

Detection and Control of Abnormal Behavior in Controlled Network System

Wenxin Qiao^{1,a}, YuLu¹, Liyun Chen¹, Changsheng Wang²

¹Information Engineering Department, Ordnance Engineering College, Shijiazhuang 050003, China;

²Information Management Center, Ordnance Engineering College, Shijiazhuang 050003, China;
^aqiaowenxin1992@foxmail.com

Keywords: controlled network, behavior control, abnormal detection.

Abstract. This paper introduced the concept, the classification and the control principal of network behaviors, discussed the concept, composition and structure, and the behavior control of the controlled network system, then proposed the detection and control model of abnormal behavior in controlled network system. This model of abnormal behavior detection was designed by combining misuse and intrusion detection mechanism, and is the specific application of the research on network behavior and controlled theory, and it controls the network behaviors especially abnormal behaviors. The theory is the basis for establishing the dynamic controllable network security system.

With the development of network and information technologies, it seems that the network size, the diversity of network equipment and the complexity of network topology structure are constantly increasing, which leads to the probability of security problems emerging also increasing. However, the traditional network security measures cannot meet the needs of the actual complex network activities, the existing information network has an urgent need to propose a new theory or new method which can reflect the overall network security and behavior control states. As a kind of efficient, scientific and reasonable network security theory, the controlled network is the integration of existing network security technologies and measures, and the aim of it is to construct a controlled network and solve the network security problems[1].

1 The basic concept

1.1 The concept of network behavior

Behavior is a form or feature of a process which is executed by an entity, and the form or feature is measurable and can be identified, and any entity has the attribute of performing all kinds of behavior. Network behavior is the performance of the abilities and the functions that the network activity entity owns, it is the concrete manifestation of all kinds of network activities, which can directly or indirectly affect the entity state in the network space[2].

The control principle of the network behavior is: By applying a certain control strategy, make the operation state and behavior of all network entities within the scope that can be predicted and mastered, and ensure the normal activities operated effectively. Using prediction and control means as far as possible to avoid the occurrence of abnormal behavior, to resolve the abnormal issues emerged by real-time response and feedback control. The procedures of behavior control can be divided into three parts: monitor of network behavior state, analysis of network behavior characteristics and control of abnormal behavior of the network, and to form a feedback loop control of the network behavior in the system, so as to improve the security of the entire controlled network[3].

1.2 The concept of controlled network

Controlled network is the core theory of network security control theory, which using control theory methods to solve the security problems, and to realize the network security index as the control target, and follow the information theory, system theory and control theory as the basic research train of thought.

As shown in Figure 1, the control unit accept the external input signal and feedback signal, do the comparison, analysis, judgment, processing, and then make decisions, the implementation of the unit to issue appropriate control signals or instructions. The execution unit receives the instruction from the control unit, identifies the instruction and executes the corresponding program according to the preset control strategy, generates the corresponding control function and applies to the controlled object. The feedback unit generates the corresponding feedback signal, and then transmits the feedback signal to the control unit, and then affect the input of the information[1][2].

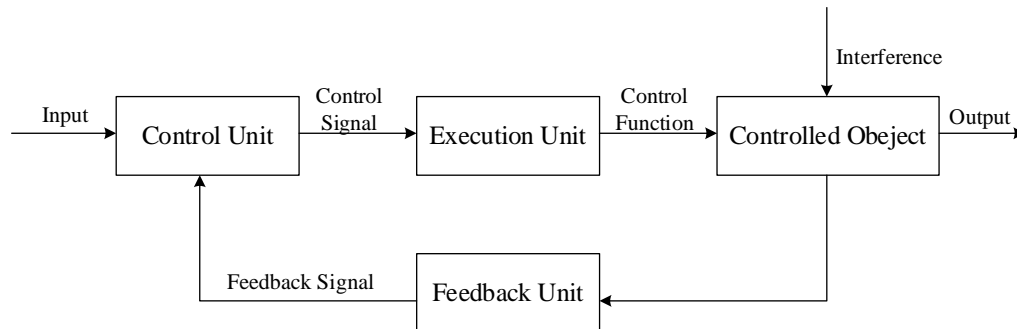


Figure 1 Control principle of controlled network system

1.3 The network behavior control in the controlled network

In the controlled network system, the aim of controlling the behavior of the network is to ensure the normal operation of the network entity activities, to predict and prevent the occurrence of abnormal behaviors. In the controlled network system, the control unit and feedback unit are composed of the control subsystems, the control unit and the security control center. The controlled object is the behavior of the whole network, including the normal network behavior and the abnormal network behavior.

Normal network behavior which is also a cooperative network behavior, which are as far as possible to show their behavior characteristics, so that the relevant control components can identify, so that behavior can be completed. Abnormal network behavior of the controlled network is a non-cooperative network behavior, the purpose of the behavior is illegal control the network and network information, and its characteristics are hidden as far as possible, trying not be found by security control system. Therefore, the key point of network behavior control in the controlled network system is the abnormal network behavior for the network security.

2 Detection and control model of abnormal network behavior

Abnormal network behavior refers to any behavior patterns that occur in the network, which is different from normal network behavior. The abnormal network behavior includes two main parts, the intrusion behavior and the false operation behavior. As shown in Figure 2, the abnormal behavior detection and control model was combined by misuse detection and intrusion detection, the model is able to achieve real-time network monitoring, analysis of user and system activities, feature extraction and modeling analysis of the abnormal behavior, identify the abnormal behavior in the system, ring and control it.

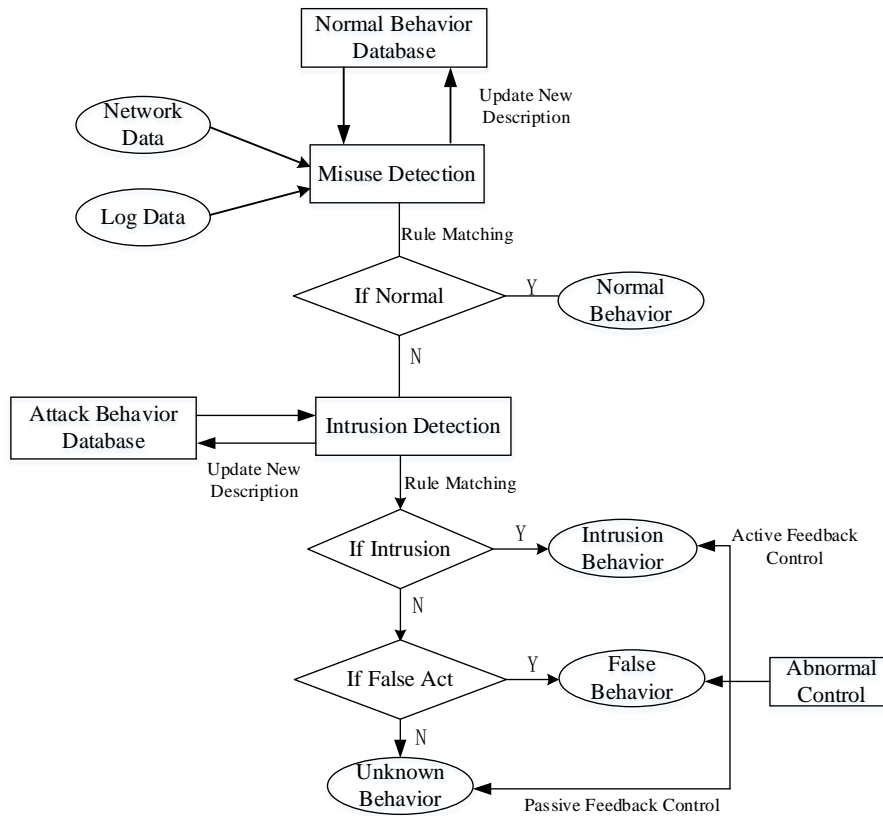


Figure 2 Model of abnormal behavior detection and control

2.1 Network behavior detection module

The network behavior detection module is reviewed according to the rules that are stored in the rule database. The rule database consists of two parts, the normal behavior description database and the attack behavior description database.

Misuse detection is based on the normal behavior matching detection, the pattern matching was carry out by the definition of normal (legitimate) network activities, to detect the abnormal behavior activities that not conform to the normal behavior[4]. The abnormal behavior refers to a host or network behavior, which is obviously different from the normal (legal) activities.

Intrusion detection, also known as attack signature based detection, it is assumed that all acts of aggression and means can be expressed as a pattern or a character, and analyze the known attacks and means, extract detection features, construct attack mode and intrusion behavior model, by contrasting system current state and attack mode and model matching degree to judge intrusion behaviors[5].

2.2 Network behavior control module

According to the abnormal behavior to implement different response strategies, abnormal control module will use the active response control and passive response combined control mode. The control object of the active response control is the control subsystem or the security agent. The control method is based on the automatic execution of the control subsystem or the security agent according to the preset response strategy[6]. When the abnormal condition is detected and the response measures are not corresponding to the knowledge base, the control method of passive response is required. Passive response control of control object is a security control center or network administrator, the control method is by a security agent will be difficult to deal with the abnormal events and to detect the problems were recorded, and then submitted to the security control center and send the alarm information and notification, and wait for the security control center system or network administrator to make decisions, for the difficult problems it will take more advanced control strategies.

2.3 The working process of the model

First, the anomaly detection module receives the preset audit data, and submits to the misuse detection unit. The misuse detection unit will compare the network object with the normal behavior rule base, if match, it will be identified as the normal behavior, if not it will be submitted to the intrusion detection unit. The intrusion detection unit compares the audit object with the attack behavior rule database, if match it will be known as the abnormal behavior, then submitted to the behavior control module for event response, if not match, then submit the error operation behavior detection unit. False operation test results match is identified as the false operation behavior, if not match, regard it as an unknown abnormal events submitted to the behavior control module.

When the anomaly detection module detects the abnormal behavior of a region node in the system, the security agent of the abnormal occurrence area will submit the abnormal event log to the control subsystem of this area, and the control method of the active response is preferred. For the known abnormal behavior, adopt preset respond strategies of the knowledge database to execute different control strategies for active response control; For unknown abnormal network behavior, there is no corresponding control strategy in the knowledge database, so it will be controlled by passive response of the system. The security agent will submit the abnormal event log to the security control center and alarm it, then the security control center or the network administrator do the control decision-making, and then the security agent and control subsystem implement feedback control according to the decision information which is given by passive response control.

3 Summary

It is an important research direction to improve the security performance of network system by analyzing and researching the activities of each entity in the network system, which is from the perspective of network behavior security control theory. Based on misuse detection and intrusion detection, combined with abnormal behavior detection and control model, this paper can be seen as the specific practice of the controlled network theory, and was proposed in order to solve the security problem and provide a new solution. With the application and popularization of large data analysis in network security condition monitoring and network behavior control, as well as the mature of modeling and analysis of network behavior characteristics, the theory and system of network behavior control will be gradually improved, which will play a more and more important role in the field of network security.

Reference

- [1] Lu Yu. Network Control Introduction[M]. BeiJing: National Defense Industry Press, 2005.
- [2] Lu Yu, Wang Yu, Wu Zhongwang. Information Network Security Control[M]. BeiJing: National Defense Industry Press, 2011.
- [3] S. Wolfgang, M Mannle. Online error detection through observation of traffic self-similarity [J]. IET Communications, 2001, 148(1): 38-42.
- [4] P. Barford, D. Plonka. Characteristics of network traffic flow anomalies [C]. In Proc. of ACM SIGCOMM Internet Measurement Workshop (IMC), San Francisco, CA, USA, 2001, 69-73.
- [5] Lei Ting, Yu Zhenwei. Wavelet weighted chaos local-region model of network traffic behavior analysis [J]. Journal of Computer Applications, 2006, 26(10): 2278-2281.
- [6] Li Zongli, Hu Guangmin. Network traffic anomaly detection method based on cascade model [J]. Application Research of Computers, 2008, 25(9): 2839-2841.