Research on Quantitative and Semi-Quantitative Training Simulation of Network Countermeasure

Jianjun Shen[1,a], Nan Qu[1,b], Kai Li[1,c]

[1]Department of Informationization Construction, Academy of National Defense Information,
Wuhan, 430010, China

[a]email:shjj06@sina.com, [b]email:619477568@qq.com, [c]email:307482359@qq.com

Keywords: Network Countermeasure; Quantitative; Semi-quantitative; OPNET; Simulation

Abstract. Network countermeasure is an important kind of combat operations in information condition, so how to implement network countermeasure simulation in simulative training applications is a crucial problem to be resolved. Therefore, the paper first proposed the architecture of network countermeasure simulation, and described its realization issue in simulative training. Secondly, the paper explained the degree-based virus spreading methods, and put forward a quantitative simulation method for virus spreading on scale-free network. Thirdly, based on the ideas of parameter setting, the paper presented a semi-quantitative simulation method for some network attack and network defense actions. As the methods presented in this paper have certain fidelity while meeting the practical application requirements of simulative training, they can solve some problems that are hardly implemented. Thus it can be seen that the research results has good application prospect.

Introduction

In information age, with the arising of new operation patterns such as information warfare, network-centric warfare, distributive network warfare and etc., the network is playing more and more important role [1]. Especially, using virus or other means to attack opponent's networks has been a common practice for both warring sides. So simulation training, as a modern technological means to sharpen the actual operational capacity, should include simulation of network countermeasure so as to practically improve the training effects.

As an excellent network simulation platform, OPNET has been used in most network simulation applications. OPNET uses object oriented 3 layers, namely network layer, node layer, and process layer for modeling and provides a large number of device models, so communication network can be modeled in an intuitive and convenient way [2]. OPNET also provided HLA interface, so that the simulation program developed based on OPNET can carry out distributive information interaction with other external applications in accordance with HLA standard.

As for simulative training applications, the training simulation of network countermeasure is different from general performance simulation. For network countermeasure performance simulation, emphasis is laid on the fidelity of the simulation results while there are no special requirements for time to be taken by simulation execution, and a longer simulation running time is permissible. But for training simulation of network countermeasure, its running process must be real time while the simulation results are not necessary to be very precise. Its key is to show the relevant characteristics of network countermeasure, so that trainees can be aware of any network change brought by network countermeasure and then take appropriate measures for further action. Furthermore, in simulative training applications, demands of directors should also be taken into account when to simulate network countermeasure. As important users of simulative training, directors can control implementation of network countermeasure by setting parameters directly.

As training simulation of network countermeasure is a difficult problem, this paper proposed a combination of quantitative and semi-quantitative methods. Quantitative method mainly applied mathematical formula to describe network countermeasure, while semi-quantitative method adopted setting parameters method in order to meet work needs of directors or address the difficulties that cannot be completely described with mathematical formulas.

The Architecture

According to functional needs, a simulative training system used network countermeasure can be composed of a directing room, a network attack operating room and a network defense operating room, and the trainees should be divided according to tasks and carry out the simulative training in the corresponding room. In the directing room, network attack operating room, and network defense operating room, all seats are interconnected through Local Area Network (LAN), realizing communication between seats based on the LAN. The directing room, network attack operating room, and network defense operating room as well as database server, HLA/RTI server, and OPNET network simulator are interconnected through a switch, forming a complete simulative training system for distributed interactive training online. The architecture of the system is as shown in Figure 1.

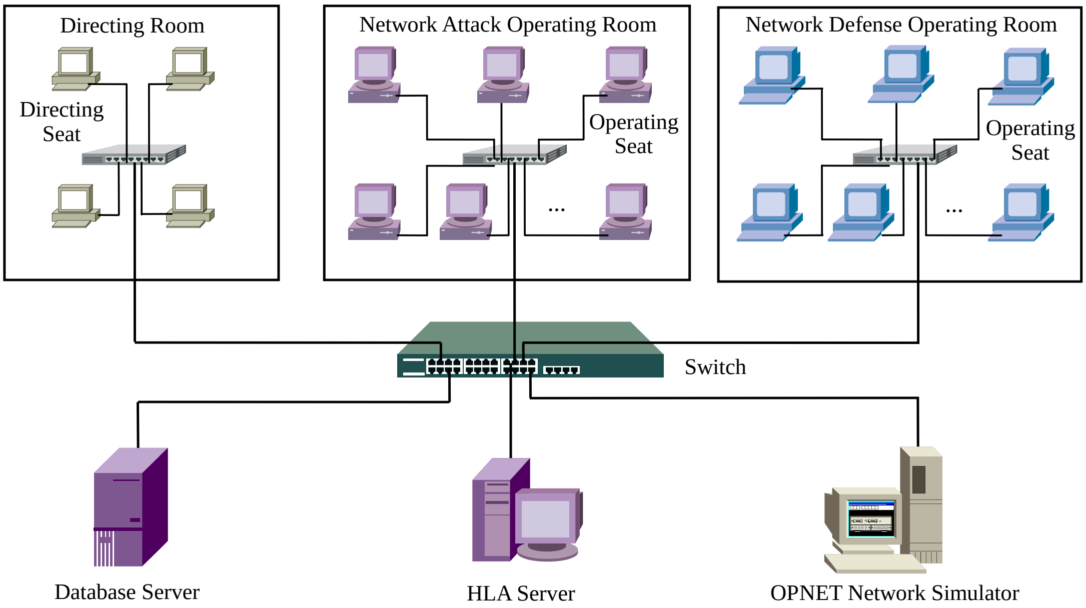

Fig.1. The architecture of the simulative training system

In Figure 1, the network attack operating room is used for carrying out simulative training on network attacks, the network defense operating room is used for carrying out simulative training on network defenses, OPNET network simulator is used for simulating the running process of network, including simulation of network attack and network defense actions, and HLA server is used for realizing the distributed interaction of training information with international standard [3]. The Information interactions between seats in simulative training process are as shown in Figure 2.

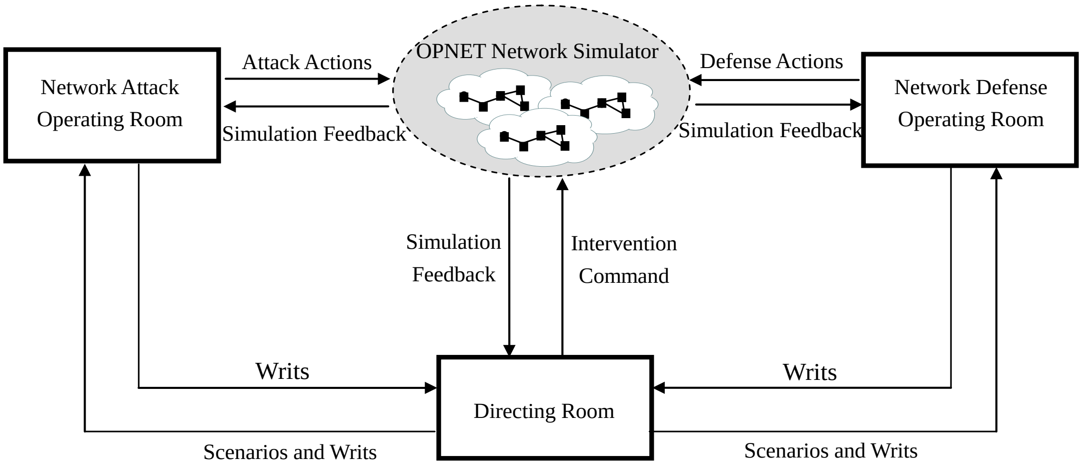

Fig.2. The information interactions between seats

As the core component of the simulative training system, OPNET network simulator needs to simulate network attack and defense actions. Quantitative and semi-quantitative simulation methods are provided below.

Quantitative Simulation Method

The use of virus in network countermeasure has become a typical practice in information conditions, so how to simulate virus spreading in OPNET network simulation is a key problem.

In recent years, researches [4][5][6] have shown that the degree distribution of many networks is obviously different from Poisson distribution. For many networks such as WWW, Internet on autonomous layer, and paper citation network, their degree distribution can be better described in power law. Networks with power law degree distribution are also known as scale-free networks, whose degree distribution is highly non-uniform: that is, most nodes have smaller degrees while a smaller number of nodes have larger degrees.

Now consider the virus spreading on scale-free networks. Take nodes in the network follow the SIS model of susceptible(s)→infected(I)→susceptible(s), let the probability of getting infected from the susceptible state be ν and that of getting recovered to the susceptible state from the infected state be δ, effective spreading rate is defined as:

$$\lambda = \frac{\nu}{\delta} \tag{1}$$

Define the relative density $\rho_k(t)$ as the probability to be infected for a node with a degree of k, the average field equation is as follows:

$$\frac{\partial \rho_k(t)}{\partial t} = -\rho_k(t) + \lambda k\left[1-\rho_k(t)\right]\Theta\left(\rho_k(t)\right) \tag{2}$$

Where, $\Theta(\rho_k(t))$ represents the probability for any given edge to connect with an infected node. Denote the steady-state value of $\rho_k(t)$ as ρ_k, for this purpose, let the right side of the equation (2) be zero, we can get:

$$\rho_k = \frac{k\lambda\Theta(\lambda)}{1+k\lambda\Theta(\lambda)} \tag{3}$$

For unrelated scale-free networks, as the probability for any given edge to point to the node with the degree of s can be expressed as $sP(s)/\langle k\rangle$, we can get:

$$\Theta(\lambda) = \frac{1}{\langle k\rangle}\sum_k kP(k)\rho_k \tag{4}$$

Combining equations (3) and (4), we can get ρ_k and $\Theta(\lambda)$. With a view to the typical example of scale-free networks—BA scale-free network, the degree distribution and average degree are respectively:

$$P(k) = 2m^2k^{-3} \tag{5}$$

$$\langle k\rangle = \int_m^\infty kP(k)dk = 2m \tag{6}$$

Where, m represents that a newly introduced node is connected to m existing nodes in BA scale-free network construction algorithm. Thus, according to equation (4), we can get:

$$\Theta(\lambda) = m\lambda\Theta(\lambda)\int_m^\infty \frac{1}{k}\frac{dk}{1+k\lambda\Theta(\lambda)} = m\lambda\Theta(\lambda)\ln(1+\frac{1}{m\lambda\Theta(\lambda)}) \tag{7}$$

Then:

$$\Theta(\lambda) = \frac{e^{-1/m\lambda}}{m\lambda}(1-e^{-1/m\lambda})^{-1} \tag{8}$$

Substituting equation (8) into equation (3), we can thus get ρ_k.

Therefore, the spread process of virus can be simulated according to the following steps in simulative training:

(1) Initially setup several nodes infected by virus.

(2) Calculate the degree k of all nodes, take the largest degree as $k_{\max}$, then calculate the steady-state infection density ρ_k of all nodes from $k=1$ to $k_{\max}$. For BA network, $\Theta(\lambda)$ is shown as follows:

$$\Theta(\lambda)=\frac{e^{-1/m\lambda}}{\lambda m}\left(1-e^{-1/m\lambda}\right)^{-1} \tag{9}$$

(3) Calculate the current actual infection density of all nodes from $k=1$ to $k_{\max}$, that is, for nodes with degree k, the ratio of the number of those infected to the total number, denote it as $\rho_k(t)$.

(4) For each $\rho_k(t)$, calculate the selection probability:

$$p_s(k)=\min(\frac{\left|\rho_k(t)-\rho_k\right|}{\rho_k},\ 1.0) \tag{10}$$

That is, if the difference between the current actual infection density $\rho_k(t)$ and the steady-state infection density ρ_k is greater, there will be a larger selection probability $\rho_s(k)$, indicating that the node with degree k is under a greater probability to be selected for infection and recover in the next step. If $\rho_s(k)$ is smaller, it indicates that the node with degree k tends to be in a steady-state, and in order to avoid damaging to the steady-state conditions, the selection probability $\rho_s(k)$ should be smaller.

(5) Perform steps (6) ~ (8) from $k=1$ to $k_{\max}$.

(6) Generate a new random number p, if $p \le p_s(k)$ then proceed to the next step, otherwise go to step (8).

(7) For the current node with degree k, if it is infected then go to step (8), otherwise find out the number of infected nodes among those k nodes connected with the said one, and take the number as s_k. Generate s_k random numbers p, if all these s_k random numbers p are larger than ν, go to step(8), otherwise change the node with degree k to an infected one.

(8) Let $k=k+1$, if $k>k_{\max}$, it indicates that all nodes have been infected, then go to the next step, otherwise go to step (6).

(9) Perform steps (10) ~ (12) from $k=1$ to $k_{\max}$.

(10) Generate a new random number p, if $p \le p_s(k)$, proceed to the next step, otherwise go to step (12).

(11) For the current node with degree k, if it is non-infected, go to step (12), otherwise generate a random number p, if p is larger than δ, go to step (12), otherwise change the node with degree k to an non-infected one.

(12) Let $k=k+1$, if $k>k_{\max}$, it indicates that all nodes have been recovered, then go to the next step, otherwise go to step (10).

(13) Go to step (3) to repeat the operation until the simulation ended.

Semi-quantitative Simulation Method

In order to meet the directors' needs of setting network countermeasure actions directly in simulative training and address some difficulties that some network countermeasure actions can't be described with mathematical formulas, this paper adopted the semi-quantitative simulation method with setting parameters for simulation of network countermeasure. Semi-quantitative simulation methods for some typical network countermeasure actions are provided in this paper as below. For simulation of other network countermeasure actions, similar approaches can be taken.

Table 1. Semi-quantitative simulation methods for network attacks

Actions	Parameters	Description
Worm attack	IP address of the attacked device Attack time Minimum waiting time delay Maximum waiting time delay	In OPNET, add a random number between the “minimum waiting time delay” and the “maximum waiting time delay” to the packets of the attacked device, to extend the queuing time of the packets, so as to reflect the effect of slowing down packet transmission as a result of slower network speed after attacks on the device.
Trojan horse attack	IP address of the host infected with Trojans Attack time Packet transmission frequency Packet length	In OPNET, the host infected with Trojan sends random packets (length is determined by the “packet length” value) in accordance with the “packet transmission frequency”, to simulate that the Trojan horse program secretly opens the port and sends data to the Trojan server after attacks of Trojans on the host.
IP spoofing	IP address of the attacking host IP address of the attacked host IP address of the spoofed host Attack time	In OPNET, when the attacked host sends packets, if the destination IP address of the packets is the same as the IP address of the spoofed host, packets are sent to and received by the attacking host, so as to simulate the effect of IP spoofing attacks.
Denial of service attack	IP address of the attacking host IP address of the attacked host Attack time	In OPNET, find the corresponding network device according to the “IP address of the attacked host” and change its parameters of the model, so that it can only receive the attacker's data, while discarding all normal service requests from other hosts, to reflect the characteristics of a denial of service attack.

Table 2. Semi-quantitative simulation methods for network defenses

Actions	Parameters	Description
Protection Level 1 (firewall + updating patch and antivirus software)	IP address of the protected host Protection time Success rate of protection	In OPNET, any action(such as sending a packet) taken by the protected host first generates a random number p, if p is smaller than the value of the “success rate of protection”, operations are carried on in the ordinary course, not affected by network attacks, so as to reflect the improvement effects brought about by taking protection measures.
Protection Level 2 (firewall + updating patch and antivirus software + IPS)		Ibid. However, because the “success rate of protection” at Protection Level 2 is higher than that at Protection Level 1, for each action taken by the protected host, its corrective probability is greater than that under Protection Level 1.
Protection Level 3 (firewall + updating patch and antivirus software + IPS + safety audit)		Ibid. However, because the “success rate of protection” at Protection Level 3 is higher than those at Protection Level 1 and Level 2, for each action taken by the protected host, its corrective probability is greater than those under Protection Level 1 and Level 2.

According to the parameters and rules given by the semi-quantitative simulation methods listed above, network attack and defense actions can be simulated. For example, for worm attacks, suppose the queuing time of packets is t_i in normal conditions, when the device is subjected to a worm attack, the queuing time of packets is:

$$t_i' = t_i + t_r \qquad (11)$$

Where, t_r is a random time between the “minimum waiting time delay” and the “maximum waiting time delay”.

When the protected host takes network defense actions, any actions (such as sending a packet) taken by it first generates a random number p , and then makes the following judgment:

$$t_i' = \begin{cases} t_i, & if\,(p < p_a) \\ t_i + t_r, & else \end{cases} \qquad (12)$$

Where, p_a is the success rate of protection, t_i' is the queuing time of packets after taking defense actions.

Conclusion and Future Work

To meet the simulative training application needs, the paper proposed a network countermeasure training simulation architecture, proposed a quantitative simulation method for virus spreading on scale-free networks, and presented a semi-quantitative simulation method for some network attack and network defense actions. Due to employment of detailed mathematical description, the quantitative simulation method has certain simulation fidelity; Applying with parameter setting, the semi-quantitative simulation method meets the practical application requirements of the simulative training, and addresses some difficulties that cannot be described with mathematical formulas. The follow-up researches will involve quantitative and semi-quantitative simulation methods on more network types and more network countermeasure actions.

References

[1] Jianjun Shen. Research on Operation Simulative Training in Information Age [C]. Applied Mechanics and Materials Vols. 411-414, 2013 2860-2864.

[2] Jianjun Shen, Kai Li, Yuqing Xu. Research on “Real-Network-in-the-Loop” Simulation Based on OPNET[C]. 2015 International Symposium on Computers & Information, 2015 655-661.

[3] Yan Zhou, Jianwei Dai. The Simulation Program Design of HLA. Publishing House of Electronics Industry, Beijing, 2002. (in chinese)

[4] Barabási A L, Bonabeau E. Scale-free networks. Scientific American, May 2003 50-59.

[5] Newman M E J. The structure and function of complex networks. SIAM Review, 2003(45) 167-256.

[6] Albert R, Barabási A L. Statistical mechanics of complex networks. Reviews of Modern Physics, 2002(74) 47-97.