A Dynamic Monitoring Method of Social Network Worm Attack Based on Improved Decision Tree

Wei Ge(✉)

Jiangxi University of Software Professional Technology, Nanchang 330041, China
gewei01475@163.com

Abstract. In the network security, worms are a kind of more aggressive virus, it is necessary to carry out a detailed discussion of worm attacks. There is a problem that the number of immune nodes is small in the application of worm attack dynamic monitoring method of social network, so a new method based on improved decision tree is designed. According to the attack infiltration theory and propagation mechanism, the worm type is identified, the worm propagation path is extracted, the copy of the worm program is transmitted to the adjacent nodes, and the heterogeneous model of topology structure is constructed by using the improved decision tree. Then the control is transferred to the function called to execute, and the dynamic monitoring mode of the worm attack is optimized. Experimental results show that the average immune nodes of this method and other two methods are 505, 363 and 373 respectively, which proves that the performance of this method is more outstanding than that of other two methods.

Keywords: Improved decision tree · Social network · Worm attack · Dynamic monitoring · Network security · Network nodes

1 Introduction

Among the network security problems, malicious code to the network causes by the largest proportion of economic losses. It mainly includes: computer viruses, a program that can infect other programs by modifying other programs to copy itself or its variants. Worms have been one of the greatest threats to network security. Every outbreak of worms has done great harm to the whole network since it first appeared. The worm belongs to a kind of computer virus, but it and the ordinary computer virus also have a very big difference. A social network worm, a program that sends itself from one node to another and launches itself through the network's communication capabilities. This paper makes a comparative analysis between worm and common computer virus from the aspects of existence form and spreading mechanism. In order to exist, ordinary computer viruses need to parasitic in the host program or file, and only when the host program or file is running, the virus is activated, with the ability to infect. A Trojan horse, a program that executes beyond the definition of a program. A compiler is a Trojan horse

W. Fu and L. Yun (Eds.): ADHIP 2022, LNICST 469, pp. 417–430, 2023.
https://doi.org/10.1007/978-3-031-28867-8_31

if, in addition to performing compilation tasks, it secretly copies down the user's source code. A worm, on the other hand, is a self-executing code file that does not need to be stored or activated.

In the transmission mechanism, the common computer virus is mainly infected with the files on the host, and the worm attack target is not only a single host, but also spread the attack program to the whole network. A logic bomb is a program that performs other special functions when the environment under which it runs satisfies a particular condition. A denial of service attack is an attack in which a user occupies a large number of shared resources so that the system does not have any remaining resources available to other users. This attack reduces the availability of system resources, including network server processors, disk space, printers, etc. The result of the attack is to reduce or lose service. Generally speaking, worms do much more harm to computer systems than ordinary computer viruses. From a technical point of view, the worm is described: a worm can run independently, and can send their own copy of the file to other computers as a virus. In addition, many people put forward the malicious code as a means of attack in cyber warfare, when network security has risen to the height of national security. The characteristics of worms are mainly determined by the attack program, so in order to better understand the characteristics of worms, the researchers have carried out a detailed study of worm attack program.

2 A Dynamic Monitoring Method of Social Network Worm Attack Based on Improved Decision Tree

2.1 Identifying Social Network Worm Types

The biggest difference between social network worms and viruses is that viral infections require users to distribute infected files to susceptible hosts. Therefore, the spread of the virus will be much slower than the spread of social network worms, this is because the spread of the virus requires manual user participation. However, social networking worms can spread very quickly and can infect a large number of hosts within a day or even a few hours. Later, it is found that the worm attack program mainly consists of four modules, which are information collection module, scanning detection module, infiltration module and self-propelling module. Because of the variety of worm propagation modes, it is necessary to divide the worm into several groups, so as to facilitate researchers, study of the worm propagation models and detection methods. Scanning worm generates the IP address of the network through a target selection algorithm, and then detects the vulnerability of the host on the IP address by vulnerability scanning, if the vulnerability exists, it will infect the host directly. Therefore, the spread of scanning worms does not require human intervention. The self-replicating nature of worms is influenced by the self-propelling module that helps worm programs form multiple copy files in preparation for a new attack [2, 3]. Active transmission of worms is affected by information collecting module, scanning detection module and attacking penetration module, which the information collecting module and scanning detection module are the preparatory stages. Scanning worm attacks have the following characteristics: attackers do not need to collect information on the network host vulnerability, easy to

write, relatively short infection time and so on. The scanning strategies include random scanning, selective random scanning, linear scanning, target list based scanning, divide and conquer scanning, route based scanning, DNS based scanning and so on.

Through the research on the function modules of worm program, the understanding of worm propagation mechanism in the network has become more in-depth. Topology worms propagate in a logical topology communication network by collecting the topology information of hosts or the hosts in the network that they carry. Morris worms collect topology information, including the Web Yellow Pages/etc./hosts and other resources to find social network worms. Mail worms are topology worms that propagate through mail. When an email user opens attachments in an email or when a vulnerable email client receives an email that has been infected by a worm, the user's host computer is infected by the worm. The process of worm propagation in the network can be divided into four stages, which are the information collection, scanning detection, attack infiltration and self-promotion. Among them, penetration is the main part of worm propagation. Therefore, it is important to study the state change of nodes in the stage of attack and infiltration. Based on the propagation mechanism of social network worms, we divide social network worms into four types, as shown in Fig. 1:

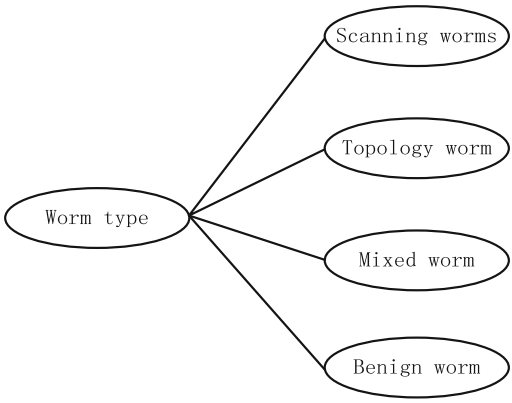

Fig. 1. Types of social network worms

As can be seen from Fig. 1, depending on the propagation mechanism of social network worms, the types of network graph worms include scanning worms, topology worms, benign worms, and hybrid worms. Based on this, the focus of the research on worms has shifted to the quantitative characterization of worm propagation. At present, the research focuses on establishing worm propagation model by mathematical modeling method, predicting worm propagation trend by simulation experiment, and finding the key factors to prevent and control worm propagation. As a kind of P2P worm, IM worm propagates through IM network. Firstly, it collects the contact information of the infected host user, then attacks the contact by IM protocol or flaw, and propagates the copy of IM worm to the attacked contact.

The behavior of attacking and infiltrating worms is called worm attack, which includes two processes: initiating attack and infiltrating. In the process of infection

of worm attack, worm program will make use of the vulnerability of node to infiltrate it. According to attack infiltration theory, the result of attack infiltration is the increase of node vulnerability and the promotion of user authority. A benign worm is a controllable, stand-alone program that can be run without the intervention of a computer user. It obtains some or all control over a computer that has a loophole in the network, and then uses the transport function to obtain assistive tools for tasks such as immunization, repairing, clearing worms, and closing the back door. Finally can safely self-destruct. Like drugs in medicine, benign worms can spread like worms, patching or removing worms from infected hosts, or both. It is found that when a node is attacked by several neighboring infected nodes at the same time, the increased vulnerability of some neighboring nodes and the promotion of user privileges may become the precondition for the node to be attacked by other neighboring nodes, so that the intrusion infiltration of the latter neighboring nodes can be completed more easily.

Hybrid worms can be spread using a combination of social network worm attack strategies, such as mail worms, scanning worms, and social network worms using network sharing attack strategies. Hybrid worms require worm writers to have a comprehensive knowledge of the attacks, and are more difficult to write than social network worms that use only one attack method. At the same time, according to the theory of cooperative intrusion, multiple attacks can constitute an attack sequence, and the information transfer between them will continuously affect the vulnerability of nodes. Based on the above theoretical analysis, it can be found that multiple attacks have correlation in the process of intrusion, and attack correlation will increase vulnerability and infection probability of nodes. In order to describe the dynamics of infection probability more accurately, the attacking correlation should be taken into account in the construction of worm propagation model.

2.2 Extract Social Network Worm Propagation Paths

Worm attacks on social networks involve two processes: transmission and infection. Propagation is the process that a worm attacks a neighbor node with the help of the host node. Infection refers to the process in which a worm program makes use of the vulnerability of the attacked node to infiltrate the worm. In the process of worm attack, worm attacks all neighboring nodes by infective nodes. The main behavior of worm attacks is to establish information transmission channels between nodes and send copies of worm programs to neighboring nodes.

Social network worm is a kind of autonomous agent, which can spread rapidly in the network, especially in the high-speed network environment, the worm outbreak rate is greatly increased, the coverage is more extensive, and the loss is greater and greater. There are three factors that affect the speed at which social network worms can spread. The first is the speed at which loopholes are discovered. The second is how many potential “fragile” hosts can be exploited. Third, the social network worm infection rate of these targets. In addition to the division based on the propagation mechanism, social network worms can be classified differently from different perspectives. According to the transport mode of social network worms, social network worms can be divided into three kinds of social network worms: automatic transmission, second channel and embedded transmission. The main determinant of worm propagation speed is the speed at which

a vulnerable host can be found, that is, how many efficient host systems can be found, which is done by the worm's scanning module. Therefore, in order to defend social network worm more quickly and effectively, we must study the propagation mechanism of social network worm from the scanning and attacking methods of worm. Assuming that the social network worm no longer accesses the visited host system, the propagation rate of the divide-and-conquer scanning worm can be expressed in the following formula:

$$L_{p+1} = \left(S - L_p\right) \times \left(1 - \frac{10^9 - \varepsilon}{\sum_{\varepsilon=1}^{n} p + 1}\right) \tag{1}$$

In formula (1), S represents the total number of host systems with exploitable vulnerabilities of social network worms, L represents the scan rate, ε represents the granularity of the address list, and p represents the number of hosts that have been infected by time p. According to the activation methods of social network worms, it can be divided into three types: manual activation, scheduled process activation and self-activation. The propagation process of worm attack can be regarded as the information transaction between two nodes. The infective status node is the initiator of the transaction and the neighbor node is the receiver. According to the analysis, it can be seen that the trust evaluation of the transaction receiver to the initiator of the transaction will affect the receiving behavior of the transaction receiver. Therefore, in the process of worm attack propagation, the neighbor node will decide its receiving behavior according to the trust degree of the infected state node.

Social network worms that use a random scan strategy scan for unassigned IP addresses, most of which are non-routable, greatly slowing down the spread of social network worms. Before the social network worm is released, knowing which addresses are routable can greatly reduce the worm's scanning space, speed up propagation and effectively evade detection. In social networks, the buffer size for most applications to hold data is fixed [4, 5]. If an attacker sends excessive data to one of these buffers, and the program does not check the size of the data, the buffer overflows. According to payload partition, it can be divided into empty payload, Internet remote control payload, spam forwarding payload, HTML proxy payload, Internet denial of service attack payload, data collection payload, sales access payload, data destruction payload, remote control payload, denial of service attack payload, search payload, damage payload, worm maintenance payload. From formula (1), the expression formula for worm propagation on mobile devices is derived:

$$\frac{S}{L} = \varphi^2 + \sqrt{(h - \varphi)^2} \tag{2}$$

In formula (2), φ represents the forward invariant set of the host, and h represents the removal rate of the virus on the mobile device. The target computer then executes the "overflow" data, just as it executes the program. If the attack buffer is in a legitimate process, the malicious program takes full control of the target computer and then does whatever it pleases, including executing commands on the target computer, stealing passwords or other confidential information, changing the system configuration, and/or

installing a back door. Based on the classification of attackers, we can divide social network worms into: curiosity, business interests, mischief, political purposes, terrorism, and cyberwar. From the point of view of worm attack, the receiving behavior of neighbor nodes affects the propagation probability of worm replicas propagated by infected nodes. In order to describe the dynamics of the propagation probability more accurately, trust should be taken into account in the construction of the worm propagation model.

2.3 Construction of Topological Heterogeneous Model by Improving Decision Tree

In the improved decision tree algorithm, entropy is used to represent the degree of confusion and the degree of possible states [6, 7]. In the field of information theory, information entropy indicates the degree of confusion, indicating the extent to which states may occur. In the field of information theory, information entropy indicates the probability of discrete random events.

The reason why buffer overflow attacks have become a common means of attack is that buffer overflow vulnerabilities are too common and easy to implement. Moreover, buffer overflows are the primary means of remote attack because they give an attacker everything he or she wants: the ability to seed and execute attack code [8]. Random scans give infected computers a chance to scan the Internet for vulnerabilities when looking for new targets, so scans target all IPv4 address spaces. The implanted attack code runs the program with buffer overflow vulnerability with certain authority, thus obtaining the control of the attacked host.

Buffer overflow is mainly divided into two types according to its overflow form: stack-based Buffer overflow and heap-based Buffer overflow. Most Buffer overflow attacks are stack based. Based on the analysis of worm propagation process, it is found that the trust of peers will affect the information transaction between peers and thus the worm attack propagation probability. The higher the trust degree of the node is, the greater the probability of successful information transaction and the greater the probability of information transmission. Based on this, this paper establishes a positive correlation between transmission probability and trust, as shown in Formula (3):

$$G_{mn} = \eta \times \frac{1}{\sqrt{W_{mn}}} \tag{3}$$

In formula (3), η represents the propagation probability, W represents the correlation coefficient, and m, n represents the trust degree of node m to node n, respectively. Both codeRed and Stammer worms use random scans, which generally have large scan address space and slow propagation. But the Stammer worm spreads very fast, mainly because it uses the UDP protocol for disconnected scanning, and uses a large number of threads to scan, making its scan mainly limited by bandwidth. In the improved decision tree algorithm, the information entropy data is used as the parameter to reflect the minimum randomness of the partition, and the amount of information of the sample is minimized. Represents the probability of the occurrence of a discrete random event. In the decision tree algorithm, the information entropy is used as a parameter to reflect the minimum randomness of the partition, and the minimum information is needed to show the probability of discrete random events.

Stack-based overflows take advantage of buffers stored on the program's stack. The stack is an area of memory where local variables are stored within each program. It is used as a buffer storage area for program subroutines. When a function is called in a program, the system first puts the arguments required by the called function on the stack in reverse order, and then puts the address of the instruction following the call on the stack. In the decision tree algorithm, the information entropy is used as a parameter to reflect the minimum randomness of the partition, and the information needed by the sample is minimized. Once the first root node is calculated, the data set can be divided into subsets, and then the information gain can be calculated on the basis of the subset, and the subset can be recursed when all the attributes have been divided, or when the subset belongs to the same category, or when the recursion is over. Sequential scanning is when a worm on an infected host randomly selects a network address to propagate. According to the local priority principle, a worm typically selects an IP address in its network. If the target address IP of the worm scan is A, then the next address IP of the scan is A 1 or A-1.Once scanned to the host network with many vulnerabilities will achieve a very good dissemination effect.

The aim of the improved decision tree algorithm is to get a set of decision rules from the training data set, so that the training samples can make correct decisions and deal with the new input samples well. There are three processes to find the optimal decision tree: attribute selection, decision tree generation and decision tree pruning. Attribute selection is the key to decision tree learning, that is, how to select the optimal attribute for partitioning nodes. The control then goes to the called function to execute, and the program typically allocates the required storage space for local variables within the called function after stacks of values that require registers to be saved.

2.4 Optimize the Dynamic Monitoring Method of Worm Attack

In recent years, heap overflows have become very common for several reasons: the lack of stack execution mechanisms, and breakthroughs in new attack technologies. If a heap buffer overflow occurs, it provides an unusable stack protection mechanism that is currently not executable, which the system can ignore, but which makes the social network vulnerable. Based on the SEIR model of worm propagation, the Markov chain of state transition is constructed, and the transition probabilities from susceptible state, latent state and infective state to recovery state are calculated.

Based on the above calculation results, the dynamic monitoring mode of the whole social network is optimized. These average times suggest the best time to take defensive measures in time. Routing worms use addresses in the BGP routing table to reduce the address space to be scanned. Because only 28.6% of the IPv4 address space is included in the BGP routing table, the probing address space will be smaller than the random scan, so the propagation speed will be increased. For the state transition dynamic equation of the susceptible state node, see Formula (4):

$$D_{ij}^{e}(\eta+1)=\frac{e+T_{ij}}{\sum_{i=1}^{n}T_{ij}-\eta} \tag{4}$$

In formula (4), e represents the number of attacks, T represents the infection probability of the node, and i, j represents the initial value of the infection probability and the change rate of the infection probability, respectively. The essence of worm attack behavior is to promote worm propagation from different angles or at different costs to achieve different objectives driven by benefit mechanism. Therefore, in order to promote the worm to spread in the network, the node will provide false trust. Assume that, at each time step, the infected state node increases its direct trust by increasing the number of successful transactions with its neighbor nodes, as shown in formula (5):

$$Q_\sigma = \frac{\|\sigma - 1\|}{2} \times \mu^2 \tag{5}$$

In formula (5), σ represents the attack propagation risk of the source node, and μ represents the number of successful transactions. Heap overflow based attacks vary greatly depending on the attack technique used, and heap based buffer overflows can be classified into three categories depending on the difficulty of the technique used: simple heap overflows, which are often caused by unintentionally supplying an overlong string and are not intended attacks. However, "routing worms" carry address information to make their own code longer, in this sense will slow down the spread of worms. In dynamic monitoring mode, divide and conquer scanning is a strategy for social network worms to collaborate with each other and search easily infected hosts quickly.

Modify the function pointer, by modifying the function pointer to point to the pre-implanted attack code, so as to achieve the goal of attack. Advanced heap overflow, which makes full use of the data structure and method of heap management in social network, is the most frequently used method of dynamic monitoring. The social network worm sends a portion of the address library to each infected host, and each host scans it for the address it gets. After Host A is infected with Host B, Host A assigns a portion of the address it carries to Host B, and Host B scans that portion. Formatting string attacks are mainly caused by programmers' laziness. String formatting output function is a commonly used means of human-computer interaction in C language. It differs from ordinary functions in that the number of parameters of such functions is variable, and the string formatting parameters guide the social network to complete the corresponding input and output work.

Because dynamic monitoring is user-triggered, it spreads slowly, but these worms do not cause communication anomalies in the discovery of targets, making them inherently more secure. The CRClean worm is a passive worm, waiting for Code Red II to probe the activity. When it detects an infection attempt, it launches a counter-attack back and forth that should infect the attempt. If the counterattack is successful, it removes the CodeRed II worm and installs itself on the machine. When the called function finishes executing, the social network frees up the stack space allocated for the local variable of the function and restores the value that already exists in the register. The return address from the stack is then sent to the instruction register in the social network, and the program starts execution at that address. The disadvantage of this strategy is that the same host may be repeatedly scanned, causing network congestion. The Hit-list scan method is one of the fastest theoretically propagating scans. It first by the worm writer by scanning and other means of detection to collect the worm can attack the network of all the host information.

The worm then attacks the collected host. Heap based buffer vulnerabilities can occur if data is copied to buffers on the heap without checking.

3 Simulation

3.1 Build an Experimental Environment

Simulation experiment is based on Python experimental platform, the scale-free network constructed in the total number of nodes N = 1000, the average length of 6 nodes. The number of nodes in each state of the network at each time was selected as observation object. The simulation experiment needs to be tested on the dataset, and the labeled dataset is usually used. There are two ways to get tagged datasets: one is to use publicly tagged datasets, such as DARPA, KDD 99, and NSL-KDD. The second is to construct a new data set from the actual network traffic. The prototype social network was deployed at the exit of the network, and we used tcpreplay software to replay background traffic and worm traffic on different hosts, respectively. Among them, the background traffic without attack is the network traffic of one month, and the worm traffic is the traffic of lion worm and mscan worm respectively.

Data collection from actual network traffic has problems of classification accuracy and labeling. The outlier-based detection method usually needs to be trained with non-attack data. However, the data collected from the actual network may not meet this requirement. The initial parameters of the network are as follows: 0.01 for infective state nodes, 960 for susceptible state nodes, 10 for infective state nodes, 10 for threatening state nodes, 10 for isolating state nodes, and 20 for immune state nodes. Under these conditions, the experiment was repeated. Shaft K. and Abbass H.A. describe methods for generating tagged datasets. The dataset consists of the background traffic obtained from the real network and the attack traffic obtained by simulation. To tag the background traffic, execute Snort IDS.

3.2 Experimental Results

In order to evaluate the effectiveness of the designed dynamic monitoring method, the data mining -based dynamic monitoring method for worm attacks on social networks and the cloud computing -based dynamic monitoring method for worm attacks on social networks are selected and compared with the designed dynamic monitoring method for worm attacks on social networks, and the number of immune nodes of the three dynamic monitoring methods are tested respectively under different runtime conditions. The experimental results are shown in Tables 1, 2, 3, 4 and 5:

As can be seen from Table 1, when the runtime is 8 h, the average number of immune nodes of the social network worm attack dynamic monitoring method and two other social network worm attack dynamic monitoring methods is: 796, 589, 582, as can be seen from Table 2; when the runtime is 16 h, the average number of immune nodes of the social network worm attack dynamic monitoring method and two other social network worm attack dynamic monitoring methods is: 624, 454, 463, as can be seen from Table 3; when the runtime is 24 h, the average number of immune nodes of the

Table 1. Number of immune nodes with 8 h running time (piece)

Number of experiment	Dynamic monitoring method of social network worm attack based on data mining	Social network worm attack dynamic monitoring method based on cloud computing	The design of the social network worm attack dynamic monitoring method
1	536	594	774
2	520	568	782
3	541	571	790
4	559	529	805
5	629	531	846
6	635	566	773
7	548	519	854
8	537	548	873
9	559	567	828
10	548	582	793
11	622	637	811
12	670	644	764
13	664	698	758
14	612	577	739
15	648	602	745

social network worm attack dynamic monitoring method and two other social network worm attack dynamic monitoring methods is: 514, 328, 362; as can be seen from Table 4, as can be seen from Table 4, when the runtime is 32 h, the average number of immune nodes of the social network worm attack dynamic monitoring method and two other social network worm attack monitoring methods is 344, 2727, 282; as can be seen from Table 5, as can be seen from Table 5, when the social network worm attack dynamic monitoring method is 40 h, the average number of social network worm attack dynamic monitoring methods are designed respectively: 177, 1747, and two other social network worm attack methods are 1747.

According to the above experimental results, this method has certain advantages in dynamically monitoring social network worm attacks. Because this paper improves the decision tree algorithm, which can identify the worm types and extract the worm propagation path according to the worm attack penetration theory and the propagation mechanism. It optimizes the way that worm attacks are dynamically monitored.

4 Conclusion

The dynamic monitoring method of worm attack in social network designed in this paper enriches the research in related fields, and provides a new method for accurately

Table 2. The number of immune nodes with a running time of 16 h (piece)

Number of experiment	Dynamic monitoring method of social network worm attack based on data mining	Social network worm attack dynamic monitoring method based on cloud computing	The design of the social network worm attack dynamic monitoring method
1	512	484	612
2	498	455	609
3	446	432	588
4	413	419	637
5	459	478	612
6	426	455	659
7	487	461	616
8	412	473	602
9	404	481	645
10	415	492	637
11	503	501	625
12	488	522	644
13	467	418	633
14	458	406	617
15	416	469	628

Table 3. The number of immune nodes that run for 24 h (piece)

Number of experiment	Dynamic monitoring method of social network worm attack based on data mining	Social network worm attack dynamic monitoring method based on cloud computing	The design of the social network worm attack dynamic monitoring method
1	331	375	476
2	302	384	555
3	294	396	561
4	316	345	423
5	338	353	565
6	349	377	488

(*continued*)

depicting the model. Aiming at the influence of social network worms on network traffic, an entropy based detection method for social network worms deployed on routers is

Table 3. (*continued*)

Number of experiment	Dynamic monitoring method of social network worm attack based on data mining	Social network worm attack dynamic monitoring method based on cloud computing	The design of the social network worm attack dynamic monitoring method
7	351	349	492
8	311	358	503
9	297	316	521
10	304	372	564
11	322	369	597
12	366	359	496
13	387	346	485
14	341	372	520
15	315	358	466

Table 4. The number of immune nodes with a running time of 32 h (piece)

Number of experiment	Dynamic monitoring method of social network worm attack based on data mining	Social network worm attack dynamic monitoring method based on cloud computing	The design of the social network worm attack dynamic monitoring method
1	265	269	303
2	288	248	312
3	226	267	344
4	293	285	319
5	267	291	306
6	253	288	358
7	249	267	347
8	278	294	369
9	282	311	366
10	264	305	384
11	259	278	375
12	277	267	317
13	301	255	345

(*continued*)

Table 4. (*continued*)

Number of experiment	Dynamic monitoring method of social network worm attack based on data mining	Social network worm attack dynamic monitoring method based on cloud computing	The design of the social network worm attack dynamic monitoring method
14	269	294	366
15	306	314	349

Table 5. Number of immune nodes with 40 h runtime (piece)

Number of experiment	Dynamic monitoring method of social network worm attack based on data mining	Social network worm attack dynamic monitoring method based on cloud computing	The design of the social network worm attack dynamic monitoring method
1	169	174	221
2	188	185	205
3	165	196	226
4	167	173	249
5	182	185	258
6	174	176	237
7	169	182	241
8	153	171	218
9	164	169	209
10	185	179	264
11	172	162	257
12	169	181	282
13	182	163	274
14	175	194	269
15	174	165	288

proposed. This method belongs to the detection method of social network worm based on traffic, that is, analyzing the statistical information of network traffic without analyzing the load of network transmission. The improved decision tree is introduced into the worm propagation process, and the heterogeneous model of network topology can better identify malicious nodes, which provides a new mechanism for preventing and combating worm attacks. At the stage of real-time worm detection, the network data entropy of the current window is calculated and compared with the learning entropy interval. If the

current window is not in the learning entropy interval, the worm is warned. It lays the research foundation for the academic circles.

References

1. Kumar, R., Kumar, P., Kumar, V.: Design and implementation of privacy and security system in social media. Int. J. Adv. Networking Appl. **13**(4), 5081–5088 (2022)
2. Li, Y., Song, M.: Trust update model considering worm propagation risk. Oper. Res. Manage. Sci. **29**(10), 163–172 (2020)
3. Li, Y., Zhang, H.: Benign worm propagation model in industrial control networks. Control Eng. China **27**(7), 1286–1292 (2020)
4. Cheng, H., Zhang, R., Zhang, S., et al.: Power failure sensitivity analysis based on improved decision tree. Microcomputer Appl. **36**(3), 144–148 (2020)
5. Li, Y., Li, W., Chen, N., et al.: Battlefield target assistant judgment technology based on improved decision tree. Command Inf. Syst. Technol. **11**(1), 62–67 (2020)
6. Achar, S.J., Baishya, C., Kaabar, M.K.A.: Dynamics of the worm transmission in wireless sensor network in the framework of fractional derivatives. Math. Methods Appl. Sci. **45**(8), 4278–4294 (2022)
7. Panigrahi, R., Borah, S., Bhoi, A.K., et al.: A consolidated decision tree-based intrusion detection system for binary and multiclass imbalanced datasets. Mathematics **9**(7), 751 (2021)
8. Zhou, L., Li, J.: Security situation awareness model of joint network based on decision tree algorithm. Comput. Simul. **38**(5), 264–268 (2021)