection system and technology of classified layered-wireless sensor network which can meet the high safety requirements of wireless sensor network. The paper was organized as follows. In section 2, a new intrusion detection technology of layered wireless sensor network is given. In section 3, the structure of intrusion detection system of classified layered-wireless sensor network is presented. Technology application and behavior analysis of this paper are also presented in section 4. Finally, our work of this paper is summarized in the last section.

2. Proposed Intrusion Detection Technology

Because of the inherent characteristic of wireless sensor network, such as the opening of medium, the high dynamic of topology, the use of distributed coordination, the lack of central control mechanism, the lack of definite protective line and the limit of node function, etc, so the network was much more weak than cable network, and it was easy to be suffered all kind of attacks. All along, the sensor network was studied, particularly in routing protocol, but the safety problem of network was rarely considered, thus it was bottle-nock problem to restrict the further development of the network. According to deal with all kind of attacks in wireless sensor network, many related security scheme was conducted and passes the simulation. Because the traditional intrusion prevention technology such as encryption and authentication only reduced the possibility of intrusion in some way, but not answered effectively to the intrusion behavior that had been formed. IDS were adopted by most existing security scheme for the precondition of natural effective work.

Notably, there was a big difference between wireless sensor network and wired network, so IDS designed in view of wired network could hardly be applied to wireless sensor network. Firstly, traditional network was largely dependent on the monitor and analysis of real-time traffic of whole networks, but the data, which provided for the intrusion detection by the environment of wireless sensor network, were limited to the local data information associated with direct communication within the field of wireless communication, IDS had to use these incomplete information to complete the intrusion detection. Secondly, the wireless sensor network was strict in communication because of the characteristic such as low speed of link, the limited bandwidth and the power supply of node depended on battery, so the communication protocol which was defined for wired IDS, was not adopted by wireless sensor network. Thirdly, according to the touting topology of dynamic change at a high speed, there were no clear boundaries between normal operation and anomalous process in wireless sensor network. The node, which sent out the wrong message, was the captive node, or the node that get out of step temporarily because of moving faster now. It was difficult to identify the real intrusion and the temporary fault of system for IDS.

Based on the analysis above, an Intrusion detection system and technology of classified layered-wireless sensor network based on agent was given.

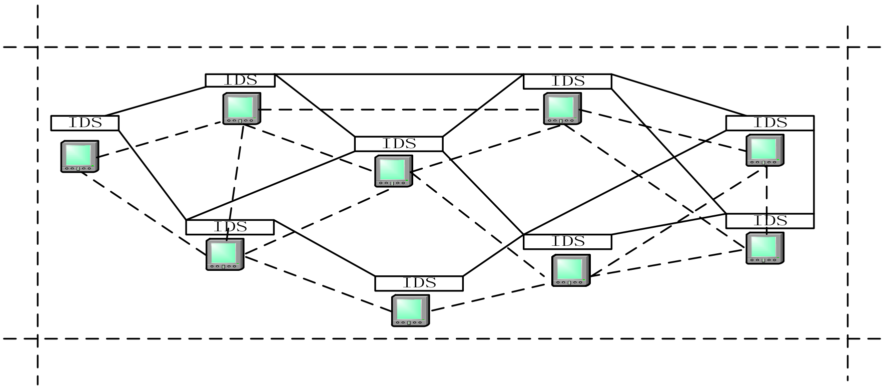

Figure 1. The Structure of Intrusion Detection System

3. Proposed System Structure

Figure 1 shown the structure of intrusion detection system of classified layered-wireless sensor network, it was two-stage structure in the diagram. The hierarchy structure could enhance the security of system effectively. In which, the sensor node in each compact cell was the lowest past, the node on the different partition bound was higher part, on the basis of the function or the importance of geographical location, some nodes could be divided based on higher past for forming more advanced past. The standard, which was divided into different region, was to consider the trust and location between nodes, and the energy condition of each node.

In case of trust mechanism, the traditional plan, which private-key certificate was combined with public-key information, was adopted, other effective methods for personal identification were also adopted. A cell consisted of the node trust each other and next to each other, but if the energy of some node in the cell was less than certain threshold, then the node would be throws out of the cell until the node regained enough energy. For the energy, we not only ensure the effectively work of each node, but also prevent abuse of security monitoring function by the captive node. Each node in network could be confirmed their own physical location by physical positioning technology (such as GPS), the node gained the information of neighbor node by the discovery mechanisms of neighbor node (such as Hello message mechanisms), thus it was certain where to be a high-level node connected with other cell or a primary node within the same cell. Generally, the robustness of hierarchical structure and the cooperating degree of member in the field were directly influenced by the establishment of effective trusting relationship; it was the key to work effectively for system.

On the whole, the above system could be used to collect the data information of node tracking and the traffic information of network according to integrate the function of intrusion detection based on core and network. The method of intrusion detection which combined IDS based on model and IDS based on exception was adopted in the process of data analysis; In which, IDS based on model had higher alarm detection rate and lower error warning rate, alarm included rich diagnostic information, but the analysis and structure of attack mode were time-consuming, and the attack mode also needed to be constantly refreshed, the new attack type, which was not recorded in pattern base, was not detected, and it had the problem of generality between different system for describing the attack mode; IDS based on exception could detect the new attack, it had good commonality, and it was independent from specific operating system and application, but it had higher error warning rate, it was difficult to deploy and achieve. Then their combination could exchange and learn from each other. In the graded system structure, a high rate of correct detection was realized in the condition of low system overhead by the way which was adopted the multiple mechanism to do the combined detection.

Each mobile terminal (node) all loaded a model of IDS for serving as IDS agent in Figure 1. Each module run independently monitored separately every node where it was. The module could collect the data such as user' behavior, system behavior and communication activity within the range of wireless communication, then detected the intrusion and responded by the results of data processing. At the same time, the intrusion detection and responses were carried out together by these IDS modules according to communicate with each other and automatically adapt to variation of the external environment.

Objectively, the internal structure of a successful Agent for the intrusion detection was very complex. But conceptually, an Agent for the intrusion detection was divided into six modules as shown in the Figure 2. Six modules were adopted in our program, but according to the structural characteristic of rating Systems, there was quite a difference between the exact make-up of module and the working principle with the general mobile agent. Besides the conventional module of data collection, detection engine was divided into local module and general module, in order to analyze and process the primary intrusion and the advanced intrusion, respectively; with the corresponding, the intrusion response module was also divided into local module and general module, in order to launch the local and full Internet defense or counterattack for the confirmed intrusion. The special guarantee module of secure communication was responsible for providing the stable and reliable working environment with the whole detection.

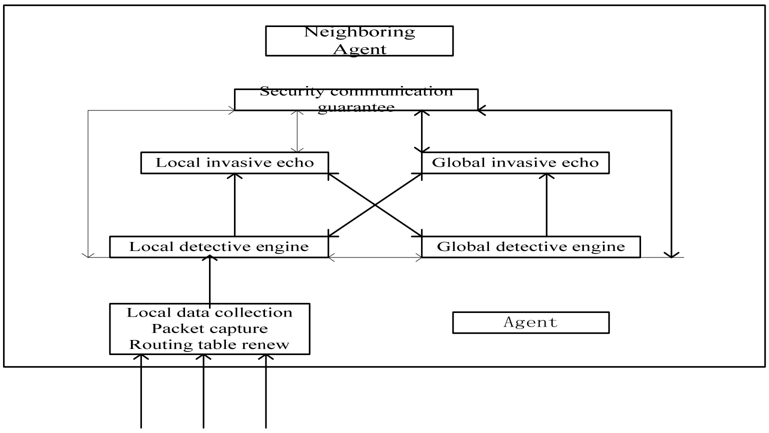

Figure 2. IDS model based Agent

Particularly, the module of data collection was responsible for collecting the local tracking data, log information, packet capture and the routing table updates, and processing them. The local detection engine could detect local exception by using the processing result, the general detection engine could provide the wider range of datasets and the coordination across Agent. In order to maximize the detection error, the detection methods based on model and exception were adopted by two detection engine, and the detection data were deal with the multiple polymerization algorithm. According to the detection result, the different response was launched by the detection response module. In which, the local response module was in charge of triggering the behavior near the node, such as sending out warning messages for the node by agent; the general response module was in charge of coordinating the behavior between the high-level nodes of different cell, such as jointing the cross-regional agent in the network to launch the remedial measure after invading. At last, the secure communication module was in charge of providing a highly reliable channel and environment for the communication of the system between all agents.

4. Technology Application and Behavior Analysis

To sum up, the intrusion detection system of classified layered-wireless sensor network based on agent had unattainable advantages than general IDS in the system structure and the application of agent.

Firstly, the intrusion detection system was based on the distributed structure, it had adapted to the requirements of the modern wireless network, especially wireless sensor network. By “distribution”, there had two implications: The first was the detection method of attack that was aimed at distribution network; the second was to use the distribution method for detecting the distribution attack. The distributed structure was effective to avoid the disadvantage that the work was not perfectly synchronized between the traditional centralized management-IDS with the wireless sensor network. Next, the IDS could be suitable for all kind of structure of goal network because of the strong portability and expansibility. Figure 1 showed a kind of structure with general applicability. In practice, the structure of system could be adjusted according to the specific requirements of goal network. For example, when the goal network belong to the simple planar structure, the region was divided by the physical distribution of node, the planar metric secondary IDS was realized; when the goal network belong to multi-level structure, IDS was graded on the basis of the layer of network, that was, the most junior agent of IDS was equipped on the lowest network., and the level of IDS based on Agent had also increased layer by layer with the increasing of layer. Besides the advantage of System construction, the robustness and practical value of system was greatly improved by the application of mobile agent in IDS. Because the task of intrusion detection system was accomplished in cooperation with Agent, the performance of Agent would be to go directly affects the success of the work of intrusion detection system. In this case, we didn’t have to change the hardware structure of the whole system, just modify the conceptual model of intrusion detection Agent. At the same time, the upgrading and optimization of the whole detection system were realized according to improve the performance of intrusion detection Agent. So not only the high cost associated with traditional system upgrades of IDS and the instability after optimizing the system were effectively decreased.

5. Conclusion

In summary, the intrusion detection system and technology of classified layered-wireless sensor network was able to meet the high safety requirements of wireless sensor network. But It should be noted that, the attacker always repeatedly toke the risk and tried to enter because of high opening of wireless sensor network, even the network was not breached in short time because of the guarantee of security technology, but the attacker could get all kind of information about network itself and the protection system from many attempts, and according to these information, they could disguised itself and carry out reinforcements. If the understanding of detection system about attack was remained in a narrow level, then the network was breached sooner or later. So, it is urgent for us to improve the identification and generalization of detection system about characters of intrusion. It required an intelligent intrusion detection system. According to realize intelligence, the effective and direct way was to add the methods which was used for identification and generalization of intrusion characters (such as neural network, genetic algorithm, fuzzy technology and immune mechanism) to the Agent function of intrusion detection. The expert system was a good model of intelligence application, it could obtain credible judgement by updating and examining the database for the actions which the general misuse detection or anomaly detection was not sure if the intrusion was formed. Therefore, the concept of expert system was put into the high intelligent system of Agent intrusion detection system, so that the system had the function of self-learning and self-adapting.

Acknowledgements

This work is supported by the funds of Key Lab of Broadband Wireless Communication and Sensor Network Technology and the special project funds of college of Fujian Province under Grant No. JK2010045 and the funds of Department of Education of Fujian Province under Grant. No. JA11199 and funds of Fuchun Communications Co., Ltd.

References

[1] Han Yu, Zhiqi Shen, Chunyan Miao. *A Survey of Trust and Reputation Management Systems in Wireless Communications.* Proceedings of the IEEE. 2010; 98(10): 1755-1772.
[2] Shaikh RA, Jameel H, d'Auriol. Group-Based Trust Management Scheme for Clustered Wireless Sensor Networks. *IEEE Transactions on Parallel and Distributed Systems*. 2009; 20(11): 1698-1712.
[3] Pursley M, Taipale D. Error probabilities for spread-spectrum packet radio with convolutional codes and viterbi decoding. *IEEE Transactions on Communications*. 2008; 35(1): 1–12.
[4] Xue Wang, Liang Ding, Sheng Wang. Trust Evaluation Sensing for Wireless Sensor Networks. *IEEE Transactions on Instrumentation and Measurement*. 2011; 60(6): 2088-2095.
[5] Guoxing Zhan, Weisong Shi, Deng J. Design and Implementation of TARF: A Trust-Aware Routing Framework for WSNs. *IEEE Transactions on Dependable and Secure Computing*. 2012; 9(2): 184-197.
[6] Di Martino, Catello, Cinque, Marcello. Automated Generation of Performance and Dependability Models for the Assessment of Wireless Sensor Networks. *IEEE Transactions on Computers*. 2012; 61(6): 870–884.
[7] Kai Lin, Rodrigues JJPC, Hongwei Ge. Energy Efficiency QoS Assurance Routing in Wireless Multimedia Sensor Networks. *IEEE Systems Journal*. 2011; 5(4): 495–505.
[8] Konstantin Knorr. *Dynamic Access Control through Petri Net Work flows.* In Proceedings of the 16th Annual Computer Security Applications Conference, New Orleans, LA: ACM. 2009: 159-167.
[9] Bell D, LaPadula L. The Bell-LaPadula Model. *Journal of Computer Security*. 2009; 4(3): 239–263.
[10] Zhang Yongguang, Lee W. *Intrusion Detection in Wireless Ad-Hoc Networks*. Proceedings of Mobile Computing and Networking technology. MA, USA. 2008; 275-283.
[11] Thuzar Hlaing. Feature Selection and Fuzzy Decision Tree for Network Intrusion Detection. *International Journal of Informatics and Communication Technology*. 2012; 1(2): 109-118.
[12] Kanubhai K Patel, Bharat V Buddhadev. An Architecture of Hybrid Intrusion Detection System. *International Journal of Information and Network Security*. 2013; 2(2): 197-202.