IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received September 1, 2019, accepted September 14, 2019, date of publication September 18, 2019,
date of current version October 3, 2019.

Digital Object Identifier 10.1109/ACCESS.2019.2942059

A Method to Improve the Security of Information Diffusion in Complex Networks–Node Trust-Value Management Mechanism

GANG WANG, SHIWEI LU, YUN FENG, AND RUNNIAN MA
College of Information and Navigation, Air Force Engineering University, Xi'an 710077, China

Corresponding author: Gang Wang (wglxl@nudt.edu.cn)

This work was supported in part by the National Natural Science Foundation of China (no. 61573017, no. 61703420).

ABSTRACT The transmission of malicious information is often accompanied with normal information flows in complex networks. For the intrusion of unknown malicious information, if there is no effective defensive method to suppress its diffusion, the network may be confronted with incredible catastrophe. In this paper, to enhance the security of information diffusion in complex networks, a node trust-value management mechanism (NTVMM) is proposed. Basically, node trust value and threshold are assigned with node importance at the beginning. According to node benefit and loss in information diffusion, the two algorithms, node trust-value updated algorithm (NTVUA) and node trust-threshold updated algorithm (NTTUA), are devised to dynamically update node trust value and trust threshold, respectively. Compared with the existing node quarantine and edge blockage schemes, NTVMM only relies on the trust relationship of nodes to suppress malicious information diffusion with no need for knowing the global infection information of the network. Besides, to further make a trade-off between information security and information loss, NTVMM is associated with the classical information diffusion model to obtain the most appropriate trust threshold. Finally, we devise the network profit function to evaluate the profits brought by different methods. The simulations are respectively carried out in two synthetic complex networks and a real-world complex network. The results of simulation demonstrate that when malicious information invades the network, NTVMM can reduce the number of infected nodes in the network and enhance the security of information diffusion. Moreover, compared with node quarantine and edge blockage schemes, the proposed scheme can obtain a better network profit, and make a trade-off between information security and information loss.

INDEX TERMS Complex network, information security, malicious information diffusion, node trust-value management mechanism, network profit.

I. INTRODUCTION

With the rapid development and continuous expansion of complex networks, many complex systems, in reality, can be modeled as complex networks for analysis, such as power networks, transportation networks, computer networks, and social networks. These networks show the complexity in structure and function. By investigating complex networks, the inherent laws of complex systems are revealed gradually, and via structure and function optimization, system performance is improved increasingly. Generally, complex network is composed of a large number of nodes and connected edges, where the function of edges is to transmit normal information flow (such as messages, voice, and videos) from one node to another connected. From the perspective of cybersecurity, malicious information, such as rumor or computer virus, can spread accompanied with normal information flow and threaten the security of information receiving nodes [1], [2]. For computer viruses, their diffusion is usually aimed at some target nodes; while rumors are usually aimless, because their purpose is to cause panic to more network users. In general, we regard the malicious information diffusion is aimless in complex networks. Although there are many traditional defense systems, such as firewall, intrusion detecting and *et al.*, to monitor malicious information with specific characteristics [3]–[6], new malicious information with unknown structures and characteristics can still bypass these external defenses and intrude the internal

The associate editor coordinating the review of this manuscript and approving it for publication was Jianquan Lu.

network. For unavoidable intrusion of new malicious information, if there is no specific defensive measure to suppress its diffusion, it may greatly threaten network performance and even incur network paralysis.

At present, solutions to suppress malicious information diffusion mainly are concerned on network node quarantine or edge blockage [7]–[11]. Related schemes can suppress malicious information diffusion in the network, but effective quarantine or blockage depends on the degree of understanding of the network structure and network infection. However, for network managers, it is usually difficult and unfeasible to collect the global infection information of the network in the process of malicious information diffusion. Moreover, these schemes result in the loss of network communication capacity due to the disconnection of network nodes or edges. Excessive operations to quarantine node or block edge cause serious loss of normal information, while deficient operations lead to malicious information still existing in the network.

To pursuit the security of information diffusion of the network itself, network automation, interoperability, and authentication capabilities should be enhanced [12]. In the aspect of identity authentication, the whitelist and blacklist mechanisms are alternative solutions for network users to identify the reliability of information sources and avoid multiple attacks. By manually adding trusted/distrusted users to the lists, users can avoid being infected by malicious information from attackers. Despite the security and speediness of information diffusion have been greatly improved through identity authentication between network users, there are still some obvious constrains. First, malicious attacks are usually persistent and discontinuous, while users in reality are imperceptible to these attacks. Thus, these attackers will escape being identified. Secondly, the manual operation of adding users to the whitelist and blacklist is relatively more cumbersome. Massive uncertain information injection will force users to deal with the authentication of information sources incessantly. In a sense, the attack is effective and defense is defective. Thirdly, excessive uncertain communication blocked by whitelist and blacklist mechanisms will lead to the blockage of normal information diffusion and reduce the basic service-bearing capacity of the network. Based on these considerations above, it is necessary to find a way out to intercept unreliable information automatically and to make a trade-off between network service-bearing capacity and security protection.

Some trust models or systems are deployed in Wireless Sensor Networks (WSNs) to automatically detect malicious information paths [13]–[16] (the specific methods of trust evaluation and management are described in the related work). It is convinced that the trust mechanism is conducive to automatic recognition of malicious information during the process of information diffusion. However, these trust models mainly face internal attack, in which trust evaluation or management is based on the analysis of data packets provided by sensors. Since common systems cannot detect new malicious information, these trust models are unavailable and have no effect on such malicious information. At present, there is no specific trust model that can use its own trust relationship to suppress the spread of new malicious information in the network and make a trade-off between network communication and network security. In Online Social Networks (OSNs), trust-based privacy management mechanisms have been applied by many scholars to protect individuals' privacy and make a trade-off between data sharing and privacy-preserving automatically [17]–[19]. These achievements show that users can share common data and maintain the privacy of stakeholders with reasonable trust-threshold selected methods after establishing an appropriate trust-value mechanism in OSNs. Thereby, we are devoted to creating a node trust-value management mechanism (NTVMM) in complex networks to suppress malicious information diffusion while considering the network communication capabilities.

Before introducing NTVMM, there are some differences between node trust-value management in information diffusion and trust-based collaborative privacy management in data sharing to be stressed. On one hand, the loss of user's privacy is a binary problem in data sharing (for example, whether posting photos would violate the interests of stakeholders is a 0 or 1 problem), but it is multivariant in information diffusion (for example, the losses of information recipient can be caused by malicious information infection, normal information losing or *et al.*). Because the trust value is updated according to user losses, the difference in user's losses will bring about differences in the trust-value updated mechanism. On the other hand, the result of data sharing comes down to multiple stakeholders and data owners can make the final judgment according to the stakeholders' opinions and trust threshold. While in information diffusion, information is usually sent from one user to another user, which doesn't involve multiple users. Thus, the trust-threshold selected method in information diffusion is different from that in privacy management. Based on the above considerations, there are two critical approaches in information diffusion to be addressed urgently before NTVMM applied in complex networks. One is to formulate a new node trust-value updated rule, and the other is to explore an appropriate trust-threshold selected method.

At present, many scholars do pay attention to the problem of network border defense. In border defense, the network is divided into intranet and extranet according to the network security requirements. For example, many companies build private networks on public networks for encrypted communications. Compared with public networks, private networks are intranets. In this paper we focus on intranet security of complex networks. Under the premise that the malicious information has infected a part of intranet network, we study how to restore the network to a healthy state with minimum cost. First, we propose a node trust-value management mechanism (NTVMM) in complex networks, in which two algorithms, node trust-value updated algorithm (NTVUA) and node trust-threshold updated algorithm (NTTUA), are devised respectively to update node trust value and node trust

threshold dynamically. Besides, NTVMM is associated with the typical information diffusion model, named Susceptible-Infected-Recovered-Susceptible (SIRS) model, to explore the most appropriate threshold for node trust judgment and to make a trade-off between network communication and network security. To compare performances of NTVMM, node quarantine, and edge blockage, we devise the network defense profit function to evaluate their network profits.

The main contributions of this paper are summarized as follows

(i) A node trust-value management mechanism is proposed to suppress the diffusion of new types of malicious information in complex networks. Besides, two algorithms, NTVUA and NTTUA, are devised respectively to update node trust value and trust threshold dynamically. In the case of no prior network infection information, NTVMM can help nodes automatically decide whether to receive information based on the reliability of the information source.

(ii) A new trust-threshold selected method is proposed to make a trade-off between network communication capability and network security. By combining NTVMM with SIRS information diffusion model, a novel SIRS information diffusion model with NTVMM is proposed to explore the most appropriate trust threshold. To further measure the network profit under different defensive schemes, we devise a network profit function according to the network security and communication loss.

(iii) The effectiveness of NTVMM in suppressing malicious information is verified via simulations respectively in two synthetic complex networks and a Gnutella P2P network. By conducting comparisons between different methods, it is demonstrated the proposed method based on NTVMM can obtain a better network profit and make a trade-off between network communication and network security.

The organization of this paper is as follows: in section II, the related work of trust-value management and information diffusion model are investigated. In section III, NTVMM is presented and the corresponding updated algorithms are devised respectively for node trust value and trust threshold. In section IV, the novel SIRS information diffusion model with NTVMM is proposed. Section V describes how to apply the proposed model to find the most appropriate trust threshold and devises the network profit function. In section VI, we give the results of simulations. Section VII concludes the paper.

II. RELATED WORK

A. TRUST-VALUE EVALUATION AND MANAGEMENT

At present, the researches of trust evaluation and management are mainly concerned on WSNs and OSNs. In WSNs, Zhang *et al.* [13] and Wang *et al.* [14] designed a fog-based hierarchical trust mechanism for cyber security deficiencies. By comparing the real-time service parameters, collecting exception information, and quantitative evaluating entities, the trust value between cloud service providers and sensor service providers can be updated. Liu *et al.* [15] proposed a trust routing scheme to avoid black holes, where the nodal trust was obtained by detecting and analyzing a number of network routes. In [16], Tang *et al.* devised an aggregate signature-based trust routing to guarantee safe data collection in WSNs. The trust of a path was evaluated according to the success rate of the path and the path with high trust was selected for data routing to increase the success rate of data gathering.

The first two schemes introduced above assume that the malicious information in the network can be detected and collected. While for the new types of malicious information, it is difficult to check whether there is malicious information in the data package. The signature-based trust routing scheme selects the appropriate routes for information transmission. The premise of this scheme is that there are multiple routes for information transmission, while in some networks, information transmission is in the form of point-to-point. In addition, the impact of trust management on network business capability is not considered in these three schemes.

In OSNs, the trust relationship between users in data sharing has been explored in academia. For peer-to-peer data sharing, Lu *et al.* [20] proposed a trust-based privacy preservation method to discuss dynamic trust assessment and the enhancement to the supplier's privacy. In [21], Squicciarini *et al.* modeled the problem of collaborative enforcement of privacy on shared data by using game theory, and offered automated ways to share images based on an extended notion of content ownership. Combined with Condorcet's preferential voting scheme, Sun *et al.* [22] proposed a trust-weighted voting scheme based on fixed trust value to aggregate different users' privacy policies. In addition, Gong and Wang [23] provided the first systematic study for the security of trustee-based social authentications and extensively evaluated various concrete attack and defense strategies using three real-world social network datasets. Recently, Xu *et al.* [19] adopted a changing trust-value mechanism related to users' privacy loss and proposed the trust-based collaborative privacy management to encourage the data owner to take consideration of stakeholders' decisions. The results demonstrated the user can get higher payoffs than setting the threshold to a fixed or random value, by applying the proposed UCB policy to determine the threshold.

At present, there are few studies using the trust-based mechanism in complex networks to suppress diffusion of new malicious information. We draw on the experience of trust mechanism for privacy preservation and propose the NTVMM to improve the security of information diffusion in complex networks. The node trust-value updated rule is related to the node benefit and loss. To further explore the most appropriate trust threshold and make a trade-off between information security and information loss, we associate NTVMM with the information model.

B. INFORMATION DIFFUSION MODEL

Both virus and rumor spread in the form of information, which we call them malicious information. In terms of

malicious information, there are two main approaches to do research on its diffusion: the microscopic approach and the macroscopic approach [24]. The microscopic approach is devoted to the development of more powerful defensive methods by analyzing the structures of the virus or the content of the rumor. However, due to the unpredictability of the structure or content of malicious information, there is a significant lag from the emergence of a new type of uncertain information to the release of a defensive method against them. What is more serious, existing microcosmic defensive methods can't provide insight into the laws of malicious information diffusion in the network, hence, they can't suppress the spread of new type of malicious information. To remedy this shortage, Kephart and White [25] proposed a macroscopic model, inspired by the biologically epidemic models, featuring the spread of computer viruses, showing that its propagating behavior can be predicted.

Since then, a series of information diffusion model has been proposed to investigate the relationship between diffusion factors. Yang *et al.* [26] proposed a modified Susceptible-Infected-Susceptible (SIS) model with an infective medium on complex networks and examined epidemic thresholds for disease spreading by using this new model. Xiong *et al.* [27] proposed a Susceptible-Contacted-Infected-Refractory (SCIR) diffusion model to characterize information propagation on online microblogs and investigate the relations between node degree and infected factor. Consider that opinion divergences and differentiations generally exist as a result of individuals' extensive participation and personalization, Liu *et al.* [28] proposed a Susceptible-Hesitated-Infected-Removed (SHIR) model to study the dynamics of competitive dual information diffusion and the results demonstrated final density of stifles increases monotonically as infection rate increases and removal rate decreases.

In addition, diffusion models are used to investigate the threshold of virus diffusion. To explore the spreading characteristics of worm in the computer network with a natural death rate, Mishra and Jha [29] presented a Susceptible-Exposed-Infectious-Quarantined-Recovered (SEIQR) model. In their follow-up work [30], they presented a compartmental Susceptible-Exposed-Infectious-Susceptible (SEIS) epidemic transmission model and analyzed the stability of equilibriums with the modified reproductive number Rv. Considering the latency of the virus, Yang *et al.* [31] proposed a Susceptible-Latent-Breaking-Recovered- Susceptible (SLBRS) model to get the strategies for eradicating viruses spreading across the Internet effectively and the research also showed the dynamic behavior of the model is determined by a threshold.

As mentioned above, the transferring parameters have an influence on the stability of the information diffusion model. In general, there exists a threshold relevant to transferring parameters for malicious information diffusion. If the threshold is lower than a specific value, there will be no infected node when the network is stable. Otherwise, the infected node will always exist in the network. Therefore, with the help of the diffusion threshold, we can choose the most appropriate trust-threshold by combining the SIRS information diffusion model with NTVMM.

III. NODE TRUST-VALUE MANAGEMENT

In this section, the initial trust value and the trust threshold of the network node are established according to node importance. In the process of information diffusion, node trust-value matrix and trust-threshold set change dynamically according to node benefit and loss. Two algorithms are prescribed to update the trust-value and trust-threshold, respectively.

A. INITIAL NODE TRUST VALUE AND TRUST THRESHOLD IN COMPLEX NETWORK

In reality, many networks can be abstracted into complex networks, such as communication network, social network, and *et al.* Suppose the total number of network nodes is N. A complex network can be represented by an undirected graph $\boldsymbol{G} = (\boldsymbol{V}, \boldsymbol{E})$, where $\boldsymbol{V} = \{V_1, V_2 \ldots, V_N\}$ is the vertices set or nodes set, and $\boldsymbol{E}$ is the edges set. If a direct relationship exists between V_i and V_j, there is a connecting edge between them, which can be denoted as (V_i, V_j). The network node, in reality, represents the user's host or other communication unit. In subsequent instructions, unless otherwise specified, we use the two terms ''node'' and ''user'' exchangeable. Generally, the adjacency relationship between nodes in the network is represented as an adjacency matrix $\boldsymbol{A} = (a_{ij})_{N\times N}$, where a_{ij} can be denoted as

$$a_{ij} = \begin{cases} 1, & \text{if } (V_i, V_j) \in \boldsymbol{E}, \\ 0, & \text{if } (V_i, V_j) \notin \boldsymbol{E}. \end{cases} \tag{1}$$

For privacy management, it is regarded that the initial trust value can be calculated by the shortest distance between two nodes in the network no matter they are directly connected or not. However, in information diffusion, information is transmitted between two directly connected nodes each time. Thus, we can only calculate the trust value between two nodes connected directly. Let $tr_{ij} \in [0, 1]$ denote the trust value of user j in user i. The more user i trusts user j, the higher tr_{ij} is. $tr_{ij}(0)$ represents the trust value of user j in user i at initial time. Because of the preferential attachment of nodes in complex network [32], [33], new nodes are more likely to connect with the node with a larger degree. That is to say, the node with a larger degree is trustworthy. Thus, the initial trust-value matrix can be set according to the node degree. Let $\boldsymbol{T}(t) = (tr_{ij}(t))_{N\times N}$ and k_j denote node trust-value matrix at time t and the degree of node j in the network, respectively. The larger k_j is, the larger $tr_{ij}(0)$ will be. Suppose $k_{\max}$ is the maximum degree of network node, then the initial trust-value $tr_{ij}(0)$ can be defined as

$$tr_{ij}(0) = \begin{cases} k_j / k_{\max}, & \text{if } a_{ij} = 1, \\ 0, & \text{if } a_{ij} = 0. \end{cases} \tag{2}$$

When node i doesn't connect with node j directly, the trust value of node j in node i is zero. According to the definition (2), we can obtain the initial trust-value matrix $\boldsymbol{T}(0)$.

Let $\boldsymbol{\lambda}(t) = \{\lambda_1(t), \lambda_2(t), ..., \lambda_N(t)\}$ represent node trust-threshold set at time t. At the initial moment $t = 0$, since there is no information transition in the network, the initial threshold set can be set as rand number set. To ensure network security, we select a reasonable rand number and give the initial threshold set

$$\boldsymbol{\lambda}(0) = \{0.1, 0.1, \ldots, 0.1\}_N. \tag{3}$$

Certainly, users can set initial thresholds according to their network environment. If there is no malicious information in the network, we can set the threshold as zero. At the beginning of information transition, if $tr_{ij}(0) \leq \lambda_i(0)$, the information from user j will be rejected by user i. In other words, the trust value of node j in i is lower than that of other nodes.

In the following two subsections, we will introduce the updated mechanisms of node trust-value matrix and trust threshold set according to node benefit and loss in information diffusion.

B. NODE TRUST-VALUE UPDATED ALGORITHM

Generally speaking, there are three kinds of cases that will bring benefits or losses to node and change the trust value between nodes in information diffusion. Fig. 1 gives the corresponding change of node trust value in each case. In case 1, the trust value of user j in user i is relatively low, thus, i refuses to receive the information from j (the information from j are denoted by j's information). Because user i doesn't receive j's information which should have been received by i at that time, we regard it is the communication loss of user i caused by j and can be denoted as l_c^{ij}. In case 2, user i receives j's information, but i is infected by the malicious information hidden in j's information. Malicious information may cause the following performance losses to user i: delete programs, destroy data stored in hard disk, clear system memory areas and important information in operating system, and *et al*. [34]. Suppose these performance losses is denoted by l_p^{ij}. In general, the level of communication loss and performance loss in reality should be determined by actual condition. For simplicity, here we use binary number to represent the losses. If j's information is not received by user i, then $l_{\mathrm{c}}^{ij} = 1$. Contrarily, user i receives the information and benefits from information acquisition, then $l_{\mathrm{c}}^{ij} = -1$. Similarly, if node i is infected by j's information, $l_{\mathrm{p}}^{ij} = 1$; otherwise $l_{\mathrm{p}}^{ij} = 0$. Under this definition, if $l_{\mathrm{c}}^{ij} > 0$ or $l_{\mathrm{p}}^{ij} > 0$, the trust value of j in i will descend. In case 3, user i acquires the normal information and benefits from j's information. Hence, $l_{\mathrm{c}}^{ij} = -1$. If the node checks that the performance is greatly affected after receiving the information or information is intercepted, it immediately changes the trust value of the information sender. Specifically, in the computer network NTVMM can be applied to existing network security software and evaluate node reliability according to recorded information of node loss by the monitoring module.

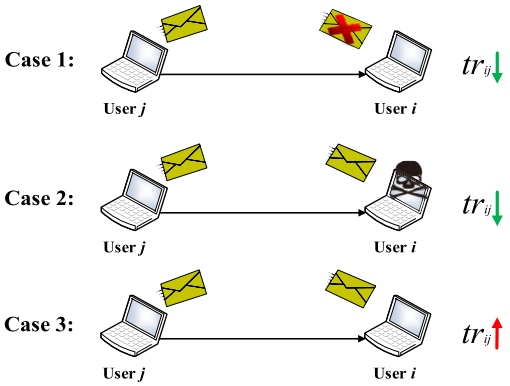


FIGURE 1. The corresponding change of node trust value in each case.

For the information diffusion in the network, there are two hypotheses

(H1) Assume that the behavior of sending and receiving information occurs only once between adjacent nodes in the network per unit time and NTVMM is used at the beginning of virus infection in the network

(H2) The capability of malicious information to infect the host is usually limited, and the individual infected probability is denoted by β.

According to the above updated mechanism of trust value, the new trust value $tr_{ij}(t+1)$ can be computed by

$$tr_{ij}(t+1) = \begin{cases} tr_{ij}(t) \bullet g(a \bullet l_{\mathrm{c}}^{ij}), & \text{if } l_{\mathrm{c}}^{ij} > 0 \&\& l_{\mathrm{p}}^{ij} = 0, \\ tr_{ij}(t) \bullet g(b \bullet l_{\mathrm{p}}^{ij}), & \text{if } l_{\mathrm{p}}^{ij} = 1, \\ tr_{ij}(t) \bullet g(c \bullet l_{\mathrm{c}}^{ij}), & \text{if } l_{\mathrm{c}}^{ij} < 0 \&\& l_{\mathrm{p}}^{ij} = 0, \end{cases} \tag{4}$$

where $g(\bullet)$ is an updated function of l_c^{ij} and l_p^{ij}. An instantiation of $g(\bullet)$ is given by

$$g(x) = \frac{2e^{-x}}{1 + e^{-x}}. \tag{5}$$

If the node i receives j's information and i is not infected, $g(x) > 0$ and the trust value tr_{ij} will increase. Otherwise, $g(x) < 0$ and the trust value tr_{ij} will descend. The parameters a, b, c in (4), belonging to interval [0,1], respectively denote the weight of information loss, performance loss, and information acquisition benefit. In consideration of the serious hazard of performance loss in network security, we suppose the performance loss has the greatest weight on trust value, and set $b = 1$. Since the information loss and information acquisition occur more frequently than performance loss, we set $a = 0.02$ and $c = 0.01$. Equation (4) can be rewritten as

$$tr_{ij}(t+1) = \begin{cases} tr_{ij}(t) \bullet g(0.02 l_{\mathrm{c}}^{ij}), & \text{if } l_{\mathrm{c}}^{ij} > 0 \&\& l_{\mathrm{p}}^{ij} = 0, \\ tr_{ij}(t) \bullet g(l_{\mathrm{p}}^{ij}), & \text{if } l_{\mathrm{p}}^{ij} = 1, \\ tr_{ij}(t) \bullet g(0.01 l_{\mathrm{c}}^{ij}), & \text{if } l_{\mathrm{c}}^{ij} < 0 \&\& l_{\mathrm{p}}^{ij} = 0, \end{cases} \tag{6}$$

Algorithm 1 NTVUA

Input: current trust-value matrix $\boldsymbol{T}(t)$, current trust-threshold set $\lambda(t)$, infection probability β, total node number N.
Output: updated trust-value matrix $\boldsymbol{T}(t+1)$

for $i = 1$ to N **do**
  for $j = 1$ to N **do**
    if $\boldsymbol{T}(t)[i,j] == 0$ **then**
      $\boldsymbol{T}(t+1)[i,j] \leftarrow 0$
    else if $\boldsymbol{T}(t)[i,j] \leq \lambda(t)[i]$ **then**
      Communication loss $l_c \leftarrow 1$
      $\boldsymbol{T}(t+1)[i,j] \leftarrow \boldsymbol{T}(t)[i,j] \bullet g(0.02 l_c)$
    else
      Create a random number rand_num $\in [0, 1]$
      if rand_num $< \beta$ **then**
        Node i is infected by j, and performance loss $l_p \leftarrow 1$
        $\boldsymbol{T}(t+1)[i,j] \leftarrow \boldsymbol{T}(t)[i,j] \bullet g(l_p)$
      else
        Normal information is acquired and node i is not infected. Communication loss $l_c \leftarrow -1$
        $\boldsymbol{T}(t+1)[i,j] \leftarrow \boldsymbol{T}(t)[i,j] \bullet g(0.01 * l_c)$
      end if
    end if
  end for
end for

The trust value at current time will be updated according to node losses. After a unit time, the trust value matrix $\boldsymbol{T}(t)$ will be updated, and the updated matrix $\boldsymbol{T}(t+1)$ can be obtained according to (6). The detail of NTVUA is described in Algorithm 1.

The algorithm NTVUA first traverses each row of current trust-value matrix $\boldsymbol{T}(t)$. For i-th row, it compares each trust value (not zero) in this row with the trust threshold of node i, and makes a judgment to determine whether the node i suffers the communication loss. On this basis, the performance loss of node i is judged again according to the infection probability of malicious information. The time complexity of NTVUA is $O(N^2)$ because the maximum time of updating trust-value matrix is spent at traversing the current trust-value matrix. The space complexity is also $O(N^2)$ in storing the current and next trust-value matrix.

C. NODE TRUST-THRESHOLD UPDATED ALGORITHM

The initial node trust-value matrix $\boldsymbol{T}(0)$ and trust-threshold set $\lambda(0)$ are obtained according to node degree. At each unit time, $\boldsymbol{T}(t)$ is updated dynamically with NTVUA. After trust value matrix is updated, we sort each row of updated trust-value matrix $\boldsymbol{T}(t+1)$ in ascending order and represent sorted matrix as $\boldsymbol{T}_{\text{sort}}(t+1)$. Trust-threshold set $\lambda(t)$ at current time can be updated by the sorted trust-value matrix $\boldsymbol{T}_{\text{sort}}(t+1)$ and the updated trust-threshold set $\boldsymbol{\lambda}(t+1)$ can be obtained.

To maintain the normal network communication, the trust threshold shouldn't be too large. Here we introduce a simple but effective threshold selected method. From the sorted trust-value matrix $\boldsymbol{T}_{\text{sort}}(t)$, we can select a certain proportion of untrusted nodes adjacent to node i. These nodes are directly connected to node i and have relatively low trust values in node i. Thus, the information from untrusted node is refused by node i. Suppose the selected proportion and the maximum trust value of the untrusted nodes at current time are respectively $sp_i(t) \in [0, 1]$ and $tr^i_{\max}$. The trust threshold of node i can be represented as

$$\boldsymbol{\lambda}_i(t) = tr^i_{\max}. \tag{7}$$

Algorithm 2 NTTUA

Require: updated trust-value matrix $\boldsymbol{T}(t+1)$, node degree set $\boldsymbol{K}$, total nodes number N, threshold selected proportion set $\boldsymbol{sp}(t)$.
Ensure: updated trust threshold set $\lambda(t+1)$

sort the trust-value matrix with ascending order $\boldsymbol{T}_{\text{sort}}(t+1) = sort(\boldsymbol{T}(t+1), 2, \text{'ascend'})$
Initialize the number set of refused nodes $\boldsymbol{Ref\_num} = zeros(N,1)$
for $i = 1$ to N **do**
  if $(\boldsymbol{K}(i) \bullet sp(t)[i] \leftarrow \lfloor \boldsymbol{K}(i) \bullet sp(t)[i] \rfloor) > 0.5$ **then**
    $\boldsymbol{Ref\_num}[i] \leftarrow \boldsymbol{K}(i) \bullet sp(t)[i]$
  else
    $\boldsymbol{Ref\_num}[i] \leftarrow \boldsymbol{K}(i) \bullet sp(t)[i]$
  end if
  $\lambda(t+1)[i] \leftarrow \boldsymbol{T}_{\text{sort}}(t+1)[i, \boldsymbol{Ref\_num}[i]]$
end for

Before the trust threshold is obtained, we should calculate the number of untrusted nodes adjacent to i. Let Ref_num_i denote the number of nodes refused by node i. Ref_num_i can be computed by

$$Ref\_num_i = \begin{cases} \lceil k_i \cdot sp_i(t) \rceil, & \text{if } (k_i \cdot sp_i(t) - \lfloor k_i \cdot sp_i(t) \rfloor) > 0.5, \\ \lfloor k_i \cdot sp_i(t) \rfloor, & \text{if } (k_i \cdot sp_i(t) - \lfloor k_i \cdot sp_i(t) \rfloor) \leq 0.5, \end{cases} \tag{8}$$

where k_i is the degree of node i, $\varepsilon_i(t)$ is the threshold selected proportion of node i at time t, $\lfloor \bullet \rfloor$ and $\lceil \bullet \rceil$ are respectively floor function and ceil function. According to Ref_num_i, the trust threshold of node i can be obtained by

$$\boldsymbol{\lambda}_i(t) = tr^i_{\max} = \boldsymbol{T}_{\text{sort}}(t)[i, Ref\_num_i]. \tag{9}$$

The trust-threshold set is updated by trust-value matrix at each time. Let $\boldsymbol{sp}(t) = (sp_1(t), sp_2(t), ..., sp_N(t))$ and $\boldsymbol{K} = (k_i)_N$ denote the threshold selected proportion set at time t and node degree set respectively. We devise the algorithm of NTTUA in Algorithm 2.

Because the nodes with 0 degree are isolated, there is no information transmitted to them. Thus, the trust threshold of isolated node can be set as zero and remain unchanged. The maximum time cost and space time of NTTUA are to sort trust-value matrix. Since different sort algorithms have different time complexity and spatial complexity, here we use the quick sort algorithm to sort the matrix. Therefore,

the time complexity of NTTUA is $O(N^2 * \log_2 N)$ and the space complexity is $O(N^2 * \log_2 N) \sim O(N^3)$

By means of NTVUA and NTTUA, the trust-value matrix and trust-threshold set will be updated automatically in information diffusion. Based on trust-value matrix and trust-threshold set, all users in network can make the judgment to decide whether the information should be received. It is worth noting the effect of judgment depends on the selected proportion. If a larger threshold proportion is selected, the communication capacity of the network will be severely degraded. On the contrary, a smaller threshold proportion will cause the malicious information still existing in the network. Therefore, to make a trade-off between information security and information loss, we associate NTVMM with typical SIRS information diffusion model and explore the most appropriate threshold proportion. Other information diffusion model is also feasible and the proposed method is universal.

IV. INFORMATION DIFFUSION MOEL WITH NTVMM

There are many information diffusion models proposed by previous studies to investigate the relations between information diffusion factor and network healthy state. We herein choose the typical SIRS model as the basis of our research [35]–[37].

A. THE TRADITIONAL SIRS INFORMATION DIFFUSION MODEL

In traditional SIRS model, all nodes in complex network are assumed to be in one of three possible states: susceptible, infected and recovered, which can be abbreviated as S, I, R. The number of three kinds of nodes at time t can be denoted as $S(t)$, $I(t)$, $R(t)$.

The model has the following hypotheses:

(H3) The total number of network node is N.

(H4) For a rand susceptible node in complex network, it can be infected with probability $\beta \langle k \rangle I(t)/N$, where $\beta > 0$ is individual infected probability and $\langle k \rangle$ is the average degree of network nodes. Without ambiguity, here the average degree $\langle k \rangle$ is abbreviated as k.

(H5) Due to the effect of treatment or immunity, every infected node in complex network become recovered with probability $\gamma > 0$.

(H6) Every recovered node in complex network loss immunity with probability $\alpha > 0$.

(H7) Owing to the appearance of new vaccine, every susceptible node in complex network acquires temporary immunity with probability $\varphi > 0$.

The process of information diffusion can be presented as the diffusion diagram in Fig. 2.

The dynamical model is established as

$$\begin{cases} \dfrac{dS(t)}{dt} = \alpha R(t) - \beta k S(t) I(t)/N - \varphi S(t), \\ \dfrac{dI(t)}{dt} = \beta k S(t) I(t)/N - \gamma I(t), \\ \dfrac{dR(t)}{dt} = \gamma I(t) - \alpha R(t) + \varphi S(t), \end{cases} \tag{10}$$

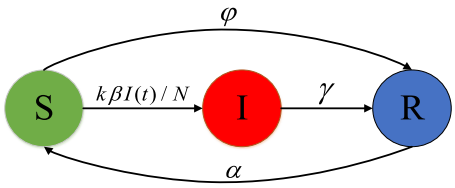


FIGURE 2. The transfer diagram of SIRS information diffusion model.

where the initial condition is $(S(0), I(0), R(0)) \in \boldsymbol{R}^3_+$. In general, the total number of network node is unchanged, thus, there is an additional condition

$$R(t) = N - S(t) - I(t). \tag{11}$$

Substituting (11) into (10) gives

$$\begin{cases} \dfrac{dS(t)}{dt} = \alpha(N - S(t) - I(t)) - \beta k S(t) I(t)/N - \varphi S(t), \\ \dfrac{dI(t)}{dt} = \beta k S(t) I(t)/N - \gamma I(t). \end{cases} \tag{12}$$

B. INFORMATION RECEPTION RELATIONS BETWEEN NODES IN SIRS MODEL

For the SIRS model mentioned above, every susceptible node can be infected by an adjacent infected node in the network with the average probability β. While the precondition of infection is that the malicious information from infected node is received by susceptible node. If the susceptible node refuses to receive information from infected node, it can't be infected by infected node absolutely. Thus, information reception relation has impact on malicious information diffusion.

Generally speaking, information transmission exists any two adjacent nodes in the network. Since our research focuses mainly on the problem whether the information sent by infected nodes will be received by other nodes, we just give a sketch to understand the information reception of infected node with the other two state nodes in Fig. 3. The information reception relation between susceptible nodes and recovered nodes isn't described in the sketch.

In Fig. 3, although the infected node B has the ability to infect other node, the susceptible node A can't be infected because it refuses information from B (B→A is No). Node D and node E can't be infected as a result of autoimmunity. Only susceptible node C is likely to be infected because it is without autoimmunity and receives information from B. Therefore, C can be infected with the probability β by B.

From above research, we know NTVMM can be used to make a trust judgment about information reception relations between nodes. Moreover, malicious information diffusion is related to the information reception relation. Hence, in next subsection, we associate the NTVMM with traditional information diffusion model to investigate the effect of NTVMM on suppressing malicious information diffusion and select the most appropriate threshold proportion.

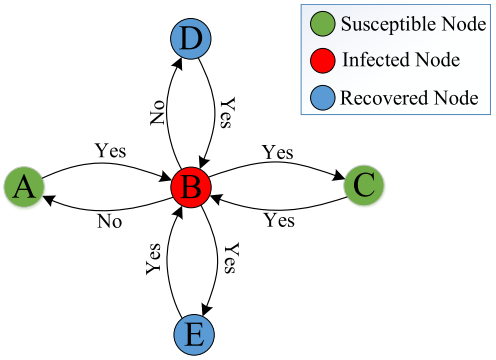


FIGURE 3. A sketch of nodes information reception in SIRS model.

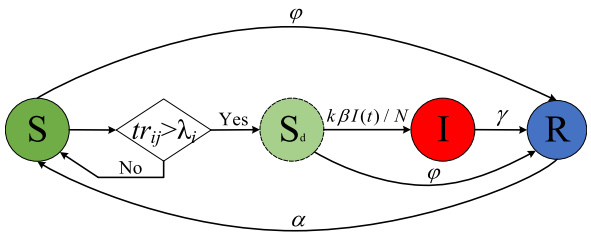


FIGURE 4. The transfer diagram of SIRS information diffusion model with trust judgment.

C. THE NOVEL SIRS INFORMATION DIFFUSION MODEL WITH NTVMM

On the basis of traditional SIRS information diffusion model, we introduce the trust judgment to determine whether susceptible node is deceived by infected node. For example, if node j is infected and $tr_{ij} > \lambda_i$, the susceptible node i will receive j's information and may be infected by malicious information. Let S_d denote the state node deceived by infected node. Since deceived state node set is a subset of susceptible state node set, we use the dotted circle to represent the deceived state in the novel model. The transfer diagram of SIRS information diffusion with trust judgment is shown in Fig. 4.

If the susceptible node i meets the judgment condition $tr_{ij} > \lambda_i$, its state will change from S to S_d. In fact, susceptible nodes in traditional SIRS model are all regarded as deceived node. While in virtue of trust judgment mechanism, the number of nodes that can be infected decreases compared to that without trust judgment mechanism. Thus, malicious information diffusion can be suppressed.

To illustrate the stability of suppressing effect, the stability analysis of the model is essential. In previous studies [30], [31], the stability of information diffusion is investigated with probability transfer model. Thus, to study the stability and get the equilibrium point of the trust judgment model, an equivalent method is proposed to deal with the part of trust judgment. Here, since the state transition process from S to S_d is only related to trust-value matrix and trust-threshold set at current time, the transition probability from S to S_d can be expressed as

$$\boldsymbol{\varepsilon}(t) = \boldsymbol{f}(\boldsymbol{T}(t), \boldsymbol{\lambda}(t)). \tag{13}$$

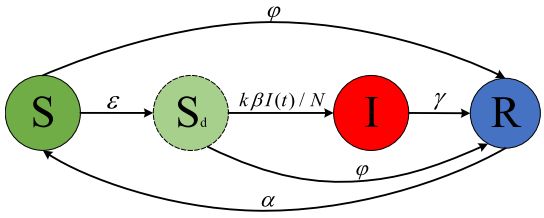


FIGURE 5. The transfer diagram of novel SIRS information diffusion model with NTVMM.

$\boldsymbol{f}(\bullet)$ is a time-varying function related to trust-value matrix and trust-threshold set. To simplify the calculation, there is an additional hypothesis for threshold selection.

(H8) Trust-threshold selected rules of all nodes are the same and time-invariant.

Under (H8), $\boldsymbol{f}(\bullet)$ can be rewritten as $f(\bullet)$. The threshold selected proportions of all nodes are the same. Thus, the following formulas can be obtained,

$$\begin{cases} sp_i(t) = sp, i = 1, 2, \ldots N, \\ \boldsymbol{\varepsilon}(t) = \varepsilon = 1 - sp. \end{cases} \tag{14}$$

On the basis of above discussion, the trust judgment in Fig. 4 can be replaced by transition probability ε and the diagram of novel SIRS information diffusion with NTVMM can be shown as Fig. 5.

The dynamical model of the proposed model is established as

$$\begin{cases} \dfrac{\mathrm{d}S(t)}{\mathrm{d}t} = \alpha R(t) - \varepsilon S(t) - \varphi S(t) \\ \dfrac{\mathrm{d}S_\mathrm{d}(t)}{\mathrm{d}t} = \varepsilon S(t) - \beta k S_\mathrm{d}(t) I(t)/N - \varphi S_\mathrm{d}(t) \\ \dfrac{\mathrm{d}I(t)}{\mathrm{d}t} = \beta k S_\mathrm{d}(t) I(t)/N - \gamma I(t) \\ \frac{\mathrm{d}R(t)}{\mathrm{d}t} = \gamma I(t) + \varphi S(t) + \varphi S_\mathrm{d}(t) - \alpha R(t), \end{cases} \tag{15}$$

where the initial condition of the proposed model (15) is $(S(0), S_\mathrm{d}(0), I(0), R(0)) \in \boldsymbol{R}_+^4$. Similarly, the number of recovered nodes can be represented as $R(t) = N - S(t) - S_\mathrm{d}(t) - I(t)$, then (15) can be rewritten as

$$\begin{cases} \dfrac{\mathrm{d}S(t)}{\mathrm{d}t} = \alpha(N - S(t) - S_\mathrm{d}(t) - I(t)) - \varepsilon S(t) - \varphi S(t), \\ \dfrac{\mathrm{d}S_\mathrm{d}(t)}{\mathrm{d}t} = \varepsilon S(t) - \beta k S_\mathrm{d}(t) I(t)/N - \varphi S_\mathrm{d}(t), \\ \dfrac{\mathrm{d}I(t)}{\mathrm{d}t} = \beta k S_\mathrm{d}(t) I(t)/N - \gamma I(t). \end{cases} \tag{16}$$

V. THE MOST APPROPRIATE TRUST THRESHOLD AND THE NETWORK PROFIT FUNCTION

For model (12) and model (15), there is no additional external nodes and removal of internal nodes. In other words, the range of the number of state nodes is [0, N]. Therefore, the local stability of two models is equivalent to global stability. In this section, we analyze the local stabilities of model (12) and model (15) to obtain their equilibrium points and basic reproductive number, respectively. On this basis,

the relationship between the most appropriate threshold and infected probability is revealed. Besides, the network profit function is designed to calculate the network profits brought by NTVMM and other defensive methods.

A. STABILITY ANALYSIS OF TRADITIONAL SIRS INFORMATION DIFFUSION MODEL

In model (12), let $\frac{dS(t)}{dt} = 0$ and $\frac{dI(t)}{dt} = 0$. And we can get two equilibrium points. One is virus-free equilibrium point $P^0(S^0, I^0, R^0) = \left(\frac{\alpha N}{\alpha+\varphi}, 0, \frac{\varphi N}{\alpha+\varphi}\right)$, and the other is virus equilibrium point

$$P^1(S^1, I^1, R^1) = \left(\frac{\gamma}{\beta k}N, \frac{\alpha\beta k - (\alpha+\varphi)\gamma}{\beta k(\alpha+\gamma)}N, \frac{\gamma(\beta k+\varphi-\gamma)}{\beta k(\alpha+\gamma)}N\right). \quad (17)$$

Let R_0 denote basic reproductive number of model (12), which indicates the number of susceptible nodes infected by an infected node during the average infected period [38], [39]. Generally speaking, R_0 can be used as a threshold of information diffusion to determine whether the virus disappears when the transition of network node state is stable. According to virus equilibrium point P^1, R_0 can be represented by

$$R_0 = \frac{\alpha\beta k}{(\alpha+\varphi)\gamma} \quad (18)$$

Equations (17) and (18) illustrate that if $R_0 \leq 1$, then $I^1 \leq 0$. Because the number of infected nodes is not negative, in this case we regard there is no infected node in network when $R_0 \leq 1$. Otherwise, infected nodes will persist in the network.

From Ref. [40] and [41], the local stability of differential equation can be proved by its Jacobian matrix. Thus, we get the follow theorems of model (12).

Theorem 1: When $R_0 \leq 1$, traditional SIRS information diffusion model in (12) is locally asymptotically stable at the equilibrium point P^0.

Proof: The Jacobian matrix of (12) can be got as follow

$$\boldsymbol{J}_1(P^*) = \begin{pmatrix} \frac{-\alpha-\varphi-\beta kI^*}{N} & \frac{-\alpha-\beta kS^*}{N} \\ \frac{\beta kI^*}{N} & \frac{\beta kS^*}{N} - \gamma \end{pmatrix}. \quad (19)$$

Using the equilibrium point P^0 in (19) gives

$$\boldsymbol{J}_1(P^0) = \begin{pmatrix} -\alpha-\varphi & -\alpha - \frac{\alpha\beta k}{\alpha+\varphi} \\ 0 & \frac{\alpha\beta k}{\alpha+\varphi} - \gamma \end{pmatrix}. \quad (20)$$

The corresponding eigenvalue polynomial of $\boldsymbol{J}_1(P^0)$ is

$$(\lambda+\alpha+\varphi)(\lambda+\gamma-\frac{\alpha\beta k}{\alpha+\varphi}) = 0. \quad (21)$$

One eigenvalue of (21) is $\lambda_1 = -(\alpha+\varphi)$, and the other is $\lambda_2 = \alpha\beta k/(\alpha+\varphi) - \gamma$. If $R_0 \leq 1$, then $\lambda_1, \lambda_2 < 0$. According to the Routh–Hurwitz stability criterion in Ref. [28] and [29], the Theorem 1 is verified.

Theorem 2: When $R_0 > 1$, traditional SIRS information diffusion model in (12) is locally asymptotically stable at the equilibrium point P^1.

Proof: Using the equilibrium point P^1 in (19) gives

$$\boldsymbol{J}_1(P^1) = \begin{pmatrix} \frac{-\alpha-\varphi-\beta kI^1}{N} & -\alpha - \frac{\beta kS^1}{N} \\ \frac{\beta kI^1}{N} & -\gamma + \frac{\beta kS^1}{N} \end{pmatrix}. \quad (22)$$

The corresponding eigenvalue polynomial of $\boldsymbol{J}_1(P^1)$ is

$$\lambda^2 + \frac{\alpha\beta k + \alpha(\alpha+\varphi)}{\alpha+\gamma}\lambda + [\alpha\beta k - (\alpha+\varphi)\gamma] = 0. \quad (23)$$

In accordance with Vieta theorem, the two eigenvalues of (23) have the following relationship

$$\begin{cases} \lambda_1 + \lambda_2 = -\frac{\alpha\beta k + \alpha(\alpha+\varphi)}{\alpha+\gamma}, \\ \lambda_1 \bullet \lambda_2 = \alpha\beta k - (\alpha+\varphi)\gamma. \end{cases} \quad (24)$$

If basic reproductive number $R_0 > 1$, then $\lambda_1 < 0$ and $\lambda_2 < 0$. According to the Routh–Hurwitz stability criterion, the Theorem 2 is verified.

B. STABILITY ANALYSIS OF NOVEL SIRS MODEL WITH NTVMM

Let $\frac{\mathrm{d}S(t)}{\mathrm{d}t} = 0$, $\frac{\mathrm{d}S_\mathrm{d}(t)}{\mathrm{d}t} = 0$, $\frac{\mathrm{d}I(t)}{\mathrm{d}t} = 0$ in (16), and the two equilibrium points are obtained as follows

$$P^2(S^2, S_\mathrm{d}^2, I^2) = \left(\frac{\alpha\varphi}{(\alpha+\varphi)(\varphi+\varepsilon)}N, \frac{\alpha\varepsilon}{(\alpha+\varphi)(\varphi+\varepsilon)}N, 0\right),$$
$$P^3(S^3, S_\mathrm{d}^3, I^3) = \begin{pmatrix} \frac{\alpha\gamma(\beta k+\varphi-\gamma)}{\beta k(\alpha\gamma+\alpha\varepsilon+\varphi\gamma+\gamma\varepsilon)}N, \frac{\gamma}{\beta k}N, \\ \frac{\alpha\beta k\varepsilon - \gamma(\alpha+\varphi)(\varepsilon+\varphi)}{\beta k(\alpha\gamma+\alpha\varepsilon+\varphi\gamma+\gamma\varepsilon)}N \end{pmatrix}. \quad (25)$$

Let R_1 denote basic reproductive number of model (16). According to virus equilibrium point P_3 in (25), R_1 can be represented by

$$R_1 = \frac{\alpha\beta\varepsilon k}{\gamma(\alpha+\varphi)(\varepsilon+\varphi)} = \frac{\alpha\beta k}{\gamma(\alpha+\varphi)}\left(1 - \frac{\varphi}{\varepsilon+\varphi}\right). \quad (26)$$

Theorem 3: When $R_1 \leq 1$, SIRS information diffusion model with NTVMM in (16) is locally asymptotically stable at the equilibrium point P^2.

Proof: The Jacobian matrix of (16) can be got as follow

$$\boldsymbol{J}_2(P^*) = \begin{pmatrix} -\alpha-\varepsilon-\varphi & -\alpha & -\alpha \\ \varepsilon & -\frac{\beta kI^*}{N} - \varphi & -\frac{\beta kS_\mathrm{d}^*}{N} \\ 0 & \frac{\beta kI^*}{N} & \frac{\beta kS_\mathrm{d}^*}{N} - \gamma \end{pmatrix}. \quad (27)$$

Using the equilibrium point P^2 in (27) gives

$$\boldsymbol{J}_2(P^2)=\begin{pmatrix}-\alpha-\varepsilon-\varphi & -\alpha & -\alpha\\ \varepsilon & -\varphi & -\dfrac{\alpha\beta\varepsilon k}{(\alpha+\varphi)(\varepsilon+\varphi)}\\ 0 & 0 & -\dfrac{\alpha\beta\varepsilon k}{(\alpha+\varphi)(\varepsilon+\varphi)}-\gamma\end{pmatrix}. \tag{28}$$

The corresponding eigenvalue polynomial of $\boldsymbol{J}_2(P^2)$ is

$$(\lambda+\alpha+\varphi)(\lambda+\varepsilon+\varphi)\left[\lambda+\gamma(\alpha+\varphi)(\varepsilon+\varphi)-\alpha\beta\varepsilon k\right]=0. \tag{29}$$

If basic reproductive number $R_1 \leq 1$, then $\lambda_1 < 0$, $\lambda_2 < 0$ and $\lambda_3 < 0$. According to the Routh–Hurwitz stability criterion, Theorem 3 is verified.

Theorem 4: When $R_1 > 1$, SIRS information diffusion model with NVTMM in (15) is locally asymptotically stable at the equilibrium point P^3.

Proof: Using the equilibrium point P^3 in (27) gives

$$\boldsymbol{J}_2(P^3)=\begin{pmatrix}-\alpha-\varepsilon-\varphi & -\alpha & -\alpha\\ \varepsilon & -\dfrac{\beta kI^3}{N}-\varphi & -\dfrac{\beta kS_{\mathrm{d}}^3}{N}\\ 0 & \dfrac{\beta kI^3}{N} & \dfrac{\beta kS_{\mathrm{d}}^3}{N}-\gamma\end{pmatrix}. \tag{30}$$

The corresponding eigenvalue polynomial of $\boldsymbol{J}_2(P^3)$ is

$$\lambda^3+\mu_1\lambda^2+\mu_2\lambda+\mu_3=0, \tag{31}$$

where the parameters are as follows

$$\begin{cases}\mu_1=\dfrac{\beta kI^3}{N}+\alpha+\varepsilon+2\varphi,\\ \mu_2=(\dfrac{\beta kI^3}{N}+\varphi)(\alpha+\varepsilon+\varphi)+\dfrac{\beta\gamma kI^3}{N}+\alpha\varepsilon,\\ \mu_3=\dfrac{\alpha\beta\varepsilon kI^3}{N}+(\alpha+\varepsilon+\varphi)\dfrac{\beta\gamma kI^3}{N}.\end{cases} \tag{32}$$

When $R_1 > 1$, $\mu_1, \mu_2 > 0$ and $\mu_1\mu_2 - \mu_2 > 0$. Hence, the eigenvalues $\lambda_1, \lambda_2, \lambda_3 < 0$. According to the Routh–Hurwitz stability criteria, Theorem 4 is verified.

By comparing basic reproductive number R_0 with R_1, we can get $R_1 \leq R_0$ when the same parameter set (except ε) is taken. It proves that when the network suffers external attack, the network with NTVMM has better ability to suppress virus diffusion than that without NTVMM.

From Theorem 3 and Theorem 4, we can conclude 1 is a critical value of basic reproductive number R_1. When $R_1 > 1$, the network will be in an unhealthy state. As is shown in (26), we can reduce the transition probability ε to make R_1 decreased. However, reducing ε will increase the threshold selected proportion sp and result in more information loss. Therefore, the most appropriate transition probability ε_{app} should be selected as follow

$$\varepsilon_{\mathrm{app}}=\frac{\varphi\gamma(\alpha+\varphi)}{\alpha\beta k-\gamma(\alpha+\varphi)}. \tag{33}$$

Substituting (33) to (26), we can get $R_1 = 1$. Thus, the most appropriate threshold proportion sp_{app} can be represented by

$$sp_{\mathrm{app}}=1-\varepsilon_{\mathrm{app}}=1-\frac{\varphi\gamma(\alpha+\varphi)}{\alpha\beta k-\gamma(\alpha+\varphi)}, \tag{34}$$

Equation (34) is the paradigm of the most appropriate threshold of NTVMM. As long as the defense software starts the NTVMM module, sp_{app} can be calculated immediately according to the transition parameters and network average degree. Certainly, the transition probabilities should be assigned according to the actual situation. At the most appropriate threshold sp_{app}, NTVMM can thoroughly suppress malicious information diffusion in the network and minimizing network loss.

C. NETWORK PROFIT FUNCTION

To quantitatively compare the impact of different methods on network security and network communication, the network profit function is constructed to measure the benefits of the method. Suppose network profit is *NP*, network security index is $NSI \in [0, 1]$, and network information loss proportion is $NSIP \in [0, 1]$. Although the all of three methods, node quarantine, edge blockage and NTVMM, can enhance the security of information diffusion, they will lead to the network information loss. Therefore, we construct the network profit function as follows:

$$NP=\mu_1 \bullet NSI-\mu_2 \bullet NILP, \tag{35}$$

where μ_1 and μ_2 are the weights of network security and network communication in the given network, respectively and meet the condition $\mu_1 + \mu_2 = 1$. If the network focus on security performance, such as banking sector network, μ_1 is bigger than μ_2. Otherwise, μ_1 is relatively smaller. The value of *NSI* depends on the number of infected nodes when the network evolution is stable. Suppose t_s represents the time when the network evolution is stable, then *NSI* can be computed by

$$NSI=1-\frac{I(t_s)}{N}. \tag{36}$$

If there is no infected node in the network, the network is secure and $NSI = 1$. Otherwise, the network is insecure and $NSI < 1$. *NSIP* is related to the amount of information lost and total information number. Suppose the number of lost information and total information at time t are $NLI(t)$ and $NTI(t)$ respectively. Network information loss proportion *NSIP* be computed by

$$NSIP=\frac{\sum_{t=0}^{t_s}NLI(t)}{\sum_{t=0}^{t_s}NTI(t)}. \tag{37}$$

In the real network environment, we can design a processing center to store lost information and record *NLI*. Certainly, after the stored information is checked or recovered, it can

be sent to the recipient again. *NTI* needs to record the network information flows. We will investigate focus on these technologies in our next research. Here, *NSIP* is calculated according to (H1). Suppose the total number of network edge is *NE*. Since only two messages are transmitted on each edge of the network per unit time, we can represent (37) as

$$NSIP = \frac{\sum_{t=0}^{t_s} NLI(t)}{2NE \bullet t_s} = \frac{\overline{NLI}}{2NE}. \tag{38}$$

$\overline{NLI}$ is the average number of lost information in the time t_s. Substituting (36) and (38) to (35), network profit *NP* can be obtained by

$$NP = \mu_1 \bullet \left(1 - \frac{I(t_s)}{N}\right) - \mu_2 \bullet \frac{\overline{NLI}}{2NE}, \tag{39}$$

From (39), if the defense method can reduce the proportion of infected nodes in the final network, the network security index can be improved. Besides, the smaller the average amount of information loss, the higher the network profit.

VI. SIMULATION

In the following subsections, the validity of SIRS model with NTVMM is verified first. In addition, the simulation demonstrates the validity of NTVMM in suppressing malicious information diffusion. Afterwards, the influence of infected probability and threshold selected proportion on basic reproductive number is illustrated and the most appropriate threshold is given to make a trade-off between information security and information loss. Finally, the network profits of different methods are given out according to network profit function.

A. THE VALIDITY OF SIRS MODEL WITH NTVMM

Information diffusion model can rapidly predict the scale of malicious information diffusion when the network is stable. However, because some practical situations are simplified or equivalent in modeling, the validity of model (12) and model (15) need to be verified. The validity of information diffusion model in (12) was already verified in [36], [37]. Here we only need to validate the validity of novel SIRS information diffusion model with NTVMM. The simulations of verification are divided into two parts. One is to simulate the process of actual node evolution in complex networks. The other is to simulate model (15) and get the evolution results of model.

In case of SIRS paradigm, there are three types of nodes in the network—susceptible node, infected node and recovered node. The premise of the research is that there are some infected nodes in the network, and then we discuss how to reduce the number of infected nodes in the final network. At the beginning of malicious information diffusion, these existing infected nodes will infect the susceptible nodes with infected rate β. In actual network evolution, we suppose that every two nodes in the network send information to each other once per unit time. If the information is sent by the infected node, it may contain malicious information. As long as information is sent from infected node and received by the adjacent susceptible node, the susceptible node may be infected with a probability β. Because of autoimmunity or vaccination, susceptible and infected nodes will respectively evolve into recovered nodes with probabilities φ and γ in each unit time. However, since immunization may be temporary, immune nodes will degenerate into susceptible nodes with probability α in unit time. In simulations, we generate random numbers per unit time to compare with theoretical probabilities and determine the state changes of network nodes per unit time. According to the method of control variables, we assume that in different networks, only the number of initial state nodes and the network topology are different, and the other evolution parameters are the same. The relevant network data sets and parameter settings are described as follows.

1) DATASET

Due to the huge cost of complex network construction, the data sets of complex networks are collected and employed to simulate and verify the theory based on complex networks. Our simulations are carried out with synthetic data and real-world data. The obtained data sets of two synthetic networks and a real-world network are all accurate and authentic. According to the generating rule of scale-free network proposed by Barabási and Albert (BA) and small-world network proposed by Watts and Strogtz (WS), the adjacency matrices of two synthetic networks are generated by our MATLAB procedures. The BA scale-free network contains 1000 nodes, 7936 undirected edges and the average degree is approximate to 8. The WS small-world network contains 1000 nodes, 4000 undirected edges, and the average degree is approximate to 4. In addition, the adjacency matrix of Gnutella peer-to-peer(P2P) network is collected from Stanford larger network dataset collection [44]. The P2P network contains 8846 nodes, 31839 undirected edges and the average degree is approximate to 3.6. After obtaining the adjacency matrices of three networks, we transform them into the CVS file that can be read by Gephi. The diagrams of BA scale-free network, WS small-world network and Gnutella P2P network are respectively shown in Fig. 6(a)-(c). In the diagrams, the bigger node represents the node with a larger degree. To observe the network structure more clearly, the Fruchterman-Reingold (FR) algorithm is used to optimize network layout in Gephi.

Three networks have different distributions of node degrees and different topology structures. To illustrate the applicability of NVTMM for complex networks, the simulations are conducted in the three networks.

2) PARAMETER SETTING

The total number of nodes N in the model depends on the specific network used for simulation. For individuals or small groups, it is not easy to make new malicious information (such as virus or rumor). Therefore, in simulation, we assume some nodes in the network have been infected, and then the

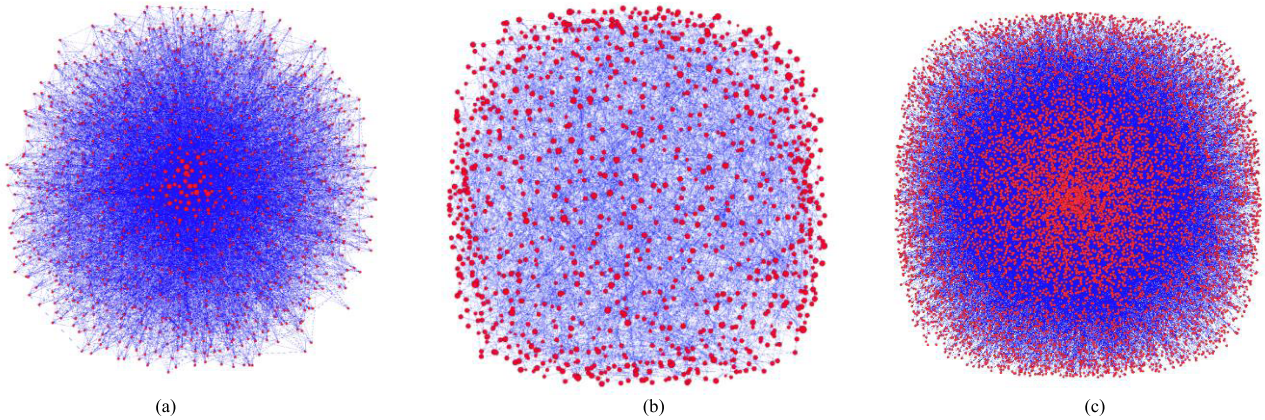


FIGURE 6. The diagrams of three complex networks. (a) BA scale-free network. (b) WS small-world network. (c) Gnutella P2P network.

malicious information propagation processes are simulated. Suppose initial number sets of state node are both set to $(S(0), S_d(0), I(0), R(0)) = (750, 0, 200, 50)$ in BA scale-free network and WS small-world network. As a result of the different node number of the P2P network, initial number set of state node in P2P network is set as $(S(0), S_d(0), I(0), R(0)) = (8346, 0, 400, 100)$. At the beginning of actual evolution, infected nodes and recovered nodes are randomly distributed in the network. Because the threshold selected proportion sp has no effect on model validity, here we set $sp = 0.1$ (i.e. $\varepsilon = 0.9$) for further simulations. In the process of actual evolution, 10% of nodes are rejected because of their low trust value. Considering that a low infected rate β results in basic reproductive number $R_1 \leq 1$ and the number of infected nodes tends to zero. In this case, the number of susceptible nodes and recovered nodes in different networks doesn't differ much. Thus, we choose a high infected probability $\beta = 0.5$ for simulations. That is to say in actual evolution, if the malicious information sent by the infected node is received by the susceptible node, it will infect the susceptible node with probability 0.5. The other transition probabilities are set as $\gamma = 0.2$, $\alpha = 0.3$, $\varphi = 0.15$ (ensure $R_1 > 1$). The specific meanings of three transition probabilities in actual evolution are the same with (H5), (H6) and (H7). In the following simulation, without special illustration, the transfer probabilities do not change.

3) NODE STATE EVOLUTIO

The actual evolution and model evolution are implemented in the three complex networks mentioned above. After the code of actual evolution is executed, the state diagram of the network node per unit time will be given, and the different state nodes are distinguished by different colors. However, to display the number of each state conveniently and get corresponding conclusions, we count the number of state node per unit time. The specific operation of actual evolution can review the script in the code. The actual evolution curve of the state node number in BA scale-free network is shown in Fig. 7(a). It should be noted that S_d is the equivalent state of S. Hence, we add the number of deceived nodes to the number of susceptible nodes and depict the curve of their sum. Fig. 7(b) gives the proportion of information loss at each time (compared with the total amount of information) caused by NTVMM. In the same transition probabilities and initial state node set, Fig. 7(c) shows the theoretical evolution curve of state node number in model (16). Fig. 8(a)-(c) and Fig. 9(a)-(c) are similar to the simulations in Fig. 7(a)-(c), but the networks used for simulation are WS small-world network and Gnutella P2P network respectively.

Comparing the evolution curves of state node number in scale-free network, WS small-world network, and Gnutella P2P network with those in model (16), we can conclude the number of state nodes and the final equilibrium points in three networks are consistent with those in model (15). In other words, the SIRS model with NTVMM can effectively describe the evolutionary process of information diffusion with NTVMM in complex networks as long as the above parameters are known. In addition, by observing Fig. 7∼9(b), 10% information in the network are practically blocked and lost as a result of NTVMM, which is consistent with the threshold selected proportion sp. Since we equate the trust judgment with the transition of node state in the model, there is a difference of node number between model (16) and actual network. But the difference doesn't exceed 5%. Thus, here we regard the equivalence is reasonable.

The validity of traditional SIRS information diffusion model (12) was verified in previous references [35]–[37]. In this subsection, model (15) is also validated to effectively describe the process of information diffusion in complex networks with NTVMM. Since in the following subsections, we only focus on the number of state nodes in the network. Therefore, in following simulations, the process of information diffusion can be simulated by the corresponding information diffusion model.

B. THE VALIDITY OF NTVMM IN INFORMATION DIFFUSION

To discover the validity of NVTMM in suppressing malicious information diffusion, the traditional SIRS model without

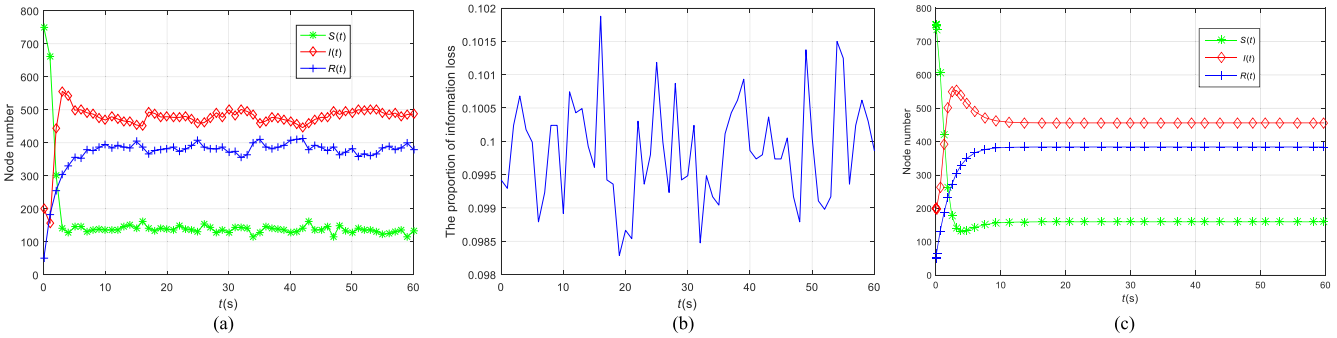


FIGURE 7. Simulation results of information diffusion with NTVMM in BA scale-free network. (a) The actual evolution curve of state node number. (b) The proportion of information loss. (c) The theoretical evolution curve of state node number in model (16).

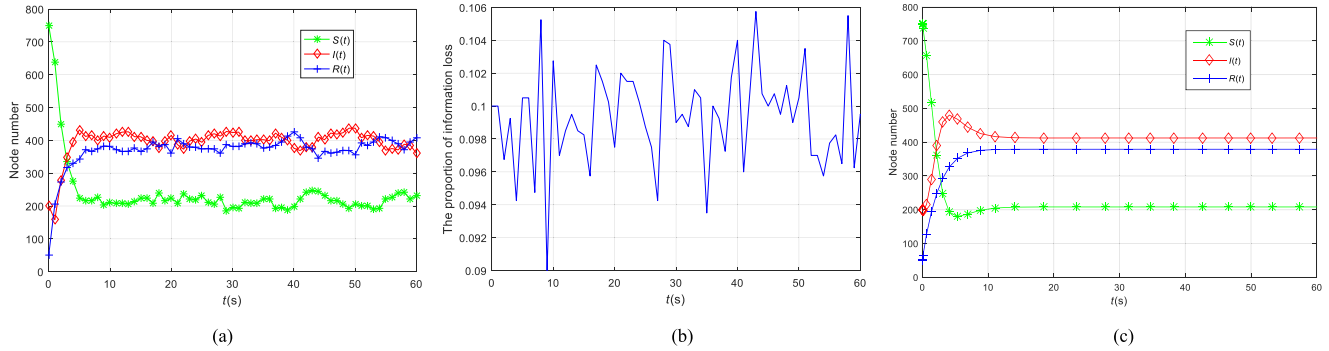


FIGURE 8. Simulation results of information diffusion with NTVMM in WS small-world network. (a) The actual evolution curve of state node number. (b) The proportion of information loss. (c) The theoretical evolution curve of state node number in model (16).

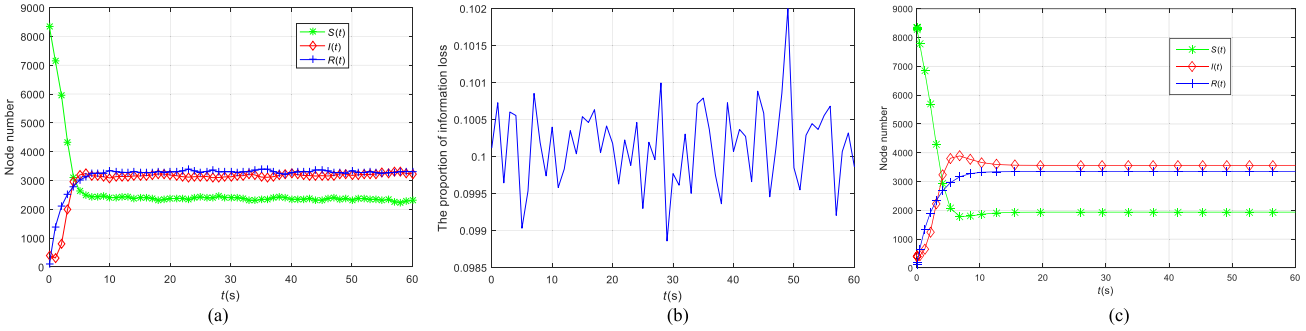


FIGURE 9. Simulation results of information diffusion with NTVMM in Gnutella P2P network. (a) The actual evolution curve of state node number. (b) The proportion of information loss. (c) The theoretical evolution curve of state node number in model (16).

NTVMM in (12) and SIRS model with NTVMM in (15) are compared. Except infected probability β, other parameters and initial node number are the same with those in Gnutella P2P network. When malicious information has a high infection probability, β is set as 0.5 to ensure the basic reproductive numbers $R_0 > 1$ and $R_1 > 1$. Otherwise, β is set as 0.05 to make $R_0 < 1$ and $R_1 < 1$. The evolution curves of the number of state nodes with high infection rate and low infection rate are given in Fig. 10(a) and Fig. 10(b) respectively. Both of the two figures compare the evolution process with NTVMM or without NTVMM.

In Fig. 10(a), we can observe that in a high infected probability, the number of infected nodes can be reduced by almost 20% after introducing NTVMM to the network. Thus, NTVMM has obvious effect on suppress the scale of malicious information diffusion in the network. In addition, suppose that there is no infected node in the network when the number of infected nodes is less than 1. In Fig. 10(b), whether there is NTVMM or not, the number of infected nodes approaches zero. However, without NTVMM, the infected node vanishes at 76(s); with NTVMM, the infected node vanishes at 60(s). Therefore, NTVMM can help the network

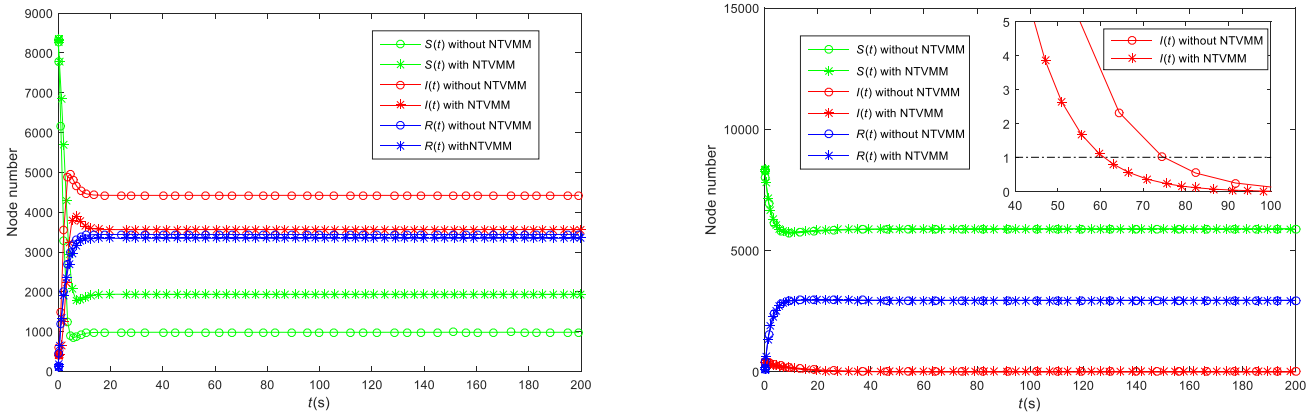


FIGURE 10. The evolution curves of the number of state nodes. (a) High infected probability $\beta = 0.5$. (b) Low infected probability $\beta = 0.05$.

recover to healthy state faster. To summarize, NTVMM is effective in suppressing malicious information diffusion.

C. THE VALIDITY OF THRESHOLD SELECTED METHOD

Equation (34) illustrates the selected method of the most appropriate trust threshold. If other transfer probabilities remain unchanged (except infected probability), sp_{app} is only related to the infected probability of malicious information. To verify the validity of threshold selected method under different infected probability, we adjust β and sp dynamically, and give the mesh grids of basic reproductive number and infected node number with these two parameters. Except β and sp, other parameters and initial node number are the same with those in WS small-world network. The results of multiple simulations, finished with same procedure in the previous section, show the stable time of model (16) is always less than 100(s). Thus, we choose the number of infected nodes at 100(s) to represents finial infected node number in the network. Fig. 11 gives the relationship of basic reproductive number R_1 with infected probability β and transition probability sp. Fig. 12 gives the relationship of infected nodes number with β and sp when the network is stable.

As is shown in Fig. 11 and Fig. 12, when $R_1 > 1$, with the decrease of infected probability β and the increase of threshold selected proportion sp, the basic reproductive number R_1 becomes smaller. Correspondingly, the number of infected nodes is reduced when the network is stable. It is consistent with actual situation. When the infected intensity of malicious information is low, the degree of network infection is low as well; when the number of rejected information is large, the spread of malicious information will be suppressed. While $R_1 \leq 1$, the number of infected nodes remains unchanged with the change of β and sp.

The simulation results are consistent with those mentioned in Theorem 3 and Theorem 4. In a certain infected probability, when $R_1 > 1$, the network security is enhanced by increasing the threshold to refuse to receive more information. It is not recommended to adopt the same operation measure when

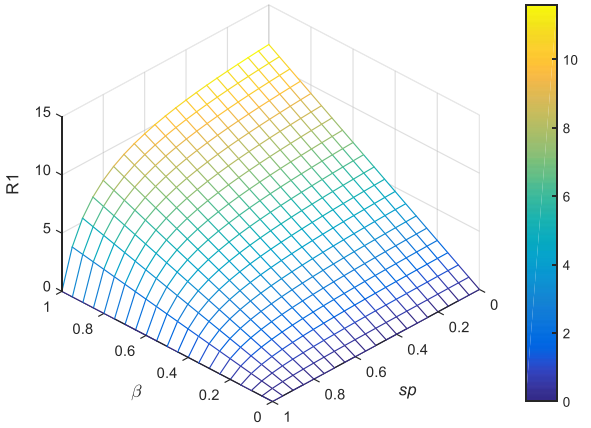


FIGURE 11. The influence of infected probability β and threshold selected proportion sp on basic reproductive number R_1.

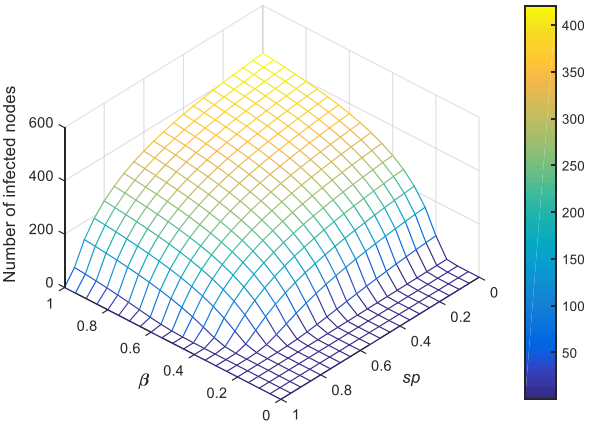


FIGURE 12. The influence of infected probability β and threshold selected proportion sp on the number of infected nodes.

$R_1 \leq 1$, because it can't continue to improve network security, but will cause the loss of network information. In other words, it is most worthwhile to select a threshold to ensure $R_1 = 1$. Therefore, the proposed threshold selected method is effective.

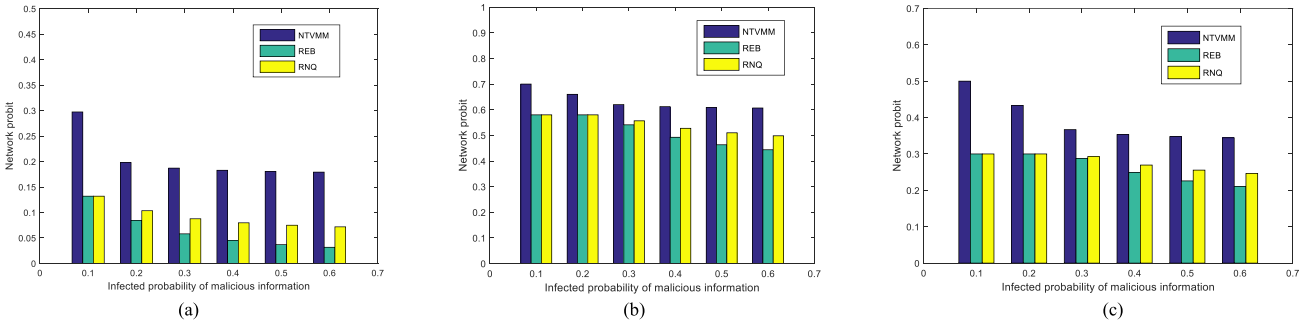


FIGURE 13. The network profits of different defensive methods in different types of networks. (a) Communication-oriented network. (b) Security-oriented network. (c) Balanced network.

D. COMPARISON OF DIFFERENT DEFENSIVE METHODS

There are three defensive methods to suppress malicious information diffusion: node quarantine, edge blockage, NTVMM. To obtain the profits of three methods in network security and communication, we calculate the network profit according to (39).

Since NTVMM is simulated without knowing the global infection of the network, the other two methods should also be simulated in this premise. Thus, the two most common network isolation methods, random node quarantine (RNQ) and random edge blockage (REB), are employed for comparison. Since the network is infected by new malicious information, it is usually difficult for network managers to grasp the direction or purpose of virus spread. In order to prevent malicious information from causing greater harm to the network, network managers will choose to temporarily stop communication between some or all nodes. However, because the termination of all communication will cause great communication loss to the network, managers usually choose a part of the nodes to isolate. Thus, managers often select random node quarantine or random edge blockage to prevent malicious information diffusion. Certainly, if the manager knows the global network information, some other targeted isolation methods can be used to suppress the spread of malicious information effectively. Here random node quarantine will select a certain number of network nodes and make them quarantine with other nodes. Random edge blockage will choose a certain number of network edge and prohibit the transmission of information in it. Because we selected several values of infected probability β for simulation, the number of isolated nodes and blocked edges remained unchanged, which is equivalent to selecting different number of quarantine nodes and blocking edges at the same infection rate.

The simulation is conducted in the three networks mentioned above. Three networks represent three different types of networks: security-oriented, communication-oriented and balanced. The parameters of network profit function are set in Table I.

Five infected probabilities, from low to high, are selected for simulation on each network. The network profits of different defensive methods are shown in Fig. 13.

TABLE 1. The parameters of network profit function.

Network	Type	Parameters
BA scale-free	communication-oriented	$\mu_1 = 0.3, \mu_2 = 0.7$
WS small-world	security-oriented	$\mu_1 = 0.7, \mu_2 = 0.3$
Gnutella P2P	balanced	$\mu_1 = 0.5, \mu_2 = 0.5$

As is shown in Fig. 13, compared with the other two methods, NTVMM obtains maximum network profits under different infected probability in different networks. Thus, NTVMM can guarantee network security with minimum information loss cost. In other words, NTVMM can make a trade-off between information security and information loss.

VII. CONCLUSION

In this paper, a node trust-value management mechanism, called NTVMM, is proposed to reduce the network losses caused by new malicious information. Under the assumption that malicious information already exists in the network, NTVMM can suppress and eliminate malicious information diffusion in the network with less communication loss. According to the gains and losses of nodes after receiving information, two algorithms in NTVMM, NTVUA and NTTUA, can automatically update the trust relationship between nodes to determine the followed information receiving relationship between network communication nodes. Besides, by associating NTVMM with SIRS information diffusion model, we propose a new trust threshold selected method to find the most appropriate threshold that can restore the network to health with minimum communication loss. Additionally, the network profit function is devised to evaluate the network profit brought by the method of NTVMM, node quarantine and edge blockage. Finally, four simulations are designed to demonstrate the validity and performance of NVTMM and the threshold selected method. The results of simulation show that NTVMM can suppress malicious information diffusion in the network and the threshold selected method is able to find the most appropriate threshold to make the network restore to health with minimum cost. Compare with node quarantine and edge blockage, NTVMM obtains the highest network profit and make a trade-off between network communication and network security.

REFERENCES

[1] Z. Tan, J. Ning, Y. Liu, X. Wang, G. Yang, and W. Yang, "ECRModel: An elastic collision-based rumor-propagation model in online social networks," *IEEE Access*, vol. 4, pp. 6105–6120, 2016.

[2] R. Ramírez-Llanos and S. Martínez, "Distributed and robust fair optimization applied to virus diffusion control," *IEEE Trans. Netw. Sci. Eng.*, vol. 4, no. 1, pp. 41–54, Jan. /Mar. 2017.

[3] S. Shirali-Shahreza and Y. Ganjali, "Protecting home user devices with an SDN-based firewall," *IEEE Trans. Consum. Electron.*, vol. 64, no. 1, pp. 92–100, Feb. 2018.

[4] R. A. R. Ashfaq, X.-Z. Wang, J. Z. Huang, H. Abbas, and Y.-L. He, "Fuzziness based semi-supervised learning approach for intrusion detection system," *Inf. Sci.*, vol. 378, pp. 484–497, Feb. 2017.

[5] F. Yousef, "How to secure Web servers by the intrusion prevention system (IPS)?" *Int. J. Adv. Comput. Res.*, vol. 6, no. 23, pp. 65–71, 2016.

[6] K. Coffey, R. Smith, L. Maglaras, and H. Janicke, "Vulnerability analysis of network scanning on SCADA systems," *Secur. Commun. Netw.*, vol. 2018, no. 4, pp. 1–21, 2018.

[7] M. A. Safi and A. B. Gumel, "Mathematical analysis of a disease transmission model with quarantine, isolation and an imperfect vaccine," *Comput. Math. With Appl.*, vol. 61, no. 10, pp. 3044–3070, 2011.

[8] J. Jiang, S. Wen, S. Yu, Y. Xiang, and W. Zhou, "K-center: An approach on the multi-source identification of information diffusion," *IEEE Trans. Inf. Forensics Security*, vol. 10, no. 12, pp. 2616–2626, Dec. 2015.

[9] H. Kang, K. Liu, and X. Fu, "Dynamics of an epidemic model with quarantine on scale-free networks," *Phys. Lett. A*, vol. 381, no. 47, pp. 3945–3951, 2017.

[10] M. Kimura, K. Saito, and H. Motoda, "Blocking links to minimize contamination spread in a social network," *ACM Trans. Knowl. Discovery From Data*, vol. 3, no. 2, pp. 1–23, 2009.

[11] J. Cai, Y. Wang, Y. Liu, J.-Z. Luo, W. Wei, and X. Xu, "Enhancing network capacity by weakening community structure in scale-free network," *Future Gener. Comput. Syst.*, vol. 87, pp. 765–771, Oct. 2018.

[12] *Enabling Distributed Security in Cyberspace Building a Healthy and Resilient Cyber Ecosystem With Automated Collective Action*, Argonne National Laboratory, Lemont, IL, USA, 2011.

[13] G. Zhang, T. Wang, G. Wang, A. Liu, and W. Jia, "Detection of hidden data attacks combined fog computing and trust evaluation method in sensor-cloud system," *Concurrency Comput., Pract. Exper.*, p. e5109, 2018. doi: 10.1002/cpe.5109.

[14] T. Wang, G. Zhang, Z. A. Bhuiyan, A. Liu, W. Jia, and M. Xie, "A novel trust mechanism based on fog computing in sensor-cloud system," *Future Gener. Comput. Syst.*, to be published. doi: 10.1016/j.future.2018.05.049.

[15] Y. Liu, M. Dong, K. Ota, and A. Liu, "ActiveTrust: Secure and trustable routing in wireless sensor networks," *IEEE Trans. Inf. Forensics Secur.*, vol. 11, no. 9, pp. 2013–2027, Sep. 2016.

[16] J. Tang, A. Liu, M. Zhao, and T. Wang, "An aggregate signature based trust routing for data gathering in sensor networks," *Secur. Commun. Netw.*, vol. 2018, 2018, Art. no. 6328504. doi: 10.1155/2018/6328504.

[17] C. Zhang, J. Sun, X. Zhu, and Y. Fang, "Privacy and security for online social networks: Challenges and opportunities," *IEEE Netw.*, vol. 24, no. 4, pp. 13–18, Jul. /Aug. 2010.

[18] L. Xu, C. Jiang, J. Wang, J. Yuan, and Y. Ren, "Information security in big data: Privacy and data mining," *IEEE Access*, vol. 2, pp. 1149–1176, 2014.

[19] L. Xu, C. Jiang, Z. Han, and A. Benslimane, "Trust-based collaborative privacy management in online social networks," *IEEE Trans. Inf. Forensics Security*, vol. 14, no. 1, pp. 48–60, Jan. 2019.

[20] Y. Lu, W. Wang, B. Bhargava, and D. Xu, "Trust-based privacy preservation for peer-to-peer data sharing," *IEEE Trans. Syst., Man, Cybern. A, Syst., Humans*, vol. 36, no. 3, pp. 498–502, May 2006.

[21] A. C. Squicciarini, M. Shehab, and F. Paci, "Collective privacy management in social networks," in *Proc. 18th Int. Conf. World Wide Web*, Apr. 2009, pp. 521–530.

[22] Y. Sun, C. Zhang, J. Pang, B. Alcalde, and S. Mauw, "A trust-augmented voting scheme for collaborative privacy management," *J. Comput. Secur.*, vol. 20, no. 4, pp. 437–459, 2012.

[23] N. Z. Gong and D. Wang, "On the security of trustee-based social authentications," *IEEE Trans. Inf. Forensics Security*, vol. 9, no. 8, pp. 1251–1263, Aug. 2014.

[24] C. Gan, X. Yang, W. Liu, and Q. Zhu, "A propagation model of computer virus with nonlinear vaccination probability," *Commun. Nonlinear Sci. Numer. Simul.*, vol. 19, pp. 92–100, Jan. 2014.

[25] J. O. Kephart and S. R. White, "Directed-graph epidemiological models of computer viruses," in *Proc. IEEE Comput. Soc. Symp. Res. Secur. Privacy*, New York, NY, USA, Mar. 1991, pp. 66–87.

[26] M. Yang, G. Chen, and X. Fu, "A modified SIS model with an infective medium on complex networks and its global stability," *Phys. A, Stat. Mech. Appl.*, vol. 390, pp. 2408–2413, Jun. 2011.

[27] F. Xiong, Y. Liu, Z.-J. Zhang, J. Zhu, and Y. Zhang, "An information diffusion model based on retweeting mechanism for online social media," *Phys. Lett. A*, vol. 376, nos. 30–31, pp. 2103–2108, Jun. 2012.

[28] Y. Liu, S.-M. Diao, Y.-X. Zhu, and Q. Liu, "SHIR competitive information diffusion model for online social media," *Phys. A, Stat. Mech. Appl.*, vol. 461, pp. 543–553, Nov. 2016.

[29] B. K. Mishra and N. Jha, "SEIQRS model for the transmission of malicious objects in computer network," *Appl. Math. Model.*, vol. 34, no. 3, pp. 710–715, 2010.

[30] B. K. Mishra and S. K. Pandey, "Dynamic model of worm propagation in computer network," *Appl. Math. Model.*, vol. 38, nos. 7–8, pp. 2173–2179, 2014.

[31] M. Yang, Z. Zhang, Q. Li, and G. Zhang, "An SLBRS model with vertical transmission of computer virus over the Internet," *Discrete Dyn. Nature Soc.*, vol. 2012, no. 12, pp. 341–379, 2012.

[32] T. Pham, P. Sheridan, and H. Shimodaira, "Joint estimation of preferential attachment and node fitness in growing complex networks," *Sci. Rep.*, vol. 6, p. 32558, Sep. 2016.

[33] G. Michael, "Mechanisms of complex network growth: Synthesis of the preferential attachment and fitness models," *Phys. Rev. E, Stat. Phys. Plasmas Fluids Relat. Interdiscip. Top.*, vol. 97, Jun. 2018, Art. no. 062310.

[34] R. K. Upadhyay, S. Kumari, and A. K. Misra, "Modeling the virus dynamics in computer network with SVEIR model and nonlinear incident rate," *J. Appl. Math. Comput.*, vol. 54, nos. 1–2, pp. 485–509, 2017.

[35] H. Guo and M. Li, "Impacts of migration and immigration on disease transmission dynamics in heterogeneous populations," *Discrete Continuous Dyn. Syst. Ser. B*, vol. 17, no. 7, pp. 2413–2430, 2017.

[36] Y. Cheng, L. Huang, R. Ramlogan, and X. Li, "Forecasting of potential impacts of disruptive technology in promising technological areas: Elaborating the SIRS epidemic model in RFID technology," *Technol. Forecasting Social Change*, vol. 117, pp. 170–183, Apr. 2017.

[37] D. Li, S. Liu, and J. Cui, "Threshold dynamics and ergodicity of an SIRS epidemic model with Markovian switching," *J. Differ. Equ.*, vol. 263, no. 12, pp. 8873–8915, 2017.

[38] P. Holme and N. Masuda, "The basic reproduction number as a predictor for epidemic outbreaks in temporal networks," *PLoS ONE*, vol. 10, no. 3, pp. 1–15, 2015.

[39] T. Li, X. Liu, J. Wu, C. Wan, Z.-H. Guan, and Y. Wang, "An epidemic spreading model on adaptive scale-free networks with feedback mechanism," *Phys. A, Stat. Mech. Appl.*, vol. 450, pp. 649–656, May 2016.

[40] T. Haruna, "Adaptive local information transfer in random Boolean networks," *Artif. Life*, vol. 23, no. 1, pp. 105–118, 2017.

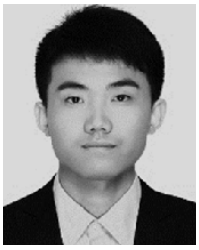
[41] M. Mahrouf, J. Adnani, and N. Yousfi, "Stability analysis of a stochastic delayed SIR epidemic model with general incidence rate," *Applicable Anal.*, vol. 97, no. 12, pp. 2113–2121, 2017.

[42] X. Chen, J. Cao, J. H. Park, and J. Qiu, "Stability analysis and estimation of domain of attraction for the endemic equilibrium of an SEIQ epidemic model," *Nonlinear Dyn.*, vol. 87, no. 2, pp. 975–985, 2017.

[43] J. Cermák and L. Nechvátal, "The Routh-Hurwitz conditions of fractional type in stability analysis of the Lorenz dynamical system," *Nonlinear Dyn*, vol. 87, no. 2, pp. 939–954, 2017.

[44] J. Leskovec, J. Kleinberg and C. Faloutsos. (2007). *SNAP Datasets: Stanford Large Network Dataset Collection*. [Online]. Available: http://snap.stanford.edu/data/p2p-Gnutella05.html

GANG WANG was born in Huanggang, Hubei, China, in 1976. He received the B.S. and M.S. degrees from Air Force Engineering University, China, in 1998 and 2001, respectively, and the Ph.D. degree from the National University of Defense Technology, in 2005. He is currently a Professor with the Information and Navigation Institute, Air Force Engineering University. His major research interests include cyberspace security and complex networks.



SHIWEI LU was born in Hanzhong, Shaanxi, China, in 1995. He received the B.S. degree in computer science and technology from Zhejiang University, in 2017. He is currently pursuing the master's degree with the Information and Navigation Institute, Air Force Engineering University, China. His major research interests include cyberspace security and computer science.

YUN FENG was born in Changzhi, Shanxi, China, in 1996. He received the B.S. degree in computer science and technology from Beihang University, in 2018. He is currently pursuing the master's degree with the Information and Navigation Institute, Air Force Engineering University, China. His major research interests include cyberspace security and computer science.

RUNNIAN MA was born in Suide, Shaanxi, China, in 1963. He received the M.S. degree in operational research and cybernetics from Shandong University and the Ph.D. degree in circuit and system specialty from the Xi'an University of Electronic Science and Technology, China.

He is currently a Professor with Air Force Engineering University, Xi'an, China. He has published more than 80 articles in graph theory, complex network theory, and network security, including more than 40 articles indexed by SCI and EI. His research interests include mathematics, operational research, and control theory.