Worm Propagation Simulation System Oriented Description Language

Mr Manish Khule[1] Ms Neha Sharma[2]
[1,2]Assistant Professor
[1,2]SCSIT, Indore, India

Abstract— Software simulation is one of the most common methods to study worm propagation. However, simulation process and software interface, which lack unified description, cause inefficiencies of worm propagation simulation. In order to achieve a unified description for worm propagation simulation process, we propose a Worm Propagation Simulation Description Language (WPSDL), which characterizes the software interfaces and parameters of each module in simulation process in a unified way. Meanwhile, we develop a simulation system of worm propagation oriented our presented language. In this system, we use related commands of the description language as interactive instructions, and then implement worm propagation simulation for different types of network worms. In addition, we conduct a series of experiments to analyse the impacts of worm propagation mechanism and network topology structure. The experiments show that increasing infection ability and scanning rate can improve the propagation scale significantly, and the propagation delay can influence the outbreak time and explosion intensity of worm propagation. The experiments not only provide support for the study of worm propagation mechanisms, but also verify the practicability of the description language and the simulation system.

Keywords: Worm Propagation, Network Security, Computer Network, WPSDL

I. INTRODUCTION

The prosperity of the Internet has created favourable conditions for the spread of network worms. The increasing complexity of network structure leads to the diversity of propagation scenarios and the increase of infection scale. The development of information interaction technique among online social network users improve propagation methods of network worms, and it brings more difficulty to the detection of network worms [1]. The official website report [2] pointed out that the number of network worms' outbreaks and the resulting damage have been increasing year by year. Network worm bringsa huge threat to network security. Therefore, the study of propagation mechanisms has become one of the important topics in field of network security. At present, there are two main categories of the research methods of worm propagation: mathematical analysis model and software simulation. Requirement.

Current mathematical models of modelling worm propagation are mostly based on the epidemic model. Staniford proposed the simple epidemic model (SEM) in the form of differential equations [3].Zou considered the factors of network congestion and host defence to put forward the two factors model (TFM) [4]. The presented model is not limited by network scale. Thus, this model has high computation efficiency. Meanwhile, it can also simulate worm propagation in large-scale networks quickly. However, the drawback of this method is that the factors taken into account are in comprehensive, and it cannot evaluate the impacts of network situations factors such as background traffic and network delay. Software simulation is usually based on network and worm simulation tools [5]. This method can take full account of the impacts of network factors and worm characteristics on the propagation process, thus attracting more attention recently. The ETH Zurich TIK worm simulator developed by the ETH Zurich University pays attention to the simulation of the worm characteristics. It can set parameters such as the scanning strategy, scanning rate, and infection ability of worms, and has good simulation results [6]. The worm simulator based on SSFNet or NS2 focuses on the network characteristics. It can realize packet-level worm propagation simulation and improve simulation accuracy [7]. In addition, with the development of distributed technologies, distributed worm simulators based on GTNetS or PDNS can implement packet-level simulation in a million-level network, and have achieved good results in both network scale and simulation granularity [8].As we can see from above, there are some achievements in the research of worm propagation software simulation. However, there are some unsolved problems as follows: On the one hand, because of simulating behaviours of worms through different methods, there is an in consistency between simulation process and software interface for propagation simulation; On the other hand, according to some requirements in the simulation process, researchers cannot configure the network situations and related worm propagation parameters flexibly and uniformly in current simulation software. Thus, we propose a unified worm propagation simulation description language, and the develop a corresponding worm propagation simulation system.

II. PROCESS OF WORM PROPAGATION SIMULATION

In order to propose a unified description of worm propagation simulation, firstly, we sort out the general process of worm propagation simulation. Secondly, we present a worm propagation simulation description language. Finally, we develop a novel worm propagation simulation system oriented this language .The propagation simulation process is shown in Figure 1. Firstly, it uses the network generator and worm generator to obtain the network required for simulation, and the worms will spread in the network. Secondly, it enters the propagation simulation module, which completes the simulation of worm propagation by simulating behaviours of worms. After the propagation simulation is completed, the visualization module follows, which completes the visualization of the network topology and the visualization of the worm propagation process. Finally, the result is stored and the simulation process is terminated. In order to achieve unified scheduling and management of the entire process, we propose WPSDL. This language defines the commands and related parameters in each stage of the process. At the same time, the language can be used as the human-computer interaction instruction in the corresponding worm

propagation simulation system. The specific design of WPSDL will be described in detail in the next section.

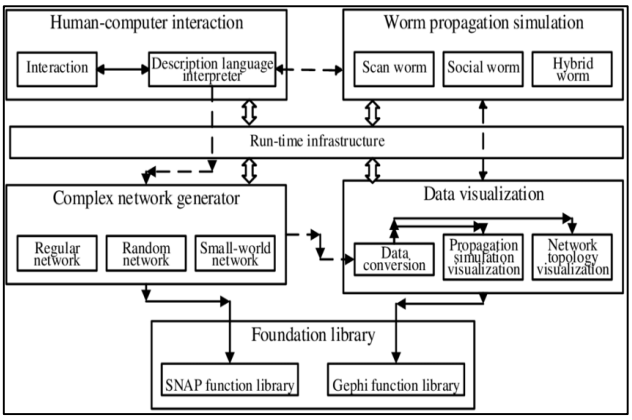

Fig. 1003A Process of visualized worm propagation Simulation

III. WORM PROPAGATION SIMULATION SYSTEM ORIENTED WPSDL

We develop a worm propagation simulation system with visualization capabilities oriented the WPSDL. This system can simulate the behaviours of worms in application layer. The system structure is shown in Figure 2 and functions of each module are illustrated as follows.

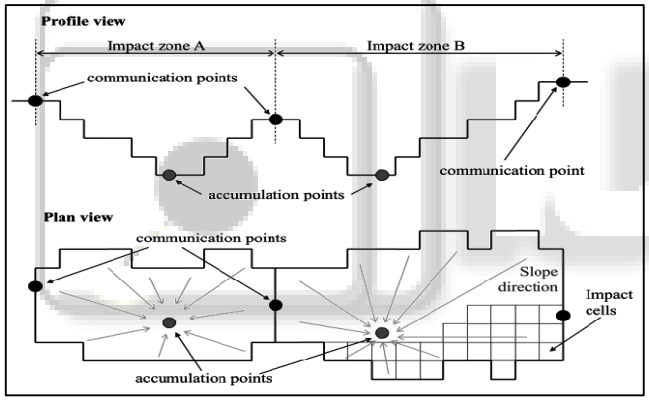

Fig. 2: Structure of system oriented WPSDL

Description language interpreter: Interpreter receives user entering commands. Then parses the commands and parameters, and calls the related functions in complex network generator to complete the following process of network generation. Complex network generator: This module generates the network used in worm propagation simulation. According to different commands and parameters, a complex network generator can generate different types of networks, such as regular networks, random networks, and small-world networks. At the same time, users can configure the network's parameters, such as IP address range, IPaddress prefix, the size of AS, and defence probability. Worm propagation simulation module: This module simulates different behaviours of worms and including propagation process of scanning worms, social worms and hybrid worms. In this module, the worm's scanning rate, propagation delay and repair method can be configured according to the experimental requirements. In addition, scanning worms can spread in the network with different scanning strategies such as random scanning [9], replacement scanning [10], and divided scanning [10]. For social worms, their message sending strategies include directed sending, all sending, and random sending [11]. Data visualization module: This module implements visualization function of worm propagation and network topology. Firstly, the data conversion module receives the worm simulation data and the network topology data. Secondly, it converts them into time-ordered data with uniform format. Afterwards the functions of visualization add labels and attributes to the data and integrate two aspects of data into a Gexf format file. Finally, the library function in the underlying platform can achieve a graphical display of the data in the Gexf file.

The foundation library: The foundation contains a set of basic functions used in the system implementation process, which mainly includes Stanford Network Analysis Project (SNAP) function library and Gephi function library. The SNAP function library provides a series of basic functions for complex network generator to generate different types of networks. The Gephi function library provides basic functions to display Gexf format data and set colour and size of elements.

IV. EXPERIMENTS AND ANALYSIS

In this section, we analyse and verify the influence of network topology characteristics and worm characteristics on propagation. We conduct our experiments on a personal computer running Windows. It has 8 GB RAM and an Inter i5 CPU of 3 GHz. In the experiments, we analyse the impacts of different parameters on propagation by means of control variables. At the same time, we reduce the impacts of accidental factors by taking the average of multiple experiments.

Firstly, we verify the impacts of the network topology characteristics on propagation. In this experiment, we generate the network with different topological features (ER random network, powerlaw network with exponent -4 and power-law network with exponent -2 [12]). Then we compare the propagation process of social worms in those networks. The command is shown in Figure 3 and the results of the experiment are shown in Figure 4.

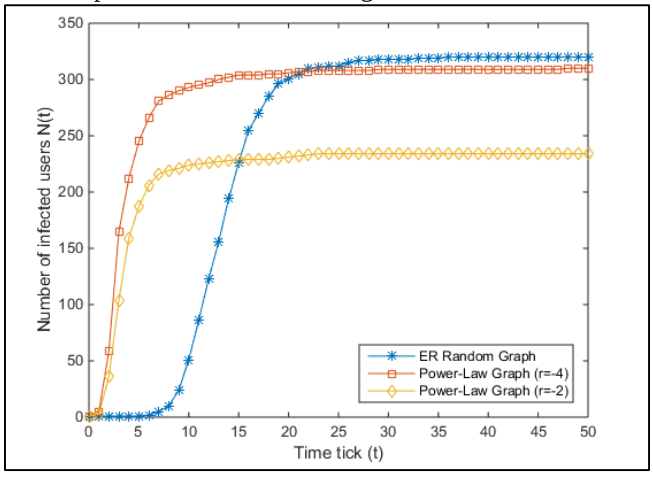

Fig. 4: Effect of topology characteristics on worm propagation.

The experimental results show that in the power-law network, the worm has faster spreading speed and shorter latency, and can quickly infect a large number of vulnerable users in short time. At the same time, for different power

exponents, the network has different disequilibrium, causing difference in the rate and scale of propagation. The Internet and social networks in real life all have the property of power distribution. Once these networks are attacked by worms, and there is no effective defence method, worms can infect a large number of hosts quickly.

In order to intuitively display the characteristics of different network topology, our simulation system also has visualization function. Users can configure the display manners by parameters

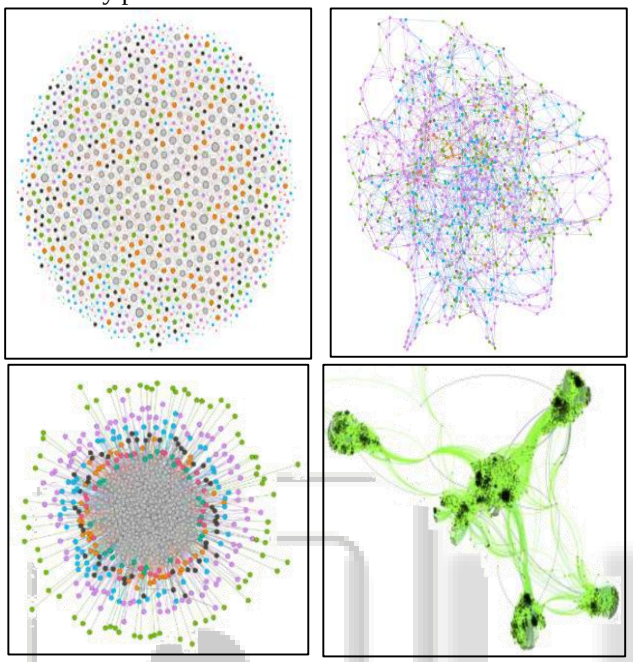

Fig. 5: Visualization results of different networks. (a) ER random graph with 1000 nodes and 5000 edges. (b) Small-world graph with 1000 nodes and number of nearest neighbour k = 3. (c) Power-Law graph with 1000 nodes and r = -4. (d) Social network of Facebook with 4039 nodes.

Secondly, we analyse the impacts of the worm characteristics on propagation. The network in the experiments is generated by network generation module. It has 23001 hosts totally and the 40 percent of them are vulnerable. In the actual case, different ways of worm propagation lead to different infection ability. In simulation process, we use infection probability to describe the infection ability of worm in propagation. Worms with stronger infection ability have greater value, and vice versa. In order to verify the effect of different infections on the worm propagation process, we set the infection probability to 0.25, 0.5, 0.75, and 1.0 respectively with the command in the experiment. The other conditions are the same. We enter the completed command in the command window of human-computer interaction module as shown in It can be seen from the experimental results that with the increase of the parameter.

The number of infected hosts increases faster, and the number of newly infected hosts per unit time increases, and the worms exhibit explosive propagation. Therefore, the stronger the worm infection ability, the more hosts it can infect in a short time, resulting in more serious damage.

In addition, the scanning rate of worms in real networks can also influence the propagation process [14]. In propagation process, the number of malicious messages sends by a scanning worm during a single time period refers to as the scanning rate of the worm, which is represented by parameter in simulation. The more malicious messages the worm sends in a single time period, the greater value of .In the experiment, we set the scanning rate to 1, 5 and 10 respectively using the command. The other conditions are the same. The completed command of this experiment is .The experimental results are Command of the experiment studying scanning rate.

The experimental results show that the increase rate of the number of infected hosts increases significantly with the increase of scanning rate, and the worm can quickly infect a large number of vulnerable hosts. Therefore, the scanning rate of the worm is also an important factor affecting the propagation. The larger the scanning rate, the faster the worm spreading speed. However, the scanning rate of the worm cannot increase infinitely. When the scanning rate increases, the worm consumes a lot of system resources and network bandwidth, and it is easier for security software to detect it.

At the same time, the scanning worm in the actual case often takes different scanning strategies to discover target hosts [15]. The common scanning strategies include random scan, replacement scan, divide scan and so on. In the experiment, we change different scanning strategies using command and keep other parameters the same.

The experimental results indicate that as increases, the spreading speed of the worm declines, the outbreak time of the worm propagation delays, and the explosion intensity also decreases. Meanwhile, there is no significant difference in the total number of infected hosts at the end of propagation. To sum up, through the above experiments, we analyse the impacts of worm characteristics and network topology characteristics on worm propagation, and obtain important factors influencing the worm spreading speed and propagation scale. Using WPSDL, we achieve a unified configuration of parameters in the simulation process and a unified description of the software interfaces in the simulation software. At the same time, the related commands of WPSDL can be used in human computer interaction directly, which improves the efficiency of simulation experiments. In addition, the successful completion of above experiments shows that our simulation system can simulate different types of worms in different network, which is suitable for worm propagation researches.

V. CONCLUSIONS

With the development of the Internet and social networks, the scenarios and methods of worm propagation is becoming diversified. In order to study the propagation mechanism of the worm better and achieve a unified description of worm propagation simulation process, we propose a description language for worm propagation called WPSDL in short. It describes the software interfaces and parameters of each module in the simulation process through a unified way. Meanwhile, we develop a novel simulation system oriented this language. The system uses the commands provided by WPSDL as interactive commands, and can implement worm propagation simulation for different types of worms in different networks. In addition, we do a series of experiments

to analyse the influence of infection probability, propagation delay, scanning rate, scanning strategy, and network topology characteristics on worm propagation. On the one hand, these experiments verify the influence of network topology characteristics and worm characteristics on propagation. On the other hand, the successful completion of above experiments also shows the practicability of the description language and the simulation system.

REFERENCES

[1] Zhou W, Jia W, Haghighi M, Xiang Y and Chen C 2015 A Sword with Two Edges: Propagation Studies on Both Positive and Negative Information in Online Social Networks IEEE T COMPUT 64 640-53
[2] J F M B 2017 Symantec Internet Security Threat Report 2016. (San Francisco: Symantec Corporation) pp 51-74
[3] Staniford S, Paxson V and Weaver N 2002 How to Own the Internet in Your Spare Time. In: Usenix Security Symposium, Aug, pp 149-67
[4] Zou C C, Gong W and Towsley D 2002 Code red worm propagation modeling and analysis. In: Proceedings of the 9th ACM conference on Computer and communications security, pp 138-47
[5] Zou C C, Towsley D and Gong W 2007 Modeling and Simulation Study of the Propagation and Defense of Internet E-mail Worms IEEE Transactions on Dependable & Secure Computing 4 105-18
[6] Wang T, Xia C and Jia Q 2017 Modeling and Simulation Study of Social Worms Oriented Hierarchical Networks Tien Tzu Hsueh Pao/Acta Electronica Sinica 45 1722-30
[7] Ebel H, Mielsch L I and Bornholdt S 2002 Scale-free topology of e-mail networks Physical Review E Statistical Nonlinear & Soft Matter Physics 66 35103
[8] Ke X U, Zhang S, Hao C and Hai-Tao L I 2014 Measurement and Analysis of Online Social Networks Chinese Journal of Computers 29-42
[9] Kim J, Radhakrishnan S and Dhall S K 2004 Measurement and analysis of worm propagation on Internet network topology. In: International Conference on Computer Communications and Networks, 2004. ICCCN 2004. Proceedings, pp 495-500
[10] Wang T, Xia C, Li Z, Liu X and Xiang Y 2017 The Spatial-Temporal Perspective: The Study of the Propagation of Modern Social Worms IEEE T INF FOREN SEC 12 2558-73
[11] Moore D, Shannon C and Claffy K 2002 Code-Red: a case study on the spread and victims of an internet worm. In: ACM SIGCOMM Workshop on Internet Measurement 2002, Marseille, France, November, pp 273-84
[12] Xiao X, Fu P, Li Q, Hu G and Jiang Y 2017 Modeling and Validation of SMS Worm Propagation over Social Networks J COMPUT SCI-NETH
[13] Newman M 2005 A measure of betweenness centrality based on random walks Social Networks 27 39-54
[14] Chen Z, Gao L and Kwiaty K 2003 Modeling the spread of active worms. In: Joint Conference of the IEEE Computer and Communications. IEEE Societies, pp 1890-900

