The Study on the Network Security Simulation for HITLS Technology

MuDan Gu[1(✉)], HuiKui Zhou[1], YingHan Hong[2], and Li Zhang[1]

[1] Nanchang Institute of Science & Technology, Jiangxi, China
583517476@qq.com
[2] Hanshan Normal University, Guangdong, China

Abstract. Network security simulation model for HITLS technology is established, which aims to solve the problems in present network security simulation, that is, the network vulnerability and lack of network attack responses. This paper studies the implement methods of this model from the angle of basic structure, network security simulation frame and simulation controlling. The simulation environment based on network security simulation model for HITLS technology can provide fast and safe prototyping, demonstration, testing, and analysis, which evaluates the safety and performance of the equipment. By comparing the numbers of success for network communication before and after signaling and link attacking, the effectiveness of this method is verified. The model has broad application prospects.

Keywords: HITLS technology · Network security simulation · Attack effect simulation

1 Introduction

HITLS refers to the loop simulation, under the premises of meeting the conditions, which puts the object into the simulation system as much as possible and replaces the corresponding mathematical model. So simulation system is closer to the actual situation, and the credibility of the simulation can be drawn. There are some key technologies which needed to be solved in network security simulation, such as difficulties in network security model, lack of responses to the network attack in application and there is no uniform standard to evaluate the effect of such attacks on network security. Loop simulation system can have the actual hardware and software modules, so the loop simulation network simulation is not only more accurate than a simple inspection of protocols and algorithms, but also requires fewer hardware and software resources than the actual number of experiments with more good experimental manipulation, which can achieve a repeatable experiment, and can achieve a larger-scale network security simulation [1].

2 Network Security Model

2.1 Formal Description of Network Security Modeling Environment

Firstly, abstracted from the static model of computer network [2], namely supposes R is first in the network router set, H is the main engine set, L is the point-to-point link

This work was supported by jiangxi subject project: JXJG-13-27-8.

V.C.M. Leung et al. (Eds.): TridentCom 2014, LNICST 137, pp. 463–471, 2014.
DOI: 10.1007/978-3-319-13326-3_45

set, C is the sharing link set, then the whole network of routing topology is $T=(R,L,\varphi)$, and the mapping φ : $L\to R\times R$ said adjacency relations. If H and C is not empty then there is a division of $\{H_1,H_2,\cdots,H_n\}$ and $\{C_1,C_2,\cdots,C_n\}$, so $\forall i\in[1,n]$, $\exists r\in R$ and $N_i=(\{r\}\bigcup H_i,C_i,\varphi_i)$ constitutes a fully connected graph, including n for LAN quantity.

On the other hand, Data packet transmission based on the discrete dynamics of computer networks and discrete event systems (DEVS) match[3]. Thus, according to automata theory and discrete event systems, Network Modeling presented a general formal description of the environment. Modeling environment automaton M, namely a 7-tuple $(Q,V,\Sigma,\Gamma,\mathrm{Y},q_0,F)$, where：

① Q representative state sets;

② V representative Area. in set;

③ Σ Representative external events set;

④ Γ Representative internal affair sets;

⑤ Y Representative transfer function sets, and: $\mathrm{Y}=\begin{cases}\{\delta_{ext},\delta_{\mathrm{int}1}\} & \sum\neq\Phi\\ \{\delta_{\mathrm{int}2}\} & \sum=\Phi\end{cases}$

$$\begin{pmatrix}\delta_{ext}:Q\times\sum\times V\times N\xrightarrow{c_1}Q\times\Gamma\\ \delta_{\mathrm{int}1}:Q\times\Gamma\times N\xrightarrow{c_1,c_2}Q\times\Psi(\Gamma)\times\Psi(\sum)\\ \delta_{\mathrm{int}2}:Q\times\Gamma\longrightarrow Q\times\Psi(\Gamma)\times N\end{pmatrix}$$

And in the formula, N expresses the real clock, Ψ expressed that (event) the output function, c_1 and c_2 are the real-time constraints.

⑥ $q_0\in Q$ for initial state;

⑦ $F\in Q$ for termination state sets;

Here, V of the element indicates the reception and processing of those events, so $V\subseteq R\bigcup H\bigcup L\bigcup C$, Σ is M and external interaction packets sets. A list used to manage internal event to be processed, the table element $(\lambda,v,t)\in\Gamma$ value that is characterized by λ inside the event, will always be received and processed by v at t time. M, able to generate a variety of network models rely mainly on the rich behavior of the transfer function, where:

$\delta_{ext}(q_1,p,v,t)=(q_2,e)$, in state q_1 that receives the external event p (Area. in v, Time t) will cause the state transition to q_2, and produce internal affair e.

$\delta_{\text{int}1}(q_1, e_1, t) = (q_2, E, P)$, in state q_1 that receives the internal affair e (Time t) will cause the state transition to q_2 , produce internal affair E and external events subset P .

$\delta_{\text{int}2}(q_1, e_1) = (q_2, E, t_1)$, in state q_1 that receives the internal affair e_1 will cause the state transition to q_2 , Time advance to t and a subset of internal events generated E .

c_1 : $rt(\delta) < t_\delta$, Which $rt(\delta)$ return after the execution time value δ for the execution of $(\lambda_\delta, v_\delta, t_\delta)$ after δ list of minimum value of t event.

c_2 : $\delta_{\text{int}1}(q_1, (\lambda_1, v_1, t_1), t) = (q_2, E, P)$ established, if and only if $0 \le t - t_1 \le \varepsilon$, where t is the current time, and ε for the regulator.

2.2 Network Security Model of Virtual Degrees Are Classified

According to the description of modeling environment formalization , definition of models of virtual degrees division was further got. $M = (Q, V, \Sigma, \Gamma, \mathrm{Y}, q_0, F)$ [4] :

① When $V = R \bigcup L$ and $\Sigma \neq \Phi$, the resulting network model is semi-virtual. Model only subnet for virtual communication, the host is located external to interact with the data model.

② When $V = R \bigcup H \bigcup L \bigcup C$ and $\Sigma \neq \Phi$, the resulting network model is quasi-virtual. Events within the model were extended to receive and process all network elements can be abstract, so the model must complete the network virtualization layers.

③ When $V \subseteq R \bigcup H \bigcup L \bigcup C$ and $\Sigma = \Phi$, the resulting network model is all virtual.

2.3 The Network Security Model and Scale Fidelity

Modeling environment using the network model has generated the fidelity problem, that is, accuracy in expressing the real system model. Fidelity is a major measure for modeling, but because of the complexity and diversity of the real system, it is difficult to obtain the fidelity of the quantitative indicators, therefore it has to be measured from the model range, the details of the number, effectiveness and other a qualitative measure of respect. [5]

3 Based on HITLS Network Security Simulation Model

The simulation model of network security based on HITLS mainly includes the following several systems: HITLS technology network security test simulation subsystem, credibility validation subsystem, subsystems of safety evaluation simulation. The subsystems based on high level architecture[6], (HLA) were integrated together, convenient for users to use simulation control platform and the demo surveillance system simulation real-time monitoring and results check.

3.1 HITLS Network Security Simulation Model of Basic Structure

Network security simulation [7] can be divided into the following steps: preparation, execution and analysis. In the implementation process, monitor the whole process of simulation when making use of simulation and control platform, to ensure HITLS network simulation loop network data conversion completed in real time and interactive, while the simulation process can be collected in the corresponding statistical data. In addition, in order to improve simulation credibility, a subsystem for verifying the credibility of a simulation should be established to inspect and verify the whole process of simulation. Diagram of network security simulation model based on HITLS as shown in Fig. 1.

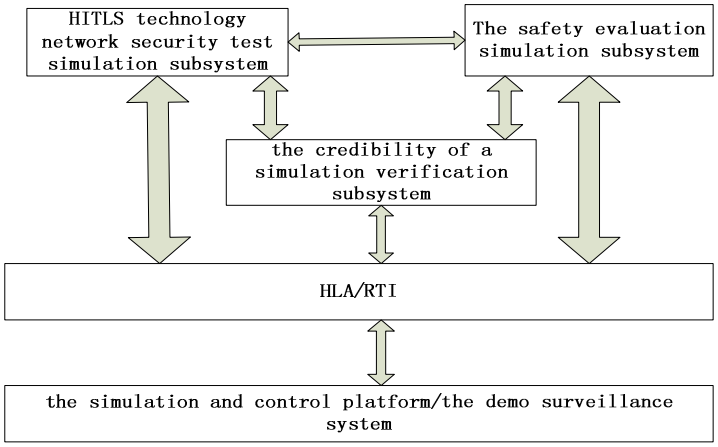


Fig. 1. HITLS diagram of network security model simulation

Network security simulation model based on simulation HITLS node will directly use the real network protocol stack TCP/IP protocol stack for the communication, the construction of the virtual node with a virtual network card, making the virtual node close to the real web presence. The virtual node network API calls directly through real TCP/IP network protocol stack to communicate with other nodes. The simulation environment management node is responsible only for construction of the link between the analog channels. And because of the direct use of real network pro-

tocol stack, the simulation results are reliable and accurate. Network simulation model is shown in Fig.2.

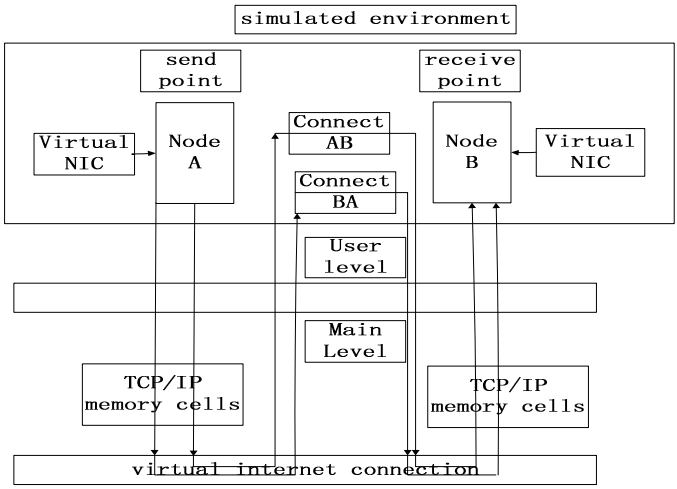


Fig. 2. Simulation model based on network security diagram HITLS

3.2 HITLS Based Simulation Framework for Network Security

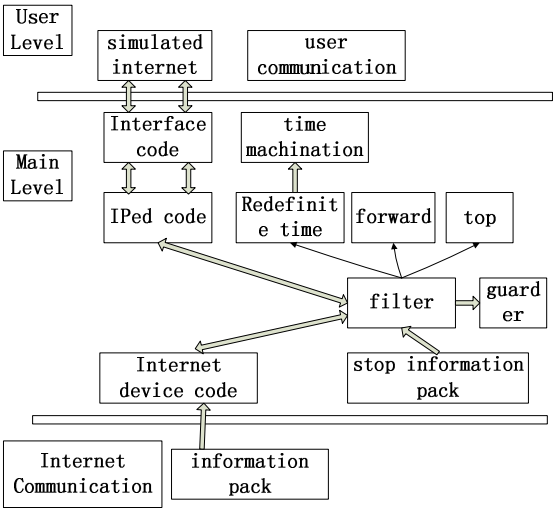
Based on the above model of new network simulation, we join simulation of the network environment and the real network environment due to the need for loop network simulation, Then we also need to provide a network emulation package intercepted, the implementation framework is shown in Fig.3 based on the design goals of general-purpose database. Intermediate driver: operate in the system kernel, and provide the underlying system functions and the hardware abstraction layer functions for the network interface user-level programs, to achieve hardware independence.

User-level library: operate in the user level, provide the main program with further abstract unified interface of the application program, call the intermediate driver to the next interface. Main documents: the application through the library calls interface applications that operate in the project that simulation platform.

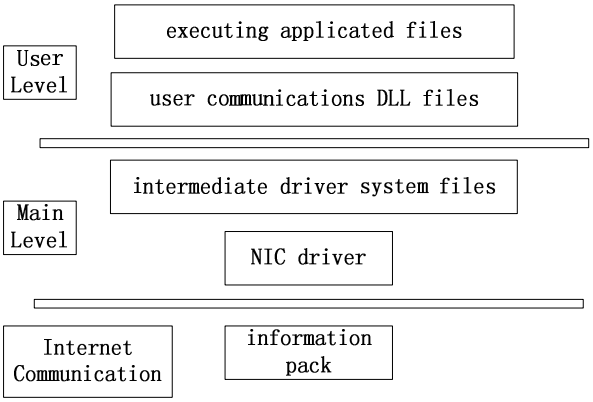
3.3 Based on Network Security Simulation Control of HITLS Technology

Simulation control is in the process of simulation, and operation of various simulation resources coordination and scheduling in general, including initialization, start, pause, resume, synchronization, stop, cancel, monitoring. In the OPNET simulation primarily through external control technology to achieve an external program of ESA OPNET simulation process control, ESA API is a set of OPNET provides external program interface functions, including simulation of process control, interface to access, input and output, blending the four function sets. Among them, the simulation process control functions are used to set an OPNET simulation and control events to advance and keep OPNET simulation clock. The interfaces to the main function is to provide external nodes and internal between the nodes for communication interface. Input/Output function will be responsible for the OPNET simulation data read or write. ODB pro-

vides the use of mixed-function to debug and observe the distribution of memory cells in memory and interaction.



(a) HITLS simulation model of network security framework



(b) File system simulation model of network security map

Fig. 3. Simulation Model Based on HITLS network security implementation framework

4 Based on Applications of HITLS Network Security Simulation Model

4.1 Simulation of Network Security Equipment

Simulation environment is established according to the network simulation model based on HITLS, provides fast prototyping, demonstration, testing and analysis. Specifically, establish the safety model and environment model under the premise of studying the basic functions and implementation principles of the safety equipment,

according to the design methodology and technical documents, and then design a variety of simulation experiments on the important security features and performance indicator simulation, and thus evaluate the safety and performance of the equipment.

4.2 Simulation of Network Attacks

Network attack simulation needs to establish the corresponding mathematical model or simulator using real network attacks, as many of the integration of existing instances of attacks and attack, for example, DOS attacks, worm propagation, DDOS [8] attacks, spoofing attacks, and then use these attacks against the system model or a variety of simulation experiments to study and verify the network parameters, the attacker when the attack effect parameters changes.

4.3 Simulation of Attack Effects

Target network and its traffic model for voice transmission to a public telephone network and its traffic model, attack models, including model and link signaling device attacks against equipment model, simulate, respectively, blocking malicious interference call and two e-attacks. Attack and attack the signaling link to the target network device model, the simulation run the entire network.

The simulation network operations, network operations in the process of collecting data such as throughput, delay and connection rate and so on. The connection rate, for example, attacks by adding, respectively, before and after the completion rate is shown in Fig.4 and Fig.5, by comparison, to analyze the attack effect. From the simulation results we have the following conclusions:

(1) Through the link to block interference, it can affect the data transmission route, add a link load, and interfere with the normal user's connection rate.

(2) By signaling attacks, for example, prevalent malicious network call information can be gathered to increase the network load, the user's information through the interference with the normal rate, in turn, can interfere with the normal operation of communication networks.

(3) Link blocking attack is to block a link, so that communication data transmitted by other routes, increasing the burden on other links. Signaling is active against a large amount of malicious traffic information transmitted through the network, increasing the burden of communication networks.

(4) Evaluation by means of attack, attack on the network effect was measured, and the link attacks and the effect of signaling the value of attack, the results are shown in Tab.1, table m that network communication distance.The average effect of two attacks were 3.27 and 1.68. Evaluation criteria for the attacker are able to give the following conclusions: the attack of two attack effect "significant"; signaling attack effect is slightly better than the link attack effect.

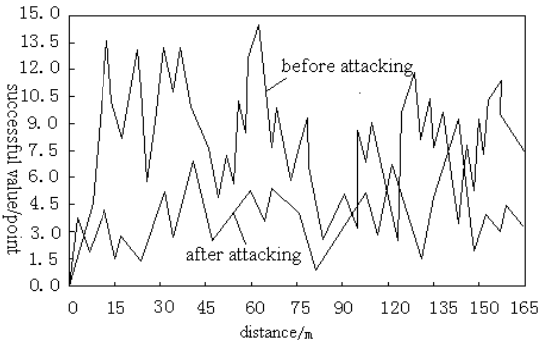


Fig. 4. Signaling attacks before and after the success of the number of network communication

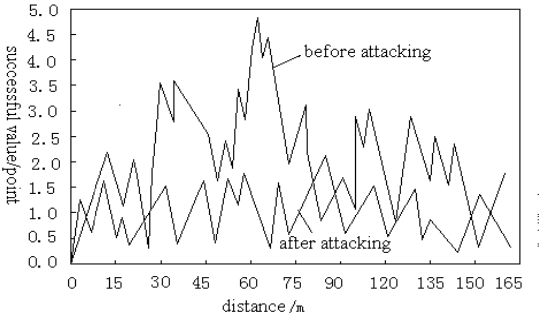


Fig. 5. Link attack before and after the success number of network communication

Table 1. Two attacking effect values

	Effect Value (link attack)	Effect Value (signaling attack)
m=0	3.0	3.0
m=15	2.0	3.7
m=30	4.3	2.3
m=45	3.2	1.2
m=60	4.0	2.4
m=75	2.0	1.5
m=90	6.3	1.2

5 Conclusions

Loop simulation is introduced into the network security simulation model, which establishes the simulation model of network security based on HITLS, including the formalized description, classification methods of virtual degrees and fidelity modeling of the network security modeling.

The simulation model of network security based on HITLS is established, which expounds on the system structure, the basic framework and the control of the network security simulation model.

The application of simulation model for network security based on HITLS is discussed, which studies the numbers of success of network traffic before and after signaling and link, and verifies the validity of the method. The model has broad application prospects.

References

1. Chen, Z.: TIFAflow: Enhancing Traffic Archiving System with Flow Granularity for Forensic Analysis in Network Security. Tsinghua Science and Technology **4**, 406–417 (2013)
2. Arun, M., Krishnan, A.: Functional Verification of Signature Detection Architectures for High Speed Network Applications. International Journal of Automation and Computing **4**, 395–402 (2012)
3. Saripalli, P., Walters, B.A.: Quantitative Impact and Risk Assess-ment Framework for Cloud Security Proceedings of IEEE 3rd International Conference on Cloud Computing, pp. 280–288 (2010)
4. Sjodin, M.: A study of Modeling and Simulation for computer and network security. University of Stockholm/Royal Institute of Technology (2005)
5. Tian, G.: A New Network Simulation Model Based on half Material Object-in-the-loop Simulation. Computer Engineering and Applications (2006)
6. Wang, S.Y., Kung, H.T.: A New Methodology for Easily Constructing Extensible and High-Fidelity TCP/IP Network Simulators. Computer Networks **40**(2), 257–278 (2002)
7. Yang, Xuelin: High-speed optical binary data pattern recognition for network security applications. Frontiers of Optoelectronics **5–3**, 271–278 (2012)
8. Webb, R.P., Yang, X.L., Manning, R.J., Maxwell, G.D., Poustie, A.J., Lardenois, S., Cotter, D.: All-optical binary pattern recognition at 42 Gb/s. Journal of Lightwave Technology **27**(13), 2240–2245 (2009)
9. Webb, R.P., Dailey, J.M., Manning, R.J., Maxwell, G.D., Poustie, A.J., Lardenois, S., Harmon, R., Harrison, J., Kopidakis, G., Athanasopoulos, E., Krithinakis, A., Doukhan, F., Omar, M., Vaillant, D., Di, N.F., Koyabe, M., Di Cairano-Gilfedder, C.: All-optical header processing in a 42.6 Gb/s optoelectronic firewall. IEEE Journal of Selected Topics in Quantum Electronics 18(2), 757–764 (2012)
10. Ren, W., Jiang, X H., Sun, T.F.: RBFNN-based prediction of networks security situation. Computer Engineering and Applications 42(31), 136–139 (2006)