RESEARCH ARTICLE

A Summary of Research on computer Network attack and Defense Modeling and Simulation

Ali J. Harriman, Alper Marshall

(Office of Engineering, Kafrelsheikh Engineering University, Egypt)

Abstract: Because of the sensitivity, real-time and large scale characteristics of the actual computer network application, it is not convenient to carry out the research work directly on the computer network, and use the modeling and simulation method to study the network attack and defense safety of the calculating machine. It not only can avoid the influence and damage to the actual computer network, but also has the advantages of flexibility, repeatability and low cost efficiency ratio. It can provide an effective reference for the practical security of the computer network. This paper summarizes the modeling methods and characteristics of computer network attack and defense behavior based on graph analysis and network worm behavior analysis, and analyzes the analysis method of computer network attack and defense effect based on cascade failure. And computer network attack and defense modeling and simulation system for security evaluation. Finally, the difficulties and shortcomings of computer network attack and defense modeling are analyzed, and the development trend in the future is forecasted.

Keywords: Computer network; modeling and simulation; network attack and defense; network security

1. Introduction

With the development of computer network technology, communication technology and its wide application in social, economic and military fields, computer network security has been paid more and more attention. Because of the sensitivity, real-time and large-scale characteristics of computer network applications, it is not convenient to carry out research work directly on them. Modeling and simulation methods can not only avoid the impact and damage to the actual computer network, but also have the advantages of flexibility, repeatability, low cost-effectiveness, and so on. They are used for computer network attack and defense. The study provides an effective way.

In this respect, scholars at home and abroad have carried out in-depth and effective research, and achieved rich results. There are different types of simulation methods, such as attack tree[1], attack graph[2], defense tree[3], epidemic model[4,5], packet model[6]. On the basis of the integration of modeling and imitating methods, a modeling and imitating system for computer network security assessment is developed, such as VCSE[7], NCR[8], NETWARS[9], GARNET[10], etc. However, due to the different application scale and characteristics of different methods and systems, there are still some problems and deficiencies in these methods and systems. For example, attack trees and attack graphs are too complex to understand and analyze when analyzing the attack and defense characteristics of large-scale networks, and most of them are only used for macro-level analysis such as network threats and risk assessment. Infectious disease model uses differential equations to analyze worm virus propagation in networks, although it has good expansion. Scalability can be used to analyze the propagation characteristics of worms in large-scale networks, but the application of the model is very good.

Many simplifications and assumptions neglect the network topology, data flow and link state changes, resulting in

doi: 10.18063/csnt.v1i2.

poor fidelity. Although packet method has good fidelity, it has low level of concern and poor scalability, and is generally difficult to apply to large-scale network worm analysis.

In order to make a better analysis of computer network security by modeling and simulation method and provide an effective reference for practical computer network security, this paper summarizes the latest representative achievements of scholars in this field in recent years from modeling methods, cascade effect modeling analysis, modeling system and so on. This paper analyzes the characteristics of different modeling methods, points out the difficulties and shortcomings in this field, and predicts the direction of further research, hoping to provide a more comprehensive support and reference for related fields.

2. Research on Modeling and simulation method based on graphic analysis

2.1 Modeling method of network attack based on attack graph

There are many methods for network attack modeling, such as attack tree, attack graph, Petri net and so on. These methods synthesize the vulnerability in the network and the attack action that the attacker may take.

Attack tree[1] is a method of denoting network attacks with tree graphics. It takes the ultimate target as the root node and the sub-target as the sub-node. It refines gradually until the leaf node represents the specific attack method. Attack tree method is mainly applied to macro level analysis such as network threat and risk assessment. Ten *et al*.[2] of Iowa State University used attack tree model to study the impact of different cryptographic mechanisms on the security of power monitoring computer networks. They take a specific computer in the attack monitoring network as the leaf node of the attack tree, and define the system threat index and the protection measure index as the vulnerability index of the system, and use the vulnerability index to measure the probability of the success of the system attack. Yan Fen *et al*.[12] based on the traditional attack tree attack modeling, redefined the attack node and quantified the attack risk of the leaf node, proposed a MLL-AT (multi-level hierarchical attack tree) modeling attack idea and method, which can represent multi-stage network attacks, and can distinguish different attacks. The different security threats of the attack sequence to the system.

Attack graph is a set of attack preplan set, which takes network topology information into account[2]. In order to overcome the shortcomings of manual, slow speed and lack of quantitative analysis, Wang *et al*.[13] improved the traditional attack graph model by using Bayesian network, and established an automatic Bayesian attack graph model. The model infers and evaluates the possible situation of each network node, establishes a probability model, detects the key vulnerable nodes of the network by the size of the probability and provides network security recommendations. Jajodia *et al*.[14] of George Mason University put forward the concept of Topological Vulnerability Analysis (TVA), which can analyze the relationship among network vulnerabilities and automatically generate network vulnerabilities by using the connection relationship between networks, combining information such as IDS, antivirus software and various vulnerability databases. Attack graphics. TVA can also simulate multi-step network attacks based on different network configurations and vulnerability models, identify critical vulnerabilities of the network and automatically generate network security recommendations. However, when the network nodes and links increase, the TVA complexity increases rapidly and the scalability is poor.

Simply relying on attack graph to analyze vulnerability and security of large-scale networks, the graph is often too complex to understand and analyze. To overcome this shortcoming, Noel *et al*.[15] added an adjacency matrix to the attack graph, mapped the edges of the attack graph into matrix elements, and mapped the nodes of the attack graph into rows or columns of the matrix, which greatly simplified the attack graph. To give a simple example, assuming that there are 100 fully connected hosts with one vulnerability per host, the resulting attack graph will have 100 nodes, 1000000 edges, which is difficult to view and analyze; if represented by adjacency matrix, using

The matrix of 100 x 100 can show that the degree of visualization is greatly enhanced. The attack graph adjacency matrix element can only directly represent the single step attack.

In order to effectively analyze multi-step attacks, Noel *et al*.[15] can also calculate the high power of adjacency matrix to obtain the possible occurrence of multi-step attacks. For example, the K power of adjacency matrix can be used

to represent the possible occurrence of k-step attacks, and the minimum attack steps between each pair of nodes can be calculated and predicted. Attack source. Ne-ol and others put forward the concept of risk adjacency matrix, which uses non-negative values to represent the elements of adjacency matrix, and color depth to represent different risks in visualization. The degree further increases the readability of the attack graph, which is conducive to further analysis of the attack graph.

2.2 Network defense modeling method based on defense graphics

Effective network defense should include various mechanisms, such as attack prevention, detection, source tracking and network protection. For these mechanisms, defense trees, Intelligent Graphics and other network defense modeling and analysis methods have emerged.

Defense tree is a graph of network attack path analysis which is obtained by adding network security measures on the basis of attack tree. Based on the concept of defense tree, Bistarelli *et al*.[3] combined with conditional preference network to optimize the defense measures that may be used in network security, and evaluated the changes of network attack behavior after taking optimized defense measures. Sommestad *et al*.[17] put forward a method to build defense tree using extended influence diagram. The influence diagram is a acyclic directed graph G = (N, A), which is composed of node set N and arc set A. To some extent, influence diagrams can be regarded as a Bayesian network. The defense tree can be easily formed by adding defense decision in the extended influence diagram, and the success probability of attacking target or its sub-target can be calculated by using conditional probability table.

In order to react reasonably to network attacks and predict the types, characteristics and possible effects of attacks, Scott *et al*.[18] proposed an intelligent graphics method to quickly assess the similarity between the detected behavior and the original or learned attack model or normal model. And issue an alarm. Users can use intelligent graphics to visually see the cause of the alarm and take further measures.

3. Research on Modeling and Simulation method based on Network Worm behavior Analysis

Network worm attack is one of the most common and effective attack methods. It is flexible, controllable and reproducible to study worm spread by modeling and simulation.

3.1 Infectious disease model

The transmission of worm virus in the network is similar to that of the infectious disease in the social domain, so the analytical model obtained in the study of infectious disease can be directly applied to the simulation of the transmission of the network virus. At present, SI, SIS, SIR, AAWP, IWMM and two-factor models are the main models of viral transmission behavior based on infectious disease model. It approximates the spread of the network virus to the spread of the epidemic, classifies the hosts in the network into infected hosts, susceptible hosts, moving out of the main computer, etc., through the number of different types of hosts, the infection coefficient, etc. Establishment of Mathematical Analytical Modules with time and Equal parameters The simulation results can be calculated and drawn by Mat- lab and other mathematical analysis software.

The differential equations set up by the number of different types of hosts, infection time and infection coefficient is a deterministic equation set; another equation set with stochastic characteristics can be established by calculating the state of the same node at different time points and the transformation probability between them, that is, by Monte Carlo method. Differential equations[19]. The state of a node and its state transition probability are related to its own state, the state of the node it contacts and the characteristics of the network. Existing network models rarely consider the impact of network topology on worm propagation. Zhang Wei and others of Beijing University of Posts and Telecommunications[20] proposed a worm propagation model based on network topology unit. The model divides worm propagation based on network topology into two parts: one is network structure analysis, which decomposes complex network into general network structure units, including Node-to-neighbor-node, Node-to-node, Multi-nodes-to-node, and the other is to calculate worm virus on-line. The propagation of worms in the whole network is calculated by using proba-

bility matrix. This method provides a way to accurately calculate the time of infection of worms in different locations.

The greatest advantage of virus propagation behavior model based on infectious disease model is its good scalability, which can simulate the network of millions or even tens of millions of nodes. However, on the one hand, this model can only reflect the general characteristics of worm propagation at the macro level because of many simplifications and assumptions; on the other hand, this method focuses on the mechanism of network virus propagation to show the changes of the number of different types of nodes in the network with time, ignoring the topological structure of the network. The change of data traffic and link state is deficient in fidelity.

3.2 Packet model

In order to reflect the impact of network protocol, topology, traffic and other network environment details on worm propagation in scalable network model, a packet-level worm propagation behavior modeling is proposed.

Deng Jie and others of Tsinghua University[6] designed and implemented a low-cost and high-performance network worm experimental environment based on SFNet, which can be used to model and simulate the network and worm in fine-grained packet level. This method divides and designs the main function modules of infected hosts, including target IP acquisition, worm packet generation, packet transmission timing, etc. The worm propagation is simulated as UDP packet transmission in the network. In addition to reflecting the change of the number of infected hosts with time, the packet-level model can also reflect the infection time of any host in the network, the influence of different initial infected hosts on the spread of worm virus, and the influence of scanning strategy on worm spread. In order to simulate worm propagation on a larger scale on a realistic basis, Kalyan *et al*. of Georgia Institute of Technology designed a packet-level "all-virtual system"[21]. The virtual system abstracts the endpoints in the network through the virtual machine technology, and realizes the unity of high simulation and high scalability to a certain extent.

Packet-level worm simulation can reflect the impact of network traffic and network topology on worm propagation, and can also reflect the use of defense strategies to a certain extent. However, because of the low level of concern, this method needs a higher computer resource consumption in building simulation truths, which can not be used in large-scale networks. Worm modeling and simulation.

3.3 Hybrid model

In view of the advantages and disadvantages of infectious disease modeling and data packet modeling, Lijenstam *et al*. of Dartmouth University Safety Technology Research Center proposed and implemented the concept of "hybrid model"[22]. Mixed model is divided into two layers: worm propagation infection model, worm scanning caused traffic model and routing information traffic change model. At a higher level, the spread of worm virus adopts the epidemic model; at a lower level, the network traffic changes caused by network topology, node distribution, protocol and virus scanning are fully considered. Different simulation mechanisms are used in different hierarchical models: infectious disease model is based on time running; packet model is based on event running. The two are coordinated by a single loop event timer.

Hybrid model simulation combines the advantages of infectious disease model and package-level model, and makes a compromise between simulation fidelity and scalability. However, the design of this method is difficult. It is necessary to distinguish reasonably between macro-level and micro-level according to the research purpose, and realize the interaction of different level models.

3.4 Network defense modeling method based on benign worms

The initial introduction of network worms is to carry out scientific computing and large-scale network performance testing, network worms themselves also reflect the characteristics of distributed computing, so we can design benign worms to defend against network malicious worms. Benign worms, borrowing from the medical concept of "attacking viruses with poison", can spread like ordinary worms, patch vulnerable hosts or remove worms from infected hosts[23].

Benign worms also scan the network when they propagate in the network, resulting in network congestion. Wang Chao *et al*.[24] proposed a novel hybrid benign worm model, that is, active strategy is adopted in the prophase of benign worm propagation, scanning the network of susceptible hosts and infected worms hosts to spread benign worms; When

the infected host is scanned to a benign worm host, it will be infected by a benign worm. On this basis, Zhou Hanson *et al*.[25] analyzed the optimal switching time of active and passive strategies, deduced the mathematical model of benign worm propagation and simulated it. Zhang Dianxu *et al*.[26] designed a SRF diffusion model, which adopted the ordering, grading and RRH-1 propagation strategy in the scanning phase, could greatly reduce the scanning detection flow, and could accurately control the creep in the propagation phase by combining the finite propagation algorithm with the frequency adaptive dynamic copy control mechanism. The number of insect replicas enables its traffic to reach a controllable level.

4. Modeling and analyzing method of network attack and defense fect based on cascading failure

In the modeling and analysis of computer network attacks, network robustness or survivability is one of the important research directions. It refers to the network in the case of random failure or deliberate attack, in the case of node or edge damage, the network can still maintain function or provide services. The cascade failure of the network considers the cascading reaction caused by the failure of the nodes, and the coupling relationship between the nodes will eventually lead to the collapse of part or even all of the network.

4.1 Network cascading failure modeling based on network static attributes

It is found that scale-free networks are robust to random attacks, but they are vulnerable to deliberate attacks, i.e. scale-free networks are "robust yet fragile"; and random networks are robust yet fragile against random attacks or deliberate attacks. Attacks are robust. Cohen *et al*. used seepage theory to analyse the robustness of the network, and gave a critical value method to calculate the network collapse caused by node removal[29]. At the same time, how to optimize the network with specific properties to obtain optimal robustness is also one of the focuses of many researchers. Valente *et al*.[30] considered that the network with more robustness in the case of random failure or deliberate attack has a bimodal distribution, while satisfying the above two conditions, the network optimal distribution has a trimodal distribution which can also increase the network robustness to fault and attack by adding or reconnecting edges.

The above literature focuses on the static properties of the network, and studies the effects of node or edge addition and removal on the network performance, including the degree distribution, shortest path, clustering coefficient and other network parameters, without considering the dynamic redistribution process of network load traffic caused by node addition or removal.

4.2 Network cascading failure modeling based on traffic reassignment

Failure of nodes in the network will lead to the redistribution of network load flow. In the case of limited bandwidth capacity of nodes, load redistribution may cause the load on some nodes to exceed their bandwidth, resulting in node failure, and then network cascade failure. Considering these factors, Motter and Lai[32] establish a load capacity linear model (ML model), and give the conditions of global cascading: the network has a highly heterogeneous load distribution and needs to remove high load nodes. Dou Binglin[33] of Fudan University and others proposed a nonlinear load capacity model with two variables on the basis of ML model, and simulated cascade failure in B-A scale-free network and Internet AS level network, which verified the feasibility of the model. Compared with ML linear model, this model has higher performance of resisting cascade failure and lower investment cost with higher robustness. However, this conclusion is obtained under the assumption that the nodes send the same traffic per unit time through the shortest path, and in the discussion of cascading process, it is assumed that when the load exceeds the node capacity, the nodes will be removed from the network without considering the control of network traffic and congestion.

Zhu Tao *et al*.[34] Aiming at the phenomenon that the nodes in the cascade failure model usually only have two states of "normal" and "failure" and are deleted from the network immediately after failure, a "load" function is defined for each node to represent the degree of node congestion, and different attackers are analyzed. The effect of the formula on cascade failures of networks with different network structures, different tolerance coefficients and different protection modes. However, the proposed cascade failure model has many simplified assumptions, which need to be supple-

mented and improved in combination with the practical application background.

5. Research on Modeling and simulation system for safety assessment

Computer network attack and defense modeling and simulation system can integrate various modeling methods, provide mature modeling tools, friendly modeling environment, greatly improve the efficiency of Network Security Modeling and analysis.

In order to evaluate the network security situation, Ingols *et al*.[35] incorporated the common attack graph into the multiple prerequisite graph and developed a NetSPA system. The system is an end-to-end attack graph generation and analysis tool. It defines a simpler network model to facilitate the system to automatically collect network data. To a certain extent, it solves the problem of automatic collection of network data and the problem of scalability of attack graph generation algorithm. NetSPA system can build a network attack graph model with 50000 hosts in 12 minutes and provide network defense suggestions. But once the vulnerability information and location of network nodes change slightly, MP graph must be regenerated, and the scalability is poor. When the nodes are too many, the graphics will be too complex and difficult to understand. GARNET system[10] optimizes the visualization technology of NetSPA system to a certain extent, but the system does not quantitatively analyze the vulnerability information of the network, only qualitative judgment, lack of credibility. To effectively evaluate the effectiveness of computer network operations, the United States has developed a Virtual Control Systems Environment (VCSE)[7], a National Cyber Range (NCR)[8], and a Network Warfare Simulation environment. NETWARS][9][36], etc. VCSE is a comprehensive simulation bed environment developed by Sandia National Laboratory for security analysis of computer network control systems. It can be used to analyze the relationship between control systems and infrastructure, determine the effective ways of network attacks, the vulnerabilities of the system, and the performance of the system after network attacks. NETWARS is a network operation simulation system for military communication network analysis. It uses the communication network modeling mechanism of "transceiver-communication equipment-link-communication service-combat platform-combat force" to evaluate the performance of military communication network at joint task force level. NCR is a simulation test bed specially used in the United States to enhance the national defense capability against network threats. It uses large-scale multi-resolution model to model the information infrastructure network and evaluate the network attack effect. It can provide an adaptive, multi-dimensional and heterogeneous comprehensive experimental platform for related research.

Because of the complexity of computer networks, such as large scale, heterogeneity and growth, it is very difficult to describe them by a single modeling method. Elder *et al*.[37] of George Mason University in the United States put forward the idea of integrated modeling by using various methods such as social network, complex network and agent-based modeling, and provided Pythia, Temper and ORA modeling tools. At the same time, systems and platforms such as CyberSim[38], Cauldron[39], network application and simulation middleware Bionet[40] based on the principle of bionics, which are used to simulate the spread of malicious software in large-scale network, also provide a good model for computer network attack and defense. Reference resources.

6. Concluding remarks

The main difficulties of computer network attack and defense modeling are as follows: on the one hand, computer network itself has large-scale heterogeneous dynamic characteristics, it contains a large number of node links, the network with different functions communicate with each other, the network itself has dynamic connectivity and growth characteristics; on the other hand On the one hand, computer network attacks have diversity, such as worm, Trojan horse, DDoS attacks, rogue software, and so on. Different attacks aim at different vulnerabilities of computer systems, and the attacking characteristics and effects are different.

The problems brought about by the characteristics of computer network mainly focus on the acquisition of network security data, which are embodied in the following aspects: the large-scale characteristics of network affect the integrity of security data acquisition; the dynamic characteristics of network structure affect the accuracy of security data; heterogeneous network and the lack of centralized management not only make network security The difficulty of data acquisition increases, and the format of data acquisition is not uniform, which brings many difficulties to modeling and anal-

ysis. Objectively speaking, most of the existing computer network attack and defense modeling methods are only for a region, a certain enterprise level of computer network security analysis, has certain limitations. The diversity of attack modes of computer networks leads to the diversity of attack and defense modeling methods, such as attack tree, attack graph, Petri net, worm virus propagation model, etc. Most of these modeling methods can only model and analyze one attack mode, and the similarity between them is very small, so it is difficult to form a network. Comprehensive analysis of safety situation.

To sum up, computer network attack and defense modeling still has many shortcomings and has great room for development. Firstly, the computer network itself can be used to strengthen cooperation and develop new information acquisition technologies to improve the integrity, accuracy and format of network security data. Secondly, the computer network itself is similar to complex networks and complex adaptive systems in structure, behavior and characteristics. The multi-agent method can be used to model the network attack behavior, and the complexity theory can be used to analyze the statistical and evolutionary characteristics of the network, such as the degree distribution of the network nodes, the average distance change and the cascade failure characteristics of the network. With the continuous development of computer network technology and application, computer network security will be paid more and more attention. Network attack and defense modeling for computer network security analysis has broad application prospects.

References

1. Dai YH, Wu KK. Application of attack tree in multi-layer network attack model [J] . Network Security Technology and Application 2009; -1: 75-76.
2. Wang GY, Wang HM, Chen ZJ. Modeling method of computer network attack based on attack graph [J] . Journal of National University of Defense Science and Technology [J].
3. Bistarelli S, Fioravanti F, Peretti P. Using CP-nets as a Guide for Countermeasure Selection [C]. Proceedings of the 2007 ACM symposium on Applied computing, Seoul, Korea 2007; 300: 304.
4. Onwubiko C, Lenaghan AP, Hebbes L. An Improved Worm Miti- gation Model for Evaluating the Spread of Aggressive Network Worms [J]. EUROCON, 2005.
5. Su F, Lin ZW, Ma Y. Worm Propagation Modeling based on Two-Factor Model [C]. In: Pro. Of the IEEE 2009; 978-1-4244-3693-4 / 09.
6. Deng J, Duan HX. Fine-grained modeling and simulation of worm propagation based on SSFNet[J] . Minicomputer system 2008; / 29(1).
7. Andjelka K, Drake EW, Laurence RP. Cyber and Physical Infrastructure Interdependencies [R]. SANDIA REPORT SAND 2008; -6192 September 2008.
8. Barbara MQ, Michael VP. National Cyber Range[R]. DARPA, 2010.
9. ETWARS Model Development Guide (Version 3.0) [S]. De- fense Information Sys tem Agency & NETWARS Program Manage- ment Office, 2007.
10. Williams L, Lippmann R, Ingols KW. Garnet: A graphical attack graph and reachability network evaluation tool [C]. In Proc. of VizSEC 2008.
11. Ten CW, Manimaran G, Liu CC. Cy- bersecurity for Critical Infrastructures: Attack and Defense Model ing [J]. IEEE Transactions on Systems. Man. and Cybernetics-Part A Systems and Humans, Jul 2010; 40 (4): 8, 5 - 8, 6, 5.
12. Yan F, Yin XC, Huang H. Study on modeling method of network attack based on MLL-AT [J] .Acta Sinica (J).
13. Wang CL, Wang YC, Dong YF, Zhang TL. Novel Comprehensive Network Security Assessment Approach[C]. In Proc. of IEEE ICC 2011.
14. Jajodia S, Noel S. Topological Vulnerability Analysis: A Pow- erful New Approach for Network Attack Prevention, Detection, and Response [J]. Indian Stat. Institute Monograph Series, Sin- gapore, 2009.
15. Noel S, Jajodia S. Understanding Complex Network Attack Graphs through Clustered Adjacency Matrices [C]. In Proceed-ings of the 21 Annual Computer Security Applications Confer-ence, Tucson, Ariz Ona, Dec. 2005; 1063-9257 / 05.
16. Ye Y, Xu XS, Jia Y. Study on the risk adjacency matrix based on attack graph [J] .Acta Sinica 2011; (5).
17. Sommestad T, Ekstedt M, Johnson P. Combining defense graphs and enterprise architecture models for security analysis [C]. Pro- ceedings of the 12th IEEE International Enterprise Computing Conference , September 2008.
18. Evans SC, Markham TS, Bejtlich R. Network Attack Visualization and Response Through Intelligent Icons [C]. IEEE 2009.
19. Zou CC, Towley D, Gong W. Email virus propagation modeling and analysis [R]. Technical Report TR-03-CSE-04v 2003.
20. Zhang W, Guo SZ, Zheng KF. Net worm propagation Model Based on network topology unit [C]. International Confer- ence on Multimedia Information Networking and Security 2009.
21. Perumalla KS, Sundaragopalan S. High-fidelity modeling of computer network worms [C]. In: Proceedings of the

20th Annual Computer Security Applications Conference (AC- SAC'04) Mber 6-10 4.
22. Nicol D, Liljenstam M, Liu J. Multi-scale Modeling and Simulation of Worm Effects on the Internet Routing Infras-truc- ture [C]. International Conference on Modeling Techniques and Tools for Computer Performance Evaluation (Performance TOOLS): 1-10.
23. Zhou HX, Zhao H. Modeling and Analysis of active benign Worm and mixed benign Worm[J] .computer research and development
24. Wang C, Qin SH, he JB. Adversarial worm based on mixed confrontation technology[J] .Acta Sinica 2007; (1)
25. Zhou HX, Zhao H. Modeling and Analysis of mixed benign Worm[J] .computer research and development.
26. Zhang DX, *et al*.Study on SRF diffusion model of benign worm [J] .Computer Engineering and Science.
27. Xia YX, Hill DJ. Attack Vulnerability of Complex Communication Networks [J]. IEEE Transactions on Circuits And Systems-II: Express Briefs, January 2008; 55 (1).
28. Deng HZ, Wu J, Li Y. Cascade failure model and analysis in double-layer small-world networks [J] .Computer Simulation 2008; 25 (10).
29. Cohen R, Erez K, ben-Avraham D, Havlin S. Breakdown of the internet under Intentional Attack [J]. Phy. Rev. Let (S0031-9007) 9007 (16): 3682-3685.
30. Valence AX, Sarkar A, Stone HA. Two-Peak and Three-Peak Optimal Complex Networks [J]. Phys. Rev. Let (50031-9007) 50031 (71): 118702 (4).
31. Hayashi Y, Matsukubo J. Improvement of the Robustness on Geographical Networks by Adding Shortcuts [J]. Physics A (S0378-4371) 2007; 380: 552-562.
32. Motter AE . Cascade Control and Defense in Complex Networks[J].Phys.Rev.Let 2004; 93 9): 098701(4)
33. Dou GL, Zhang SY. Loading capacity Model of Cascade failure on complex Networks [J] .Journal of system Simulation: 23 (7).
34. Zhu T, Chang GC, Zhang SP, Guo RX.Study on command and control level failure model based on complex network [J] .Journal of system Simulation 2010; (8).
35. Ingols KW, Lippmann R, Piwowarski K. Practical attack graph generation for net-work defense [C]. In Proc. of ACSAC, 2006.
36. Hu XF, Wang ZY, Si GY.Overview of modeling and simulation of Cyberspace[J] .Proceedings of the Chinese Academy of Electronic Sciences.
37. Elder RJ, Levis AH. Use of Multi-Modeling to Inform Cyber Deter-rence Policy and Strategies [R]. George Mason University. Washington, DC, June 10-11 / 2010.
38. Santhi N, Yan G, Eidenbenz S. Cyber- Sim: Geographic, Temporal, and Organizational Dnamics of Mal- ware Propagation [C]. Proceedings of the 2010 Winter Simulation Conference 2010; 2876-2887.
39. Jajodia S, Noel S, Kalapa P, Williams J. Cauldron: Mission-Centric Cyber Situational Awareness with Defense in Depth [C] .The 2011 Military Communications Con- ference-Track3 Cyber Security and Network Operations 2011; 1339-1344.
40. Suda T, Nakano T, Moore M, Enomoto A, Fujii K. Biologically Inspired Approaches to Net-works: The Bio-Networking Architecture and the Molecular Communication [C]. Sp Ringer-Verlag Berlin Heidelberg 2008; 241-254.