A CONTROL POLICY OF INFORMATION FLOW BEHAVIOUR MODEL BASED ON NODE HETEROGENEITY

Tao Yu,* Zhao-Wen Zhang,** Wen-Bin Zhao,** Tong-Rang Fan,** and Jilong Wang*

Abstract

The development and improvement of Internet technology has made network information richer and more attractive. Users can access networks more easily and enjoy greater network services. While the Internet provides rich and convenient service, Internet networks also provide greater conditions now for the breeding and spreading of harmful information. The user is subject to information dissemination on the network, and the user's behaviour in information flow has a tremendous impact on information dissemination. In this paper, based on the heterogeneity of the nodes in a network, an information flow model is established, wherein the factors influencing a node's information flow behaviour are researched and categorized as factors internal and external to the node. The internal factor entails the autonomy of a node, which contains the degree of interest and the subjective judgment of the node. The external factors comprise the network structure, the location of the node, and the relationships among the nodes. Considering the issue of the spread of harmful information, a complex network model is built based on the information flow behaviour of the nodes, and a control policy to address harmful information is established.

Key Words

Information flow, complex network, heterogeneity, behaviour, control policy

1. Introduction

Currently, the vast numbers of users in Internet networks provide the essential condition for information dissemination. To an increasing extent, people communicate *via* instant messaging (IM). IM allows users to share information and resources and exchange and publish their views anytime and anywhere. This network organization format and the content transmission mode, which is considered user centric, focus on the user's consciousness of his or her own conduct, and the essence of this network organization is to meet the user's demand for diversified and personalized service. Users are the main participants in social networks. The dissemination and diffusion of rumour, opinion, behaviour, and other information in the network have a huge impact on people's lives and the social fabric. Research on the flow of information in social networks has become a research hotspot. Using instance data from real networks and other fields' knowledge is a popular and common way to study information networks [1], [2]. With respect to individual heterogeneity, some scholars have classified individuals in a network and studied the influence of authoritative nodes in information transmission [3]. Others study the impact of human heterogeneity on information transmission [4]. Furthermore, recent studies have confirmed that a number of complex cognitive mechanisms such as the memory effect, social strengthening effect, and attenuation in a message play a key role in the communication process [5]. Shu [6] proposed a strain message model on the basis of the susceptible infected recovered (SIR) model, which takes the impact of the memory effect on the dissemination of information into account. Other researchers established a function reflecting cumulative memory effects [7]. Yet, a key factor is the fact that ignoring memory capacity is different for each individual on the network. In a complex network of individuals, some cannot avoid interacting with other individuals, and when an individual in a network makes decisions about an event, it is inevitable that he seek the views of other individuals or seek proposals; and when there is more than one neighbour featuring a message about an individual to the same individual or featuring proposals, the individuals are more likely to receive the message or suggestion [8], [9]. Even if the individuals are independent and rarely accept recommendations from other people, it is hard not to be affected. Thus, the subjective nature of individual strength is particularly important. For the main factors of message propagation in a network, information concerns

* Institute of Network Science and Cyberspace, Tsinghua University, China; e-mail: yu_tao@mail.tsinghua.edu.cn, wjl@cernet.edu.cn

** School of Information Science and Technology, Shijiazhuang Tiedao University, China; e-mail: {1289356001, zhaowb.email}@qq.com, fantr@stdu.edu.cn, fantr2009@126.com

Corresponding author: Tong-Rang Fan

Recommended by Dr. Xiaonv Hu

(DOI: 10.2316/Journal.206.2018.5.206-0069)

the internal appeal and interaction between individuals. For the interactions between individual factors of message spread, a case would be analysed by message propagation delay between two individual factors [10]. In individual interactions, however, we still have to take into account individual heterogeneity in complex networks. Individual acceptance of other individuals suggests seeing if they are highly subjective. Considering the heterogeneity of individual subjectivity and the memory effect, we built an information flow model based on the SIR model.

This paper establishes an information flow mode based on the heterogeneity of nodes in a network and researches the factors, both internal and external, that influence the information flow behaviour in a node. The internal factor is the autonomy of a node, which contains the degree of interest and the subjective judgment of the node. The external factors are the network structure, the location of a node and the relationships among the nodes. To address the issue of the spread of harmful information, a complex network model is built based on the information flow behaviour of the nodes, and a control policy for harmful information is established.

2. Related Work

2.1 Information Flow

An effective way to research network information flow is to approach it from the perspective of physics. For example, by studying the information propagation in mobile ad networks, the relationships between the behaviour of the information flow in the network and the number of nodes, mobility, and network coverage, *etc.*, can be discovered [11]. The force between the nodes' representation is built to analysis and control of network information behaviour [12], on the basis of some factors affecting the communication between nodes, such as resources, demand, and others.

Lin [13] used a "bridge" to solve the problem of "structural holes", easing the issue of being dependent on only one node in the information flow process. Briscoe and Marinos [14] regarded the request for service at the cloud computing platform as a service process of the information flow. Zhijie [15] and others considered the nodes' energy, historical information, and current network topology, *etc.*, to put forward an algorithm based on geographic routing and topology control to effectively guide the transmission flow.

The strength of the relationships between the nodes in social networks is an important factor in the process of information dissemination. In the traditional representation of propagation behaviour for the dissemination of information in a social network, the network users pay more attention to the degree of interest in this information [16], the degree of involvement of other users of the information, such as user comments [17], the number of discussions [18], [19], and other factors in information dissemination. Thus, the propagation behaviour of a user on the propagation behaviour of other users and information diffusion in the network has a very important role.

2.2 Node Importance

Because of the complex nature of network structures and their exceptionally large-scale data, how to measure the importance of a node using a quantitative analysis method in large-scale networks is one of the most important problems to be solved in Jian-Guo *et al.* [20]. Several works explore a number of ways to effectively measure the importance of nodes from different starting points. For instance, in terms of local node topology, Zhuo-Ming [21] presented an evaluation method for node importance based on neighbour information and the convergence factor. In terms of global property, the researcher analysed node importance using vector properties. For example, in the cumulative nomination centrality method [22], there is less computation and fast convergence features for a large and multiple-branch network effect. Closeness centrality is also an effective methodology as it involves the nodes that have high closeness and are maybe closer to the network centre [23]. Except for the node's local and global properties for analysis of node importance, Zhang *et al.* [24] defined the Kernel function and Freeman [25] did so in 1977. Because of the different starting point of these methods, they have different effects in different types of network. Yet, these studies only consider the active node location in the network topology and ignore the nature of the differences in each node. However, in many real networks, such as Twitter and other micro-social networks, the factors affecting the flow behaviour of a node involve not only the location of the nodes in the network but also the heterogeneity of the nodes.

2.3 Node Heterogeneity

Recently, heterogeneity has emerged in greater numbers of works in all areas of research in the literature [26]. For example, Lu *et al.* [27] presented a class of network models based on the heterogeneous industry cluster, using the Cobb–Douglas function to do quantitative description and analysis of Internet groups' heterogeneity and to define the parameters of a cluster network structure. Inspired by the Pareto distribution, as well as various specialized works in the literature, Yang *et al.* [28] considered both the diversity and heterogeneity of meaning in heterogeneity.

3. Information Flow Behaviour Model Based on Node Heterogeneity

To research the influence of a node's heterogeneousness on the node's information flow behaviour, a model M represents the message being passed, the collection $V = \{v_1, v_2, \ldots . v_N\}$ represents a collection of individuals in the network, and N is the network number of individuals. The model rules are defined as follows:

(1) The heterogeneity of individual subjective properties σ $(0 < \sigma < 1)$: for the strength of the individual's ability to accept messages, the more subjective the heterogeneity is, the stronger the individual subjectivity will be, and users will be less easily influenced by others and exercise higher vigilance toward a message.

(2) The heterogeneity properties of the individual memory effect α $(0<\alpha<1)$: this represents the capability of individuals staging the messaging, heterogeneity indicates that the memory effect of each individual is different in the network. The stronger is the memory effect of an individual, the stronger is the individual's ability to stage messages, and the higher is the probability that the individual will accept a message as time progresses.

(3) The individual states: based on the SIR model, we can define three individual states, susceptible, infective, and removal in each time step. If an individual never hears about a message, we call it S, while the individual who tries to send a message to his neighbours at each time step with a probability is called I. The removal individual will not spread the message.

In the SIR model, if an S individual has one I neighbour, it will be infected with probability λ. At each time step, an I individual will be R with probability μ. If there are k I neighbours around S individual, the S individual will be infected with the probability calculated in (1)

$$p = 1 - (1-\lambda)^k \tag{1}$$

Taking into account the heterogeneity of individual subjectivity, a new probability that S individual is infected by I individual in (2) can be obtained on the basis of (1):

$$p = (1-\sigma) * \left(1 - (1-\lambda)^k\right) \tag{2}$$

In this formula, σ means the strength of the individual's ability to accept messages. The greater the heterogeneity of the subjectivity, the less vulnerable the individual will be to the effects of other individuals.

At each time step T_s, each S individual may be moving toward I with a certain probability. Thus, this probability is calculated as follows:

$$p = (1-\sigma) * \left(1 - (1-\lambda)^{N_t(T_s)+\alpha_i \sum\limits_{t<T} N_t(t)}\right) \tag{3}$$

where α_i represents the memory effects of individual i. T is a constant, which means when in time step $t<T$, and all I neighbours is what this S individual has. $N_i(t)$ indicates at time step t and the number of I neighbours of individual i.

4. Analysis and Control of Information Flow Behaviour

4.1 SEIR Model

The information flowing in a network does not have the characteristics of infectious disease, so the network nodes can decide their information behaviour on their own. To better simulate the network user's process of receiving and forwarding information, this article proposes the susceptible-exposed-infected-recovered (SEIR) model, based on the SIR model. The SEIR model increases the E state (dormant state) to simulate how the node receives information but does not disseminate information, and there is potential for the dissemination of information in the case at later time. There is a wide variety of information in a real network, and a network user is not interested in all information, which means the user does not need all the information. At the same time, this does not happen with the forwarding behaviour. This point will also be reflected in the model.

Various information in the network, in which some information presents certain dangers, such as with rumours, and some information can generate benefits for the recipient, such as healthy behaviour, is defined here as variables where *Revenue* represents the information earned. When the information is disseminated to a node, the node receives the information only if it is interested in the information, and its behaviour often depends on autonomy. The forwarding behaviour node exhibits certain characteristic factors which are classified into two types, internal and external. Internal factors mean a node's autonomy; external factors sum up the relationship, *i.e.*, the (*Strength*) between the nodes and the intensity (*Revenue*) information as profitability. For general nodes, the number of common neighbours between two nodes is the measure of the relationship strength between the nodes [29]. A network is represented as $G=(V,E)$; in which, V is the set of nodes and E represents the set of relationships. For two nodes in the network u_i and u_j, the set of adjacent nodes $friendset_i$ and $friendset_j$ can be calculated based on the chart G, and the equation for the familiarity $familiarity(u_i,u_j)$ of these two nodes is (4).

$$familiarity(u_i,u_j) = \frac{|friendset_i \cap friendset_j|}{|friendset_i \cup friendset_j|} \tag{4}$$

For network intimacy, two strong nodes will be treated differently. The node representing the force of an external influence is calculated as (5).

$$P_{\text{out}} = p_1 Strength + p_2 Revenue \tag{5}$$

Therefore, the node forwards the information probability calculated as (6).

$$P_T = p_{\text{out}} P_{\text{out}} + p_{\text{in}} P_{\text{in}} \tag{6}$$

where P_T represents each time step, P_{in} indicates the strength of the node autonomy, p_{in} represents the proportion of its impact; and p_{out} is represented by the node's external influence. Due to the heterogeneity of the nodes, P_{in} of each node is set at random.

Suppose the network has A, B, C three kinds of information flow. The probability of the node receiving and forwarding information is shown in Table 1:

The nodes in the network will show different information behaviours based on the different types of information, and the corresponding value in the table indicates the probability of receiving and forwarding nodes for different categories of information. The corresponding value in the table indicates the probability of a node receiving and forwarding information for different categories.

Table 1
Probability of the Node Receiving and Forwarding Information

Node Number	Information Type					
	A (Harmfulness)		B (Profitability)		C (Normality)	
	Receive	Forward	Receive	Forward	Receive	Forward
1	1	1	0.8	0.8	0.3	0.5
2	0.9	0.5	0.2	0.6	0.9	0.5
3	0.3	0.3	0.3	0.5	0.5	0.6
4	0.0	0.0	0.6	0.6	0.9	0.5
5	0.4	0.5	0.5	0.6	0.9	0.6
6	0.8	0.5	0.6	0.7	0.4	0.5

4.2 A Control Policy for Information Flow

If the spread of a network flow can be controlled, the diffusion of bad information can be restrained effectively and the coverage of useful information will be expanded. Then, the steady and healthy development of a network that benefits society can be achieved. Through the research, a network will know that some nodes are very important for network information dissemination in complex networks. Therefore, with these important nodes in the network, an effective strategy for network flow control can be established. The network flow control strategy is mainly divided into the three steps.

Step 1. Use the K-core decomposition method to extract the important nodes in the network. Based on the K-core theory, delete the nodes with degrees of 1 and the edges connecting these nodes, until there are no nodes with degree of 1. These nodes' K-nuclear value is 1, $K_s = 1$. Then, the rest of the nodes can be treated in the same manner.

Step 2. Use the influence of the important nodes to build a harmful-information rapid response network that is made up of important nodes in the network. To avoid the interference of harmful information, the early warning information or the dangerous information has been found in the harmful information rapid response network.

Step 3. To enhance the authority of the important nodes, Steps 1 and 2 handle the warnings about harmfulness and information sharing about these warnings in two ways. The next task is to make most of nodes in the network believe the early warning messages released by the important nodes. Enhancing the authority of important nodes can solve this problem. Only the important nodes with authority can remind the other nodes to take measures to prevent spreading of harmful information.

5. Experiment

The proposed model is performed on scale-free networks to verify its viability. The individual subjective heterogeneity and memory effects are researched based on the individuals' behaviour in spreading information in the network. Thus, this experiment uses a scale-free network for the network data. The number of nodes is 5000, $\langle k \rangle = 8$. To reduce the time as much as possible, we set $\mu = 0.8$ to speed up the end of the experiment, while pre-processing those individuals whose degree was 0 in the network. To study the effects of the individuals' heterogeneity in spreading the message, the information scope R (the percentage of the number of R individuals) and the life cycle T (the time steps starting from the seed individuals beginning to spread the message to all individuals to the time it stopped spreading) are shown in the simulation results below.

5.1 Validation and Analysis of Node Subjective Heterogeneity

In Fig. 1, we can see that with increases of λ, regardless of σ, the R of the message will slow growth. This is due to the increase of λ, leading to an increase in the probability of an individual accepting the message, so the R increases as a result of this. In addition, we compared situations where there is σ or not. The gap in R is not as big on the premise of each particular λ, but R will be small with the existence of σ on the whole. This is due to the existence of individual subjective heterogeneity, which results in individuals maybe refusing to accept a message in some cases, and this restrains the message diffusion in the network to a certain extent.

In Fig. 2, we can see that with the increase of λ, the number of time steps in the message proliferation is reduced, regardless of whether σ is there. Yet, one can plainly see when there is no σ, the maximum time step is 60, in contrast, is 90, which is an increase of nearly 50%. This is due to the existence of individual subjective heterogeneity, which results in a need for considerable time for the same individuals to spread the message so that it is accepted. Ultimately, given the proliferation of the message, the time step needs to be substantially increased.

With the increase of σ, the message scope R grows more slowly and becomes smaller. This is due to the stronger subjectivity of the individuals regarding the network messages, as they do not easily believe the messages

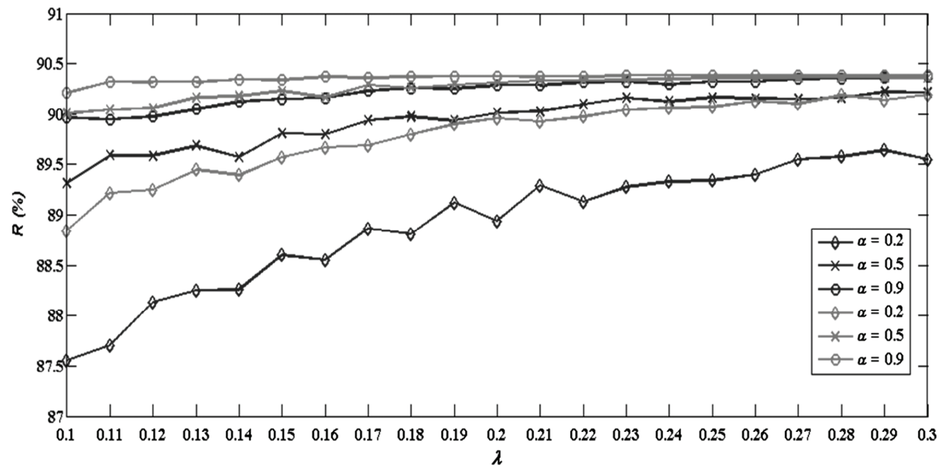

Figure 1. Blue is with σ and red is not; $\alpha = 0.2$, $\alpha = 0.5$, and $\alpha = 0.9$.

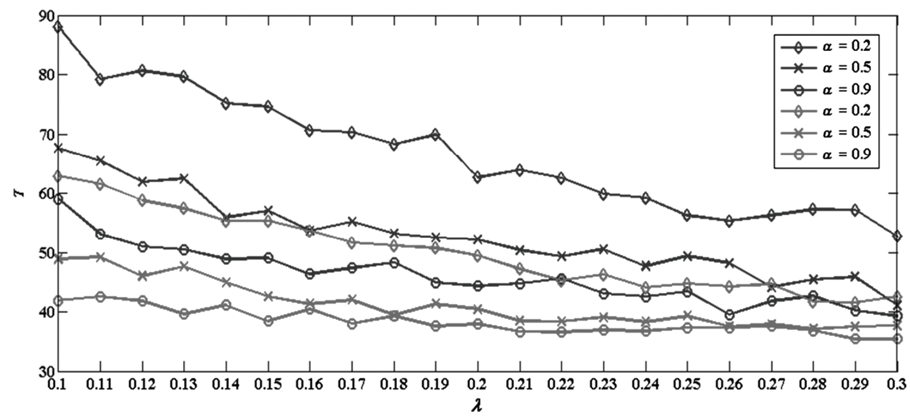

Figure 2. Comparison of T with heterogeneity and without heterogeneity: $\alpha = 0.2$, $\alpha = 0.5$, and $\alpha = 0.9$.

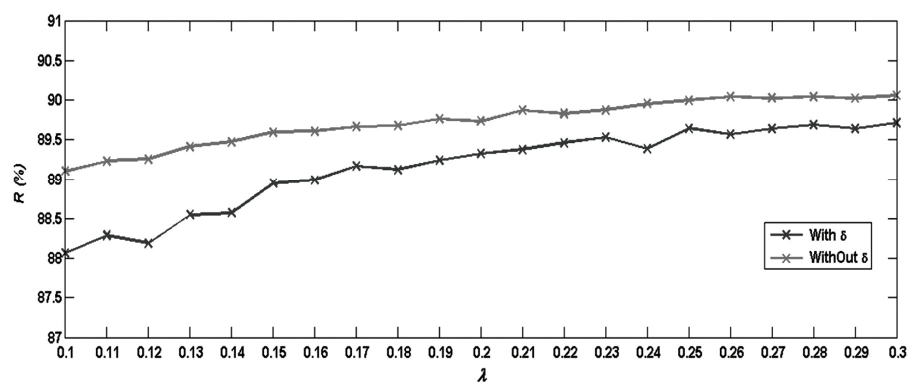

Figure 3. Comparison of R with heterogeneity and without heterogeneity: α with different values.

from their neighbour individuals. The lower the probability of the message being accepted and spread, which inhibits the proliferation of the message in the network, the slower the growth will be and the final value will be smaller.

To study the effect of individual memory heterogeneity on the dissemination of information, we randomly assigned a fixed value α_i for each individual. In Figs. 3 and 4, it is easy to see that with and without subjective heterogeneity in individual cases, the trend in the scope of dissemination of information and the time step changes with the increasing λ, and there is no difference with the results shown in Figs. 1 and 2. On the premise of individual subjective heterogeneity, this paper discusses the differences in individual memory effects and their impact on the spread of information, based on the premise of individual subjective heterogeneity. From Figs. 5 and 6, it can be seen that when there is a difference in the individual memory effect, R may

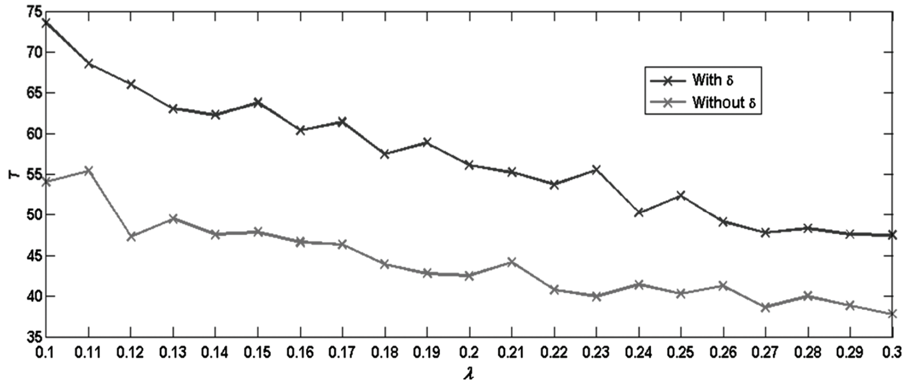

Figure 4. Comparison of T with heterogeneity and without heterogeneity: α with different values.

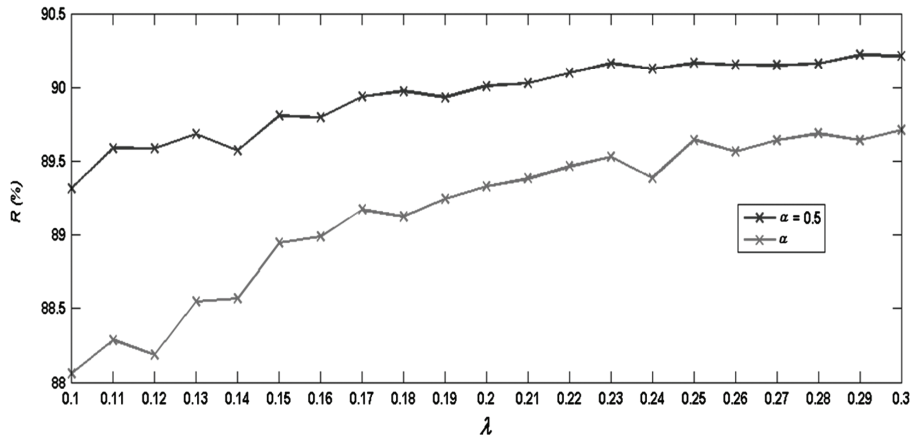

Figure 5. Comparison of R when $\alpha = 0.5$ and α with different values with heterogeneity.

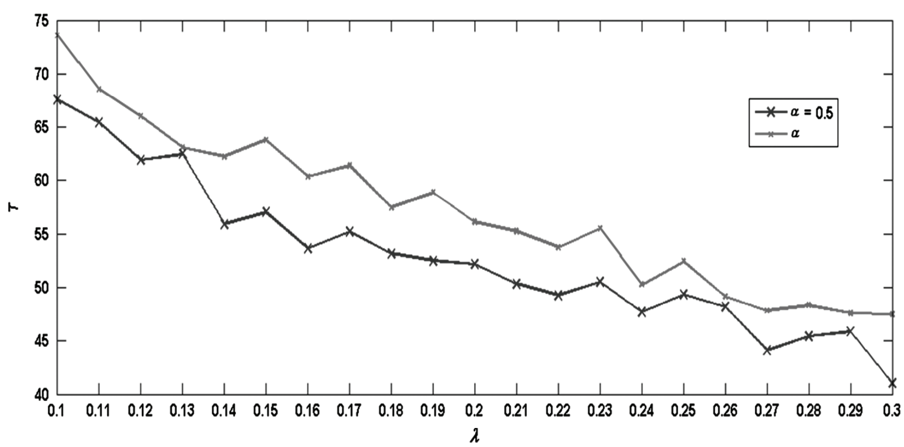

Figure 6. Comparison of T when $\alpha = 0.5$ and α with different values with heterogeneity.

be smaller but the T is bigger. More importantly, the mean value of all the individual memory effects is $0.55 > 0.5$.

With the increase in α, the R will increase and T will be reduced, in the preceding results and analysis; however, the results here are the opposite. This may be due to the existence of certain individuals with a poor memory effect, which is caused when the information is transmitted to the individual, and he has a the very low probability of receiving the information, and this affects the process of information dissemination in the network.

5.2 Node Interest Effect on Information Flow Behaviour

To simulate the interest effects of a node on its flow behaviour, a certain number of nodes have no interest in the

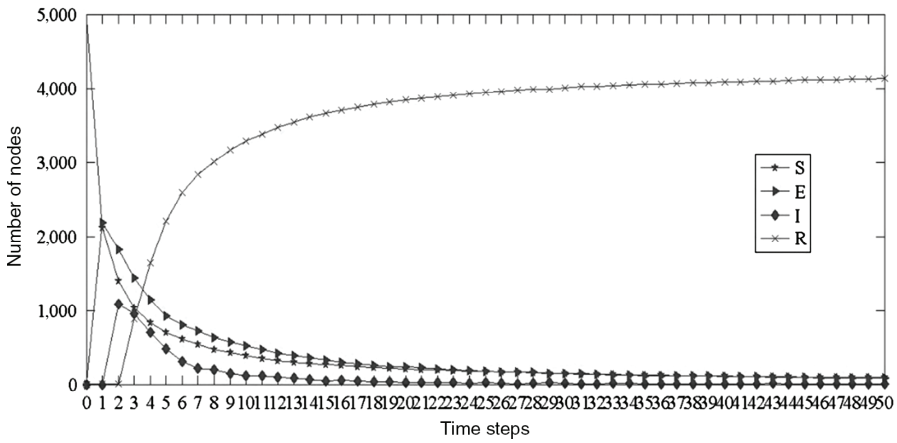

Figure 7. The number of nodes with different states.

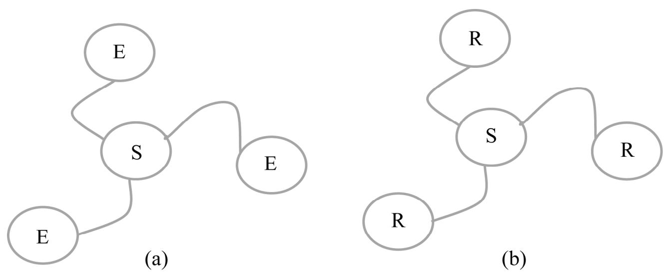

Figure 8. Structural holes in the experiment.

dissemination of information in the experimental initialization. In the experimental results, these nodes made the node state convert from S to R, thereby shortening the process for the node state transitions. The path information spread from one part to other parts in network was cut because of the existence of this node, causing an inhibition of information diffusion, as shown in Fig. 7, in the 0–5 time steps. In addition, the number of I state nodes in the network was not very high. This is due to when some E nodes tried to convert to I, the other I nodes had been in an R state. Thus, at some time steps, the low number of I state nodes, leading to a small probability, resulted in a decline in the spread of information. When the number of nodes uninterested in network I is increased, the final spread of information will be smaller. When a greater number of nodes are closer to the seed node, there is a significant decrease in the spread of information decreased more significantly.

In addition, this paper found, due to low interest node existed in information, led to the appearance of an EEES network structure as shown in Fig. 8(a), although these E nodes may spread information to their neighbours in a moment in theory. However, the very low probability puts some nodes in the S state almost forever, and this seriously inhibits the diffusion of information. Empirical proof, such as in the Fig. 8(b) network structure, is almost ubiquitous. In this experiment, we found that uninterested nodes lead to an increased number of this type of structure.

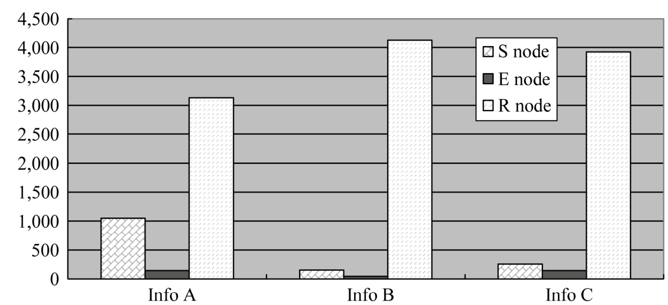

Figure 9. Number of nodes when different information is disseminated.

5.3 Node Revenue Effects on Information Flow Behaviour

For information disseminated in the network, those nodes with earnings information spread more quickly and more widely, while those with dangerous information showed the opposite result, as shown in Fig. 9.

As can be seen from Fig. 9, when Info B and Info C spread in the network, the number of E and R nodes (including uninterested nodes) was higher than that for Info A spread in the network. This is because when the nodes in the network are able to identify dangerous information, they will adopt a cautious attitude toward, or even combat these hazards. This node behaviour inhibits the spread of information in the network.

5.4 The Effect of External Factors on Information Flow Behaviour

With respect to the flow behaviour of a node in a complex network, a larger value of p_{out} results in the flow behaviour of a node being similar to its neighbours' flow behaviour performance. From a global view of the network, when most the nodes have a larger value of p_{out}, the information flow behaviour of nodes in the network appears as a cascade phenomenon. As shown in Fig. 10, when p_2 is large and p_{in} is small, this means that the nodes' subjectivity

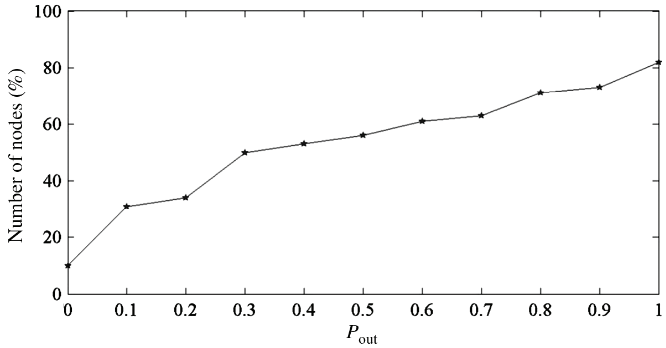

Figure 10. The number of nodes displaying a cascade phenomenon with p_{out}.

Table 2
Results Showing Adoption of the Information Flow Control Policy

Spread Area/%	Information Flow Control Policy/Time Step	
	Not Adopted	Adopted
20	5	9
50	25	40
80	60	–

is relatively poor, and the dissemination of information in the network with earnings, results in some nodes with low interest taking into account the "relationship" between the nodes and the "returns".

5.5 Harmful Information Flow Control Policy

Based on the above analysis, harmful information, such as rumours, is often highly deceptive, and this deception is enough to deceive most nodes, especially with regards to revelations of its dangers. It is clear that network nodes can recognize rumours, but that number of nodes is not in the majority. Table 2 shows the hazardous information flow control policy, and the information spread in the network. If this policy is not adopted, after the 60 o'clock time step, information dissemination achieves 80% of the spread area.

6. Conclusion

Using the characteristics of a node's information flow behaviour, this paper built a complex network information flow model based on node heterogeneity. Through a simulation experiment, it was found that the nodes with greater heterogeneity in a complex network have an important influence on the diffusion and flow of information in the network. The subjective heterogeneity of a node can effectively inhibit the proliferation and flow of information in the network. The heterogeneity of a node's memory effect can promote the diffusion of information flow in a network. In complex networks, the appeal of information, the relationship among the nodes and the location of the nodes in the topology are important factors which influence the information flow. Using personalized tagging methods, the influence of information's appeal and the node's interest on the information flow in a complex network is simulated and verified. Using the links between nodes, the influence of intimacy between two users on a node's information flow behaviour is simulated in a real network. When the closeness between the nodes is greater, the probability that they will show similar information flow behaviour is higher. Thus, the increase in number of nodes promotes the appearance of a behavioural phenomenon. A control policy is formulated in this paper aimed at harmful information flow in networks. The experiment shows that this policy can successfully inhibit the spread and flow of harmful information.

Acknowledgement

This research was financially supported by the National Natural Science Foundation of China (Grant No. 61373160), and the Standardization Processing and Application System Development of Science and Technology's Big Data Project (Grant No. 17210113D) of the Science and Technology Department of Hebei Province.

References

[1] D. Gruhl, R. Guha, D. Liben-Nowell, *et al.*, Information diffusion through blogspace, *Proceedings of the 13th International Conference on World Wide Web. ACM*, 2004, 491–501.
[2] D. Liginlal and L. Khansa, Information contagion: An empirical study of the spread of news on Digg and Twitter social networks, *Eprint Arxiv*, 52, 2010,166–176.
[3] S. Yan, S. Tang, S. Pei, *et al.*, The spreading of opposite opinions on online social networks with authoritative nodes, *Physica A: Statistical Mechanics and its Applications*, *392*(17), 2013, 3846–3855.
[4] Z.-Q. Zhu, C.-J. Liu, J.-L. Wu, J. Xu, and B. Liu, The influence of human heterogeneity to information spreading, *Journal of Statistical Physics*, *154*(6), 2014, 1569–1577.
[5] P. Cui, M. Tang, and Z.X. Wu, Message spreading in networks with stickiness and persistence: Large clustering does not always facilitate large-scale diffusion, *Scientific Reports*, *4*, 2014.
[6] P. Shu, Effects of memory on information spreading in complex networks, *Computational Science and Engineering (CSE), 2014 IEEE 17th International Conf. on. Computational Science and Engineering*, Chengdu, China, 2015, 554–556.
[7] Y. Zhang and J. Xu, A rumor spreading model considering the cumulative effects of memory, *Discrete Dynamics in Nature and Society*, 2015, *2015*(204395), 1–11.
[8] S. Staab, P. Domingos, P. Mike, *et al.*, Social networks applied, *IEEE Intelligent Systems*, *20*(1), 2005, 80–93.
[9] I. Kanovsky and O. Yaari, Viral opinion spreading model in social networks, *Social Computing (SocialCom), 2013 International Conf. on. IEEE*, 2013, 971–974.
[10] J. Huang, C. Li, W.Q. Wang, *et al.*, Temporal scaling in information propagation, *Scientific Reports*, 2014, *4*(5334), 1–6.
[11] Z.J. Zhang, G.Q. Mao, B.D.O. Anderson, On the information propagation in mobile ad-hoc networks using epidemic routing, *Proc. of the 54th Annual IEEE Global Telecommunications Conf.: "Energizing Global Communications", GLOBECOM 2011*, New York, Institute of Electrical and Electronics Engineers Inc., 2011.
[12] J. Waters and M.G. Ceruti, Modeling and simulation of information flow: A study of info dynamic quantities, *Proc. of the 15th International Command and Control Research and*

Technology Symposium, San Diego, Space and Naval Warfare Systems Center Pacific San Diego Ca, 2010, 117–131.

[13] C.N. Lin, K.L. Hsieh, J. Roan, *et al.*, The application of structural holes theory to supply chain network information flow analysis, *Information Technology Journal*, *10*(1), 2011, 146–151.

[14] G. Briscoe and A. Marinos, Digital ecosystems in the clouds: Towards community cloud computing, *IEEE Digital Ecosystems and Technologies*, *12*(7), 2009, 103–108.

[15] H. Zhijie, H. Liusheng, W. Ruchuan, *et al.*, A location-based routing algorithm combined with the topology control for wireless sensor network, *Journal of Computer Research and Development*, *47*(z2), 2010, 128–132.

[16] R. K. Pon, A.F. Cardenas, D. J. Buttler, *et al.*, Measuring the interestingness of articles in a limited user environment, *Information Processing & Management*, *47*(1), 2011, 97–116.

[17] Q. Li, J. Wang, Y.P. Chen, *et al.*, User comments for news recommendation in forum-based social media, *Information Sciences*, *180*(24), 2010, 4929–4939.

[18] D. Lu and Q. Li, Exploiting semantic hierarchies for Flickr group, *Active Media Technology*, *6335*, 2010, 74–85.

[19] R.A. Negoescu and D. Gatica Perez, Modeling Flickr communities through probabilistic topic-based analysis, *IEEE Transactions on Multimedia*, *12*(5), 2010, 399–416.

[20] L. Jian-Guo, R. Zhuo-Ming, G. Qiang, W. Bing-Hong, Node importance ranking of complex networks, *Acta Physica Sinica*, *62*(17), 2013, 1–10.

[21] R. Zhuo-Ming, S. Feng, L. Jian-Guo, *et al.*, Node importance measurement based on the degree and clustering coefficient information, *Acta Physica Sinica*, *62*(12), 2013, 1–5.

[22] R. Poulin, M.C. Boily, and B.R. Masse, Dynamical systems to define centrality in social networks, *Social Networks*, *22*(3), 2000, 187–220.

[23] G. Sabidussi, The centrality index of a graph, *Psychometrika*, *31*(4), 1966, 581–603.

[24] J. Zhang, X.K. Xu, P. Li, *et al.*, Node importance for dynamical process on networks: A multiscale characterization, *Chaos: An Interdisciplinary Journal of Nonlinear Science*, *21*(1), 2011, 016107.

[25] L.C. Freeman, A set of measures of centrality based on betweenness, *Sociometry*, *40*(1), 1977, 35–41.

[26] Z. Wenbin and Z. Zhengxu, Research on engineering software data formats conversion network, *Journal of Software*, *7*(11), 2012, 2606–2613.

[27] L. Lu, J. Geng, Q. Gao, Industrial clusters trading network based on heterogeneity, *Complex Systems and Complexity Science*, *11*(2), 2014, 44–51.

[28] J. Yang, J. Zeng, and J. Zhang, Structural heterogeneity of open-source software communities based on complex networks, *Journal of South China University of Technology*, *41*(12), 2013, 136–144.

[29] M.A. Aydin, A.H. Zaim, and K.G. Ceylan, A hybrid intrusion detection system design for computer network security, *Computers and Electrical Engineering*, *35*, 2009, 517–526.

Biographies

Tao Yu was born in 1981 and received his Ph.D. from the College of Computer Science, Wuhan University. In 2016, he became a full-time postdoctor in the Institute of Network Science and Space at Tsinghua University. His research interests include network architecture, network security, SDN/NFV, cloud computing, network technology and information processing.

Zhao-Wen Zhang was born in 1991 and is a graduate student of the School of Information Science and Technology, Shijiazhuang Tiedao University. His major fields of study are network technology and information processing.

Wen-Bin Zhao was born in 1985 and received his Ph.D. from the School of Information Science and Technology, Shijiazhuang Tiedao University. His major fields of study are network technology and information processing.

Tong-Rang Fan was born in 1965 and received her Ph.D. at the School of Information Science and Technology, Shijiazhuang Tiedao University where she is now a professor. Her main research interests include network technology and information processing.

Jilong Wang received his Ph.D. in Computer Science at Tsinghua University in 2000. In 2010, he became full professor in the Institute of Network Science and Cyberspace at Tsinghua University in China. He serves as the NOC director of several large-scale Internet infrastructures including CERNET2, TEIN, IPv6-CJ, NSFCNET, and the Tsinghua campus network, since 2004. His research focuses on network management and surveying. He is the founder of the DragonLab federation testbed and co-founder of the Internet Innovation Union which is based on DragonLab. He is also co-founder of the ZhongGuanCun Cloud Computing Union and acts as the vice chair.