Network Intrusion Detection Based On Cluster Analysis And Multiple Core Set

Gao Ruimei[1,a], Chen Shuyu[2]

[1]Department of Educational Technology Center, Southeast University Cheng Xian College, NanJing City, China

[2]Department of Nanjing Research Institute, Zte Corp, NanJing City, China

[a]gaoruimei1103@163.com

Keywords: adaptive mechanism; artificial immune; Intrusion Detection; Cluster Analysis; Multiple Core Set

Abstract. This thesis takes researches on Network Intrusion Detection Based On Cluster Analysis And Multiple Core Set. The distributed immune intrusion detection system and the packet marking theory are used to find out the network data features of the real-time analyses; and the immune intrusion detection system is used to guide the dynamically processing of path signs technology; what's more, the path signs technology is adopted to dynamically adaptive different methods of characteristics of network data. After that, the attack paths can be quickly identified to provide path information for feature detector on attack path in the immune intrusion detection system. Experiment results show that this scheme can quickly reconstruct the attack path information, and the performance on the aspects of the convergence is with efficiency rate and false positive rate, which is superior to the current probabilistic packet marking algorithm and can provide characteristic path information for immune intrusion detection system.

Introduction

Computer network security technology is a multi-disciplinary, multi-disciplinary comprehensive discipline, including traditional firewall technology, access control technology, encryption technology, intrusion detection technology, IP trace back technology and so on[1]. Network security technology research includes dual nature, that is, offensive and defensive, in which the immune intrusion detection and IP trace back technology represent the technology of both ends of the network security technology. Although it is not ripe yet at this stage, as an important direction of development network security technology, it received sustained attention by experts and scholars.

The thought of immune intrusion detection system derives from the recognition and treatment of the "non-self" material in biological immune system [2-4]; this system does not rely on a large number of signatures to determine whether invaded or not, but the characteristics of normal network flow are modeled; once the current network characteristics are not within the normal range, the system will consider that the potential attacks are discovered. So the immune intrusion detection system has a good dynamically adaptive capacity and high sensitivity for unknown attacks, and it is very suitable for the current changing network environment [5].

System Model and Module Design

Technical models building and core concept of the path sign based on immune intrusion detection system are locating the analysis of the immune intrusion detection system and response module into the transmission network, and after the real-time analysis of network data, the attack source trace back algorithm module are dynamically used according to the data characteristics of decision-making.

By referring to the "Distributed Intrusion Detection System and Distribution open intrusion detection and response framework" IDRA technology and DDoS distributed processing thinking, an open track-type immune response server is located in the critical path in the transmission network

(such as network border routers) shown in Figure1 ; the server does not belong to a separate intrusion detection system, but can provide services for any immune intrusion detection system and work together; the server match the passing packets with the immune detector, which is used to determine whether the packet needs to respond, to treatment or trace back attack path, and then cooperate with the existing various routers to realize route signs; tracing algorithm is converged quickly and promptly traced to the desired position.

Attack source tracing algorithm based on immune Intrusion detection system can be divided into tracking / responding server algorithms, router algorithm and path reconstruction algorithm. The module design is shown in Figure 1:

Tracing algorithm only trace back unusual packet. Though to achieve synergies algorithm needed by routers is seemingly relatively complex, the vast majority of normal packets transmitting in the network will not be processed. Compared to other tracing algorithm it can reduce the load of routers and network, however, immune response server needs to have better performance, and can identify attacks path to provide the path packet information for the immune intrusion detection systems.

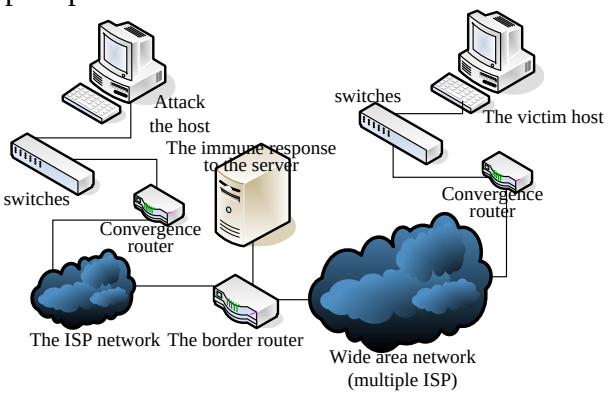

Figure1. Location diagram of the immune response server

Immune Response Algorithm

The algorithm is used in the immune response module of immune response server. Algorithm uses the “memory” immune detector and “characteristic” immune detector in the immune nodes to compare with the passing packets, in where the “memory” immune detector is the further heritable variation of “characteristic” immune detector after its life cycle is over, while the “characteristic” immune detector comes from the training and submitting of the private immune intrusion detection system of attack host. Once the packet is matched with the “characteristic” immune detector, it considers that the packet belongs to attack behavior, which can be deleted; if it matched with the “memory” immune detector, it considers that the current packet is similar with the previous attack behavior, which belongs to the potential attack and can be traced.

Of course, in order to further improve the recognition abilities of the immune response nodes to the potential attack，“memory” detector can accept this immune response server via local data features to establish a long-term normal model, and after that via the “positive selection” algorithm to generate the “non-self’ immune characteristics, which can be processed by the specific situations of the dealing performance of the immune response server and feature modeling. This thesis will not discuss further here.

Immune response algorithm is as follows:

Step1 Processing the next packet and controlling the packet in regional location 1

Step2 Extracting the features in the packet

Step3 Matching the features of the packet and immune features detector submitted in the immune intrusion detection system with the same destination IP, which successfully delete the packet and back to Step 1, otherwise the progress continues

Step4 Matching the characteristics of the packet and the set of the memory detector; if fail, back to Step 5, or to Step 7

Step5 Checking to find out whether exists the path sign F with the same destination IP; if exist, F

will be marked into the path and be forwarded; if not, it will be directly forwarded.

Step6 Back to Step 1

Step7 the packet information is recorded and then submitting it to the tracking module for processing path signs via controlling the tracking algorithm.

Step8. Back to Step 1

Experimental Conclusions

In experiment under the attack of a single path, the convergence time of the tracking algorithm is compared with different situation of the distance between the attack host and the victim host from 1 to 30. If the immune response server is located in the position of the five hops, the improved probabilistic packet out of the control area is adopted for tracking. The results are shown in Figure 2.

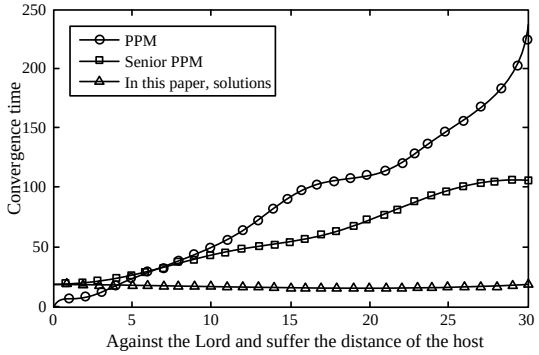

Figure2. Distance and convergence of attack path

From the experimental results it can be seen that the existence of the immune response server can assist the system to mark the attack path; when the proposed marking algorithm of immune path are attacking, the convergence time is reduced to constant level compared to the other two algorithms; as long as the distance between the first immune response server in the attack path and the victim host does not exceeds 32 hops, the attack path can be quickly found. Although the convergence algorithm out of the control area is still using the marking improved program in probabilistic packet, it can be seen from the experimental results that the algorithm can converge quickly because of relatively small number of hops. The two kinds of marking schemes in probabilistic packet are in direct proportion of the number of hops on the convergence time; when the distance of the between the attack host victim and host is increased, the issue of weakest chain will stand out slowly; although the senior probabilistic packet is greatly improved on the convergence time compared to the marking scheme of basic probabilistic packet, it is really hard to apply in practice for it need to know the network topology.

Conclusion

Experimental results show that the proposed scheme is superior to the traditional tracking algorithms on the aspects of convergence efficiency, false positive rate and so on. Although the immune response server is needed to support the processing, the server is not only located for the path marker, but for processing attack packets as an immune node in the switched network.

References

[1]FORREST S, PERELSON A S, ALLEN L. Self-nonself Discrimination in a Computer: In Proceedings of IEEE Society Symposium on Research in Security and Privacy and Privacy, 1994. Massachusetts, USA, 1994: 202-212.

[2]Y. Geng, J. Chen, K. Pahlavan, Motion detection using RF signals for the first responder in emergency operations: A PHASER project, 2013 IEEE 24nd International Symposium on Personal Indoor and Mobile Radio Communications (PIMRC), London,Britain Sep. 2013

[3]GONZALEZ F, DASGUPTA D, Nino L F. A Randomized Real-valued Negative Selection Algorithm: In Proceedings of Second International Conference on Artificial Immune Systems, 2003. Edinburgh, UK, 2003: 261-272.

[4]Twycross J. Stochastic and Deterministic Multiscale Models for Systems Biology: an Auxin-transport Case Study. BMC Systems Biology, 2010, 12(9): 29-41.

[5]Y. Geng, J. He, K. Pahlavan, Modeling the Effect of Human Body on TOA Based Indoor Human Tracking[J], International Journal of Wireless Information Networks 20(4), 306-317