International Journal of Security and Its Applications
Vol. 10, No. 11 (2016), pp.119-130
http://dx.doi.org/10.14257/ijsia.2016.10.11.11

Internet Immunization Strategy based on Relations of Nodes

Fan Tongrang[1], Qin Wanting[2], Zhao Wenbin[3*], Wang Qian [4] ,Yu Tao[5]

[1,2,3,4] *School of Information Science and Technology, Shijiazhuang Tiedao University, Shijiazhuang, Hebei 050043, China*
[5] *Institute of Network Science and Cyberspace, Tsinghua University, Beijing, 100084, China*
[1]*fantr@stdu.edu.cn,* [3*]*zhaowb.email@qq.com*

Abstract

Inspired by the biological immune system against outside invasion in nature, this paper propose a network security strategy using Agent technology. The Agents with independent behavior capacity are set for resisting network intrusion using their spontaneous coordinate organization. Based on the comparisons of existing immunization strategies, such as target immune, acquaintance immune and random immunity, it is found that the importance of nodes in network are influenced by interaction between nodes, degree of nodes, information flow, and other factors. If the nodes are more important, they have a greater influence over the whole network. When important nodes are infected by virus, there will be a higher probability of spreading of hazard information. Therefore, this paper proposes a network security model using Agent technology, where important nodes are implanted with relationship immunization strategy. Experimental results show when the network suffered from random or malicious attacks, relationship immunization strategy is more effective than others existing methods.

Keywords*: Immunization Strategy; Relationship Immunization Strategy; Nodes Relationship Model; Information Flow.*

1. Introduce

With the increasingly serious network security problems, it is becoming a focus research that introducing the immunization strategy to solve the spread of virus in computer network, which can be divided into the random, target, and acquaintance immunization strategies. In the random immunization strategy proposed by Pastor-Satorras et al. [1], nodes are random selected for immunization where all nodes are treated equally. However, the node with higher degree has higher priority in the target immunization strategy [2], which has limitation of needing to know the global information of Internet. Gomez-Gardenes et al. [3] improve it by translating global issues into regional issues, which has a good result that through the link of node looking for the high degree node and immune it. The acquaintance immunization is proposed by Cohen et al. [4], where a node is first randomly selected and then immune to its neighbor nodes until a specified threshold is obtained.

Base on the acquaintance immunization, Liu et al. [5] propose the common acquaintance immunization, which find the common neighbor of nodes in the network for immunization. Gallos et al. [6] choose neighbor nodes with more links than a given threshold for immunity. These methods increase successful rate of the acquaintance immunization strategy. Nian et al. [7] propose a high risk immunization strategy which similar with acquaintance immunization strategy. At each time step, it only immune some high degree neighbor of infected nodes because the high degree nodes have a greater probability to become infected nodes.

ISSN: 1738-9976 IJSIA

However, the above immunization strategies only consider the immune effect of node without the correlation among node characteristics. Zhang et al. [8] propose a model to measures the relationship between two nodes, where more closely the links between nodes are more likely to become infected nodes. This paper presents a new relational immunization strategy which considers correlation between network nodes based on the above model.

2. The Relational Immunization Strategy

In this section, the network security principle based on Agent is first reviewed, then our relational immunization strategy is introduced based on the Agent model.

2.1. Agent Network Security Strategy

2.1.1. Role Assignments of Agent

Nature of biological systems against outside invasion brings us inspiration in network security research, especially the ability about how to identify itself in the immune system. In the biological immune system, B and T cells are all independent functional unit of life. B cells can detect intrusion while producing plant pathogenic proteins, and record pathogen and coping strategies. When the same pathogen attacks once again, it will activate the B cell. Inspired by the above biological system, we use the intelligent Agent by Luo et al. [9] technology to simulate the operation mechanism of the immune system in network, which make network also has the ability to spontaneously against viruses. The agents have capacities of independent behavior and spontaneous coordination organization against the danger of invasion. In network, the agents can be divided into the following categories:

- **Monitor agent.** It is mainly used to detect whether there exits some behaviors that threaten normal operation of network. Based on perception and detection of the local network environment and various behaviors of network, the monitor agent make response and analysis, especially when the network environment other agents have changed.
- **Query agent.** It is mainly used to receive dangerous information from the monitor agent, and the query itself if there is a solution security policy in the library to deal with it. If the query agent don't have a solution policy to deal with it, that means the monitor agent detect a new dangerous which has never seen. Now we need make a solution, and activate the decision agent.
- **Decision agent.** Its functionalities are using decision analysis to generate relevant specifications and strategies to deal with new hazards and activating the attack agent.
- **Interaction agent.** It primarily communicates with the other interaction agents in the network while interacting updating its security policy.
- **Attack agent.** It is mainly against the invasion of the dangerous information. The attack agent carries solutions and move to risk node nearby when it activated, then use the solution for dealing with hazardous. If the treatment is unsuccessful, the decision agent will be reactivated and making a new solution to deal with the hazardous. If the treatment is successful, the interaction agent will be activated.

2.1.2. Principle of the Agent Model

According to the above agent model in the last section, the proposed network security mechanism works as follow shown in Fig. 1:

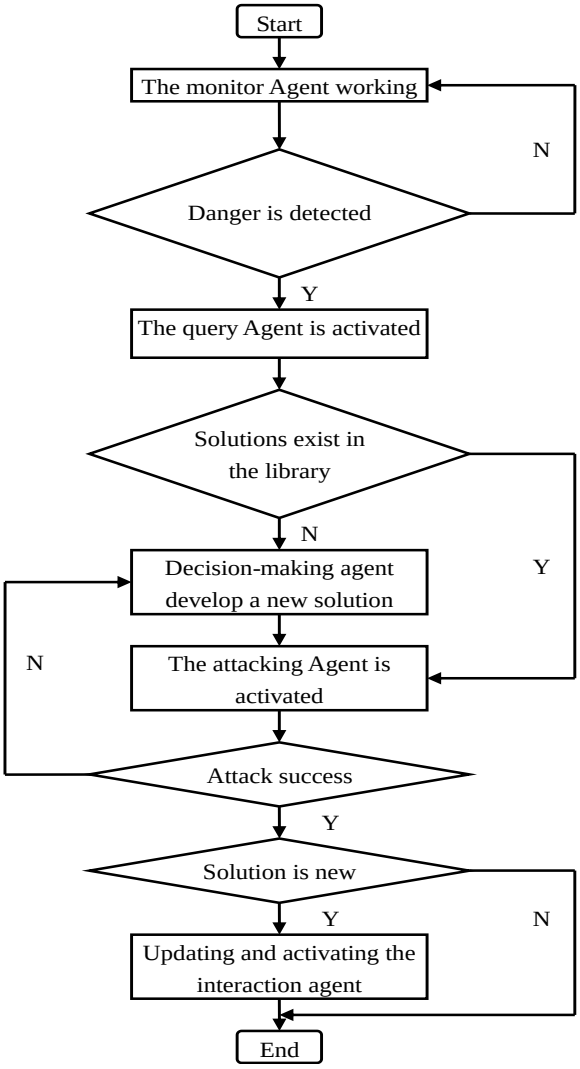


Figure 1. Security Operation Process

Step 1: The monitor agent constantly detects whether there exits dangerous information which endanger to the healthy and stable operation of the network. When dangerous information is found, go to step 2.

Step 2: The query agent seeks the possible solutions of the detected dangerous information in its library. If the solutions are exited, go to step 4, else to step 3.

Step 3: The decision agent analyze related policy for the detected new risks.

Step 4: The attack agent move to the node which carries the dangerous information, and deal with the dangerous based on the queried solution. If it fails, then go to step 3 to re-design solution until the hazard information is resolved. When it resolved, if the carrying solution is a new one, go to step 5, else ending.

Step 5: Updating the solution library, the interaction agent sends new immunization strategies to other nodes according to the immunization strategy.

When the node successfully resisted the spread of dangerous information, how the "vaccine" propagated between nodes in the network will affect the efficiency of network security. In the last section, we will propose a novel immunization strategies based on node relationships.

2.2. Immunization Strategies via Node Relationships

After a successful defense by the attack agent, the interaction agent will pass the defense solution to other nodes in order to immune the new dangerous information in the network, which will prevent the virus spreading on a large scale in the network. Viruses spread from one node to another one through a certain probability. If a node frequently interacts with the other node, which indicates that the node in the network has an important position. The important nodes transmit the virus to the surrounding nodes with a high probability. Therefore, we can set the immunization on these important nodes to effectively suppress transmission of the bad information. In this section, the relationship immunization strategy will be introduced inspired by the concepts from physics by Xu et al. [10]. Considered the characteristics of nodes include activity *Nod_Act*, the ability of process *Nod_Pro*, resources *Sou_Vis*, the path status of the node to a destination node *Net_Jam*, the relationship strength between nodes i and j in k value $str(i, j, k)$, familiarity between nodes $fam(u_i, u_j)$ by Xu et al. [10], the attraction force F_i of node i to the other nodes is defined as follows:

$$F = \frac{Sou\_Vis \times Nod\_\Pr o \times Nod\_Act}{Net\_Jam} \times (\sum_{k=1}^{k=3} str(i, j, k) + fam(u_i, u_j)) \quad (1)$$

According to the relationships between nodes model, we can obtain degree of intimacy between the nodes in the following two aspects.

The summary of the node's forces:

$$\sum_{i=1}^{i=n} F_i \quad (2)$$

Node betweenness is the proportion between the path through the node and the total number of the shortest path in the network. Therefore, the node betweenness has identified the importance of nodes in the network. In order to get the betweenness of all the nodes in the network, Martin Everett Everett et al. [12] introduce individual centrality as the following equation.

$$Bet = \sum \frac{1}{A^2[1-A]_{i,j}} \quad (3)$$

Where A is the adjacency matrix for a network graph, $A_{i,j}$ contains the number of walk of 2 length connecting i and j.

Based on these factors, the node importance degree is finally defined as

$$W = \sum F_i \times Bet . \quad (4)$$

The force of node and betweenness illustrate the importance of nodes and leverage in the network. Viruses through important nodes will easily spread to whole network. Therefore, making immunization strategy focusing on important nodes can effectively guarantee the network security. The steps using node importance for developing immunization strategy are as follows:

(1) Finding the node which carry risk information, then plant immunization strategy to the node and its connected nodes.

(2) Sending the immunization strategy to the adjacent node of the immunized nodes, whose important degree called W , is the largest. New immune nodes propagate immunization strategy in the same way until the number of immune nodes reaches the critical value.

(3) When the neighbor node has not been immune, and the node which has a maximum value W has more than one, then we randomly select a node for immunization.

3. Simulation and Analysis

In this section, the experiments of the proposed immunization strategy are compared with random, acquaintance and target immunization strategies. Their relationships are also analyzed.

3.1. Simulation Process

3.1.1. Establishment of Experimental Network

Since most of the real network meeting the power law distribution which belongs to the scale-free network, this experiment is based on this model to construct scale-free networks. We will build an algorithm form, Pastor-Satorras et al. [1] using MATLAB for simulation. First we construct a scale-free networks with 500 nodes, and set add and preferential attachments.

Add: We start from a small number m_0 of disconnected nodes. Each time step a new node is added, with m links that are connected to an old node i . Here we set $m \le m_0$.

Preferential attachment: Defined p_i as a probability which a new node connected to an old node i and k_i as degree of node i . The node j and the degree k_i have a relationship as the following equation:

$$p_i = \frac{k_i}{\sum_j k_j} \tag{5}$$

Here we set $m_0 = 6, m = 5$. With the growth of number of nodes and edges in a network, we stop when the node number reaches 500 shown in Fig. 2.

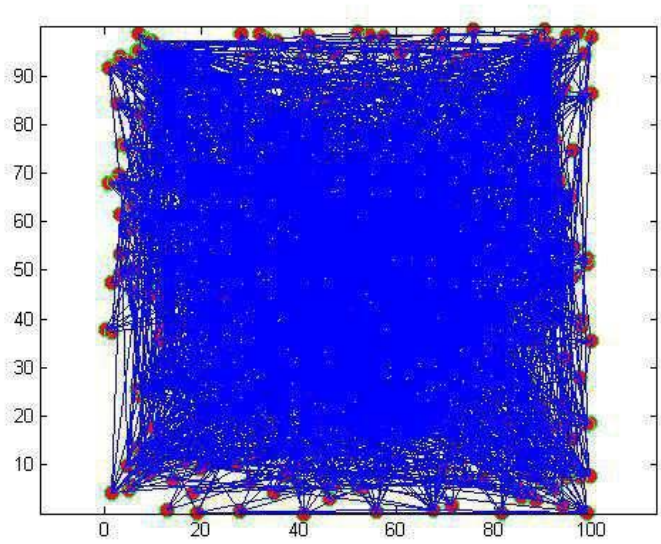


Figure 2. The Scale-free Network Simulation

In this network, the relationship between nodes more closely, the greater the likelihood of information flow between nodes, then virus may be transmitted between nodes. The force between the nodes and the betweenness decided the importance of node. Interaction between nodes and nodes is based on the dissemination of information flow records and the center property of node. If the central node is invaded, it will spread the virus to more nodes. So dig out the center node distribution in the network has an important significance for the network security strategy formulation. In our experiment, importance of node distribution is shown in Fig. 3, where the node importance of distribution is similar to the node degree distribution, and only a small number of nodes dominate in the network.

3.1.2. Attack Strategy

The scale-free network is with extremely uneven degree distribution characteristics, if nodes with high degree are attacked by virus, the virus will quickly spread throughout the network. Therefore, two virus transmissions will be set in our experiment: random propagation and malicious propagation. Random propagation is that when a node is infected, the virus will randomly spread its links to one of adjacent nodes. Malicious propagation is that when a node is infected, viruses only propagate its links to the adjacent nodes which has a high degree.

Using the simple network shown in Fig. 4, we illustrate the process of viruses spread.

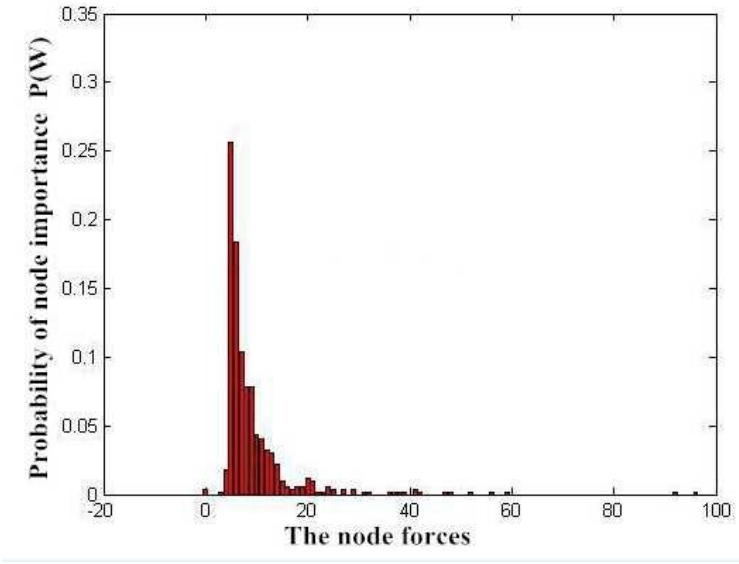


Figure 3. The Distribution of Importance Nodes in the Network

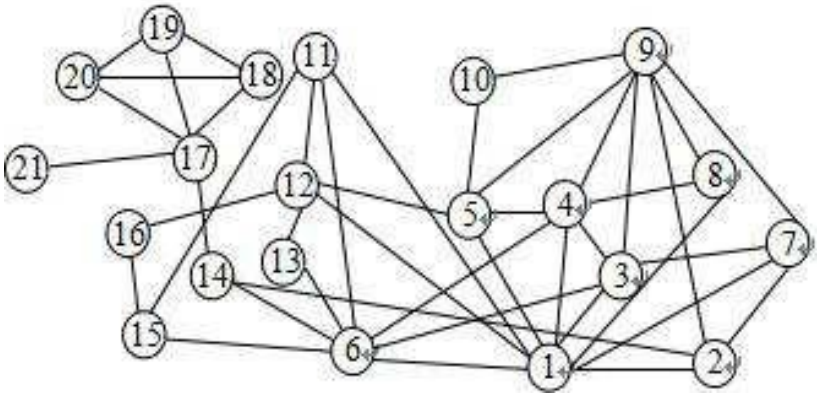


Figure 4. Simple Network

• **Random propagation.** When the node 11 is infected, viruses will pass with 4 nodes which connected to the node and then randomly selected one for propagation. The infected nodes infect other nodes in the same way.

• **Malicious propagation.** When the node 11 is infected, there are 4 nodes connected to the node 11: node 1, node 6, node 12 and node 15. The degree of node 1 is 9; other three nodes of degrees are 7, 5 and 3. So node 1 will be infected because of the maximum degree.

Then node 1 infects other connected nodes in the same way. When two nodes have the same degree, the random infection is one of them. The number of infected nodes in the network is basically unchanged.

We assume that a virus spreads for a while until the virus infects the most of node in the above set of scale-free networks. And we apply random, acquaintance, target and relationship immunization strategy proposed in this paper to inhibit the spread of the virus. Finally, under the four immunization strategies, we statistics out the number of nodes which needed to prevent the spread of the virus. The simulation of flow chart is shown in Fig. 5.

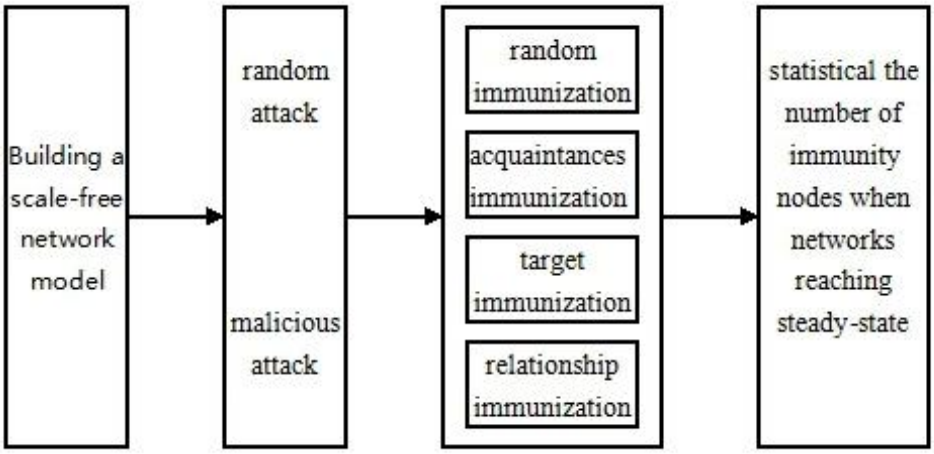


Figure 5. Simulation of flow chart

The random attack steps in our experiment are as follow:

(1) Initialization: according to the scale-free networks algorithm described in our paper to construct a scale-free network.

(2) Planting the virus in the resulting network in first step, which spread in the network for random.

(3) After a period of time, we are immune to network nodes in random.

(4) When virus transmission is blocked and stabilized, we counted how many nodes can stop the spread of virus when apply this random immunization strategy.

This experiment is repeated three times, where the third step in the random immunization is replaces to acquaintance, target and relationship immunization strategy respectively. After completing the above four experiments, we obtained four sets of data.

Finally we obtain a comparison chart which includes four immunization strategy immunization required number of nodes. Then, we also need a series of experimental in a malicious attack. It is similar with random attacks experiment, and only need change the random spread of the virus to spread virus to high degree of nodes in second step. Then repeat it three times with acquaintance immunization strategy, target immunization strategy and the relationship immunization strategy. Now we have eight experiments and divide to two groups: malicious attack and random attack. In the spread of the virus when steady-state is reached, each performing different immunization strategies. Steady-state here refers to the continuous detect the number of infected nodes and the number of propagate nodes in the network until five times in a row the number of infected nodes and propagate nodes changed in a small range and the number of infections is not less than 50%, then we perform immunization strategy. When the steady-state of the immune network is achieved, we count the number of immune nodes needed to prevent the spread of the virus. The immune steady-state here refers to the continuous detect the number of infected nodes and the number of propagate nodes in the network until five times in a row the number of infected nodes and propagate nodes changed in a small range and the number of infections is less than 5%.

3.2. Simulation Analysis

When network suffering malicious attack, virus spread among the nodes in the network. When the dissemination of steady-state is reached, implanted immunization strategy to prevent the spread of the virus, when it reaches the stable immune status, stop implantation immunization strategy. Statistics the number of nodes which perform such immunization strategy finally need to be immune. After four times experiments, we got four immunization strategy statistical figure as shown in Fig.6 for random attach and in Fig. 7 for malicious attack.

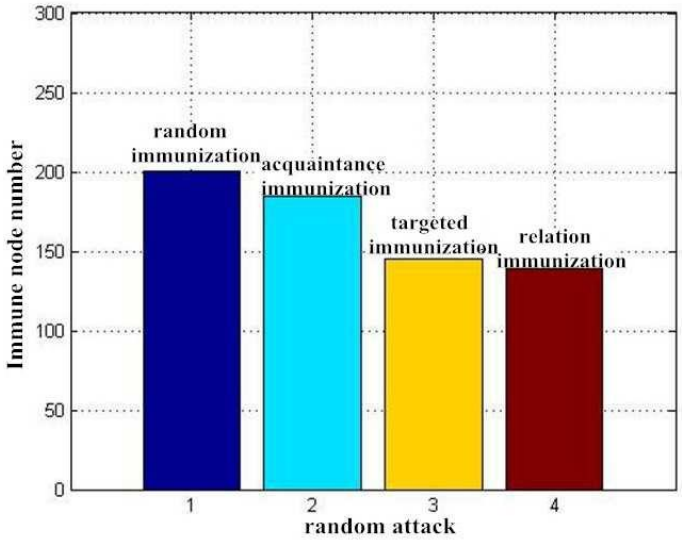


Figure 6. Compared with Four Immunization Strategies in Random Attack

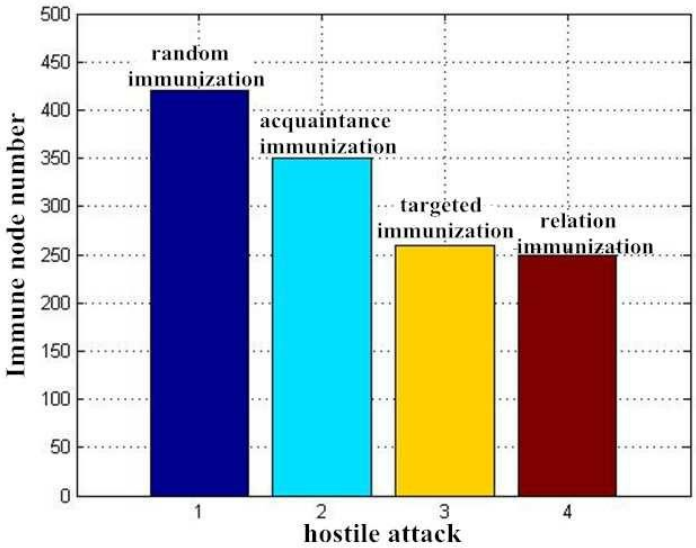


Figure 7. Compared with Four Immunization Strategies in Hostile Attack

We can draw a conclusion from Figs. 6 and 7 that when the network is subjected to random attacks and malicious attacks, the number of nodes required of relationship immunization strategy is less than random immunization strategy, acquaintances immunization strategy or target immunization strategy. So the relationship immunization strategy proposed in this paper is the best in the four immunization strategy. The relationship immunization strategy is efficient because it considered the importance of nodes in the network. In this experiment, the relationship immunization strategies is better than target immunization strategy due to relationship immunization strategy taking into account the information flow of propagation characteristics. While propagation characteristic of virus is similar with the information flow, which consider the resources, betweenness and propagation of records of the node, the target immunization strategy does not take into account these, it only sort of node degree size, and in turn to immune.

Meanwhile, in scale-free networks, the characteristics of a few nodes have a large number of links lead to the network's robustness and vulnerability. In random attacks, the probability of infected nodes is equal. While malicious attack is more damage than random attack, which infect the nodes that has high degree so that we should immune more node to prevent the infection. Compared with Fig. 6 and Fig. 7, malicious attack needs more nodes to immune than random attack. From the perspective of actual network, it is impossible to get global information in large network, and relationship immunization only needs to know the information from surrounding nodes that connected, so relation immunization strategy have more actual operational. Through the experiments we prove the feasibility of relation immunization strategy. So when the dangerous information flow spread in the network, we can use the relationship immunization strategy to control the spread of dangerous information. For example, when we find a virus in the computer network, we can query the anti-virus programs in virus library, and disinfect the essential computer nodes. Similarly, when we find bad information in the social network, we can control the key nodes in the network to prevent the spread of harmful information.

4. Conclusion

Setting by some entities agent in the network, this paper introduces a method about how to reduce the spread of viruses in the immune system, simulates on an ecological network, and develop an eco-network mechanisms. When new threats have been successful addressed in the network, the solutions will be passed to the other node in the network. We use the relationship between the nodes to develop a vaccination strategy, and pass the solution through the immunization strategy to other nodes in the network. The relationship immunization strategy adapts to distributed network environments, because it does not need to know the global information but also can guarantee network security. Experimental results show when the network suffered from random or malicious attacks, relationship immunization strategy is more effective than others existing methods. It is concluded that the relationship immunity has a high suitability.

Acknowledgement

This study is funded by the National Natural Science Foundation of China (#61373160).

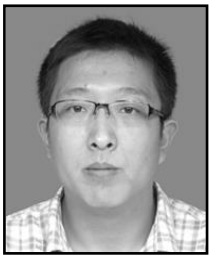
References

[1] Pastor-Satorras, R., Vespignani, A. 'Epidemic spreading in scale-free networks', Physical review letters, **(2001),** 86(14):3200–3203.
[2] Albert, R., Jeong, H., Barabási, A.L. 'Error and attack tolerance of complex networks', Nature, **(2000)** 406(6794):378–382.
[3] Gomez-Gardenes, J., Echenique, P., Moreno, Y. 'Immunization of real complex communication networks', The European Physical Journal B, **(2006),** 49(2):259–264.
[4] Cohen, R., Havlin, S., Ben-Avraham, D. 'Efficient immunization strategies for computer networks and populations', Physical Review Letters, **(2003)**, 91(24):247901–247901.
[5] Liu. P., Miao. H., Li. Q. 'A common acquaintance immunization strategy for complex network', Computer and Information Science, **(2009)**, 8(8):1129–1139.
[6] Gallos, L.K., Liljeros, F., Argyrakis, P. 'Improving immunization strategies', Phys. Rev. E, **(2007)**,75(4):1–4.
[7] Nian, F., Wang, X. 'Efficient immunization strategies on complex networks', Journal of Theoretical Biology, **(2010)**, 264(1):77–83.
[8] Zhang. J., Jin, Z. 'The analysis of an epidemic model on networks', Applied Mathematics and Computation, **(2011)**, 217(17):7053–7064.
[9] Luo, J.Y., Shao, Z.Q. 'Development and application of agent technology', Computer Applications and Software, **(2009)**, 26(3):179–180.
[10] Xu, R.F., Fan, T.R. 'Study of information flow behavior on conditioned energy networks', Computer Science, **(2012)**, 39(10):82–85.

[11] Daly, E.M, Haahr, M. 'Social network analysis for information flow in disconnected delay-tolerant MANETs', IEEE Transactions on Mobile Computing, **(2009)**, 8(5):606–621.
[12] Everett, M., Borgatti, S.P. 'Ego network betweenness', Social networks, **(2005)**, 27(1):31–38.

Authors

Fan Tong-rang, born in 1965, Professor. Ph.D. School of Information Science and Technology, Shijiazhuang Tiedao University. Her main research interests include network technology and Information processing. Email address: fantr@stdu.edu.cn; fantr2009@126.com.



Zhao Wen-bin, born in 1985, Ph.D. School of Information Science and Technology, Shijiazhuang Tiedao University. His major field of study is network technology and information processing. Email address: zhaowb.email@qq.com.