Research on Controllable Information Network Framework

Hua Li* and Chang-sheng WANG

Information Technology Room, Shijiazhuang Campus, Army Engineering University, Shijiazhuang Hebei, China

*Corresponding author

Keywords: Controllable network, Multi-level feedback, Coordinated control.

Abstract. The current single, isolated network security technologies make it hard to deal with diversity, hidden network attacks, the existing network security architectures are facing various challenges. According to the network control theory, the basic closed-loop structure can be adopted to the network architecture, so that the whole network system can work in a stable and self-running form. The concepts of system-level feedback and component-level feedback are firstly proposed. The component-level feedback control loop includes security function units, and system-level feedback control loop mainly includes security controllers. Furthermore, the vertical expansion structure and the lateral expansion structure are proposed. Finally, a novel controllable information network framework is proposed, which combines multi-level feedback and coordinated control. This provides a novel way to solve the problem of network security and design the future network framework.

Introduction

With the rapid development of network security technologies and applications, the Internet gradually becomes complex and heterogeneous, the vulnerability of the network framework is gradually exposing [1]. The development of the current network framework puts forward higher requirements for network security, thus ensuring the confidentiality, integrity, authenticity, usability and non-repudiation of information network system [2]. Existing network defense technologies, such as Firewall, Intrusion Detection System, work in an isolated format, and then cannot solve the problem of diversified network attacks.

Nowadays, the current attacks (such as Advanced Persistent Threat [3]) become diversified, and has a strong latent and targeted. These attacks make it difficult to detect before the system or the component is seriously damaged. Therefore, there is an urgent need to propose a novel framework, which can solve the various attacks at the same time.

Many scholars at home and abroad have focused on the research on the future network framework. Software-defined Networking (SDN) [4] is a new network architecture proposed by Stanford researchers in 2008. Its main role is to separate the control layer from the data layer via OpenFlow, and realize the programmable centralized control of the network. However, node failure in the single one controller is becoming increasingly apparent. According to the existing researches, Greenberg et al. [5] proposed a new 4D network control model, which classified the network framework into four logic planes including Data Plane, Discovery Plane, Dissemination Plane and Decision Plane. Its main role is to decouple the network control logic and the network routing protocol, and directly send the control instructions on the data layer. 4D network control model has some advantages in terms of running time, resource cost, but it cannot consider the whole network view, collaborative decision and optimal control. Luo et al. [6] proposed a trustworthy and controllable network architecture model, which is a joint design of three-dimensional protocol layer model, and its advantage is to achieve the isolation of network control and transmission, and enhance the control ability of network nodes through the management plane perpendicular to the network, but failed to give the specific controllable model. Lin et al. [7] conducted the thorough research to the next generation of trustworthy and controllable network, this paper proposes an adaptive network architecture, whose
advantages is disturbed the situation in the network environment, thus realizing the adaptive optimal allocation of control parameters of network equipment, network protocol and related mechanism.

In the paper [8-9], the controllable network is deeply studied, and the controllable network theory is put forward. The core idea is to solve the network security problem by using the automatic control principle [10]. The controllable network theory is the combination of system science and computer science. To achieve the goal of network security performance, it follows the basic research ideas of system theory, control theory and information theory, it is the general theory of basic concepts and methods of the application of control theory to study the network system, it is a general theory about the process of feedback and control network system [11-12]. Based on the theory of controllable network, we firstly proposed the concepts of controllable information network, and the controllable information network framework. The novel controllable information network system works in a multi-level feedback and coordinated control format.

The Controllable Information Network Concept

The Network Feedback Control Principle

The core of the controllable information network system is the feedback control loop. The most basic feedback control loop is usually composed of four parts: control system, controlled system, implementation system and feedback system. The feedback control structure reference model is shown in Figure 1.

![Figure 1. The Basic Feedback Control Structure.](image)

As shown in Figure 1, the implementation system is composed of the controller. According to the analysis of the whole view of the network, the controller adopts the specific control strategy and sends the corresponding control instructions to the actuator. The controlled system includes a variety of network equipment, network equipment including communication switching equipment (such as switches and program-controlled machine etc.), network equipment (such as repeaters, router, firewall) and system equipment (such as host and server etc.). A control system consists of an actuator, in which the actuator is responsible for the execution of control instruction, and the system can arrive at a predetermined steady state under the effect of control. Control information is the logical combination of instruction flow, control effect and transmission medium. The feedback system is composed of sensor, observer, and decision maker. The feedback system senses, detects and makes decision on the network status, and makes the control system take corresponding control strategies in a timely manner. Feedback information is the logical combination of state flow, global view and transmission medium.

The specific process of network feedback control is as follows:

1. In the case of external interference, the sensor is used to sense the network status of the network equipment and collect network behavior information (data transmission, resource allocation, etc.). The sensor sends the extracted useful information to the observer for analysis.
2. The observer extracts the useful state information according to the sensor, detects, identifies and analyzes the abnormal behavior, and provides a global view of the network state for the decision maker, thus providing the basis for correct decision and judgment.

3. The decision maker according to the observer analysis of the network state of the global view, the situation assessment and system alarm, and to control in the form of instruction flow to the control system.

4. The implement system according to the decision-making analysis of the current situation, match the corresponding control strategy. The actuator processes the control instruction submitted by the implementation system, generates control for the purpose, and configures the control parameters in an adaptive manner in a timely manner.

5. Control and disturbance at the same time to network equipment, the network feedback control process by controlled system, control system, implementation system and feedback system to complete together, and make the operation of the system gradually tend to a stable state.

When the network system is closed loop feedback control, the state space of the network feedback control is composed of three states, the control state, the steady state and the decision state, and the state transition diagram is shown in Figure 2. The network system mainly completes the acquisition and monitoring of network status in the steady state, the flow behavior of related characteristic parameters of steady state network has always been in the license area. The network system is disturbed in decision state, complete situational awareness, data analysis behavior in the decision-making process. In the control state, the corresponding control effect is generated, and the network system is constantly adjusted, eventually return to stable state, thus forming a closed loop self-diagnosis and self-recovery network system.

![Figure 2. The Network Feedback Control State Migration Process.](image)

**The Two-Level Feedback Control Loop**

Controllable information network is one or more feedback control loops are connected into a complex feedback control system, which is composed of a closed loop different scope and level, divided into functional unit level loop and system level loop, namely two feedback control loops. The function of unit level loop feedback control in the safety equipment or parts on the level of their composition, such as security agent network terminal control units, the router control unit, functional unit level loop is only a network-controlled object and a local control equipment, it is characterized by the closed-loop function of its own units to reach safe and controllable target. System level loop is the feedback control implemented on the system level, such as firewall system, access control, intrusion detection system, and the closed loop which is composed of the security control center, the system level loop consists of one or more controlled objects and a security control center, which is characterized by a feedback control loop formed under the global coordination and overall analysis of the safety control center.

The two-level feedback control state space is based on the basic network feedback control state space, and the two-level feedback control state transition diagram is shown in Figure 3. The network system is the external disturbance into the decision state, first through multiple unit decision state awareness, data analysis and decision making. If some data flow state information in unit level decision range, is directly to the specific control measures to control, into the unit level control state, and finally returned to steady state; Otherwise, these dates are analyzed by global coordination and whole analysis via system level decision state in the form of state flow, and then enter the system level.
control state, finally gradually to a steady state, thus forming a closed loop structure system level loop nested function unit level loop, and enhancing the overall performance of the network.

The Expansion of Two-Level Feedback Control Loop

With the expansion of network scale, the information processing capability of single centralized controller is limited. The two-level feedback control loop can be developed vertically and laterally, thus improving the information processing capability of the overall network controller in the form of multiple controllers.

The Lateral Expansion Structure

The distributed control is adopted in the vertical feedback control of the two-level feedback control loop. The structure increases the number and function of the local controller, and then improves the overall performance of the network. The lateral expansion structure is shown in Figure 4.

Each local controller after the lateral expansion is at the same level of the control plane. In physics, each local controller is in different areas, and the safety control center is responsible for all the local controllers. In size, the local controller distributed across a network through lateral expansion, each local controller can timely grasp the responsible for the network equipment in the area, to avoid the information interaction of time delay, but also solve the failure problem of single point single centralized controller. In the aspect of service function, network abnormal behavior shows the trend of integration, and it also requires the network monitoring system to be integrated [13]. After the expansion of the structure, the decentralized and isolated network security control technology will play a role in the same security control center, and the network security system will be shifted from passive defense to active defense. At the same time, the security control center receives the state information of each local controller (transmission and load network state) to form a global view of the network. The security control center adjusts the mapping relation between the local controller and the
network device in real time, and centrally manages and coordinates the network resources, thus achieving the flexibility adjustment, the control scale and the efficiency.

**The Vertical Expansion Structure**

Two-level feedback control with multilayer vertical expansion loop, increase the intermediate level between the controller units and system level controller, realizes data acquisition, network operation state detection at different levels, and provide the corresponding control abnormal behavior. The vertical expansion structure is shown in Figure 5. After the vertical expansion, the control plane is divided into system level, intermediate level and functional unit level, and the information processing ability has priority from the top down. The safety control center has the biggest decision-making power in the whole system, and is responsible for the coordination of the whole network information. The intermediate controller avoids the frequent interaction between the data information and the security control center, and at the same time shares the load of the security control center, thus enhancing the capability of the functional unit level controller processing. When the network equipment is processing the data flow, the nearest local controller is asked firstly, and the local controller responds quickly if the state information of the data flow is within the control range of the local level controller. If the status information of some data flow is not in the control range of the local level controller, it will consult the intermediate controller, and usually the majority of the data flow in the middle level controller can be controlled and managed. If the intermediate controller is unable to process the data flow, it will eventually ask the security control center and distribute the relevant control information to the network equipment step by step.

![Figure 5. The Vertical Expansion Structure.](image)

**The Mixed Structure of Lantern and Vertical Expansion Structure**

Combining the advantages of lateral and vertical expansion, a lateral and vertical mixed structure of multi-layer distributed control is designed, as shown in Figure 6. The security control center controls each intermediate controller according to the time-sharing mode. It combines the whole network view, not only generates the corresponding control instruction according to the state information, but also decides the control time allocated among the intermediate controllers. The security control center adjusts the mapping relation of each intermediate controller and each local controller in real time, and flexibly coordinates the control strategy and mechanism. Each intermediate controller combines the instruction of the safety control center and the network situation information feedback to match the corresponding control strategy, and each local controller executes the corresponding control behavior according to the control instruction.
A Novel Controllable Information Network Framework

Based on the above two-level feedback control loop, the lateral and vertical mixed structure is developed. The security control center integrates the current isolated network security technology, and then constructs the multi-level feedback and coordinated control network architecture, as shown in Figure 7.

As can be seen from Figure 7, the controllable information network architecture includes functional unit systems, safety sub centers, safety control centers and corresponding feedback control loops. Among them, the security control center is the core of the controllable information network system. The security sub center includes access control center, transmission control center, storage control center, structure control center and behavior control center. All kinds of control technology using functional parts of the system, the access control technology mainly includes the identity authentication, firewall and access control, the transmission control technology mainly includes the flow control, routing control and encryption transport, storage control technology mainly includes encryption storage, virtual storage and data hiding, structure control technology mainly includes the boundary control and isolation control, behavior control technology mainly refers to the intrusion detection and deep packet inspection.

In the controllable information network framework, the state information and control information are transmitted in each node. The control information is uppermost, from the safety control center to
the safety sub center and the safety control agent. The status information is from top to bottom, from security control agent, security sub center to security control center. In such a controllable information network architecture, functional unit feedback control loops are formed between each function unit and the security control agent, which mainly aims at some aspects of security problem control technology. The security control center fuses all kinds of security control technology, and through the global coordination and overall analysis of the control center, a feedback loop of system level is formed. From the information structure mode, control information and status information channels constitute a closed loop; From the information interactive mode, is a function of information interaction between the unit level controller and system level controller, another is the interaction between system level controllers. The architecture of controllable information network based on the above scheme has the following unique advantages:

1. It incorporates the basic closed-loop structure of the principle of automatic control, which provides the state information of the operation of the network system and imposes certain control so that the whole network system can run in closed loop form and gradually tend to set a steady state. The network system can achieve self-diagnosis, self-recovery effect, to solve the problem of network security provides a new way of thinking.

2. The use of multi-level feedback, coordinated control of the way, at different levels to provide network operation status, more effective from the network system for situation information and data analysis, decision-making and implementation control. This method has obvious advantages in running time and information processing, etc., and improves the information processing capability and efficiency of the whole network system.

3. The establishment of an internal correlation monitoring system, which changes the traditional network security components of a single and passive defense functions, all kinds of security control technology integration in the same security control platform centralized scheduling and coordination, not only increased the information exchange between the security control components, but also has the effect of flexible adjustment control scale, effectively deal with a wide range of network attacks and sabotage.

Conclusion

At present, the types and complexity of network services are increasing rapidly. However, the external, isolated network security control technology has been unable to cope with the diversity and concealment of network attacks. The basic principle of automatic control of the closed-loop structure into network system, based on the concept of system level and functional unit level two level feedback control, feedback control of the main function units in a security control strategy and mechanism of global coordination and overall analysis of control system level security control center feedback. The establishment of a multi-level feedback, coordinated control of the controllable network information architecture, making decentralized isolated network security control technology can be integrated in the same security control center to play a role in ensuring the information network security control system security and controllability. The controllable information network feedback control architecture to provide a sound network security control system to provide theoretical support and basis for solving network security issues and the construction of next-generation network architecture has a certain guiding significance.

Acknowledgement

This work was supported by the National Natural Science Foundation of China under Grant No.61271152 and the military science program of the National Social Science Fund under Grant No.15GJ003-184.
References

[1] Lin Chuang, Jia Zi-xiao, Meng Kun. Adaptive Future Network Architecture. Journal of Computers, 2012 (6), 1077-1093.

[2] Lu Yu, Li Xi, Wu Zhongwang, Wang Yu. Preliminary research of controllable network. Journal of Ordnance Engineering College, 2015 (3), 38-43.

[3] Lu Yu. Instruction and Control Discipline Development Report. China Science and Technology Press, 2016 (4), 123-124.

[4] McKeown N, et al. Openflow: Enabling innovation in schools networks. ACM SIGCOMM Computer Communication Review, 2008, 38 (2), 68-74.

[5] Greenberg, et al. A clean slate 4D approach to network control and management. ACM SIGCOMM Computer Communication Review, 2005, 35 (5), 41-54.

[6] Luo Junzhou, Han Zhigeng, Wang Liangmin. A Trustworthy Controllable Network System and Protocol Structure. Journal of Computers, 2009 (3), 391-404.

[7] Lin Chuang, Ren Fengyuan. Controllable and trusted can be extended to a new generation of Internet. Journal of software, 2004,15 (12), 1815-1821.

[8] Lu Yu, Wu Zhong Wang, Wang Yu, Lu Jun. Network control theory. Beijing: National Defense Industry Press, 2005.

[9] Lu Yu, Wang Yu, Wu Zhong Wang. Information Network Security Control. Beijing: National Defense Industry Press, 2011.

[10] Hu Shousong. Automatic control principle. Beijing: Science Press, 2013.

[11] Yang Shuanghua. Internet-based control system. Beijing: Electronic Industry Press, 2014.

[12] Lu Yu, Chen Xingkai, Chen Liyun, Qiao Wenxin. Controllable network - the cornerstone of the allegation network. Journal of instruction and control, 2015, 1 (2), 170-174.

[13] Lin Chuang, Peng Xuehai. Research on trustworthy network. Journal of computer science, 2005, (5), 751-758.