# Security Monitoring System of Ideological Guiding Network Environment Based on DDOS Offense And Defense

Chen Ruiping
Yunnan Land and Resources vocational college
Kunming,652501, Yunnan, China

**Abstract**:This article is based on DDos offense and defense, taking the security monitoring mechanism of college network ideological and political management as the research object, starting with the analysis of the basic connotation of college network ideological and political education management mechanism, and expounding the definition, characteristics and functions of college network ideological and political education management mechanism. Through demand analysis, the design idea of the network information security monitoring system is given, and the system design framework and functional module division are described. Secondly, taking the security attack of the ideological network as an example, the security defense measures for constructing the ideological education network are proposed from the practical level.

**Keywords**: Ideological Guiding, Network Environment, DDOS Offense, Security Monitoring System

## 1. INTRODUCTION

Facing the wave of the global digital economy, my country has successively issued a series of documents such as "Made in China 2025", "Outline of Action for Promoting Big Data Development" [1], and "Outline of National Informatization Development Strategy", In this paper [2], the RGB three-component signals of the color confidential image block are embedded in the pseudo-invisible image respectively [3]. The RGB three components of the fused image are thus generated to generate a pseudo-fused image that hides confidential information [4]. For the extraction of confidential information, the key information is used to extract the RGB three-component signals of the color confidential image block from the [5] RGB three-components of the secret pseudo-fused image respectively [6]. Image edge detection is an important processing link in computer vision and digital image processing [7]. It plays an important role in image segmentation, texture feature extraction, shape feature extraction and image recognition. [8].

More and more network application systems in our country contain a lot of valuable information [9], but they are still in a state of slack fortification, and there are great security risks and hidden dangers [10-12]. It can be said that the network security issues we face are very serious, and the insecure factors in the network are mainly concentrated in the areas of viruses, intrusions [13], and interception. Early views all defined it as the practice of using online media to carry out moral education [14]. The concept of its scientific system first appeared in the year, when some scholars proposed "using information networks [15] to carry out ideological and political education for students". Someone defined it in 1988 as "Ideological and political education based on the theory of communication and ideological propaganda, using computer networks." [16]

In addition, some scholars start from studying the relationship [17] between traditional education and the network, and define it as a modern education method, a combination [18] of computer network and traditional education. These are all definitions of the Internet as an educational tool [19]. Passing

ideological concepts, political views, and ethics to the audience enables them to form social practices that meet [20] the needs of the class. That is, the use of the Internet, in a purposeful, planned, and organized manner, exerts an influence [21] on citizens' ideological concepts, political concepts, ethics and information literacy, thereby forming a two-way online [22] interaction of ideological and political morality and information [23] literacy that meets the needs of certain social development Virtual time activities. This truly reveals its essential relationship [24].

Therefore, we can define it as a discipline that uses the influence of the Internet on the public to study its intrinsic, essential, and inevitable connections in the process of its effect on education. Foreign research on network ideological and political education is scattered in related researches such as computer ethics, information ethics, and network ethics. For example, Negroponte's "Digital Survival", Bainu and Rogerson's "Information Ethics: Second Generation", Moore's "What is Computer Ethics", and Manius Custer's "Internet The Rise of Society, Davis Mosheira's "The Wave of Power-The Development and Prospects of Global Information Technology (1964-2010)"... Scholars have a great influence on the Internet, especially the impact of the Internet on society after its emergence , Especially the impact on social ethics and moral education and the way out. There has been a lot of attention and research on network ideological and political education in colleges and universities in China, and a number of results have been produced.

On December 23, 2017, the results of a search on the China Knowledge Resources Database (CNKI) using the keyword "University Network Ideological and Political Education Research" in the paper showed that 8679 results were fuzzy matches and 1132 exact matches (918 journal papers) , There are less than 90 doctoral dissertations). The number of papers is very limited, and they mainly focus on the definition, content, methods of online ideological and political education, and comparative research on foreign research. The firewall is the most used security device on the network and an important cornerstone of network security. But firewalls are not

omnipotent. At present, firewall technology is not yet fully mature. As a useful supplement to firewall technology, In the aspect of building extraction, by researching edge detection methods, we can select an appropriate method for reliable and accurate detection of building edges in images, which is of great significance for assisting the effective extraction of buildings.

## 2. THE PROPOSED METHODOLOGY

### 2.1 The DDos Offense and Defense Security Check

The establishment of the product model includes the product There are some differences in information and data between different fields. The system constructed in this paper realizes the integration of information and data of different models. However, due to the complexity of complex mechanical products themselves, the established product model involves a large number of parameters. And the variant of the assembled product is a knowledge-based and parameter-driven process.

Network information security is a wide-ranging issue, and its goals mainly include confidentiality, integrity, availability, controllability, and non-repudiation. The Internet is an open system for the public. This openness of the Internet and network information security are a contradictory unity. Steal secret attacks, computer viruses, illegal access, etc. Under this situation, various network information security technologies have emerged, and they have always developed and progressed in the fierce intellectual confrontation between the "offensive" and the "defender". Today's commonly used network information security technologies include network security access control technology, network security identity authentication technology, network security content security technology, and network security audit and tracking technology.

At the same time, in order to build a complete network security system, people put forward a network security model, which emphasizes the role of dynamic security protection in network security. Traditional security technologies such as firewalls, encryption technologies, digital signatures, etc. are all static security mechanisms. They lack an active response to the ever-changing attack methods in the network environment. Simple use can no longer meet the needs of network security. Therefore, traditional security technologies are comprehensively used. At the same time, detection tools and monitoring methods must be used to provide a deep and diverse protection for the network system.

### 2.2 The Ideological Education Network Environment

Network ideological and political education is a new type of education, which uses modern network technology as a means and the Internet as a platform, and has strong characteristics of the times. First, it makes the form of ideological and political education more vivid and more comprehensive. Traditional ideological and political education has a lot of static content, and the content is old and has no new ideas, the update cycle is slow, the education form is single, and it lacks vitality. In contrast, it contains richer information, vivid and vivid content, and can effectively use sound, pictures, images and other forms, vivid and intuitive, and extremely appealing. Secondly, it gives new ways to traditional ideological and political education. Traditional classroom teaching and

publicity education is restricted in time and space and the education coverage is small.

This method relies on human experience and judgment, and the interaction and cooperation are blind, and the reconfigurability of the cooperation relationship is poor. In order to enhance the pertinence of interaction and collaboration, expands the audience of education, and is conducive to the formation of a good campus environment and learning atmosphere. Finally, the interaction, timeliness and equality of education have been strengthened. In August 1994, some scholars adopt the directional gossip transmission strategy that "we must make full use of various mass media to form an overall atmosphere for patriotic education". It is not difficult to find that ideological and political educators in colleges and universities have noticed that they must rely on the Internet to carry out positive publicity and education work, and actively manage and regulate the online behavior of college students. However, during this period, due to the insufficient ability to use Internet resources, the positive publicity and education in the education process lacked attractiveness and influence compared with the Internet. Faced with the free cyberspace and the diverse cultural imagination on the Internet, it was insufficient to cope with it. The main work of network ideological and political education is to prevent the negative effects of the network by censoring and filtering network information.

Taking the innovation of ideas as the forerunner and driving the overall innovation of educational content, methods and technology is the key the ddos attack experiment is set up in the network security technology experiment course of the school of computer, heilongjiang university of science and technology in colleges and universities is essentially the work of being a person under the network environment, and the fundamental purpose is to educate people. the purpose is to let students understand the principle and technology of DDoS attack . This paper mainly expounds the realization of DDoS attack experiment based on OpenStack's network security experiment platform.

### 2.3 The Security Monitoring System for Ideological Education Network Environment

Management refers to the process by which managers optimize the allocation and effective use of organizational resources through planning, decision-making, organization, coordination, and control, and make full use of all favorable conditions to achieve the set goals. Mechanism originally refers to the structure and operating principles of machines, but later generally refers to the laws of internal organization and operation changes of natural phenomena and social phenomena. In management, through the formulation and implementation of plans, systems, and decisions, new mechanisms and corresponding functions can be generated, and scientific mechanisms play a role in activating competition and promoting progress. Intrusion detection system is used to identify illegal attacks against computer systems and network systems, or information systems in a broader sense, including detecting malicious attacks or probing by illegal intruders from outside, and illegal behaviors of internal legitimate users that exceed the use authority.

This paper analyzes the special problems of network confrontation, analyzes the mainstream technologies of DDoS attacks, and conducts in-depth analysis of the main defense strategies of DDoS attacks, and criticizes the further

development of DDoS attacks in the field of network confrontation. Direction of development. Usually the pattern matching or pattern matching sequence of the message is used to define the rules. During detection, the monitored message is compared with the rule, and the result of the comparison is used to determine whether there is abnormal network behavior. It can be seen that there are many factors that affect the evolution of the collaborative relationship network, and there are correlations between various factors. Therefore, only by fully considering these influencing factors, can a cooperative relationship optimization algorithm that meets the requirements be designed. DDoS attack refers to the use of distributed large-scale denial of service attacks. The attacker builds a DDoS attack network and sends attack instructions to the attacking server and attacker in the attacking network to launch the attack: Handler is accepting the attacking command from attacker.

## 3. CONCLUSIONS

A large number of Agents send attack packets to the victim when they receive the command from Gongxin. The main sleigh or Que network of the victim cannot provide normal services, thus achieving the purpose of denial of service attacks. It consumes the resources of the target system with massive data packets that exceed the processing capability of the attacked target, and eventually leads to the paralysis of network services. In addition, multiple defense agents in the same subnet will also aggregate into a defense team through business cooperation.

## 4. REFERENCES

[1]Zhu Jing, Wu Zhongdong, Ding Longbin, etc. DDoS attack detection based on DBN in SDN environment[J]. Computer Engineering, 2020, 46(4):6.

[2] Sun Yangu. Research on DDoS attack detection based on artificial intelligence algorithm under SDN[J]. Journal of Huainan Teachers College, 2019, 21(5):4.

[3] Jin Lei. Design and implementation of DDOS detection system based on big data analysis[J]. Automation and Instrumentation, 2018(11):4.

[4] Yu Xueshan, Han Dezhi, Du Zhenxin. DDoS attack detection system based on intelligent bee colony algorithm[J]. Computer Science, 2018, 45(12):7.

[5] Song Yubo, Yang Huiwen, Wu Wei, et al. Software-defined network DDoS joint detection system[J]. Journal of Tsinghua University: Natural Science Edition, 2019, 59(1): 8.

[6] Chen Li. Application research of SDN-based DDoS attack detection and defense methods [D]. Xi'an University of Science and Technology, 2020.

[7] Shu Yuejie. DDoS attack detection mechanism based on deep learning under SDN network architecture [D]. Harbin Institute of Technology, 2020.

[8] Wei Min, Yang Tao, Mao Jiuchao, et al. A method for detecting and mitigating DDoS attacks in industrial SDN networks: CN108289104A[P]. 2018.

[9] Zhang Jinglong. Overview of DDOS attack detection methods [J]. Science & Technology Economic Guide, 2020, v.28; No.710(12):23-24.

[10] Bu Youjun, Wang Han, Wang Ji, et al. DDoS attack protection system and method based on SDN and BGP process specifications:, CN110830469A[P]. 2020.

[11] Chen Haojie, Jia Chuanghui, Shao Weizhuan. Research progress of DDoS attack detection in SDN environment[J]. Modern Computer, 2019(5): 5.

[12] Guo Shuai. Research on DDoS Attack Detection Method Based on Convolutional Neural Network [D]. Shandong Normal University, 2019.

[13] Zhao Zhenzhong, Liao Jun. Shrew DDos attack detection based on DSP[J]. Information Security and Technology, 2019, 010(006):1-8.

[14] Yu Junqing, Yu Chang, Li Dong. A method and system for DDoS attack detection and defense in software-defined networks:, CN109005157A[P]. 2018.

[15] Tang Kunjian. DDoS attack detection method based on load prediction[J]. Network Security Technology and Application, 2018(1): 2.

[16] Cui Jie, Wang Mingjun, Zhong Hong, et al. Server DDoS attack detection and defense method based on double entropy in SDN environment: CN108848095A[P]. 2018.

[17] Teng Jian, Chen Junjun, Zhao Ying. DDoS attack detection based on user network behavior model [C]// China Computer Users Association Network Application Branch 2018 22nd Network New Technology and Application Annual Conference Proceedings. 2018 .

[18] Jia Jingyi, Shi Yijie. Research on DDoS Attack Detection Algorithm in SDN Environment[J]. 2020.

[19] Gao Xiaoqian, Luo Chao. Function and implementation of network security monitoring device for power monitoring system[J]. Communication World, 2019, 26(4): 2.

[20] Yu Ke, Yu Yisheng. Common problems and countermeasures of power system network security monitoring devices[J]. 2020.

[21] Jia Kun, Wang Junnan, Liu Feng. DDoS detection and mitigation mechanism in SDN environment[J]. Journal of Information Security, 2021, 6(1):15.

[22] Sayavong Lounnapha. Research on DDoS attack detection based on CNN and SVDD [D]. Lanzhou Jiaotong University, 2020.

[23] Ma Lele. Research on DDoS attack detection and defense methods in SDN environment [D]. Anhui University, 2019.

[24] Jiang Wentian. SDN-based server load balancing and DDoS attack detection technology [D]. Nanjing University of Posts and Telecommunications, 2019.