Computer Simulation of Denial of Service attack in Military Information Network using OPNET

Lichun PEI, Chenhui LI, Runfeng HOU, Yanjun ZHANG, Hongyan OU
Air Defense Forces Academy
Zhengzhou, China
e-mail:Lichenhui_zz@163.com

Abstract. According to designing DoS attack model, the methods based on OPNET of simulating DoS attack which can be achieved are summarized. The attack model is given from simulating SYN flood attack. Simulation results show that the network simulation is a productive approach to analyze and estimate the impact of the DoS attack on the military information network and to develop appropriate safety measures, which provides a reference method for the establishment of the other attack models.

Keywords: discrete event system simulation; OPNET; DoS attack; attack model

1. Principles and simulation method of DoS attacking

In military information network, in order to achieve accurate and efficient command of armed forces, the transmission of documents or data must reach the specified combat units promptly and accurately. Typically, the data of transferring is encrypted complicatedly. To intercept and decipher the data, you need professional decryption means. But blocking the network to delay or prevent the normal transmission of the data is extremely easy. Denial of Service attack (DoS) refers to attacking the network protocol to achieve defect or exhaust the resources of the object being attacked through various means, so the attacked computers or network cannot provide normal services, until the system stops response even collapse. Therefore, denial of service attack has become the first choice for destruction of military information networks.

Recently, research institutions abroad have a preliminary research and exploration of network attacks and network security simulation[1]. The modeling of security and system project (MOSES) ,which is jointly funded by the U.S. Defense Advanced Research Projects Agency (DARPA), the National Science Foundation

(NSF) and the National Security Agency is using the technique of modeling and simulation to analyze computer network, mainly concerning the simulation of large-scale network system security. In addition, there are a number of network attacks using simulation tools to simulate, such as Shabana Razak, University of Florida, reproduced a variety of attack data collecting from the flowing files in the simulation network environment building by OPNET, and used the simulated attack packets to verify an intrusion detection algorithm based on character[2]. Five scholars from SABANCI University of Turkey built attacking model for the DSR ad hoc routing protocol in OPNET, and analyzed attacking effect of the model to routing discovery mechanism of DSR[3].

OPNET is mainly used for the simulation of network efficiency, equipment utilization, network configuration and so on, with the character of the full supporting of the protocol programming, users can arbitrarily control the level of detail of the protocol simulation. In addition to the security protocols, OPNET can accurately simulate variety of common network protocols, the modular hierarchies in the standard node providing by OPNET is shown in Figure 1. In addition, the code of the various protocols in OPNET is completely open, so users can easily modify existing protocol model or add a new one. That makes it possible to build a model of denying service attacks against the protocol model in OPNET, but the simulation of attacking model must be based on the defects of network protocol and not the vulnerabilities of operating system or application. Protocol attack is using the vulnerabilities of network protocol security, the attack will take unusual network action to the abnormal conversion or normal action to cheat and use the network protocol, with the essence of abusing network protocols.SYN Flood is the most typical form of protocol-based attack in a variety of denying service attack.

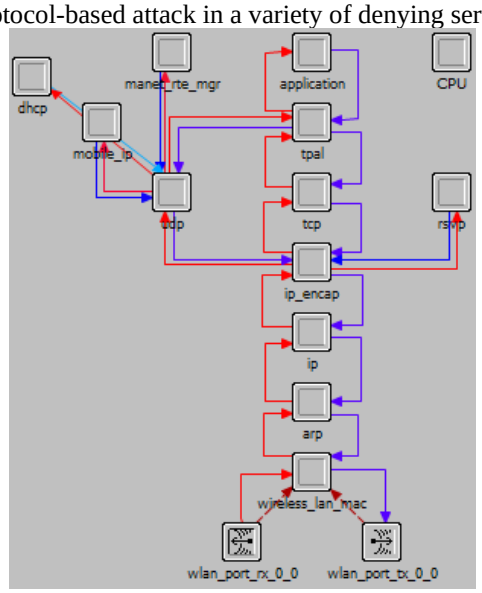

Figure 1. Node module framework

Most of preventing techniques against SYN flood attacks, whether to use filtering gateway or reinforce the TCP/IP protocol stack, are related to the maximum number and time-out threshold settings of half-connection [4]. That can be effective against SYN attack by increasing the TCP maximum number and shortening the time-out value of half-connection. However, it is very difficult to determine the specific value in the process of setting, because most of the target machine memory resources will be occupied when the number of half-connection is too much, and the target machine will refuse legitimate connecting requests when the time-out threshold of half-connection is too small. Typically, the operating system only gives default value of the maximum number and time-out threshold of half-connection, but the parameters must be based on the network environment in practice.

Simulating SYN flood attack is to confirm whether a system can be DoS attack and obtain the condition and extend of DoS attack. From the simulation analysis, we can get the impact of the attacks on the protocol stack and the target network, and use the correct quantitative data to describe the effect of SYN attacks in different network environments, ultimately obtain the effect and the rate of SYN attack in specific network conditions and the relationship between the maximum allowed number of concurrent connection in TCP and time-out threshold of TCP half-connection. So the network managers in the real network can properly set the TCP key parameters to more effectively defense SYN attacks.

2. The process design of SYN flood attack model

According to the analysis, the process structural design of the attack model is shown in Figure 3. As a network management process, gna_clsvr_mgr process is responsible for the attack of analyzing property and open of server-side listening port. As a business specification management process,gna_profile_mgr process need to determine when the attack begin, and notify the target and duration of the attack management sub-process and the attack rate. Being the sub-process of gna_profile_mgr process, gna_synflood_mgr process is to control the duration and rate of the attack. The gna_synflood_cli process is responsible for the specific implementation of aggressive behavior, such as sending out the TCP connection request packet.

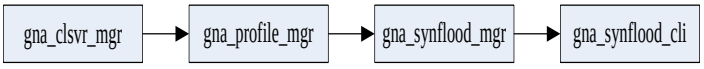

Figure 2. Process structure flow chart

Being a network management process, gna_clsvr_mgr process is to attack analyzing property and opening server listening port. The attack on analyzing property is related to the definition of related data type and the design of analytic functions, and it does not need to modify the network management process when the server port is open, because the gna_clsvr_mgr process already contains all the features

of the server-side. The start and open state in the network management process are still responsible for opening the listening port of the server. The enumerated type GnaT_App has been defined in the attack on analyzing property, which contains a port value of 1688 for Synflood applications. If the server supports Synflood application, the network management process would get the corresponding port value, after that the start and open state will open the 1688 port of the server through function gna_clsvr_mgr_open ().

gna_clsvr_mgr process creates and activates the business specification management process gna_profile_mgrto simulate each of the business specification. It is mainly to complete two tasks: one is responsible for controlling interval and duration of the business specifications, the second is creating and activating the corresponding management processes for each of applications contained in the business specifications and sending them necessary information.

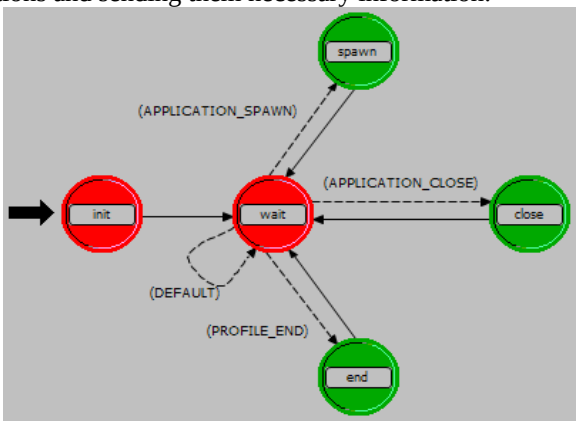

Figure 3. Process gna_profile_mgrstate chart

The state transition of gna_profile_mgr process is shown in Figure 3. Close state and end state are responsible for controlling the interval and duration of the business specifications, spawn state is responsible for creating and activating the corresponding application management process for each of application contained in business specifications.

As attack management process, gna_synflood_mgris to manage specific aggressive behavior, according to a variety of attack parameters coming from the business specification management process, its state transition is shown in Figure 4. It contains four states and two jump conditions: the role of init state is to initialize variables; wait state is to judge jump conditions; end state is to end attack and destroy attack management process when the duration of the attack reach; attack state is to activate the gna_synflood_cli sub-process to complete the attack after the attacks began, according to the attack rate. Jump condition START_ATTACK and ATTACK_END are macro defined in the header area, START_ATTACK means that the value of interrupt code is 1, ATTACK_END means that the value is 2.

Being attacks execute process, gna_synflood_cliis used to initiate a TCP connection and implement the behavior of attack. The process only contains execute state, because it does not involve the sending and receiving of data.

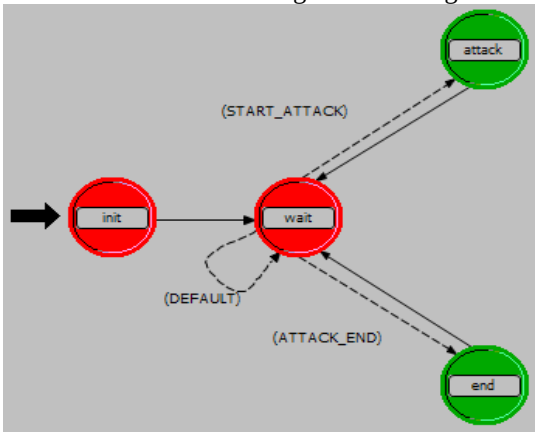

Figure 4. Process gna_synflood_mgrstate chart

3. Analysis of the simulation results of SYN flood attacks

SYN flood attacks model is constructed on the basis of standard modules, so it can run in a variety of simulation network environment based on the TCP/IP protocol. Information network architecture designed in this paper is just a special case, in the model (Figure 5), Server provide services to LAN1 of the local area network users and remote users LAN2, and an attacker try to SYN flood attacks on the Server.

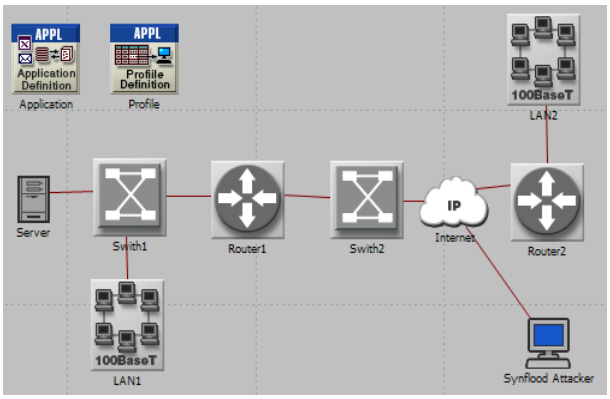

Figure 5. Network framework

The simulation results of attack model can include successful probability of denial of service attack (PDS), fault time of server, and user delay. Due to visually

representing the effect of attack, the simulation output PDS as result, the formula is as follows[5]:

PDS(successful probability of denial of service attack) =1-(the number of successful service request/the total number of request) (1)

In the formula, the number of successful service requests the total number of TCP connection successful requests in throughout the simulation time of legitimate users; the total number of requests represents the total number of TCP connection requests in throughout the simulation time of legitimate users. According to integrating statistical analysis of the model simulation output PDS, We get three sets of simulation data, corresponding to different values of timeout period for the server half-connection, the maximum number of connections allowed by the server and the rate of service requests of attackers.

Firstly, the relationship between timeout threshold of server half-connection and PDS is shown in Figure 6.The PDS is 0approximately, when the server timeout threshold t is less than 30 seconds. PDS rises from 0 to 0.2 and from 0.3 to 0.8, when the server timeout threshold rises from 30 seconds to 50 seconds and from 100 seconds to 1000 seconds, which means the effect of attack is significantly enhanced. And PDS has not notable increase when the server timeout threshold rises from 50 seconds to 100 seconds. Therefore, server timeout threshold should be set between 50 seconds to 100 seconds in the specific network conditions.

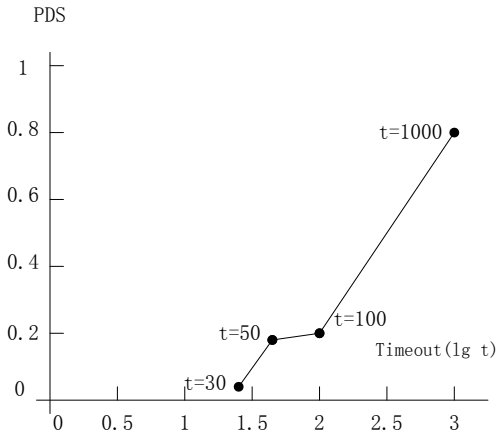

Figure 6. Comparison of PDS and overtime threshold value

The relationship between the maximum of half-connection allowed by the server and PDS is shown in Figure 7: when the maximum of half-connection c is less than 100, PDS is almost 1; with the maximum of half-connection increasing, the PDS decreases gradually almost to zero, when it reaches 2000. Therefore, it conforms to reality that the maximum of half-connection should be set more than 1500.

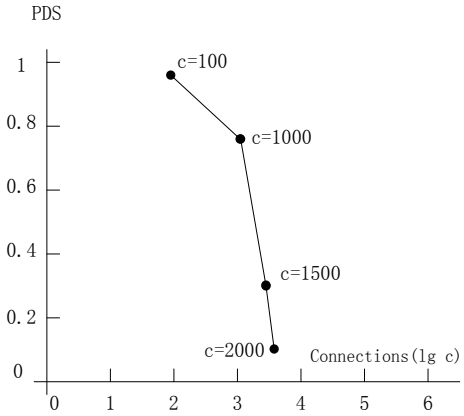

Figure 7. Comparison of PDS and half-connect value

The relationship between the attacking rate of the attackers and PDS is shown in Figure 8: the probability of successful attack is zero when the rate r is 1 or 2 per second, in the condition of server certain settings; the probability of success is still small (less than 0.2),when the rate r is 10 per second; and it increases significantly when the rate rises to 20 per second.

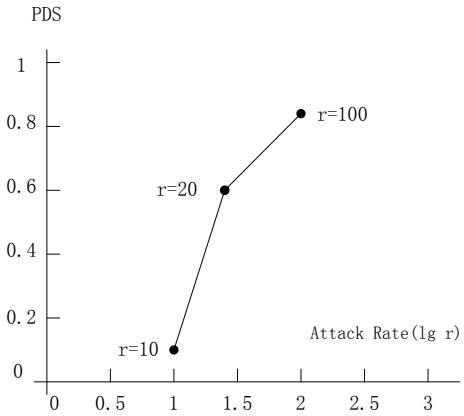

Figure 8. Comparison of PDS and attack speed

4. Summary

From simulating the denial of service attack, we sum up the types of denial of service attacks that can be simulated, according to setting up the attack simulation model. Construction and analysis of the simulation model of the SYN flood attack, proves that the network simulation technology is a productive approach to analyze and estimate the impact of the denial of service attacks on the network and to de-

velop appropriate safety measures, which provides a reference method for the establishment of the other attack models.

5. References

1. Mattisa Bjorlin,“A study of Modeling and Simulation for computer and network security,” University of Stockholm/Royal Institute of Technology, July 2005.
2. Shabana Razak, Mian Zhou, Sheau-Dong Lang,“Network Intrusion Simulation Using OPNET. School of Electrical Engineering & Computer Science and National Center for Forensic Science,” University of Central Florida,Orlando.
3. Albert Levi,“A Probabilistic Routing Disruption Attack on DSR and Its Analysis,” Sabanci University,Faculty of Engineering and Natural Sciences.
4. Christoph L.Schuba, Ivan V.Krsul, Markus G.Kuhn, Eugene H.Spafford,“Analysis of a Denial of Service Attack on TCP,” Department of Computer Sciences Purdue University.
5. W.J.Blackert, D.M.Gregg, A.K.Castner, E.M.Kyle, R.L.Hom and R.M.Jokerst,“Analyzing Interaction Between Distributed Denial of Service Attacks And Mitigation Technologies,” The Johns Hopkins University Applied Physics Laboratory.