SCIENCE CHINA
Information Sciences

• **RESEARCH PAPER** •

May 2016, Vol. 59 xxxxxx:1–xxxxxx:12
doi: 10.1007/s11432-015-5467-7

A secure routing scheme based on social network analysis in wireless mesh networks

Yao YU[1], Zhaolong NING[2,3]* & Lei GUO[1]

[1] *College of Information Science and Engineering, Northeastern University, Shenyang* 110819*, China;*
[2] *School of Software, Dalian University of Technology, Dalian,* 116620*, China;*
[3] *State Key Laboratory for Novel Software Technology, Nanjing University, Nanjing,* 210093*, China*

Received January 1, 2015; accepted January 1, 2015

Abstract As an extension of wireless ad hoc and sensor networks, wireless mesh networks (WMNs) are employed as an emerging key solution for wireless broadband connectivity improvement. Due to the lack of physical security guarantees, WMNs are susceptible to various kinds of attack. In this paper, we focus on node social selfish attack, which decreases network performance significantly. Since this type of attack is not obvious to detect, we propose a security routing scheme based on social network and reputation evaluation to solve this attack issue. First, we present a dynamic reputation model to evaluate a node's routing behavior, from which we can identify selfish attacks and selfish nodes. Furthermore, a social characteristic evaluation model is studied to evaluate the social relationship among nodes. Groups are built based on the similarity of node social status and we can get a secure routing based on these social groups of nodes. In addition, in our scheme, nodes are encouraged to enter into multiple groups and friend nodes are recommended to join into groups to reduce the possibility of isolated nodes. Simulation results demonstrate that our scheme is able to reflect node security status, and routings are chosen and adjusted according to security status timely and accurately so that the safety and reliability of routing are improved.

Keywords wireless mesh networks, node selfish, social network analysis, secure routing, Markov chain

Citation Yu Y, Ning Z L, Guo L. A secure routing scheme based on social network analysis in wireless mesh networks. Sci China Inf Sci, 2016, 59(5): xxxxxx, doi: 10.1007/s11432-015-5467-7

1 Introduction

Due to their advantages of being self-organizing and self-configuration and because they are simple, cost-effective and quick to lay, wireless mesh networks (WMNs) have good prospects for home, business, campus and military applications [1]. WMNs have a flexible topology structure, which expands the number of new application fields. However, due to the characteristics of wireless communication and distributed control, WMNs have many potential security issues such as selfish attacks [2]. Selfish attack is caused by cooperation deficiency, which occurs when nodes refuse to provide transmission services for other nodes [3]. The traditional solution is to build an incentive mechanism in which only the nodes that offer a transmission service will receive a reward, while the nodes that refuse to forward for others will be isolated as punishment [4]. Although some intelligent and incentive mechanisms have been studied

* Corresponding author (email: Corresponding author (Email: zhaolongning@dlut.edu.cn))

to ensure nodes cooperate in message forwarding [5,6], the traditional methods always assume that all nodes have the same social status in the network architecture.

In fact, it has been demonstrated in [7] that most nodes have social selfish features in real networks, and nodes may set the priority for transmission services according to their social relationships [8]. Thus, nodes will attempt to save their resources by refusing to forward packets for nodes with weak social relationship. Moreover, nodes with weak social relationships will find it rather hard to receive rewards under these mechanisms, and these nodes are more likely to be isolated or deteriorate to become malicious nodes, which will decrease network performance significantly.

In this paper, we propose a secure routing mechanism by considering social network and reputation evaluation. Here groups are built with nodes of similar social status and behavior reputation. Friend nodes are recommended to join into the same group to reduce the possibility of isolated nodes. Relay nodes are elected in the groups to provide secure routing. Thus, network performance can be greatly improved since nodes are willing to cooperate because of both active and passive incentive mechanisms. The rest of this paper is organized as follows. Related work is illustrated in Section 2. A novel reputation evaluation algorithm is introduced in Section 3. In Section 4, we utilize the presented scheme to resolve the problem of social selfish attacks in WMNs. Simulation results are demonstrated in Section 5 and Section 6 draws the conclusion.

2 Related works

Malicious and selfish behaviors are a serious threat to routing in delay-tolerant networks (DTNs). The iTrust scheme for secure routing establishes efficient trust [9], which analyzed node behavior according to the collected routing evidence and probabilistically checking. The authors in [10] presented a dynamic trust management scheme for secure routing in DTNs, and a comprehensive analysis of this method demonstrated that it can handle selfish behaviors and is resilient against trust-related attacks. A routing metric based on an expected forward counter was proposed in [11] to deal with the packet dropping problem caused by selfish nodes in WMNs, which utilized the MAC cross-layer design and routing layers to select high-reliability transmission paths. The authors in [12] presented a fair charging policy to stimulate node cooperation by charging the source and destination nodes when both of them benefit from the communication. Furthermore, a small-size check is generated during each routing process and a check submission method is utilized to reduce check number and protect against collusion attacks.

A secure and efficient trust method based on Bayesian theory was presented in [13]. The method detects malicious nodes by considering node attacks. The trust values of nodes are calculated by their father nodes in the route and secure routes are selected by the modified Diffie-Hellman key agreement protocol. Although the effectiveness of the low-energy adaptive clustering hierarchy (LEACH) routing protocol has been demonstrated, security is one of its problems. The authors in [14] classified secure LEACH schemes into cryptographic-based and trust-based solutions, reviewed the corresponding development of different methods and presented a qualitative comparison of secure LEACH methods based on different security metrics. A scheme based on the dynamic source routing (DSR) protocol for network security was proposed in [15], which calculated the round trip time (RTT). The presented method not only can protect DSR against wormhole attacks in ad hoc networks, but it also considered the processing and queuing delays in the calculation of RTTs between neighboring nodes.

3 Node role oriented reputation evaluation scheme

Based on the above discussion, we want to build a secure routing scheme to defend against social selfish attacks. First, we present a role-oriented dynamic reputation evaluation model (DREM) to assess node reputation and the cooperation between different nodes. Through evaluating a node's behavior, this model can effectively detect a selfish attack. Then we study the effect of node selfishness and design a social associated dynamic reputation evaluation model (SADREM) to evaluate the social relationships between nodes. Finally, we propose a secure routing scheme based on the social groups. The details of DREM will be described in the following parts of this section.

3.1 Node reputation

In this reputation evaluation mechanism, reputation is evaluated from node behavior, which involves control messages and processing of data packets during routing. Thus, reputation can reflect the capability of a node in dealing with other nodes' requests (i.e., messages or packets). The security status of a node can be determined through its reputation value, known as behavior reputation (BR). This scheme chooses nodes with a higher value as relay nodes to ensure reliability of communications.

Assume the activity of each node is random (i.e., the node movement velocity is uncertain). We evaluate the BR of each node by period and assume that the BR from nodes i to j in the tth evaluation is es_{ij}^t. Therefore, the sequence set of BR from nodes i to j during n periods can be described as $ES_{ij} = \{es_{ij}^1, es_{ij}^2, \ldots, es_{ij}^t | \forall es_{ij}^t = 0 \text{ or } 1\}$, where 0 and 1 denote negative and positive evaluations, respectively. Since each cooperative action is independent, each sample $X = ES_{ij}$ needs to satisfy $X \sim B(n,p)$, where $B(n,p)$ is the binomial distribution. Its probability density can be written as

$$P(X = x) = \binom{n}{x} p^x (1-p)^{n-x}, \quad x = 0, 1, 2, \ldots, n, \tag{1}$$

where x is the number of positive evaluations.

Assume that $h(p)$ is the prior probability density of p. Thus, the posterior probability density of p can be calculated as

$$f(p|x) = \frac{h(x,p)}{m(x)} = \frac{\binom{n}{x} h(p) p^x (1-p)^{n-x}}{\binom{n}{x} \int_0^1 h(p) p^x (1-p)^{n-x} \mathrm{d}p} = \frac{h(p) p^x (1-p)^{n-x}}{\int_0^1 h(p) p^x (1-p)^{n-x} \mathrm{d}p}, x = 0, 1, 2, \ldots, n; 0 \leqslant p \leqslant 1. \tag{2}$$

We assume that p takes value equiprobably between 0 and 1, so that $h(p)$ has a uniform distribution between 0 and 1. Therefore, the above equation can be written as

$$f(p|x) = \frac{p^x (1-p)^{n-x}}{\int_0^1 p^x (1-p)^{n-x} \mathrm{d}p}, \quad x = 0, 1, 2, \ldots, n. \tag{3}$$

According to the definition of the β function, $f(p|x) = \frac{p^x(1-p)^{n-x}}{B(x+1, n-x+1)}$. Since $B(x,y) = \frac{\Gamma(x)\Gamma(y)}{\Gamma(x+y)}$, we get

$$f(p|x) = \frac{p^x (1-p)^{n-p}}{\frac{\Gamma(x+1)\Gamma(n-x+1)}{\Gamma(n+2)}} = \frac{\Gamma(n+2)}{\Gamma(x+1)\Gamma(n-x+1)} p^x (1-p)^{n-x}. \tag{4}$$

Similar with the derivation in [16], the probability of Bayesian estimation for successful forwarding is

$$\bar{p} = E(p|S_{ij}) = \frac{S_{ij} + 1}{n+2}, \tag{5}$$

and the possibility of Bayesian estimation for failure forwarding is

$$\widetilde{q} = \frac{F_{ij} + 1}{n+2}. \tag{6}$$

The analysis stated above assumes uniform distribution, which is $\mathrm{Beta}(1,1)$. Without loss of generality and according to conjugate prior distribution, if $\mathrm{Beta}(\alpha, \beta)$ is adopted for prior distribution, $f(p|x)$ follows Beta distribution with parameter $(x + \alpha, n - x + \beta)$. Thus, $\alpha = S_{ij} + 1$, $\beta = F_{ij} + 1$, $\bar{p} = \frac{\alpha}{\alpha+\beta}$, and $\widetilde{q} = \frac{\beta}{\alpha+\beta}$.

$\bar{p}$ and $\widetilde{q}$ are the predicted values to illustrate the successful and failure possibilities, respectively. It can be seen that if two nodes have no interaction, node reputation equals to 0.5. If the reputation of one node is less than 0.5, this node can keep the value of its reputation by changing name constantly. In order to avoid this circumstance, the successful forwarding possibility should not be the only factor to calculate node reputation, and the reputation based on difference between forwarding success and failure rates can be calculated by

$$R_{ij} = \begin{cases} \bar{p} - \widetilde{q} = \frac{\alpha-\beta}{\alpha+\beta}, & \alpha > \beta, \\ 0, & \text{else}. \end{cases} \tag{7}$$

It can be observed in (7) that the larger gap between the successful and the failure estimation values of Bayesian rule exists, the higher node reputation is. Then we analyze the change of reputation. The total derivation of (7) will be calculated by Reputation algorithm based on difference between forwarding success rate and failure rate (RFSF) in our work.

$$dR_{ij} = \frac{2\beta}{(\alpha+\beta)^2} d\alpha - \frac{2\alpha}{\alpha+\beta} d\beta. \tag{8}$$

Therefore, both the values of α and β should be considered in analyzing the change of reputation value. If β remains unchanged while α increases, the reputation value increases according to (7). No matter whether the value of α and β is larger, the reputation value will be rise. Since $\alpha > \beta$, then $\left|-\frac{2}{\alpha+\beta}\right| > \left|\frac{2\beta}{(\alpha+\beta)^2}\right|$, and vice versa. Thus, reputation improves over a smaller range than over which it decreases, which accords with our view of reputation.

Although the presented method can reflect reputation change, the recent behavior of node cannot be reflected. For example, consider Case 1: $ES_{ij} = \{1,1,1,0,1,1,1,0,1,0,1,1,1,0,1,1,1,1\}$, and Case 2: $ES_{ik} = \{1,1,1,1,1,1,1,0,1,1,1,1,1,1,1,0,0,0\}$. It is easy to see that Case 2 is the typical behavior in a selfish attack. Case 1 reflects the non-cooperative behavior of a node, which is rational for social selfish nodes beyond the scope of the network monitor. Although the calculated reputation values are the same, the behavior of node j is better than that of node k, which means the above presented scheme does not consider timeliness. Since the current reputation is considered to have more influence than the historic behaviors, the corresponding weighting factors of historic behaviors should be reset. If the information from nodes i to j is forwarded successfully, $es_{ij}^t = 1$, otherwise, $es_{ij}^t = 0$. The corresponding weighting equations are shown follows. If the $(n+1)$th time forwarding is successful, $\alpha_{n+1} = \omega\alpha_n + es_{ij}^{n+1}$. where ω is the weighting factor that considers attenuation according to the historic behavior.

We then discuss how to select the value of ω. According to the evaluation sequence $ES_{ij} = \{es_{ij}^1, es_{ij}^2, es_{ij}^3, \ldots, es_{ij}^t, \ldots, es_{ij}^n | es_{ij}^n = 0 \text{ or } 1\}$, we can derive the value of α when the $(n+1)$ times transmission is forwarded successfully, this value is

$$\alpha_{n+1} = es_{ij}^{n+1} + \omega es_{ij}^n + \omega^2 es_{ij}^{n-1} + \cdots + \omega^n es_{ij}^1 + \omega^{n+1}. \tag{9}$$

Assume the successful transmission possibility p is a constant value, if the value of $n+1$ is large enough, $E(\alpha_{n+1}) = \frac{p}{1-\omega}$. Define $m = \frac{1}{1-\omega}$, the expectation becomes the Bayesian estimation after m times forwarding. Furthermore, the selection of ω should satisfy $\alpha_n \leqslant (\alpha_{n+1} = \omega\alpha_n + 1) \leqslant \alpha_n + 1$ to avoid α_n converges to $\frac{1}{1-\omega}$. Since $1 - \frac{1}{\alpha_n} \leqslant \omega \leqslant 1$, set $m = \frac{1}{1-\omega}$ and we can obtain $m \geqslant \alpha_n$. That is m and α_n has the same order of magnitudes, set $m = 10^{(\lg\alpha_n)+1} > \alpha_n$ and $\omega = 1 - \frac{1}{10^{(\lg\alpha_n)+1}}$. Similarly, after $(n+1)$ times failure transmission, the value of β can be calculated by

$$\beta_{n+1} = (1 - es_{ij}^{n+1}) + \omega(1 - es_{ij}^n) + \omega^2(1 - es_{ij}^{n-1}) + \cdots + \omega^n(1 - es_{ij}^1) + \omega^{n+1}. \tag{10}$$

Therefore, if the information is forwarded successfully and $\alpha_n \geqslant 1$, set $\omega = 1 - \frac{1}{10^{(\lg\alpha_n)+1}}$, otherwise, $\omega = 1 - \frac{1}{10^{(\lg\beta_n)+1}}$, $\alpha_{n+1} = \omega\alpha_n + 1$ and $\beta_{n+1} = \omega\beta_n$. If the information is failed for transmission and $\beta_n \geqslant 1$, set $\omega = 1 - \frac{1}{10^{(\lg\beta_n)+1}}$, otherwise, define $\omega = 1 - \frac{1}{10^{(\lg\alpha_n)+1}}$, $\alpha_{n+1} = \omega\alpha_n$ and $\beta_{n+1} = \omega\beta_n + 1$. This scheme is named improved RFSF.

The more information acquired from the neighboring nodes, the more accuracy to make correct decision for the corresponding nodes. Since the interactions between the local and neighboring nodes are only a small portion of all the interactions, it will result in the judgment of node information has some limitation, and cannot detect the potential threat, therefore, indirect reputation should be introduced to evaluate node performance. Indirect reputation is a comprehensive evaluation from the aspect of the third party to provide more information so that the evaluation accuracy can be enhanced. Define T_B^A as the recommended reputation between entities A and B, thus the reputation of entity A recommended by entity B becomes $T_C^{B\to A} = T_C^B \otimes T_B^A$, where $\otimes$ stands for transfer operator. The direct and indirect reputations are combined to calculate the overall reputation of the evaluation subject. Since there are multiple recommended paths between subject A and evaluation object C, namely $B_1, B_2, \ldots, B_n$, the calculated reputation, which includes direct and indirect reputations, is shown as

$$R = R_d + \sum_{i=1}^{n} [T_{B_i}^A \otimes T_C^{B_i}]. \tag{11}$$

3.2 Calculation of cluster reputation

In this section, we first introduce the impact factor, by which the influence degree of node in the cluster can be defined, and then the weighting factor is assigned according to the influence degree to calculate the reputation of cluster. The impact factor consists of four parts: node reputation, times forwarded by malicious node, times of reputation volatility and forwarded times. Eqs. (12) and (13) are utilize to describe the corresponding node membership:

$$r_{ij} = \frac{x_{ij} - \min(X_j)}{\max(X_j) - \min(X_j)}, \tag{12}$$

$$r'_{ij} = \frac{\max(X_j) - x_{ij}}{\max(X_j) - \min(X_j)}. \tag{13}$$

The objective matrix X can be transformed into $R = (r_{ij})$, and according to the definition of complementary function, we have $R' = (r'_{ij})$, and $r'_{ij} = 1 - r_{ij}$.

In the fuzzy network system, the impact factor has different weighting values, which can be set by: $\omega = (\omega_i)$, $\omega_i = (\omega_1, \omega_2, \ldots, \omega_m)^{\mathrm{T}}$ and $\sum_{i=1}^{m} \omega_i = 1$. The distances between scheme j together with inferior methods are

$$d_{jg} = \left\{ \sum_{i=1}^{m} [\omega_i (1 - r_{ij})]^p \right\}^{\frac{1}{p}}, \tag{14}$$

$$d_{jb} = \left\{ \sum_{i=1}^{m} [\omega_i (r_{ij} - 0)]^p \right\}^{\frac{1}{p}}. \tag{15}$$

According to the theory of relative membership degree, the shorter (longer) distance between scheme j and d_{jg} (d_{jb}), the larger influence our scheme has. The corresponding normalization of scheme j can be illustrated as

$$u_j = \frac{1}{1 + p\sqrt{\frac{\sum_{i=1}^{m} (\omega_i (1 - r_{ij}))^p}{\sum_{i=1}^{m} (\omega_i r_{ij})^p}}}, \tag{16}$$

where p is the distance coefficient, and commonly set to 1 or 2.

Node reputation is set to 0.6, and other factors can be calculated by entropy weight method. At first, the entropy of the ith index H_i can be defined as

$$H_i = -k \sum_{i=1}^{n} f_{ij} \ln f_{ij}, \tag{17}$$

where $f_{ij} = \frac{1 + b_{ij}}{\sum_{i=1}^{n} (1 + b_{ij})}$ and $k = \frac{1}{\ln n}$. Set the entropy weight of index j as ω_j, the weight factor of different indexes can be shown as

$$\omega_j = \frac{1 - H_j}{n - \sum_{j=1}^{n} H_j}. \tag{18}$$

The reputation of cluster includes the reputations of cluster head and other inside nodes, defined as $R_{\text{all\_node}}$ and R_{CH}, respectively. The corresponding weight values are ω_1 and ω_2, satisfying $\omega_1 + \omega_2 = 1$. The calculation of cluster head is illustrated as

$$R_{\text{C}} = \omega_1 R_{\text{all\_node}} + \omega_2 R_{\text{CH}} = \omega_1 \sum_{j=1}^{n} \frac{u_j}{\sum_{j=1} u_j} R_{\text{node\_}j} + \omega_2 R_{\text{CH}}. \tag{19}$$

3.3 Update of node reputation

Although the members do not communicate with each other via routing forwarding, they can affect network communication among cluster by attacking the cluster head. Therefore, the reputations of both cluster head and members inside should be updated to encourage the cooperation among nodes. The reputation is adjusted according to the forwarding result, if the information is forwarded successfully,

$$\varepsilon_C = \frac{m+1-n}{m+n+2+1} - \frac{m-n}{m+n+2}, \tag{20}$$

$$R_C^{\text{new}} = R_C^{\text{old}} + \varepsilon_C, \tag{21}$$

herein, m and n are the numbers of times that information can be forwarded successfully and unsuccessfully. ε_C is the fluctuation quantity of reputation, the update calculations for member and head in the cluster are shown as

$$R^{\text{new}}_{\text{node\_CM}} = \begin{cases} R^{\text{old}}_{\text{node\_CM}} + 0.6 \times \varepsilon_C \times 1/R^{\text{old}}_{\text{node\_CM}}, & \varepsilon_C > 0, \\ R^{\text{old}}_{\text{node\_CM}} + 0.3 \times \varepsilon_C \times 1/R^{\text{old}}_{\text{node\_CM}}, & \varepsilon_C < 0, \end{cases} \tag{22}$$

$$R^{\text{new}}_{\text{node\_CH}} = \begin{cases} R^{\text{old}}_{\text{node\_CH}} + 0.6 \times \varepsilon_C, & \varepsilon_C > 0, \\ R^{\text{old}}_{\text{node\_CH}} + 0.3 \times \varepsilon_C, & \varepsilon_C < 0, \end{cases} \tag{23}$$

where $\varepsilon_i \in [-1, 1]$ represents the reputation variation of cluster C_i. The reputation of cluster nodes depends on the reputation of the head node. This is because on one hand, the head node has more important responsibility for the security of the whole cluster; on the other hand, this method can shrink the difference value between nodes, and improve the communication quality of nodes.

4 Node evaluation scheme based on social character

Most existing routing protocols assume nodes would like to forward packet for other nodes, which means full cooperation is considered. However, if network resource is constrained, in order to maximize its own benefit, node would refuse to forward packets for other nodes to save network resource, which is called social selfishness [17]. Due to node selfishness, they prefer to forward information for the nodes with strong relationship. Therefore, in this section, we study the effect of node selfishness and design a SADREM while considering network security.

According to node occupation, network is divided into two non-overlapping communities V_1 and V_2, which consists of M and N mobile nodes, respectively. It has been demonstrated in [18] that the communication of any two nodes follows Poisson distribution with parameter $\widetilde{\lambda}$. Define the communication probabilities within and without the community are λ_i and λ_o, respectively. The source and destination nodes do not belong to the communities V_1 and V_2, and the probability for node communication is λ. Due to node selfishness, if two nodes are in the same community, the forwarding probability is p_q, otherwise, this probability is p_o. Packet forwarding is modeled into two-dimensional continuous time Markov chain, where $m(t)$ and $n(t)$ stand for the numbers of nodes that have packets for transmission.

The initial state is (0,0), and the number of the transition state is $S = (M+1) \times (N+1)$. The generated matrix $\boldsymbol{Q}$ is

$$Q = \begin{pmatrix} D & R \\ 0 & 0 \end{pmatrix}, \tag{24}$$

where the submatrix $\boldsymbol{D}$ consists of $S \times S$ factors, and $D_{i,j}$ is the transition probability from states i to j. $\boldsymbol{R}$ is an $1 \times S$ submatrix, $R_{i,D_{\text{st}}}$ stands for the transition probability from state i to absorbing state D_{st}. Consider node selfishness, the transition probabilities can be demonstrated as

$$D\{(m+1,n)|(m,n)\} = (M-m)(\lambda + mp_i\lambda_i + np_0\lambda_0), \quad \text{for} \quad n \in [0,N],\ m \in [0,M-1], \tag{25}$$

$$D\{(m,n+1)|(m,n)\} = (N-m)(\lambda + mp_0\lambda_0 + np_i\lambda_i), \quad \text{for} \quad n \in [0,N-1],\ m \in [0,M], \tag{26}$$

$$R\{(D_{\rm st})|(m,n)\} = (m+n+1)\lambda, \quad \text{for} \quad n \in [0,N],\ m \in [0,M], \tag{27}$$

$$D\{(m,n)|(m,n)\} = -D\{(m+1,n)|(m,n)\} - D\{(m,n+1)|(m,n)\} - R\{(D_{\rm st})|(m,n)\}. \tag{28}$$

The transmission delay D_d and cost C_d are utilized to evaluate network performance. D_d is the average consumed time for packet transmission to the destination node successfully, which can be calculated by $D_d = e \cdot (-D^{-1}) \cdot I$. e is the $1 \times S$ vector, which stands for node initial state $e = [1, 0, \ldots, 0]$, I is the vector that all the elements inside equal to 1. C_d is the average number of times that this information is copied before reaching destination node. By generation matrix $\boldsymbol{Q}$, we can work out the transition possibility matrix $\boldsymbol{P}$, and the factor $p_{i,j}$ is shown as

$$p_{i,j} = \begin{cases} -q_{i,j}/q_{j,i}, & j \neq i, \\ 0, & j = i, \end{cases} \tag{29}$$

where $P_{1,S+1}$ is the transition possibility from the initial state (0, 0) to D_{st}, $P^2_{1,S+1}$ is the transition possibility from (0, 0) via (1, 0) and (0, 1) to D_{st}. Thus, the transmission cost C_d can be calculated by $C_d = \sum_{i=1}^{M+N} i \cdot p^i_{1,S+1}$.

In this section, we describe the social relationship of different nodes. Assume that all the nodes could be represented by their characteristics, and all the characteristics belong to one same characteristic space. One M-dimensional vector is taken to present this characteristic space and M is the number of characteristics. We can set the type and characteristic number according to network applications.

Once we have defined the concept of characteristic space, we can assign the M-dimensional vector $\boldsymbol{A}$ to represent the characteristic of node A. With the characteristic vector, we can evaluate social relationship orientation of node A which is its ID from social relationship.

We can compare node characteristic vector to represent its social similarity, which also represents the relevance of node's social relationship. Vectors $\boldsymbol{A}$ and $\boldsymbol{B}$ represent the characteristic vector of nodes A and B, the vector angle $\Theta(A,B)$ is defined as

$$\Theta(A,B) = \cos(\angle AB) = \frac{A \cdot B}{\|A\|\,\|B\|}, \tag{30}$$

where $\|X\|$ represents the length of vector $\boldsymbol{X}$.

From the above equations, we can find out that $\Theta(A,B) \in [0,1]$. $\Theta(A,B)$ with high value means these two nodes have strong social relationship. Thus we achieve the measurement of social relationship by the angle of characteristic vector. We define w_{ij} as the transmission possibility to represent the probability of node i to transmit packet to node j, shown as, $w_{ij} = \Theta(A,B)$.

Group is the result of social network and we can find the prototype in real community. In our real life community, the interactive action mostly depends on the trust within the members in the community. In the presented algorithm, we collect the nodes with similar characteristic into one group and update the information of group according to the nodes' relevance in their routing behavior.

Assume that all the nodes are independent and there is no coordinated attack behavior. The basic principle of group construction is shown as follows:

Principle 1. Node A invites node B, which has the most similarity with node A. If the reputation of these two nodes is larger than the threshold, this group can be constructed. The inviter and invited nodes are the leader and associate leader of the group, respectively.

Principle 2. The leader and the associate leader invite other nodes to join into the group according to their reputation and similarity.

Principle 3. Each node can be the leader of only one group. If it is not a group leader, it can be the associate leader of only one group.

The reputation evaluation can accurately evaluate the reputation of each node. In our scheme, we apply reputation evaluation in the route protocol to assess routing security, and present a security scheme in the routing discovery phase so that the trust nodes can transmit packets while the incredible nodes will

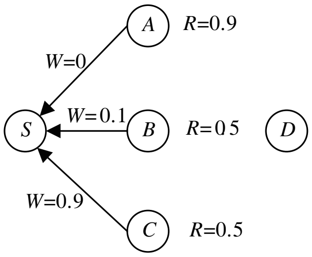

Figure 1 Examples of willingness-aware forwarding.

not be considered. The application and core idea of reputation algorithm is to avoid the node with low reputation during the routing selection. Since the presented method will cause node selfishness, two judgment criterions are introduced to select routing effectively.

The application and core idea of reputation algorithm is to avoid the node with low reputation during the routing selection. Since the presented method will cause node selfishness, two judgment criterions are introduced to select routing effectively.

As shown in Figure 1, node S intends to transmit packet to node D, during the routing selection process, three next-hop nodes, namely A, B and C are found. W stands for forwarding will and R is reputation value. If only reputation is considered, node A will be the next-hop node, however, the will for node A to forward packet from node S is 0, which means these two nodes will not cooperate, thus the packet will be discarded. Through comprehensive consideration, node C will be the next-hop node. By the analysis stated above, the forwarding possibility N_A^B is utilized to evaluate node reliability, which can be shown as

$$N_A^B = W_{AB} \times R_B. \tag{31}$$

By incorporating with the reputation evaluation scheme, the SADREM scheme is proposed.

5 Simulation results

In this section, network performance is evaluated by employing VC and NS-2 in simulations. We consider a WMN with 100 nodes. Each node can move in a square of 1000 m by 1000 m. Traffic is produced using a traffic generator, which randomly creates constant bit rate sessions. The size of a data packet is 512 bytes. It is assumed that the initial reputation value of each node is 0.5, and the cluster structure has already been built at the beginning of the simulation.

Rapidity and convergence are important indexes in the reputation evaluation algorithm, and the convergence speed and the reputation value of cluster head are shown in Figure 2. The algorithm for comparison is reputation-based framework for sensor networks (RFSN), which was presented in [19]. In RFSN, a single node based reputation algorithm is presented, where node status are equal and no cluster head nodes together with gate nodes are inside. It can be observed that by our proposed DREM scheme, node cooperation stimulates the change of reputation to speed up, this is because our method considers the relationship among nodes while this factor is ignored in RFSN scheme.

Next, we consider other network factors including packet deliver rate, overhead, delay and average throughput. The packet delivery rate is defined as the ratio of the number of received data packets and the number of sent data packets. The overhead is the ratio of the number of control packets and the number of data packets. The network delay is the difference between the end time and start time of a delivery. The average throughput is the total number of transmitted packet bytes within the transmission time. The related simulation results and analysis are as follows.

Figure 3 shows the change of delivery ratio according to the variance of delivery rate. In this simulation, 24 nodes are divided into six clusters, and there are two selfishness nodes in the network. In additional, no reputation evaluation scheme is operated on AODV routing protocol. From the figure, we can find that the achieved delivery rates of the schemes RFSN and DREM are much larger because of reputation evaluation. As the delivery rate enhances, network performance affected by attack becomes more serious.

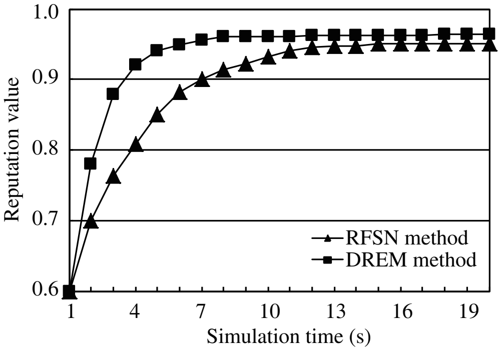

Figure 2 Reputation change with time.

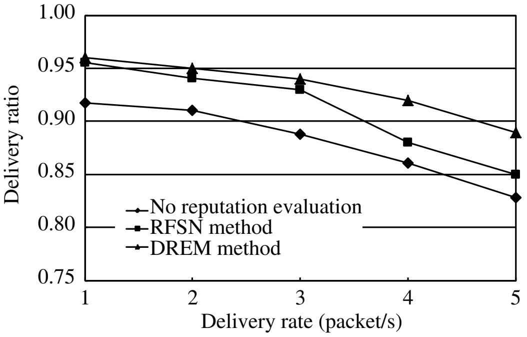

Figure 3 Delivery rate under different packet sending rates.

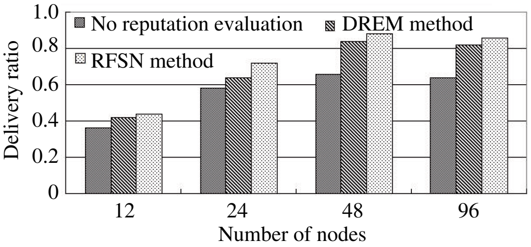

Figure 4 Delivery rate under different numbers of nodes.

Our presented DREM scheme evaluates node reputation according to node actual performance, therefore, delivery ratio decreases more slowly as the delivery rate increases.

Figure 4 is the change of delivery ratio according to the number of network nodes, where the total number of nodes varies from 12 to 96 and the number of selfish nodes changes from 1 to 4. The amounts of connection links are 3, 6, 9 and 12, respectively, and the packet transmission rate equals to 2 packets per second. It can be observed that when the total number of nodes equals to 12, no matter which methods are adopted, big amount of packet loss exists. The reason is that the node density is low and the communication among nodes is rare. Under this situation, node selfishness is not the main reason for packet loss. When the number of nodes increases, the presented DREM scheme can decrease packet loss effectively. It can also be observed that when the number of network node is 48, the packet loss is the lowest.

Figure 5 illustrates the delivery ratio under different numbers of node connections, where the total number of nodes equals to 24, transmission rate is 2 packets per second. It can be seen that as the number of node connection pair increases, the packet delivery rate decreases due to node selfishness. By the presented DREM method, the harmful effect brought by node selfishness can be eliminated. This is because our method can effectively avoid the route including selfishness node. Moreover, packet delivery rate does not deteriorate so quickly.

It can be observed in Figure 6 that as node movement speed enhances, packet delivery rate decreases. This is because node communication range is fixed, if the node moves too fast, the frequencies of link connection and disconnection are high, which affects communication quality seriously. Under the same situation, our presented SADREM method can achieve the highest delivery ratio, which shows it can accommodate the variance of node speed.

It can be observed in Figure 7 that when node movement speed is low, the SADREM algorithm has a higher network cost than DREM, since the former has a more complex routing discovery process. As node speed increases, SADREM has more advantages since node reputation is considered during routing selection.

Figures 8–10 evaluate network performances achieved by different schemes. There are 48 network nodes

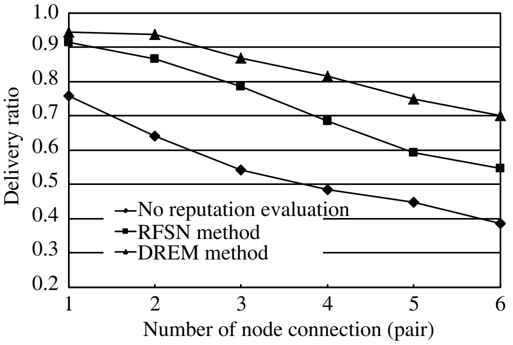

Figure 5 Delivery rate under different numbers of connections.

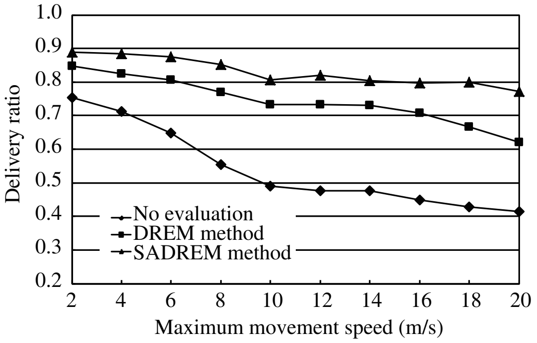

Figure 6 Delivery rate under different speeds of nodes.

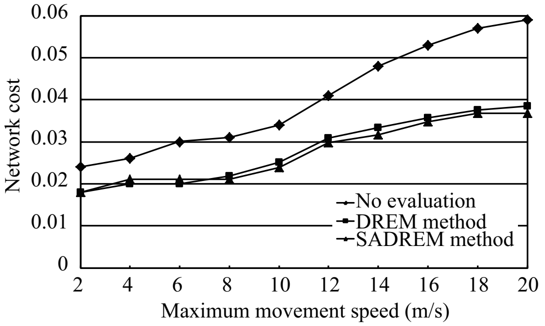

Figure 7 Overhead under different speeds of nodes.

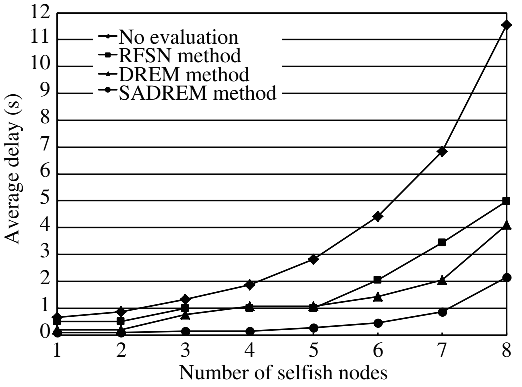

Figure 8 Average delay under different numbers of selfish nodes.

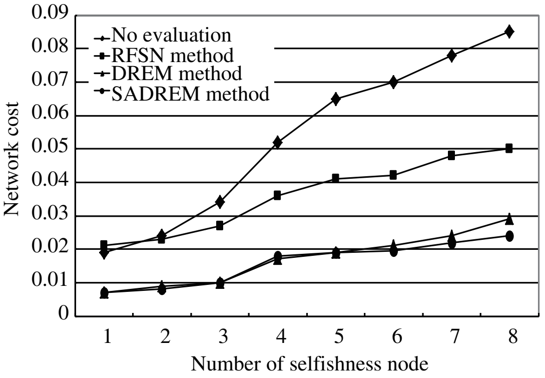

Figure 9 Overhead under different numbers of selfish nodes.

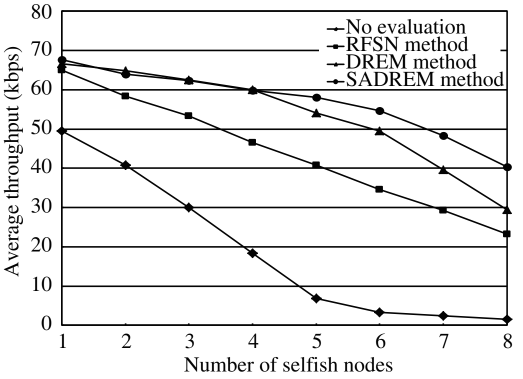

Figure 10 Average throughput under different numbers of selfish nodes.

in the network and the number of node connection is eight.

From Figure 8 we can find that as the number of selfishness nodes increases, network delay enhances. Meanwhile we need to pay attention to the change trend of the different schemes. AODV protocol does not consider the protection of selfishness node, and is affected seriously by node attack. Although node behavior based RFSN can reduce network delay to some extent, when the number of selfish nodes is more than five, delay increases sharply. Compared with RFSN, DREM can reduce delay further since node roles are treated differently so that node behavior can be evaluated more accurately. For SADREM, when the number of selfishness node exceeds eight, network delay is just more than 1 second, which demonstrates its superiority.

Figure 9 shows the network cost for different numbers of nodes. The network cost of AODV rockets due to node selfishness. When the number of selfishness nodes is less than three, DREM has a lower cost than SADREM since the computation complexity of the latter is high. The average throughput with different number of selfishness node is shown in Figure 10. As the number of selfishness node increases, network throughput decreases obviously especially for AODV. For RFSN, the decrease of throughput is approximately linear.

6 Conclusion

Focusing on selfish node attack, this paper has presented routing schemes to eliminate the effect brought by selfish nodes. Since selfish attack will cause packet loss due to limited node resource, we have first presented the DREM method according to node dynamic reputation. The advantage of DREM is utilizing different reputation calculation schemes based on node role, so that the evaluation accuracy can be improved. Then node selfishness is considered, and by combining node reputation, the SADREM scheme has been proposed. Since selfish attack affects the selection of next-hop node according to the social relationship, by denoting node social character and utilizing vector intersection angle to describe the social relationship among different nodes, routing can avoid the node with weak social relationship so that the harmful effect brought by selfishness node can be reduced. Simulation results have demonstrated that our methods are more accurate and efficient than the existing schemes. In the near future, we will investigate the reputation deceiving issue as we have assumed that the reputation is true and objective.

Acknowledgements This work was supported in part by National Natural Science Foundation of China (Grant Nos. 61302071, 61172051, 61471109, 61502075), Liaoning Province Doctor Startup Fund (Grant No. 201502263), Fundamental Research Funds for the Central Universities (Grant Nos. DUT15QY06, DUT15RC(3)009), and State Key Laboratory for Novel Software Technology, Nanjing University (Grant No. KFKT2015B12).

Conflict of interest The authors declare that they have no conflict of interest.

References

1 Zhang Z S, Huangfu W, Long K P, et al. On the designing principles and optimization approaches of bio-inspired self-organized network: a survey. Sci China Inf Sci, 2013, 56: 071301

2 Huangfu W, Zhang Z S, Chai X M, et al. Survivability-oriented optimal node density for randomly deployed wireless sensor networks. Sci China Inf Sci, 2014, 57: 029301

3 Jo M, Han L, Kim D, et al. Selfish attacks and detection in cognitive radio ad-hoc networks. IEEE Netw, 2013, 27: 46–50

4 Beres E, Adve R. Selection coorperation in multi-source cooperative networks. IEEE Trans Mobile Comput, 2008, 7: 118–127

5 Zhang Z, Long K, Wang J, et al. On swarm intelligence inspired self-organized networking: its bionic mechanisms, designing principles and optimization approaches. IEEE Commun Surv Tut, 2014, 16: 513–537

6 Zhang Z, Long K, Wang J. Self-organization paradigms and optimization approaches for cognitive radio technologies: a survey. IEEE Wirel Commun, 2013, 20: 36–42

7 Mei A. Social-aware stateless forwarding in pocket switched networks. In: Proceedings of IEEE International Conference on Computer Communications (INFOCOM), Shanghai, 2011. 251–255

8 Szott S. Selfish insider attacks in IEEE 802.11s wireless mesh networks. IEEE Commun Mag, 2014, 52: 227–233

9 Zhu H, Du S, Gao Z, et al. A probabilistic misbehavior detection scheme toward efficient trust establishment in delay-tolerant networks. IEEE Trans Parall Distr, 2014, 25: 22–32

10 Chen I, Bao F, Chang M, et al. Dynamic trust management for delay tolerant networks and its application to secure routing. IEEE Trans Parall Distr, 2014, 25: 1200–1210

11 Paris S, Nita-Rotaru C, Martignon F, et al. Cross-layer metrics for reliable routing in wireless mesh networks. IEEE/ACM Trans Netw, 2013, 21: 1003–1016

12 Mahmoud M, Shen X. FESCIM: fair, efficient, and secure cooperation incentive mechanism for multihop cellular networks. IEEE Trans Mobile Comput, 2012, 11: 753–766

13 Guo J, Zhou X, Yuan J, et al. Secure access control guarding against Internal attacks in distributed networks. Wirel Pers Commun, 2013, 68: 1595–1609

14 Masdari M, Bazarchi S, Bidaki M. Analysis of secure LEACH-based clustering protocols in wireless sensor networks. J Netw Comput Appl, 2013, 36: 1243–1260

15 Qazi S, Raad R, Mu Y, et al. Securing DSR against wormhole attacks in multirate ad hoc networks. J Netw Comput Appl, 2013, 36: 582–592

16 Yu Y, Guo L, Wang X, et al. Routing security scheme based on reputation evaluation in hierarchical ad hoc networks. Comput Netw, 2010, 54: 1460–1469

17 Li Q, Zhu S, Cao G. Routing in socially selfish delay tolerant networks. In: Proceedings of IEEE International Conference on Computer Communications (INFOCOM), San Diego, 2010. 15–19

18 Yong L, Hui P, Jin D. Evaluating the impact of social selfishness on the epidemic routing in delay tolerant networks. IEEE Commun Lett, 2010, 14: 1026–1028

19 Ganeriwal S, Srivastava M. Reputation-based framework for high integrity sensor networks. In: Proceedings of ACM Workshop on Security of Ad Hoc and Sensor Networks (SASN), Hamburg, 2011. 66–77