A Simulation Analysis of Abnormal Traffic-Flooding Attack under the NGSS environment

Hwan-Kuk Kim*, and Dong-il Seo*

* Group of Network Security Research, ETRI, Korea
(Tel : +82-42-860-3823; E-mail: {rinyfeel,bluesea}@etri.re.kr)

Abstract: The internet is already a part of life. It is very convenient and people can do almost everything with internet that should be done in real life. Along with the increase of the number of internet user, various network attacks through the internet have been increased as well. Also, Large-scale network attacks are a cause great concern for the computer security communication. These network attack becomes biggest threat could be down utility of network availability. Most of the techniques to detect and analyze abnormal traffic are statistic technique using mathematical modeling. It is difficult accurately to analyze abnormal traffic attack using mathematical modeling, but network simulation technique is possible to analyze and simulate under various network simulation environment with attack scenarios. This paper performs modeling and simulation under virtual network environment including NGSS[1] system to analyze abnormal traffic-flooding attack.

Keywords: network security, simulation, information security, hacking

1. INTRODUCTION

It is not in doubt that the information society of the 21st century is based on the Internet internationally inter-connecting millions of computers used by billions of users. Advanced countries have been engaged in fierce competition to make the Internet network more sophisticated. However, in reality, counterproductive threats against information security, such as hacking, diffusion of viruses, breach of intellectual property rights and cyber crimes, are rampant because the Internet is an open network easily accessed by anyone.

In accordance with such threats, various security systems have been developed and introduced, and these systems have been individually implemented and managed with products focused on access control and system security. However, cyber terror attack techniques have responded and gradually become integrated into an overall and coherent system from the previous scattered pieces. In particular, attempts to integrate the rapidly spreading worm viruses with the hacking skills that can destroy systems and networks have surged. Attempts to hack that cause paralysis of global networks have been tried through attacks into network nodes and simultaneous generation of heavy network traffic. Individual security systems have limited capacity to defend themselves from these types of attacks. These attacks are becoming more intelligent and sophisticated day by day [1].

These network attack threat becomes biggest threat could be down utility of network availability. Therefore, need high efficiency information protection system development [2].

Most of the techniques to detect and analyze abnormal traffic are statistic technique using mathematical modeling. It is difficult accurately to analyze abnormal traffic attack using mathematical modeling, but network simulation technique is possible to analyze and simulate under various network simulation environment with attack scenarios.

This paper performs modeling and simulation under virtual network environment including NGSS system to analyze abnormal traffic-flooding attack. Accordingly, we analyze the characteristics of NGSS and explain the method used to model NGSS components, and analyzes simulated result of NGSS at the level of virtual network topology included with the NGSS components. And then, describe the configuration of virtual network topology using NS-2, the generation of abnormal traffic flooding attacks for the target of configured topology including modeled NGSS components, the simulated behavior of NGSS and then analyzes the result of the simulation.

2. MODELING OF NGSS

The NGSS consists of three components and interface providing their interactions: security management node(SMS), security node(SGS,SRS). The SMS(Security Management System) which is security management node should be able to collect attacks and abnormal traffic information and forward corresponding policy about attack to security node. The SGS(Security Gateway System) and SRS(Security Router System) which are security node detect attacks and abnormal traffics and apply receiving policies from SMS node[3].

Figure 1 shows the logical structure between NGSS components.

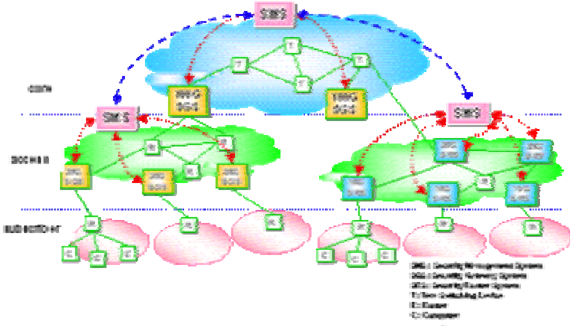

Fig. 1 The logical structure between NGSS components.

The following NGSS components and their main functions were modeled: a traffic generator for causing attack packets and abnormal traffic, security management agent, security agents and NGSS Link.

2.1 traffic generator

It is necessary to distinguish abnormal traffic from normal traffic to simulate the detection and the response solution to

[1] The NGSS (Next Generation Security System) is a high performance network security system that is being developed by ETRI. This system performs overall protection for traffic passing through transferring networks such as public and ISP networks at a global network level, and detects and resolves attacks on networks.

abnormal traffic by using NS-2. There are three packet header formats:

The following could be newly defined to generate these three types of packets.

(1) CBR(Constant Bit Rate) : an object source provided from NS-2

(2) M CBR(Modified CBR) : a traffic object source modified from CBR class

(3) M Exponential(Modified Exponential) : a traffic object source modified Exponential class.

Table 1 The type of packet header format.

Type of pakcet	Explanation
PT NORMAL	packet type for general back-traffic environment
PT ANORMAL	packet type for abnormal traffic flooding attack
PT ATTACK	packet type for various patterns of attacks

M CBR traffic generator generates traffic on UDP agents and has 3 setting variables: *rate* , *packetSize* , *trafficType* .

(1) The *rate* variable sets the volume of traffic per second at the rate of 25%, 50% and 75% bandwidth.

(2) The *packetSize* variable sets the size of generated packets.

(3) The *trafficType* variable sets that three types of packets is normal, abnormal and attack.

During simulation based on the value of variables set, traffic is generated to target nodes via agents.

2.2 Modeling of NGSS structure

This section modeled the main components of NGSS. In this modeling, security agents indicate SGS and SRS of NGSS components because the basic mechanism of SGS and SRS is similar.

Security agents have four basic functions : (1) detection of abnormal traffic, (2) transmission of alert, (3) receipt of policies, and (4) blocking of detected attack packets.

Security management agent (1) receives alert incoming from security agents, (2) determines defensive policies for the received alert and (3) transfers the determined policies to each security agent.

When the event of abnormal traffic and the occurrence of attack packets are occurred, security agents detect these and transfer alerts for the detected data to SMS agent. And then, the SMS agent receives an alert incoming from security agent(SRS/SGS), generates the defensive policies based on the received alert and transfers it to the corresponding agents. Finally, Security agents receive policies sent from SMS agent and then respond according to the policies.

Table 2 shows rule parameter, ranges, and types of corresponding policy for SMS agent.

Table 2 parameter , ranges, and types of policy.

Parameter	Ranges	Type of policy
abTrafficRate	0~100%	if(ϕ =*abTrafficRate*) *Policy traffic drop*
bwLimit	0~100%	if(λ = *bwLimit*) *Policy bw drop*
attackCnt	1~1000	if(cnt(alert) = *attackCnt*) *Policy packet drop*

(1) *abTrafficRate* is a threshold value to control the rate of abnormal traffic. If ϕ value exceeds *abTrafficRate* threshold value, security management agent send *Policy traffic drop* to drop abnormal trffic.

(2) *bwLimit* is a threshold value to limit the link bandwidth connected to security agents. If traffic exceeds the threshold value of link bandwidth, security management agent send *Policy bw drop* to control link bandwidth below *bwLimit*.

(3) *attackCnt* is a threshold value to detect attack packets. If the count of attack exceeds the threshold value, security management agent send *Policy packet drop* to drop the packet.

3. SIMULATION AND ANAL SIS

This chapter describes the configuration of virtual network topology using NS-2, simulates attack and protection of abnormal traffic attack under configured virtual network topology including NGSS system, and then analyzes the result of the simulation.

Fig.2 shows the virtual network topology for simulation. The virtual network topology is divided into two network domain.

(1) NGSS domain include NGSS agents (SMS, SRS, SGS), (2) Legacy domain configured with normal nodes generating normal back-traffic and nodes generating abnormal traffic.

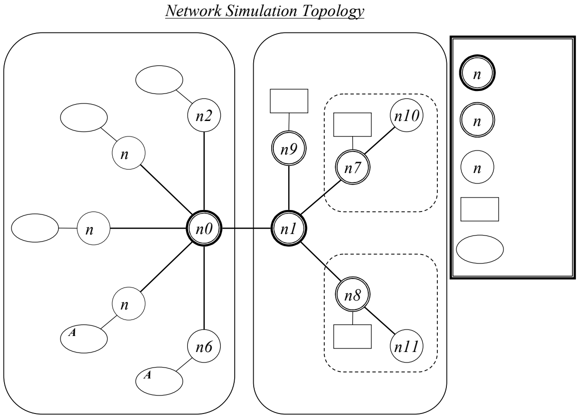

Fig. 2 The logical structure among NGSS components.

NGSS domain consists of two networks. (1) *Network 1* is the network included SGS agent, (2) *Network 2* is the network included SRS agent. The agents in NGSS domain are classified SMS, SRS and SGS agent.

Finally, there is a traffic generator application in legacy domain. The link connected to each node is set as a bidirectional link.

3.1 Scenario 1: simulating abnormal traffic flooding attack

This scenario 1 simulate an abnormal traffic flooding attack on the environment include NGSS node. When a traffic source generates normal back-traffic and abnormal traffic, SGS agent detects the abnormal traffic and sends an alert to SMS. SMS sends SGS the policy to prevent the abnormal traffic according to the set rule. SGS performs an experiment to block the abnormal traffic according to the policy received.

Fig.3 graphically displays the result of analysis for the tracing of simulation by using GnuPlot. The x-axis is simulation time and the y-axis is throughput before and after passing through SGS node.

In the graph, *traffic1.tr* is the total throughput of normal/abnormal traffic before passing through SGS node, and *traffic2.tr, /traffic .tr, traffic .tr* are throughput of traffic after SGS node, as SGS node detects abnormal traffic and sends SMS node alert, then the policy for blocking abnormal traffic is processed. *traffic2.tr* is the result of simulation in case of ϕ=1 for the rate of abnormal traffic, *traffic .tr* is the result in case of ϕ=2 for the rate of abnormal traffic and *traffic .tr* is the result in case of ϕ=3 for the rate of abnormal traffic.

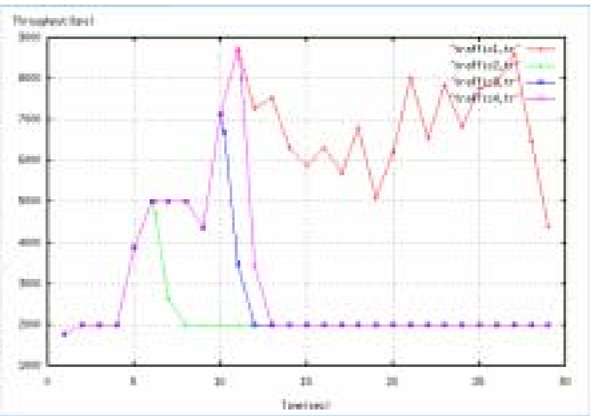

Fig. 3 displays the result of analysis for scenario 1

3.2 Scenario 2: limiting link bandwidth

This scenario 2 simulates the function of limiting the bandwidth to connect. The SMS agent transfers the policy of limiting bandwidth to SRS agent according to the *rate limit* setting value set by rule.

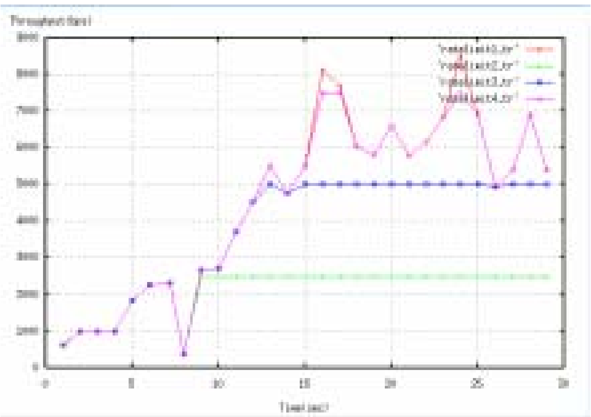

Fig. 4 displays the result of analysis for scenario 2

Fig.4 graphically displays the result of analysis for the tracing of simulation by using GnuPlot. The x-axis is simulation time and the y-axis is throughput before and after passing through SRS agent after setting the *rateLimit* .

In the graph, *ratelimit1.tr* is the total of throughput of normal and abnormal traffic before passing through SGS node, *ratelimit2, ratelimit , ratelimit* are throughput of traffic after passing through SGS node, as SGS node detects abnormal traffic and transfer an alert to the SMS node, and then it processes policy for blocking abnormal traffic. *ratelimit2.tr* is the result of simulation in case of λ=25% for the rate of abnormal traffic, *ratelimit .tr* in case of λ=50% and *ratelimit .tr* in case of λ=75%.

4. CONCLUSION

This paper has performed modeling and simulation under virtual network environment including NGSS system to analyze abnormal traffic-flooding attack.

To perform abnormal traffic-flooding simulation under NGSS environment, we have analyzed the characteristics of NGSS and explained the method used to modeling NGSS components.

For simulation, we have described the configuration of virtual network topology using NS-2, generated and abnormal traffic flooding attacks to the target of configured topology including modeled NGSS components, and then analyzed the result of the simulation.

REFERENCES

[1] K.W.Kim, H.K.Kim, J.N.Kim, A Study on the Intelligent correspond to Traffic Flooding Attack , *Journal of Korea Internet Information*, Vol. 5, No.1, Mar. 2004

[2] Michael Liljenstam, ougu uan, BJ Premore, David Nicol, A Mixed Abstraction Level Simulation Model of Large-Scale Internet Worm Infestations , *10 th IEEE Int l Symp*. On MASCOTS 02, 2002

[3] H.K.Kim, D.I.Seo, A Simulation Analysis of Abnormal Traffic Flooding Attack using Network Simulator , *Conference of Next Generation Communication Software 200* , On NCS 2004, 2004