Mitigation of Abuse Attack for Large Scale Network

Xiao Lin Qiao

Abstract—**With the deepening of Internet applications, people increasingly dependent on the network, the Internet has revolutionized the way people live. Internet has gradually become an indispensable tool for daily life. But with the deepening of Internet applications, once the network paralysis, will result in huge economic losses. The Internet is a huge open a system, its own design and implementation of the agreement that there are many defects, plus upper layer application software itself vulnerabilities, the security of the Internet has increasingly become a focal point. This paper presents a wavelet-based preprocessing algorithm for early warning of worms. And malicious attacks on users to make a special packet processing. The terminal server to a reasonable allocation of its resources. To avoid consuming resources during an attack, the malicious user abuse of resources is a result of normal user cannot obtain effective services.**

Index Terms—**Network resources, consumption-based attacks, network security**

I. Introduction

Comparing with other network security threats such as network intrusion, network virus, and others, consumption-based attacks of network resources has wider incidence, faster attack speed and bigger destructive power [1]. In November, 1988, Morris worm spread quickly on network, made thousands of computers to paralyse in short hours, caused more than 6000 network servers to paralyse for infection in several days and led to the earliest network denial-of-service attacks. The loss from it exceeded 10 millions dollars [2]. On July, 19th, 2001, Code Red worm, which is a worm using buffer overflow vulnerability of Microsoft IIS, exploded. It infected 250 thousand host computers in 9 hours, and made the loss more than 2 billion dollars [3]. In the same year, Nimda worm exploded, which worked by infecting Windows operational system like Code Red worm. Due to many different routs of transmission of Nimada, all the host computers in the world were infected in half an hour. Moreover, the data of loss evaluation from Nimda kept increasing after increasing from 0.5 billion to 2.6 billion, and could not evaluate any longer now. In the beginning of 2003, slammer worm exploded, and inflected at least 70 thousand host computers only in 10 minutes to make ATM network of most of American banks paralyse. In August, 2003, Blaster worm exploded, and infected 12 billion host computers in 3 days [4]. This worm ever led to the paralysis of Canadian airline, and caused the economic loss at least 2 billion dollars and at most 10 billion dollars. As early as 2000, the bigger internet content suppliers of the world such as Yahoo,eBay,Buy.com, CNN and other famous website suffered denial-of-service attacks which stopped legal network flow for several hours and even made some paralyse for a few days. The appearance of network makes the harm of denial-of-service attack more terrible, the first network of our country was founded in 2004 [5]. The attacker could control hundreds of thousands of host computer resources through network and issue normal and legal network traffic at random to form consumption-based attacks of high bandwidth network resources.

II. The Definition to Consumption-Based Attacks of Network Resources

Network attacks could be divided into two catalogues [6]: a) use security vulnerabilities of information system to skirt around security protection measures of information system and enter into information system so as to control information system. This kind of attack is usually called as controlling attack. b) This network could not control information system, but it has the serving ability reduced or lost completely for largely consuming the resources of information system, such as memory resources, computational resources, bandwidth resources and so on. This kind of attack is usually called as resource consumption-based attacks. According to the target types of consumption-based attacks of network resources, it could be divided into two classes:

Purposeless resource consumption-based attack; in the period of attacking, this attack has no specific target to attack, but has bigger influence on the middle router. It is mainly used to exhaust certain network resource, such as bandwidth capacity of communication link and transponder capacity of grouping of router [7]. It is called as I attack in this article.

Purposeful resource consumption; this attack takes terminal server as attack objective during attacking to make the resources such as CPU of terminal server, memory and communication link have overload. The attack to Web server by network belongs to this attack. It is called as II attack in this article.

Worm is the typical representative of I attack in recent years. It could have numerous host computers with vulnerabilities infected in very short time, even in several minutes. However, each host computer infected tries to send great amount of data to objective host computer through middle router, so numerous data flows to certain middle router, makes the performance of high-speed router decline sharply, even cannot finish transponding other legal data flow, and leads to large-scale congestion collapse of network within a second. So network worm is considered as one of the biggest security threats in Internet.

From the analysis mentioned above we could know that

Manuscript received November 27, 2012; revised February 15, 2013.

Xiaolin Qiao is with the Shenzhen Polytechnic, Nanshan District, Shenzhen, Guangdong, China (e-mail: xiaolin102@126.com).

DOI: 10.7763/IJFCC.2014.V3.255

consumption-based attack of network resources has great destructive power, and is a danger which is could not be neglected at present and foreseeable future. Due to the complexity of modern software project, it is impossible to establish a security system without vulnerability. Miller puts forward a research report about the popular operating system and application program, pointing that it is impossible to have software without defect, and that it is rather difficult to design and achieve a whole security system. This provides a necessary condition for the existence of consumption-based attack of network resources [8]. Furthermore, because internet has the characteristics of openness, interconnection and sharing, each explosion of network resources consumption-based attack will bring huge destruction to the society.

III. Detection and Precaution of Network Worm Based on Connectivity

A. *Distributed Worm Containment System Structure*

The explosion of worm will bring great amount of economic loss. Because, with the penetration of internet application, every country in the world more rely on Internet Huge economic loss will be suffered once the network paralyses, so network worm is considered as one of the biggest security threats in Internet. The economic loss is mainly embodied in: worm could infect the host computer with vulnerability in the whole Internet in a few hours (such as Code Red) or in a few minutes (such as Slammer), so when worm explodes, large number of worm messages will be produced to occupy bandwidth in network, to use up great amount of routing resources and lead to congestion of network. AQM algorithm of traditional routing node is to suppose that terminal user network could have sensitive feedback for network congestion, detect network situation, and cooperate to control network congestion. It means that the terminal of data resource will reduce the sending speed of data flow so as to make the network come back to healthy status when congestion happens. But, worm has the characteristics of non-TCP friendliness and nonreactivity when sending data packet, so when worm explodes in network, algorithm of traditional router queue management cannot maintain the fairness of normal network data flow and worm data flow to make worm data flow get priority for transponding data by occupying routing queue and obtain higher bandwidth, it also could not make data flow of other normal users obtain lower bandwidth, even lead to the paralysis of network in serious situation. Although an early warning of worm for precaution is proposed before, a design for a proper algorithm which could effectively detect the worm and discard adaptively the data packet of worm according to network status will be significant for protecting network resources. Fully considering the transmitting feature of worm, this article puts forward a new self-adapting method for worm detection and containment, proposes worm detection and containment method based on connectivity according to analytic results. And that, this article uses theoretic analysis and experiment results to testify that this method could find unknown worm, adaptively adjust containing rate according to worm status, effectively contain the transmission of worm, and guarantee very small interference to normal network action.

The explosion of large-scale worm generally brings huge network flow.

The network flow produced by hundreds of thousands of host computer will gather to border router, make the performance of high-speed router sharply decline, even can not finish transponding other network data, and cause large-scale congestion collapse of network within a second, even make router produce denial-of-service in higher form. So, network worm is considered as one of the biggest security threats in Internet. For fast transmitted worm, an automatic containment strategy is needed. When detecting the explosion of worm, the host computer infected by worm shall be insulated fast so as to effectively contain the transmission of worm and better protect network device. Relying on terminal network security system (firewall and intrusion detection system), traditional single-point network security system has difficulty to handle large-scale worm explosion with big flow and high bandwidth. In network security, traditional single-point detection and terminal protection method can not effectively deal with malicious data flow, which is shown in detail as:

In the area of network management, traditional single-point network security system needs the participation of human for the control to the response for network worm. But for the worm fast transmitted, an automatic containment strategy is needed. When detecting the explosion of worm, the host computer infected by worm shall be insulated fast so as to effectively contain the transmission of worm and better protect network device. While the participation of human could reduce the responding speed of network precaution, and increase the possibility for the network devices to be attacked by worm.

Traditional network security system is basically single point, and does not adopt entire network cooperation method. The worm adopts distributed attack, and when it explodes, hundreds of thousands of computers will send worm packet in different subnet. So the adoption of single-point protection cannot effectively contain the transmission of worm so as to better protect network devices. Then, a distributed worm containment system is proposed. This system could effectively contain the transmission of worm with large flow and high bandwidth by worm detection and losing-packet strategy.

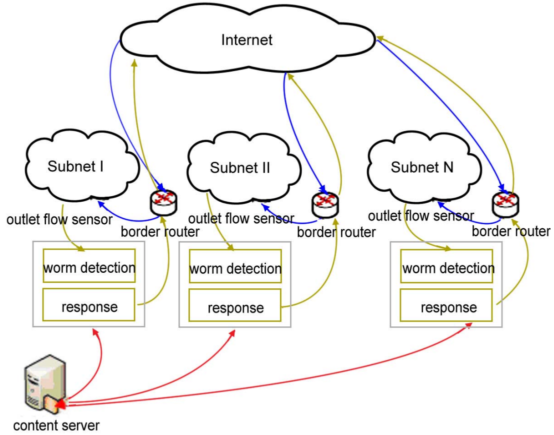

Fig. 1. Frame diagram for distributed worm containment system

In order to effectively contain the transmission of worm and better protect network devices, distributed worm containment system shall have the following characteristics in function:

Distributed cooperative; Distributed cooperative worm containment system is mainly embodied in: the whole system is made up of the nodes distributed in different networks; each of them could cooperate and has connected information to increase the efficiency of system; in addition the communication of the nodes shall not cause too much network overloading.

Rapid detection and in-time response: Distributed containment system is required to detect the worm rapidly, to respond in time and control the transmission of worm, and to better protect the running of network devices.

Expandability; this article establishes distributed system by node cooperation. With the scale to protect network increasing, new network border router could be added into system by node certification.

Usability and practicability; the system shall take the current traditional network structure of TCP/IP protocol as the foundation, carry no adjustment for large-scale network from structure, and emphasize the realizability and practicability.

Fig. 1 shows the frame diagram of distributed worm containment system. From the point of system function, the system is mainly made of two functional modules.

Flow sensing module

Contents server

Contents server could be arranged in any position of network. Each enabling or disabling to a border detection point needs to make registration or logout in contents server. Central contents server is mainly made of three big modules:

Communication module: mainly make communication and information exchange for the detecting points distributed in the subnets to achieve enciphered communication for central content server and the detecting points.

Registry module: reserve the initialized registration information corresponding to each detecting point, and make central content server to maintain the status information of each detecting point.

Statistic module: central content server receives the detecting results from sensor to count the number of host computers that have been infected, then sends the statistical result to the sensor of each subnet.

Flow sensing modules are arranged on border router of each subnet or outlet gateway, which are also called as border detecting points. It analyzes the action of network user, detect if worm attack happens, and if worm attack happens, it could take some strategy to discard these attack message and contain the transmission of worm. Flow sensing module could be divided into four big parts: network monitoring part, worm detecting part, the part to computing the attack status of worm, self-adaptive losing-packet strategy part.

B. Performance Analysis for the Algorithm of Single Worm Attack

Firstly, the containment effect of algorithm for only one worm attack on network shall be analyzed. When single worm attack happens, our simulation platform simulates RED Code worm. The simulation parameters are set as: the number of host computer with vulnerabilities is N 360,000, the scanning rate of worm is subject to the normal distribution of N(358,802), the objective terminal is 138, the number of host computer to be infected at the beginning is 10. Fig. 2(a)-2(c) show the monitoring results by monitoring algorithm in the continuous K time periods. The detecting result as Fig. 2(d) could be obtained with the detection algorithm of formula (4-6). In Fig. 2(d), abscissa is host computer, coordinate is detection result: 1 means that this host computer is abnormal; 0 means that this host computer is normal; red means the detection result is correct; green means the detection result is wrong. From Fig. 2(d) we could know that detecting algorithm could detect the host computer infected by worm rightly on the condition of having certain false alarm rate.

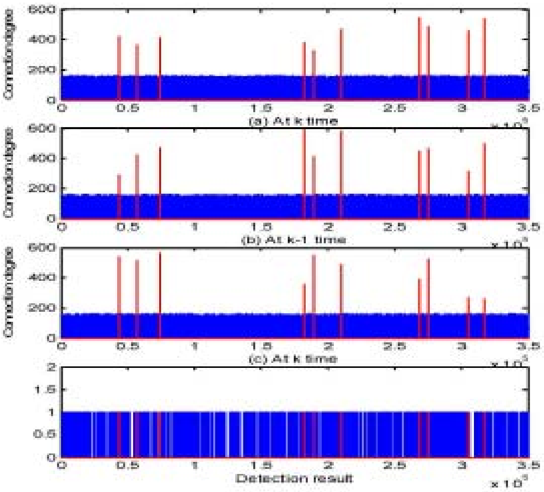

Fig. 2. The monitoring result in continuous k time periods and the detecting result of detecting algorithm

IV. Conclusion

This article gets some achievements after deeply discuss and study the detection and precaution for denial-of-service attacks. According to the understanding of the author in research, the work could be developed from the following aspects:

Now, worm is transponded more and more snugly, and the method for transponding is more and more. When worm obtains the host computer with vulnerabilities by slow scanning, the its network feature will not change in nature, so worm detection and precaution technology for slow scanning needs further searching.

The appearance of network makes the danger of denial-of-service attacks more terrible. The attacker could control hundreds of thousands of host computer resources through network and issue normal and legal network traffic at random to form consumption-based attacks of high bandwidth denial-of-service attacks. Therefore, the detection and precaution for network will be the focus in future research.

Reference

[1] H. Bose, *On the effectiveness of route-based packet filtering for distributed DoS attack prevention in power-law Internets*, 2001.

[2] M. Gayson, *Changing the default for directed broadcasts in routers*, Sept. 2005, pp. 156-199.

[3] C. Hoare, *Network ingress filtering: Defeating denial of service attacks, which employ IP source address spoofing*, Nov. 2001.

[4] X. Jones, *The latest in denial of service attacks:"smurfing" description and information to minimize effects*, Jan. 1996.

[5] Z. Kobayashi, *Cert advisory-2000, Denial of service developments*, 2004.

[6] O. Kumar and Moore, *Research on network resource*, Oct. 2002, 78-86.

[7] K. Martin and Y. Thompson, *Study on network security*, June 1999.

[8] J. Quinlan, *A study of protection and development countermeasures for consumption-based attacks*, July 2003, 1-17.

Qiao Xiaolin was born in Shenyang in January 1963. She graduated from Wuhan University, computer application majors, Major research computer network and software

She is an associate professor working in the Shenzhen Polytechnic, computer school, computer basic teaching department.

She published "Visual Basic Programming Practical Guide" (2007), as deputy editor. Have paper in "Computer Engineering and Disign" (2008-17,4430-4432).The title is "The Data Capture Model Design of Network Security Base on Honeypot", as the first author.