STUDY OF IMMUNIZATION STRATEGY UNDER THE CLOUD

Yanjing LI[1]

In the cloud network, users can connect to the cloud by using any Internet-connected device. And then they can use all kinds of software and services provided by the cloud network. How to protect the users' privacy information is the focus and challenges of the cloud network. Currently, passive elimination of the virus cannot be satisfied with the increasingly serious problems of network security any more. It has to immunize the uninfected host to solve the large-scale virus infection effectively in the early stages of virus outbreak. How to get the maximum benefit by immunize the least network nodes in the early stages of virus outbreak become the focus of the problem. In order to promote the research and practical application of the cloud network, this paper focused on the security problem of the cloud especially the virus propagation and immunization strategy of the cloud. The hierarchy immunization strategy which is fit for cloud network is proposed. Combine the security mechanism under the cloud and the hierarchy immunization strategy to ensure the safety of the cloud. The effectiveness of the hierarchy immunization strategy is verified by the experiment. Compare to the target immunization strategy, acquaintances immunization strategy and the random immunization strategy, the hierarchy immunization strategy is more suitable for the cloud network with the characteristics of large-scale, distributed and dynamic.

Keywords: network security, propagation model, hierarchy immunization strategy, security mechanism, artificial immune

1. Introduction

Almost all the IT resources can provide as a service in the cloud environment [1]. Users no longer to buy the high-performance hardware and various of software under this model. They can process and store the data in the cloud directly by the software and services of the cloud network [2-3]. The cloud network which shows the significant small-world phenomenon is a typical scale-free complex network. This kind of distributed network is consistent with the power-law distribution with the index of 2~3 [4]. It is robust for the random attack and fragile for the malicious attack under the power-law distribution. If a large number of nodes in the network are removed randomly; the scale-free network can still maintain the basic connectivity. But few highest nodes are removed deliberately, then the connectivity of the network can be damaged seriously.

[1] Lecturer, Dept of Information Engineering, Shijiazhuang University of Applied Technology, China, e-mail: liyanjing860508@126.com

Infectious diseases spread rapidly and widely because of the small world and scale-free characteristics of the network. Due to the limitation of immune quantity or the high cost, current research is focus on how to immune the network by the least immune individuals [5-7].

At present, the research on the security of cloud environment is not thorough enough. In order to promote the related research and practical application of cloud network security, this paper makes in-depth analysis and exploration on virus transmission and immunization strategy forwarding in cloud environment by using artificial immune technology for reference.

2. Related work

In recent years, many immunization strategies have been proposed to deal with the deliberate attack vulnerability of scale-free networks with power-law distribution [8-11]. The earliest immunization strategies include random immunization strategy [12] and target immunization strategy [13]. A collection of nodes which are selected randomly are immunized in the random immunization strategy. In the target immunization strategy, the nodes are immunized by the descending order of the degrees. Currently, the target immunization strategy is considered the most effective strategy. This strategy needs to know the global information, so it is not suitable for the real network.

In addition, W. Guang-Lin proposed a targeted edges immunization strategy, which prevents the epidemic by immune a certain number of the most important edges from the perspective of protecting transmission path [14]. L. Jiming etc proposed the node-betweenness immunization strategy [15]. The node-betweenness strategy in which the nodes or edges with the high betweenness are immunized shows the excellent results. Marcel Salathé etc proposed a CBF algorithm for the community network [10]. The CBF algorithm can find the nodes connected to multiple communities, and then immunize the nodes. L. Jiming etc proposed a distributed immunization strategy used the Agent mechanism [16]. A group of Agents are deployed in the distributed environment, each Agent stays in the nodes with the highest degrees of its local environment, and then the nodes which the Agents stay in are immunized. This strategy integrated the characteristics of the distributed network fully can inhibit the spread of the virus effectively. Li-Chiou Chen proposed that the immunization strategy can propagate through a different network – social network [17]. He attempts to propagate the immunization strategy on a network separated to the virus propagation. In that kind of network, the immunization strategy whose speed is faster than the virus can inhibit the spread of the virus effectively.

In this paper, we propose a hierarchy immunization strategy for cloud environment, considering some characteristics of virus propagation (for example,

the nodes with higher degrees are more likely to be infected). The degrees of all nodes should be arranged in descending order in the target immunization strategy, and then immune the nodes according to the degrees of the nodes. But, in the cloud environment, the degrees of nodes is dynamic. We cannot get the global information of the cloud network. Therefore, in hierarchy immunization strategy, we obtain nodes dynamically with high degree in local area for immunity by agent technology, so that the vaccine can play the greatest value! In addition, this paper proposes the security mechanism of cloud environment. This mechanism can obtain the threat information of the network dynamically, analyze the threat information and extract the immunization strategy. Then the immunization strategy is distributed by the hierarchy immunization strategy. Combining the hierarchy immunization strategy with the security mechanism of cloud environment, a security ecosystem suitable for cloud environment is constructed.

3. Key technologies and Methods

The security mechanism of cloud network with ecological characteristic which is achieved by Agent is proposed in this section. According to the principle of artificial immune and the characteristics of cloud network, we proposed a hierarchy immunization strategy for cloud network. It can effectively guarantee the security of cloud network when we combined the hierarchy immunization strategy with Agent-based security mechanism.

3.1 Security mechanism of the cloud network

Due to the sharing of execution environment and the out of control about cloud infrastructure for users, the cloud users suspect the security of the services provided by the cloud provider. Cloud environment needs to ensure the safety of two aspects. On the one hand, the security of cloud provider. The cloud provider needs to improve the security of virtual environment so that the users shared the virtual machine can’t be infected by each other. On the other hand, it musts ensure the security of the cloud user. The user accessed to the cloud musts be the uninfected user. Then it can prevent the cross-infection among different users.

Siani Pearson proposed a design principle to ensure that the privacy information of users and enterprises is not disclosed in the process of cloud computing service design [18]. Lionel Litty etc made a comparative analysis of various internal detection methods of virtual machine [19]. The above solutions only focus on one aspect, and cannot guarantee the security of the cloud environment comprehensively and absolutely. In order to implement a security strategy suitable for the cloud environment, we should not be limited to a specific aspect, we should study various behaviors throughout the whole cloud service process.

The security of cloud environment presents complexity and ecology. A security mechanism of cloud network with ecological characteristics is proposed, which can solve the inherent security problems in cloud network. The mechanism is achieved by Agent.

The security mechanism creates the Monitor Agent for the node accessed to the cloud to ensure its security. The Monitor Agent collects the related information to analyze whether the node has malicious behaviour. If the node has malicious behaviour then the Monitor Agent will extract the antigen, re-encoding, activate the Query Agent and send the antigen to it. Query Agent query the solution in the security policy of this node. If the Query Agent finds the solution then it will repair the node. If the Query Agent cannot find the solution then it will activate the Decision Agent to create the solution of the malicious behaviour. The effective new solution will send to the other nodes in the cloud after it repairs the node. The local security policy will be updated. This method can greatly reduce the response time of the new threats for the nodes in the cloud and promptly deal with the new attacks emerged in the network. The security mechanism is simulated by the Agent. There are Monitor Agent, Query Agent, Decision Agent, Attack Agent and Transmission Agent in the network. The function of each Agent is as follows:

Monitor Agent: Monitor Agent is represented by a quad $\langle TQ(l), BM(m), JH, Cycle \rangle$, in which $TQ(l)$ is used to extract the feature of the IP reached to the node in the network and get a binary string of length l; $BM(m)$ is used to compress encoding for the antigen to reduce the communication traffic among the Agent; JH is a Boolean variable, $JH = 0$ represents the healthy node; $JH = 1$ represents that the Monitor Agent monitored the hazard information; $Cycle$ represents the life cycle of Monitor Agent. The security mechanism creates the Monitor Agent for the users accessed to the cloud to monitor the behavior of the host. Monitor Agent filters the obtained information to extracts the antigen and then send the information to Query Agent after re-encoding. The Monitor Agent will die out when the user exits from the cloud.

Query Agent: Query Agent is represented by a Quintuple $\langle Infor, JM(Infor), db(), CH, Cyc \rangle$, in which $Infor$ represents the information received from the Monitor Agent; $JM(Infor)$ represents the decoding function to decode the compressed code. $db()$ represents the contrast function which is used to compare the information of the decoded antigen and the antibody library to find the appropriate antibody information. CH is a Boolean variable. $CH = 0$ represents that no antibody information is found. And then Query Agent will activate the Decision Agent and send the antigen information to it. $CH = 1$ represents that antibody information is found. Then, Attack Agent will be

activated. Cyc represents the life cycle of Query Agent. Query Agent is activated by the Monitor Agent. It carries the information of antigen and finds the solution of antigen by comparing with the antibody in the local network antibody library. If the Query Agent find the solution then the Attack Agent is activated, else the Decision Agent is activated.

Decision Agent: Decision Agent is represented by a quad $\langle Mes, Des(Mes), DH(), Dcyc \rangle$, in which Mes represents the received antigen information; $Dec(Mes)$ function makes decision by analyzing antigen information. $DH()$ used to activate the Attack Agent and then send the decisions to the Attack Agent. $Dcyc$ represents the life cycle of Decision Agent. The Decision Agent which is activated by the Query Agent creates the new solution of the antigen and then activates the Attack Agent.

Attack Agent: Attack Agent is represented by a Quintuple $\langle JCInfor, Location, Assisa, GH, JCcyc \rangle$, in which $JCInfor$ represents the decision information received from other Agent; $Location$ represents the location of the malicious node; $Assisa$ represents the auxiliary measure such as disconnection of the link; GH is a Boolean variable. $GH = 0$ represents the failed attack. The decision information will be send to the Decision Agent for re-analysis. $GH = 1$ represents the successful attack. The Transmission Agent will be activated. The decision information will be send to the Transmission Agent. $JCcyc$ represents the life cycle of Attack Agent. Attack Agent which is activated by Decision Agent or Query Agent carries the appropriate security policy to attack the intrusion of the malicious node. The security policy will be send to the Transmission Agent after the successful attack. Then the Attack Agent dies out.

Transmission Agent: Transmission Agent is represented by a sextuple $\langle V_{Deg}, V_{neighbor}, S, comm, AimLoc, CLcyc \rangle$, in which V_{Deg} represents the degree of the node that the Transmission Agent stays on; $V_{neighbor}$ represents the address information about the neighbors of the node; S represents the states of the node such as healthy, susceptible, infection and immune; $comm$ represents the received decision information(antibody information); $AimLoc$ represents the address of the target immune node; $CLcyc$ represents the life cycle of Transmission Agent. Transmission Agent is activated by the Attack Agent. It carries the antigen solution. The solution will be send to the specified node according to the certain immunization strategy.

The operation process of the security mechanism based on the cloud network is as follows:

(1) The security mechanism creates the Monitor Agent for the node accessed to the cloud. The Monitor Agent collects the information, and then extracts the

antigen information when it found a malicious node. The antigen information will be send to the Query Agent after re-encoding.

(2) The Query Agent searches the corresponding antibody information in the local antibody library of the node. If the Query Agent found the corresponding antibody information then turn to step (4), else turn to step (3).

(3) If the local antibody library of the node dose not have the corresponding antibody information then the Decision Agent is activated. The Decision Agent will generate the related standard and strategy of the new antibody through analysis.

(4) The Attack Agent is activated and move to the malicious node to disconnect the link between the malicious node and its neighbor. Then the Attack Agent against the intruders. If the Attack Agent failed, then the Decision Agent is activated to generate the new solution to against the intruders until success. The Attack Agent will restore the link of the node, and then update the security strategy of the node. It dies after sending the security strategy to the Transmission Agent.

(5) Transmission Agent transmits the strategy according to hierarchy immunization strategy. The node which activates the Transmission Agent receives the immunization strategy. Then the node sends the immunization strategy to its direct neighbors. The direct neighbors send the immunization strategy to its non-immune neighbor who has the maximum degrees. The immunization strategy is spread layer by layer in the network until it reaches the immune critical value.

Through the cloud network security mechanism, we can obtain the security state of new nodes dynamically, and control the virus intrusion to a certain extent. When a virus is found, a new antibody can be generated according to its own decision analysis, which shortens the response time to the virus. Through the forward of immunization strategy, the infected nodes are immunized step by step to make the network healthy. Through this security mechanism, cloud network can become a security ecosystem with self-healing ability!

3.2 Hierarchy immunization strategy

If the Monitor Agent finds a node with malicious behavior, then this node is considered to be an infected node. The immunization strategy is send from the initially infected node. The nodes in the cloud environment are dynamic, so the degrees of the nodes are dynamic too. The target immunization strategy which is considered to be the most optimal immunization strategy needs to know the global information, so it is obviously not suitable for the cloud environment. Therefore, the target immunization strategy is improved in the paper. The new immunization strategy which is more suitable for the cloud network only needs to know the information of its neighbors rather than the global information. The Transmission Agent of every node in the network only saves the local information in the

hierarchy immunization strategy. The information of the Transmission Agent will be updated when the neighbors of the nodes access to or exit from the cloud network. The local information needed by Transmission Agent is shown in Fig. 1.

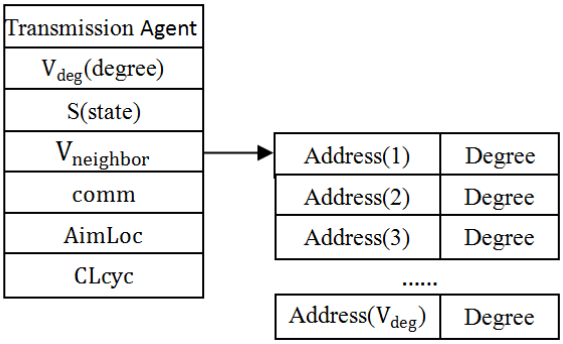


Fig. 1. The local information needed by Transmission Agent

The process of the hierarchy immunization strategy has two steps:

Step 1: The node which triggers the security mechanism is the first node to immune. Then its direct neighbors are immunized.

Step 2: The Transmission Agents of the nodes received the immunization strategy in the step 1 are activated. The nodes whose Transmission Agents are activated send the immunization strategy to their non-immune neighbor with the maximum degrees. The immunization strategy is spread in the network layer by layer. If the neighbors of the immune node are all immunized then take the random jump process to jump out of the local immune. The immunization strategy will be spread until the given proportion of the nodes are immune. If there are more than one nodes with the maximum degrees and non-immune in the neighbors of the current immune node, then the next immune node will be selected according to the risk value of the node. The random jump process and the risk value of the node are defined as follows:

Random jump process: if the neighbors of the current immune node are all immunized, then the the neighbor with the maximum degrees is regarded as the current immune node to spread the immunization strategy according to step 2.

Risk value: the risk value of the node is defined as $W = \sum_i unimmunity(j)$, in which $\sum_i unimmunity(j)$ represents the degrees sum of the non-immune nodes connected with the node i.

A simple network with 21 nodes is given in Fig. 2. And then the transmission of immunization strategy is simulated on this network.

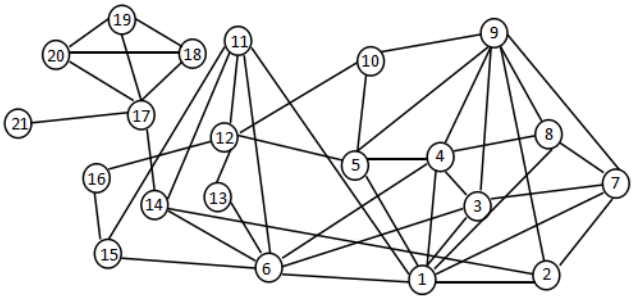


Fig. 2. A simple network with 21 nodes

The degrees of the nodes in the network are listed in Table 1:

Table 1

The degrees of the nodes in the network

Node ID	Degrees	Node ID	Degrees	Node ID	Degrees
1	8	8	4	15	3
2	4	9	7	16	2
3	5	10	3	17	5
4	6	11	5	18	3
5	5	12	5	19	3
6	7	13	2	20	3
7	5	14	4	21	1

It is suppose that the Monitor Agent of the node 13 detects the malicious behaviors, and then the security mechanism of the cloud environment is activated. The Query Agent or the Decision Agent provides the security policy, and then the Transmission Agent transmits them according to the hierarchy immunization strategy. The neighbors of node 13 are immunized in the first time. So the node 13, node 6, and node 12 are immunized in the first step seen from figure 2. Then the vaccines are spread by two paths: node 6 and node 12. The spread path is shown in Fig. 3:

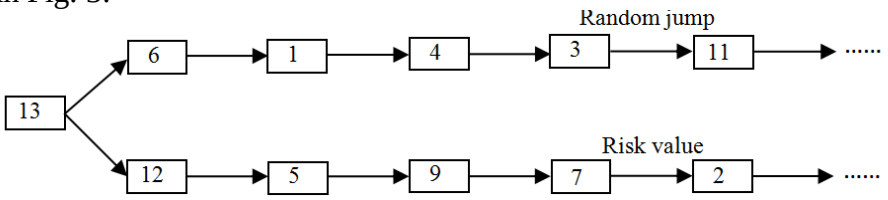


Fig. 3. The spread path of the vaccine

Along to the spread path of node 6, the neighbors of the node 3 are all immune when the vaccine spread to node 3. Then the neighbor with the maximum degrees of node 3 is regarded as the current immune node according to the random jump process. Node 1 is the neighbor with maximum degrees of node 3. So the node 1 is the current immune node. The neighbor which has the maximum

degrees and non-immune of the node 1 is node 11, and then the node 11 is the next immune node. The random jump process ended.

Along to the spread path of node 12, the non-immune neighbors of node 7 who have the maximum degrees are node 8 and node 2 when the vaccine spread to node 7. Then it needs to calculate the the risk values of the two nodes to judge the direction of the vaccine. The risk value of the node 8 is $W_8 = 0$, the risk value of the node 2 is $W_2 = 3$. Obviously $W_2 > W_8$, so the next immune node is node 2. If the node 8 is selected as the next immune node then it needs random jump process. It avoids the random jump process when select the node 2. The method of risk value can speed up the propagation velocity of the vaccines.

3.3 The inhibition for the virus spread flow of the hierarchy immunization

The virus spread flow and the vaccine spread flow both exist in the network when there is not immunization delay in the network. The virus tends to infect the nodes of high degree, but obviously it not as quickly as the targeted unidirectional spread of the vaccine. So the vaccines can immune the node of high degree before the virus. Suppose that a infection node infects its neighbors by the probability τ. The probability of any edge linked to the infection node with degrees k is $\frac{I}{N} \times \frac{k}{N\langle k \rangle}$, in which $\langle k \rangle$ represents the average degrees of the nodes in the network; I represents the number of the infection nodes; N is the total number of nodes in the network. Then the infection rate of the node with degrees k is:

$$\rho_k = \left[1 - \left(1 - \frac{I}{N} \times \frac{k}{N\langle k \rangle} \right)^k \right] \tau \tag{1}$$

And the probability of any edge linked to the immunized node with degrees k is $\frac{R}{N} \times \frac{k}{N\langle k \rangle}$. Then the probability of every non-immunized node with degrees k linked to the immunized node with degrees k is:

$$\lambda_k = 1 - \left(1 - \frac{R}{N} \times \frac{k}{N\langle k \rangle} \right)^k \tag{2}$$

It can be considered that the number of the infected nodes I and the number of the immunized nodes R obey: $I \approx R$when there is no immune delay. Because of $0 < \tau < 1$, then for the large k it can get the immune rate $\lambda_k > \rho_k$ when compare formula (1) and (2). So the propagation velocity of the vaccine is higher than the virus on the nodes of high degree. Then the virus will not outbreak

on the nodes of high degree. These nodes can prevent the propagation of virus effectively.

Suppose that the inhibition rate of the virus flow is $f_r \approx \frac{\sum_{k=1}^{\infty} kR_k}{\sum_{k=1}^{\infty} k(I_k + R_k)}$ when it consider the immune delay, in which R_k represents the number of the immunized nodes with degrees k; I_k represents the number of the infected nodes with degrees k; the value of f_r depends on the degrees of the immune nodes existed in the network. The degrees of most nodes are small. The degrees of a few nodes are relatively large because of the power-law characteristics of the scale-free network. So the inhibition rate of the virus flow f_r will be affected when the nodes of high degree are immunized as soon as possible. Every time the Transmission Agent selects the node of highest degree in the local environment to immune in the hierarchy immunization strategy. So the hierarchy immunization strategy can achieve the good effect in the respect of the inhibition rate of the virus flow.

4. Experiment and Results

We verify that the hierarchy immunization strategy is more effective than random immune, target immune and acquaintance immune by the simulation experiment in this section.

The performance of the hierarchy immunization strategy is compared in the random attacks and malicious attack on the BA scale-free network model by using the HSIR propagation model [20]. The experiment compares the effect of the hierarchy immunization strategy with the target immunization strategy, acquaintance immunization and random immunization. BA scale-free network has six nodes in the initial case and add a node with 5 degrees linked to the nodes existed in the network in a unit time, that is $N = 10^3$, $m_0 = 6$, $m = 5$. The initial rate of the infection nodes is set to 0.5, and the transmission rate is $\lambda = 0.25$. When the network is built successfully, P (P is a random integer, $P \in [-5,5]$) nodes are added to the network in a unit time. This process simulates a dynamic cloud network.

In the experiment of random attack, we choose the same proportion of nodes as infected nodes randomly in the same network, and then implement different immunization strategies. The efficiency of the immunization strategies is measured by observing the transmission rate of the virus in different proportion nodes. The efficiency of the immunization strategies is measured by comparing the transmission rate of the virus when the nodes with the same proportion are immunized.

In the experiment of malicious attack, we choose the nodes with the same proportion and higher degrees as the infected nodes, and then implement the immunization strategies to compare the efficiency of different immunization strategies. The process of the experiment is shown in Fig. 4:

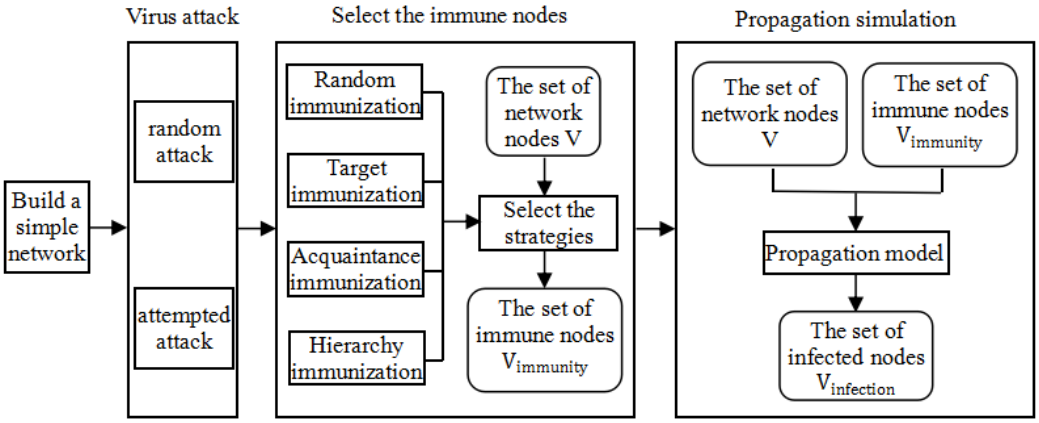
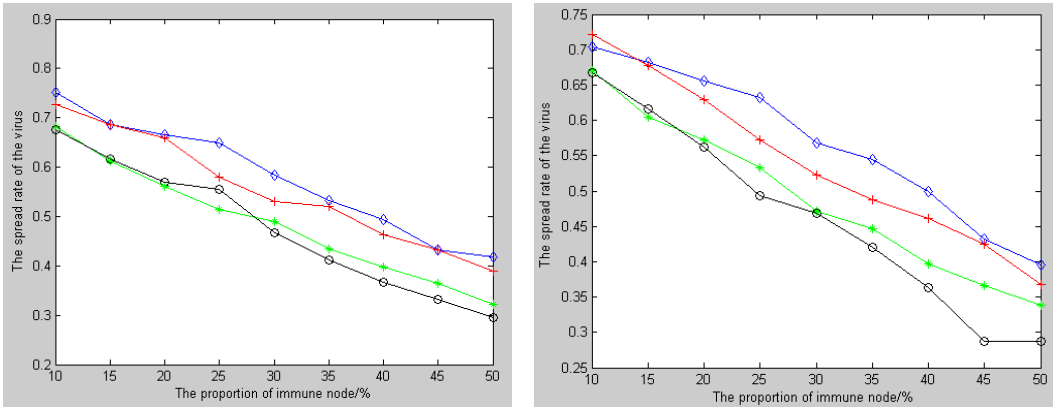


Fig. 4. The process of the experiment

The efficiency of the immunization strategy is measured by the spread rate of the virus in the stable state. The spread rate of the virus is $\rho = \frac{\rho_f}{\rho_0}$, in which ρ_0 represents the final infection density of the network without the immunization strategy; ρ_f represents the final infection density of the network with the immunization strategy. The Fig. 5(a) represents the final spread rates of the virus under the four immunization strategies when immune the nodes of different proportions in the random attack.



(a) (b)

Fig. 5. The compare of the four strategies in random attack (a) and malicious attack (b)

Fig. 5(b) represents the final spread rates of the virus under the four immunization strategies when immune the nodes of different proportions in the malicious attack. The efficiency of the hierarchy immunization strategy under different attacks are shown in Fig. 6.

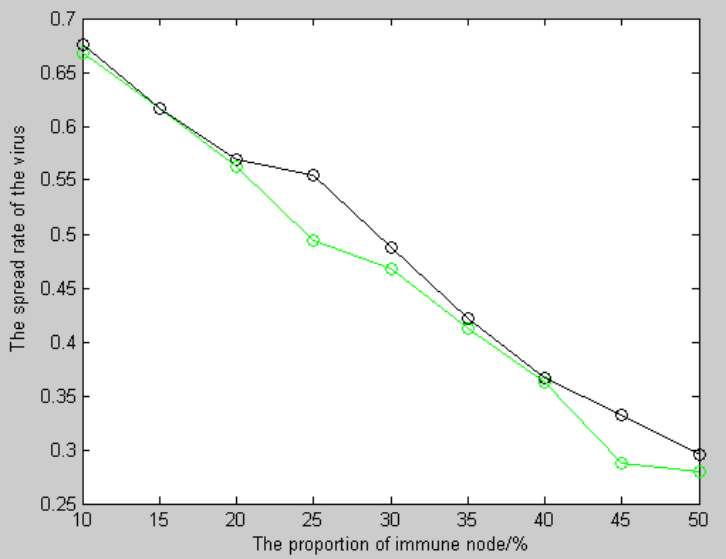


Fig. 6. The efficiency of the hierarchy immunization strategy under different attacks

5. Discussion

The hierarchy immunization strategy is better than the random immunization strategy and the acquaintance immunization strategy both in the random attack and malicious attack seen from Fig. 5. The efficiency of hierarchy immunization strategy is higher than that of target immunization strategy, when the immune proportion increases seen from Fig. 5.

It is easy to understand that the efficiency of the hierarchy immunization strategy is better than that of the target immunization strategy. The hierarchy immunization strategy considers the spread direction of the virus, so the propagation of the virus can be inhibited rapidly. The spread direction of the virus is not considered in the target immunization strategy which immune the nodes according to the degrees of the nodes, so its efficiency is lower than the hierarchy immunization strategy. In addition, the global information is not needed in the hierarchy immunization strategy. The global information of the practical network can not be obtained, so the hierarchy immunization strategy is better than the target immunization strategy in the aspect of implementation.

The hierarchy immunization strategy is more effective under the malicious attack seen from the Fig. 6. So the hierarchy immunization strategy is more suitable for the cloud environment which is weak under the malicious attack.

In the experiment, the hierarchy immunization strategy based on the ecological operation mechanism of cloud network can monitor the node which is added dynamically and quickly get the threat information. In the process of forwarding, we can quickly get the most valuable immune nodes according to the local information, so that the vaccine can play the maximum effect.

6. Summary

This paper uses some views and knowledge of ecology. Based on the common characteristics of the complex adaptive system, this paper puts forward the security mechanism and hierarchy immunization strategy for the cloud environment. The security mechanism of cloud network monitor the added users and then generates the corresponding immunization strategy according to their own decision analysis when discovering the virus. Then, the network is gradually restored to health, through the forwarding rules of hierarchy immunization strategy. Finally, we get a self-healing cloud network.

The study of the immunization strategies is significant for the inhibition of the virus in the network. The immune technology of the network based on the propagation characteristics of the virus can effectively suppress the large-scale diffusion of the virus in the network. The characteristics of the cloud environment are large-scale, distribution and dynamic. So the cloud environment has strong robustness for the random attack and high vulnerability for the malicious attack. The hierarchy immunization strategy was proposed based on these characteristics of cloud network. The hierarchy immunization strategy which is suitable for the cloud environment needs not to know the global information. It can effectively ensure the security of cloud network when we combined with the security mechanisms and the hierarchy immunization strategy. In addition, the paper verified the effect of the immunization strategy by the experiment. Compare to the traditional immunization, the proposed strategy satisfy the cloud network.

Unfortunately, we only proved the superiority of the hierarchy immunization strategy in theory at present, but not in practice. In the future research, we will verify its applicability in the actual cloud network.

REFERENCES

[1]. *A. Lenk, M. Klems, J. Nimis, S. Tai, T. Sandholm*, What's Inside the Cloud? An Architectural Map of the Cloud Landscape. Vancouver: In ICSE Workshop on Software Engineering Challenges of Cloud Computing, 2009.

[2]. *A. Aboulnaga, K. Salem, A. A. Soror*, et al, "Deploying Database Appliances in the Cloud", in Bulletin of the IEEE Computer Society Technical Committee on Data Engineering, **vol. 32**, no 1, 2009, pp. 13–20.

[3]. *M. Christodorescu, R. Sailer, D. L. Schales*, et al, Cloud Security is not (just) Virtualization Security: CCSW 2009: Proceedings of the 2009 ACM workshop on Cloud computing security, Chicago, 2010.

[4]. *M. E. J. Newman*, "The Structure and Function of Complex Networks". in SIAM Review, **vol. 45**, no. 2, 2003, pp. 167-224.
[5]. *A. Maulana, M. Kefalas, T. M. Michael*. "Immunization of Networks Using Genetic Algorithms and Multiobjective Metaheuristics", in Computational Intelligence. IEEE, 2018.
[6]. *F. Taghavian, M. Salehi, M. Teimouri*, "A local immunization strategy for networks with overlapping community structure", in Physica A: Statistical Mechanics and Its Applications, **vol. 467**, no. 1, 2017, pp. 148-156.
[7]. *Y. Min, Z. Jiayue, Z. Damin*, "Immunization strategy based on discrete particle swarm optimization algorithm in BBV network", in International Conference on Intelligent Systems & Control. IEEE, 2017.
[8]. *X. Li, J. Guo, C. Gao*, et al, "A hybrid strategy for network immunization", in Chaos Solitons & Fractals, **vol. 106**, January 2018, pp. 214-219.
[9]. *F. Nian, X. Wang*, "Efficient immunization strategies on complex networks", in Journal of Theoretical Biology, **vol. 264**, no. 1, 2010, pp. 77-83.
[10]. *M. Salathe, J. H. Jones*, "Dynamics and Control of Diseases in Networks with Community Structure", in Plos Computational Biology, **vol. 6**, no. 4, 2010, pp. 1-11.
[11]. *Y. Kai, W. Lei, G. Wenqiang, et al*, "A transmission-limit inspired immunization strategy for weighted network epidemiology", in International Journal of Modern Physics B, **vol. 32**, no. 23, 2018, pp. 1850251.
[12]. *R. S. Pastor, A. Vespignani*, "Epidemic spreading in scale-free networks", in Physical review letters, **vol. 86**, no. 14, 2001, pp. 3200-3203.
[13]. *J. Gomez-Gardenes, P. Echenique, Y. Moren*, "Immunization of real complex communication networks", in The European Physical Journal B - Condensed Matter and Complex Systems, **vol. 46**, no. 2, 2006, pp. 259-264.
[14]. *W. G. Lin, C. Peng, T. W. Liao*, " Research on edges immunization strategy for complex network based on SIS-CA mode", in Procedia Manufacturing, **vol. 17**, 2018, pp. 1065-1072.
[15]. *L. Jiming, G. Chao, Z. Ning*, "Virus Propagation and Immunization Strategies in Email Networks", in Lecture Notes in Computer Science, **vol. 5678**, 2009, pp. 222-233.
[16]. *L. Jiming Liu, G. Chao, Z. Ning*, A Distributed Immunization Strategy Based on Autonomy-Oriented Computing, in ISMIS '09 Proceedings of the 18th International Symposium on Foundations of Intelligent Systems, Prague, Czech Republic, September 2009.
[17]. *L. C. Chen, K. M. Carley*, "The Impact of Countermeasure Propagation on the Prevalence of Computer Viruses", in IEEE Transactions on systems, Man And Cybernetics-Part B: Cybernetics, **vol. 34**, no. 2, 2004, pp. 823-833.
[18]. *S. Pearson*. Taking Account of Privacy when Designing Cloud Computing Services. In ICSE Workshop on Software Engineering Challenges of Cloud Computing, Vancouver, Canada, May 2009.
[19]. *L. Litty, H. A. Lagar-Cavilla, D. Lie*. Computer meteorology: Monitoring compute clouds. In Proceedings of the 12th Workshop on Hot Topics in Operating Systems (HotOS 2009), May 2009.
[20]. *F. Tongrang, L. Yanjing, G. Feng*, "Study of Virus Propagation Model in Cloud Environment", in International Journal of Security and its Applications, **vol. 7**, no. 4, 2013, pp. 257-265.