Yu *et al. EURASIP Journal on Wireless Communications and Networking* (2019) 2019:83
https://doi.org/10.1186/s13638-019-1397-1

EURASIP Journal on Wireless Communications and Networking

RESEARCH Open Access

Quantitative social relations based on trust routing algorithm in opportunistic social network

Genghua Yu, Zhi Gang Chen*, Jia Wu* and Jian Wu

Abstract

The trust model is widely used in the opportunistic social network to solve the problem of malicious nodes and information flooding. The previous method judges whether the node is a cooperative node through the identity authentication, forwarding capability, or common social attribute of the destination node. In real applications, this information does not have integrity and does not take into account the characteristics and dynamic adaptability of nodes, network structures, and the transitivity of social relationships between nodes. Therefore, it may not be effective in solving node non-cooperation problems and improving transmission success rate. To address this problem, the proposed node social features relationship evaluation algorithm (NSFRE) establishes a fuzzy similarity matrix based on various features of nodes. Each node continuously and iteratively deletes the filtered feature attributes to form a multidimensional similarity matrix according to the confidence level and determines the weights under different feature attributes. Then, the social relations of nodes are further quantified. The experimental results show that, compared with the traditional routing algorithm, NSFRE algorithm can effectively improve the transmission success rate, reduce transmission delay, ensure the safe and reliable transmission of information in the network, and require low buffer space and computing capacity.

Keywords: Opportunistic social network, Malicious nodes, Information flooding, Cooperative node, Feature attributes, Social relationship

1 Introduction

In recent years, as wireless networks have penetrated into our daily lives, the application scale of the network has been increasing. As a new type of self-organizing network, it has attracted the attention of researchers at home and abroad [1, 2]. In order to get rid of the restriction of establishing the end-to-end communication path to achieve network communication, the concept of the opportunistic social network is proposed. This concept has been widely used in animal tracking, vehicle network, and other fields [3, 4]. Opportunistic social networks belong to intermittent connectivity networks. Opportunistic social network nodes are characterized by typical mobility, openness, and sparseness. Nodes have low encounter rates and lack fixed and secure connectivity links. Generally, the “Storage-Carrying-Forwarding” mechanism [5] relies on the opportunity brought by node mobility to realize routing. This model requires that all nodes cooperate to forward the routing messages of other nodes in a coordinated manner and realize communication hop by hop through the chances of encounters caused by node movement.

Due to the limitations of energy, computational capacity, network bandwidth, and buffer space of the nodes in the opportunistic network [6, 7], as well as the instability and uncertainty of node connections, existing trust modeling schemes are difficult to directly applied to the opportunistic social networks. These may lead to the following problems: (1) It is difficult to collect the evidence of direct trust accurately and timely. Because of the dynamic nature of the node, it is possible to leave the connected domain after delivering the message to the next hop node. Therefore, the evidence of successful forwarding cannot be collected by using neighbor node monitoring methods, and there is no credible authorization center. (2) The node’s

* Correspondence: czg@csu.edu.cn; jiawu5110@163.com
School of Computer Science and Engineering, Central South University, Changsha 410083, China

uncooperative behavior results in the inability of a trusted authority to verify whether the next-hop node is a trusted node. Because in the process of transmitting information, the node may mask or not forward the received message for some reason. If the message is passed to more uncooperative nodes, the node's transmission success rate will be reduced. (3) The computational power and cache space of the nodes are limited. Existing trust modeling schemes [7] need to spend a lot of money on trust relationship acquisition, trust relationship maintenance and evaluation, and cache space. If they are forwarded to all nodes unconditionally, they will consume network resources [6–8]. Therefore, nodes in the resource-constrained opportunistic social network need to pay as little cost as possible to realize reliable message delivery.

In this paper, to address the challenges above, we propose a secure routing method named Node Social Features Relationship Evaluation (NSFRE) algorithm for screening trusted nodes based on social relations. To prevent the packet forwarding performance caused by packet forwarding in a flooding manner and thus causing network congestion, we introduce the relevant eigenvalues in the routing algorithm. NSFRE uses interaction records to establish feature information and network structure information of mobile nodes such as the number of connections, geographical location, and transitivity of relationships. NSFRE also establishes a fuzzy similarity matrix based on fuzzy feature vectors of nodes, and then iteratively computes social relationship values between nodes. According to the calculation results, the trusted nodes are selected, and it is considered that the same threshold is a trusted node, and a method is provided for a message source node to select a next-hop node with higher trustworthiness. This forwarding method easily finds the best path to the destination node. In this paper, through in-depth study of the internal relations between node activity rules and social relations, a trust routing table for node message forwarding is established, and the cooperative nodes that can forward the messages to the destination node are discovered and selected. Finally, it solves the problem of information flooding and node non-cooperation in the opportunistic social network and improves the real-time and reliability of information transfer between nodes. The algorithm performs experiments on real data sets and uses Stanford University's road structure as a network topology for simulation experiments. The experimental results show that our algorithm is superior to the four classic routing algorithms.

Specifically, the main contribution of this paper can be summarized as the following three aspects:

1. This paper studies the application of trust mechanism based on social relations in the network. In the network of opportunities, we proposed a method for filtering information by computing trust scores based on the value of social relations. This promotes that data packets in the network are always transmitted along trusted nodes, which reduces the blindness of information transmitted by other routing methods. The method minimizes the negative impact of uncooperative nodes on the network and improves the overall network performance
2. In the calculation of the value of a node's social relations, we are no longer only aimed at a single social attribute or adopting a subjective method such as the average weight method. In this paper, we calculate the value of social relations by first screening out the available nodes according to the characteristics of nodes, calculating feature weights according to the characteristics of node characteristics and social relations transitivity. Then, the social relationship values of the filtered nodes are calculated by the weight of each feature and the nodes that satisfy the characteristics. It reduces the subjective elements that give weights to features and increases the feasibility of screening mobile nodes for transmitting information.
3. In calculating the value of social relations, we consider that social relations change dynamically with time and increase the flexibility of social relations. In the new round of message information transmission process, according to the dynamic changes of social relations at different times, we will regenerate a new routing table, so that the social relationship calculation model has sufficient adaptability to the dynamic changes of the network and improve the accuracy of the model.

2 Related works

In order to reduce the harm of uncooperative nodes to the network, there have been many researches on the trust-based mechanism in the network at home and abroad, but the research on the trust mechanism in the opportunistic social network is still in its infancy. In the network, it is difficult to establish an end-to-end communication path between source and destination. Therefore, ad hoc routing protocols cannot be directly applied to opportunistic social networks. Instead, it uses a store-and-forward mechanism to communicate. However, selfish nodes will delete some data obtained from other nodes and thus seriously affect network performance. People have designed a trust-based routing protocol [9] (TRP) that combines various practical algorithms to reduce the negative impact of malicious nodes.

For many uncooperative nodes in the opportunistic social network, the uncooperative nodes are mainly divided into two types: (1) The received information is not forwarded. (2) The information is rejected and not forwarded. These uncooperative nodes have been able to detect packet loss behavior through some uncooperative node detection algorithms such as LARS [10]. However, the uncooperative nodes could use more concealed uncooperative behaviors to conceal themselves. For example, the probability of losing packets is controlled to be less than the threshold so as to avoid being punished. Therefore, many researchers propose to reduce the impact of uncooperative nodes on network resources based on the social trust model. Among them, a social trust model is proposed for secure routing in the opportunistic network [11]. This algorithm uses the node state forwarding capabilities and common attributes to evaluate social trust values.

For malicious nodes, in the harsh environment where node density is sparse, slow-moving nodes do not have the opportunity to join network routes because they cannot effectively use the opportunities encountered to achieve self-organized authentication. There is no need to establish a complete mutual authentication for each dialog. People are aware of the inadequacy of the idea of "authenticating" nodes to determine trust relationships. Therefore, people proposed a new trust management scheme based on behavior feedback information [12]. By using a certificate chain based on social attributes, the mobile node gradually establishes a local certificate graph and implements an "identity authentication" trust relationship.

For the network based on model trust proposed by people, you first need to use the proposed method to detect malicious nodes. When quantifying the trust of node, most existing methods rely on the number of final ACK messages received by the node. If the final ACK message cannot be reliably received, it will affect the reliability of the malicious node's judgment. Therefore, the researchers proposed a "double-hop feedback method" [13] to design a dynamic trust framework. It promotes the node to obtain the trust value of another node based on the behavior of the latter node to detect the selfish malicious node.

Furthermore, people apply social relations to networks. The analysis of social relationships is generally based on the structure obtained by social networks and uses the user's information flow to analyze the strength of the user's relationship, and then uses the weights on the edges of the graph [7] to establish trust model. In the opportunistic network, it has been proven that the user's social profiles are useful for finding suitable forwarding nodes in a delay tolerant network. A Social Relationship Opportunistic Routing Algorithm (SROR) [14] was proposed for mobile social networks. Social relations and profiles between nodes were used as the key indicators for calculating the optimal forwarding node in the route to maximize the packet transmission probability.

In addition to using social relationships to select the optimal forwarding node, people also propose a method extracting information from people's social interactions to quantify the trust relationship between nodes. Some researchers believe that acquiring trust from real-world social interactions can play an important role in understanding social behavior. Therefore, an opportunistic sensing system [15] is proposed, which can detect social interactions based on the real world and acquire and quantify trust relationships among people through smartphones.

Through the above analysis, we can see that the existing work is mainly focused on the limited communication radius and the nodes can be trusted. The information is transmitted accurately through multiple hops. The working method is similar to the WSN, except that the original static node is extended to the dynamic mobile node. As long as the communication between nodes is reachable, the data can be transmitted, but without considering the trust relationship delivery between nodes. There have been social relations calculations that start from a real scenario to analyze a specific attribute, or treat social relationships between nodes as static, without taking into account the dynamic changes in node social relations, and the decision feature that affects the quantification of social relationships is not enough considered. Therefore, this paper uses the research results of trust model and social computing in social networks to determine the trust relationship between nodes based on the dynamic characteristics and social relationships of mobile nodes based on social network theory. Through analyzing the characteristics of the social network of mobile nodes in the opportunistic social network, the corresponding feature information such as interactive quality feature Q, position feature P, trust quality characteristics T, and social relation feedback feature S are extracted to study the social relationships among mobile nodes. Then, based on the theory of information entropy, rough set, and so on, a mobile node social relations computing model is proposed. The model is used as the quantification of social relations between nodes and the weight distribution of decision features, so that the trustworthiness between nodes can be calculated to filter out the next hop node set for information forwarding.

3 Social characteristics analysis of nodes

In the opportunistic social network scene, cognition of social relationships is through the use of various sensing devices (mobile phones, PDAs, etc.) attached to mobile nodes [4]. The real-time information such as the activity rules and interaction records of the nodes can be obtained in real time to analyze the key feature influencing the social relations and explore the internal relations among them [16, 17]. Quantifying social relations can more objectively and accurately reflect the changes in the relationship between mobile nodes. Through the analysis of social networks, it shows that the social relations between mobile nodes have the following characteristics:

(1) Diversity: The information transmission of opportunistic social networks mainly relies on mobile nodes. Social relationship is the tie of the mobile node and also affects the activity rule of the mobile node. Due to the spatiotemporal characteristics of the mobile node, the calculation of the relationship involves many factors such as behavior and environment, and it is difficult to accurately quantify and predict [3].
(2) Inconsistencies: It refers to the directionality of social relationships in the interaction process of mobile nodes. This directionality causes the relative social relationships between the two parties to differ due to their internal and external factors [4, 6], namely the different perceptions of the same event and information. For example, the social relations between nodes u and v are $M(u, v) = 0.8$, whereas the relations between v and u may be $M(v, u) = 0.6$.
(3) Mobility: The value of social relations is a variable over time. With the change of decision features such as the law of activity and degree of interaction between each other, the social relations change dynamically. For example, the social relationship between nodes u and v may be $M(u, v) = 0.6$ for a period of time, and $M(u, v)$ may be 0.3 at the next moment as various network features change.
(4) Transitivity: When calculating social relations among mobile agents indirectly through judgments made by other nodes or environmental information rather than based on direct contact with each other, we call this process the transitivity of social relations. For example, nodes u and v, v, and w have social relations, then nodes u and w can establish social relations through v under certain conditions.
(5) Sociality: In the scene, the node behavior is not disordered, but is influenced by the characteristics [18] of individual consciousness, social role, demand, etc., and has certain social characteristics. For example, the daily activities of office workers are driven by events such as scheduling.

Through the above analysis, it can be seen that social relations are inherent manifestations of different modes of interaction among nodes and involve a variety of factors. Considering the complex and diverse characteristics [16, 17, 19] of the interaction patterns among nodes in the information delivery service for opportunistic social networks, we introduce various types of decision features to describe the spatial and temporal characteristics of social relations of nodes. Through the collection, analysis of the history record of connections between nodes and calculating interactive quality feature Q between each other, the interaction rules between each other are found out. Position feature P reflects the trajectory characteristics of nodes in the time period. It statistically analyzes the trajectory characteristics of nodes based on different geographical position and studies the frequency of different mobile nodes reaching the same sensing area within a certain period of time. The defined trust quality characteristics T represent the mobile node's evaluation of historical interaction information records, which reflects the satisfaction of service requesters with service providers in former information interactions. Similarly, the social relation feedback feature S is defined to reflect the transitivity of social relations between nodes [17, 19] and further improve the accuracy of quantitative social relations.

It can be seen that the social relationship cognitive model building process includes the following features:

(1) Real-time perception of mobile node information.

Mobile node through its own terminal equipment can obtain various behavior information of the user in real time [20–22], such as location information, network information, current status of the active node, etc. Through the classification and preprocessing of the original information of the nodes, the perceived service center extracts the trajectory information [22–24], connection records, and historical information interaction records of the nodes to provide data support for the next decision feature calculation and social relations quantification.

(2) Calculation of mobile node decision feature.

In the opportunistic social network, the forwarding of message is based on the social relations between nodes. The dynamic changes of social relations are determined by both space and time. Therefore, we introduce Q, P, T and S to describe the dynamic social relations of nodes.

(3) Mobile node decision feature weight assignment.

Social relationships of mobile nodes change over time, and at different times, states are interrelated. In this paper, the decision feature knowledge base is obtained by using rough set theory. Based on the information entropy, the decision feature is dynamically and rationally weighted. Finally, the nodes' next-hop nodes are screened by its social relation quantification algorithm to form a node forwarding domain, which provides the decision-making basis for the realization of the opportunistic social network information transmission.

From the above analysis, we can see that the quantitative modeling of social relations of mobile nodes is of great significance for expanding the scope of information transmission, reducing transmission delays and improving the quality of information transmission in opportunistic social networks. It is embodied in (1) using the main perceptive devices of the network to form a virtual social network, analyzing and calculating the social relations. In addition, a new intelligent network of object-matter, human-object, and human-human interaction is truly realized [19], so that when the next hop node is filtered by the source node, we can better integrate the dynamic characteristics of the network (2) in the social relation calculation, giving full consideration to the characteristics of the mobile node attributes and network structure characteristics. From different perspectives for feature analysis and node screening modeling, social relationship calculation is more comprehensive, objective, and reasonable; (3) social relations is the basis of this node to choose the next hop node to transfer information, and the follow-up work is based on this expands.

4 Quantitative model of social relations

In this paper, we consider various features that affect social relations and introduce decision features such as *P*, *Q*, *T* and *S* to describe the complexity, transitivity, and uncertainty of social relations from different perspectives.

4.1 Multi-dimensional decision feature of node calculation

Definition 1 The quantified value of social relations $M(u,v)$ between node u and v is:

$$
\begin{aligned}
M(u,v) &= \sum_{i=1}^{m} w_i f_i(u,v) \\
& s.t.\ 0 \le w_i \le 1 \\
& \sum_{i=1}^{m} w_i = 1 \\
& u, v \in N
\end{aligned}
\tag{1}
$$

where f_i represents different types of decision feature and ω_i represents the weights of different decision feature; m is decision characteristic number, and N is the set of nodes in the network. When $M(u,v) = 0$, there is no social relationship between nodes u and v. On the other hand, when $M(u,v) = 1$, u and v are the same nodes, that is, $u = v$.

As mobile smart terminals accelerate people's information exchange and the evolution of their social relationships, analyzing the model of connection between mobile nodes can reflect the social relations and interaction rules among different nodes. For example, the interaction model between friends may be different to strangers.

Definition 2 The total time for the mobile node u to establish a connection in the period and the total number of connections are denoted as T_u^K and N_u^K, respectively. The connection time and the number of connections between nodes u and v are denoted as $T_{u,v}^K$ and $N_{u,v}^K$, then the interactive quality feature $Q(u,v)$ of nodes u and v can be expressed as:

$$
Q(u,v) = \sqrt{\sum_{k \in \{\text{req},\text{res}\}} \left(\frac{T_{u,v}^k}{T_u^k} \cdot \frac{N_{u,v}^k}{N_u^k} \right)}
\tag{2}
$$

where $k \in \{\text{req}, \text{res}\}$ represents the request and response record.

We can divide the sensing area into areas of different radius according to the different types of services perceived by the mobile terminal. There may be a deviation in the final stop position of the mobile node entering the same area multiple times. Therefore, by clustering the staying positions in the trajectory of the node, the staying positions of the same area are divided into the same cluster. In this way, the trace of the mobile node can be expressed as a time sequence reaching different areas.

Definition 3 The trajectory information of mobile node u in the time period is expressed as $L = \{U(q_i, c_i, p_i, \gamma)\}$, where q_i, c_i are the time sets when the node arrives and leaves the region respectively, p_i is position information of the sensing area of the ith track information, and γ is the time threshold, which is used to control the time interval between different nodes reaching the target area. Then, the location feature $P(u,v)$ of nodes u and v are expressed as:

$$
P(u,v) = \frac{\sum_{i=1}^{n} B\left(L_u^i, L_v^i\right)}{T}
\tag{3}
$$

In the above formula, T is the time period, $B(L_u^i, L_v^i)$ is a similarity function between mobile nodes u and v in position p_i, which reflects the duration of the encounter between different nodes at the same location by the result which can be calculated by Eq. (4). Among them,

n is the total number of trajectory information in the T time period, and γ is the time threshold used to control the time interval between different nodes reaching the target area.

$$B\left(L_u^i, L_v^i\right) = \max\left\{q_u^i, q_v^i\right\} - \min\left\{c_u^i, c_v^i\right\} \\ s.t.\ \left|q_u^i - q_v^i\right| \leq \gamma \tag{4}$$

In the process of information transmission of nodes, the evaluation of the quality of connections established between nodes indicates the degree of stability of the information transmitted from the requesting connector to the receiver. Therefore, establishing the connection between the two parties to the stable evaluation of information transmission will change the social relationship between each other, while the trust quality factor reflects the property that the social relationship dynamically changes with the change of node connection stability.

Definition 4 Assume that the evaluation of mobile node u for v in the last n connections is recorded as $R(u, v) = \{t_{u,v}^1, t_{u,v}^2, \ldots, t_{u,v}^n\}$, $0 \leq t_{u,v}^i \leq 1, i \in [1, n]$, where the elements are arranged according to the historical interaction time, n is the historical interaction record threshold. The quality of trust characteristics between nodes can be expressed as

$$T(u, v) = \begin{cases} \sum\limits_{i=1}^{n} \dfrac{t_{u,v}^i \cdot \sigma(i)}{n}, & n \neq 0 \\ 0, & n = 0 \end{cases} \tag{5}$$

In the formula above, $\sigma(i)$ is the attenuation function used to weight the interaction feedback evaluation that occurs at different times. Note that we give a higher weight to the latest interaction records evaluation. The attenuation function $\sigma(i)$ is calculated as:

$$\sigma(i) = \begin{cases} 1, & i = n \\ \sigma(i-1) = \sigma(i) - 1/n, & 1 \leq i \leq n \end{cases} \tag{6}$$

In calculating the social relations between nodes u and v, we should considering the transitivity of social relations; in addition to directly calculating the social relations between u and v, u can indirectly obtain the social relations values about v from other nodes. As shown in Fig. 1, nodes A and D are indirectly connected, and the social relations among them can be transmitted through other peers in the path. Therefore, we can use the feedback aggregation process which calculates the social relationship values of different information feedback nodes to the target node according to the transitivity between social relations. Due to different relationship information feedbacks having different number of hops from the source node, the reliability of the feedback information is different, and so, a simple arithmetic average calculation cannot be adopted. This paper uses the aggregation algorithm [25, 26] to calculate the social relation feedback feature between different mobile nodes.

Definition 5 Suppose the node that receives the information and feedback set as $\{b_1, b_2, \ldots, b_n\}$ and $M(b_i, v)$ represents the social relationship value between the ith information feedback and the mobile node v. Then, u and v $(u, v \in N)$ social relation feedback feature is:

$$S(u, v) = \begin{cases} \dfrac{\sum\limits_{i=1}^{n} (w(b_i) \cdot M(b_i, V))}{\sum\limits_{i=1}^{n} w(b_i)}, & n \neq 0 \\ 0, & n = 0 \end{cases} \tag{7}$$

In the above formula, n is the number of relationship information feedback nodes, and $S(u, v) = 0$ and $w(b_i)$ are

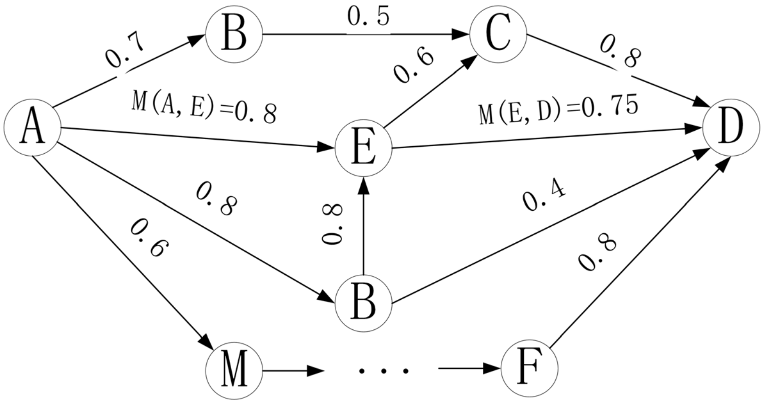


Fig. 1 Transitivity of social relations

the feedback weighting functions when there are no feedback nodes providing information in the opportunistic social network.

$$w(b_i) = \begin{cases} \prod_{i=0}^{l-1} M(a_i, a_{\text{next}}), & l > 1 \\ 1, & l = 1 \end{cases} \tag{8}$$

Among them, $M(a_i, a_{\text{next}})$ represents the social relationship value between the node a_i and its next node in the social relation transfer path from the source node u to the destination node v. And l represents the distance between the information feedback node and the source node.

4.2 Decision feature weight distribution

In the process of quantification of social relations, the size of weight reflects the status of each attribute index in the quantification of social relations decision-making, which directly affects the quality of service of the subsequent node information delivery. Therefore, an important precondition for solving the quantitative problem of social relations is designed—a reasonable and effective weight distribution method.

Rough set theory is a tool to deal with the uncertainty of knowledge, and the information entropy [26] is often used to describe the knowledge uncertainty.

Definition 6 The system uncertainty can be expressed as entropy [26] $E(X^*)$, which is

$$E(X^*) \ = -\sum_{i=1}^{n} P(A_i)\ \log_2^{P(A_i)} \tag{9}$$

where X^* is the partition of X on domain U, $X^* = U/X = \{A_1, A_2, \ldots, A_n\}$.

Definition 7 Let Y be another kind of equivalence relation on domain U, $Y^* = \{B_1, B_2, \ldots B_m\}$, then X^* is known, the conditional entropy of Y^* is:

$$E(Y^*|X^*) = \ - \ \sum_{i=1}^{n} P(A_i) \sum_{j=1}^{m} P\left(B_j|A_i\right)\ \log_2^{P\left(B_j|A_i\right)} \tag{10}$$

Definition 8 The amount of mutual information of* knowledge *reflects the amount of information that Y gets from X and can be expressed as

$$I(X^*; Y^*) \ = E(Y^*) - \ E(Y^*|X^*) \ = \ E \ (X^*) - H(X^*|Y^*) \tag{11}$$

4.3 Node social features relationship evaluation algorithm

The quantitative model of social relations in the process of information transmission of opportunistic network nodes is based on the analysis of social characteristics of nodes and calculate decision feature that affects the change of node relationships. The decision feature and the entropy theory are combined to determine the weight distribution of different decision feature. Finally, for the social relationship between mobile nodes to make a reasonable quantification, the following is given the overall realization of this model process.

Algorithm 1 Node Social Features Relationship Evaluation Algorithm (NSFRE).

Input: characteristic information of node N

STEPS:

1. First of all, input the characteristic information of the node, including the location information, connection information, interaction information, feedback information, time information, and other features, and then select the nodes that contain the relevant features in turn, and remove the nodes with less features.

2. Calculate the characteristic attribute of mobile node according to Eqs. (2)–(8).

3. There are n sample objects, each of which has m feature vectors due to a total of m decision features. Then some sample objects can be expressed in matrix as:

$$A = \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{bmatrix}$$

4. We establishing a fuzzy similarity matrix [26] between objects and object $R = (\lambda_{ij})_{n \times n}$. The method is as follows:

$$\lambda_{ij} = \sum_{k=1}^{m} \left(a_{ki} \wedge a_{kj}\right) / \sum_{k=1}^{m} \left(a_{ki} \vee a_{kj}\right) \tag{12}$$

5. We find its transitive closure matrix by fuzzy similarity matrix, that is

$$t(R) = R^{2^k} \leftarrow \cdots \leftarrow R^4 \leftarrow R^2 R^{2^k} = R^{2^{\frac{k}{2}}} \circ R^{2^{\frac{k}{2}}} \tag{13}$$

We can classify by fuzzy similarity matrix. Similar classes on similar relations can be merged into equivalence classes about their transitive closures. Mergers corresponding to high-threshold equivalence classes can directly obtain equivalence classes corresponding to low thresholds, so the principle of merging is: If $\lambda_{ij} = \delta$, the equivalence class $[a_i]_{t(R)}$ is merged with $[a_j]_{t(R)}$, where $[a_i]_{t(R)}$ represents the equivalence class containing the element $a_i \in U$ in the transitive closure relation $t(R)$, and δ is the threshold. In this way, we can choose the threshold δ from large to small and realize the classification of different needs.

6. Sort λ_{ij} from large to small as the basis for selecting threshold δ.

7. Select the maximum value δ_1, and take a_i and $a_j$satisfying $\lambda_{ij} = \delta_1$ as a class. If $\lambda_{ij} = 1$, then a_i and a_j satisfying $\lambda_{ij} = \delta_1$ at this time are exactly the elements in the same equivalence class in the rough set.

8. Taking the second largest value δ_2 in λ_{ij}, directly find the element pair (a_i, a_j) whose similarity is equal to δ_2 from $(\lambda_{ij})_{nxn}$, and correspondingly $[a_i]_{t(R)}$ and $[a_j]_{t(R)}$ merge.

9. Repeat step (7) until the selected value is less than the predetermined threshold δ_0.

10. The last merge will be undone and form the final classification $C_i(i = 1, 2, \ldots, \zeta)$.

We classify the domain U by sorting λ_{ij}, the classification results are recorded as $C_i(i = 1, 2, \ldots, \zeta)$; ζ is the classification number. Second, after deleting each attribute from all attributes in turn, repeat steps 4–9 to determine the number of categories within the same threshold range, denoted as C_j, and the like, examining the impact of each attribute on the classification and storing the result into the decision feature classification knowledge base.

11. Calculate the amount of mutual information $C_{i,\ j}$ of nodes that have been selected as feature factors of screening condition within the same threshold range by C_i, C_j, and Eqs. (9)–(11), and calculate the trustworthiness of nodes under different characteristic attributes by the following formula:

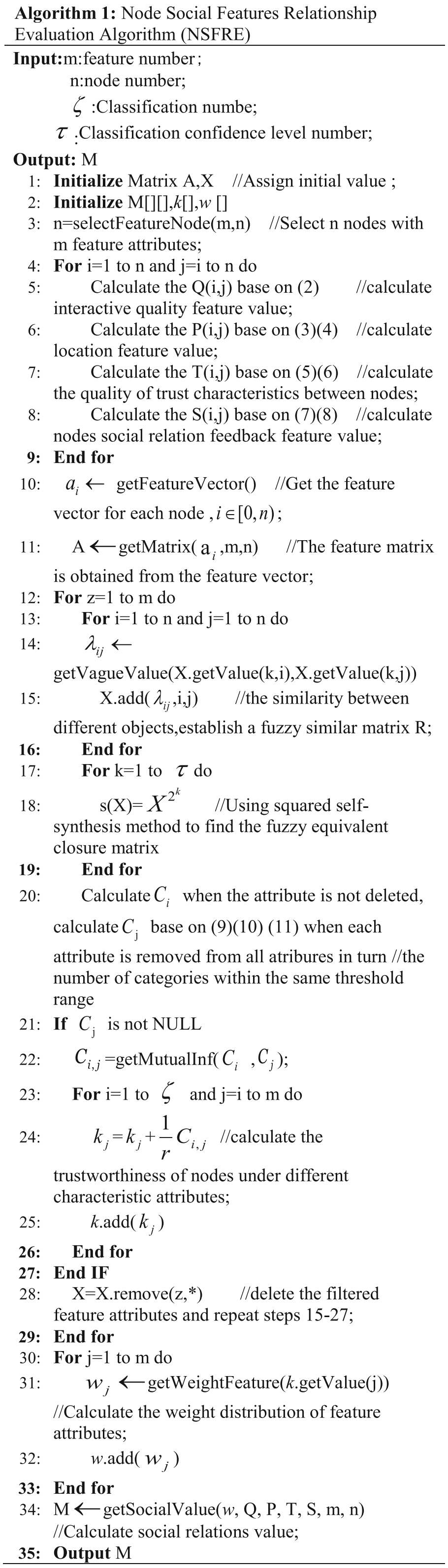
$$\theta_j = \sum \frac{1}{\gamma} \left\{ C_{i,j} | i, j \in [1, \zeta] \right\} \tag{14}$$

12. Calculate the weight of each characteristic attribute according to the value of the trustworthiness of the characteristic attribute. The weight distribution formula of the decision feature is as follows:

$$w_j = \frac{\theta_j}{\sum_{j=1}^{n} \theta_j}, (j = 1, 2, \cdots, m) \tag{15}$$

13. According to Eq. (1) to calculate the mobile node social relations quantitative value V, and finally output social relations value.

14. Output social relations value, the end.



Algorithm 1: Node Social Features Relationship Evaluation Algorithm (NSFRE)

```
Input:m:feature number;
       n:node number;
       $\zeta$ :Classification numbe;
      $\tau$ :Classification confidence level number;
Output: M
 1: Initialize Matrix A,X    //Assign initial value ;
 2: Initialize M[][],$k$[],$w$ []
 3: n=selectFeatureNode(m,n)    //Select n nodes with m feature attributes;
 4: For i=1 to n and j=i to n do
 5:        Calculate the Q(i,j) base on (2)       //calculate interactive quality feature value;
 6:        Calculate the P(i,j) base on (3)(4)    //calculate location feature value;
 7:        Calculate the T(i,j) base on (5)(6)    //calculate the quality of trust characteristics between nodes;
 8:        Calculate the S(i,j) base on (7)(8)    //calculate nodes social relation feedback feature value;
 9: End for
10:   $a_i \leftarrow$ getFeatureVector()    //Get the feature vector for each node , $i \in [0, n)$;
11:    A $\longleftarrow$getMatrix( $a_i$ ,m,n)     //The feature matrix is obtained from the feature vector;
12: For z=1 to m do
13:     For i=1 to n and j=1 to n do
14:      $\lambda_{ij} \leftarrow$ getVagueValue(X.getValue(k,i),X.getValue(k,j))
15:         X.add( $\lambda_{ij}$ ,i,j)       //the similarity between different objects,establish a fuzzy similar matrix R;
16:     End for
17:     For k=1 to  $\tau$ do
18:         s(X)= $X^{2^k}$       //Using squared self-synthesis method to find the fuzzy equivalent closure matrix
19:     End for
20:     Calculate $C_i$  when the attribute is not deleted, calculate $C_{\text{j}}$  base on (9)(10) (11) when each attribute is removed from all atribures in turn //the number of categories within the same threshold range
21: If  $C_{\text{j}}$  is not NULL
22:    $C_{i,j}$ =getMutualInf( $C_i$  ,$C_j$ );
23:    For i=1 to  $\zeta$  and j=i to m do
24:         $k_j = k_j + \frac{1}{r} C_{i,j}$  //calculate the trustworthiness of nodes under different characteristic attributes;
25:         $k$.add( $k_j$ )
26:    End for
27: End IF
28:    X=X.remove(z,*)       //delete the filtered feature attributes and repeat steps 15-27;
29: End for
30: For j=1 to m do
31:       $w_j \longleftarrow$getWeightFeature($k$.getValue(j))
      //Calculate the weight distribution of feature attributes;
32:       $w$.add( $w_j$ )
33: End for
34: M $\longleftarrow$getSocialValue($w$, Q, P, T, S, m, n)
    //Calculate social relations value;
35: Output M
```

5 Experiment analysis

In this paper, The One Simulator is used to simulate the proposed algorithm, and some opportunistic network classical routing algorithms are compared. The performance of the NSFRE algorithm is evaluated from the aspects of transmission success rate, routing overhead, and transmission delay.

5.1 Simulation tools and scenes

In the experiment, the Stanford University Topology was used as a simulation scenario. The simulation scenario is set as follows (Fig. 2):

The data we use in the simulation scenario is a real data set of Stanford University. We design different numbers of pedestrians, cars, and electric tracks to simulate the effect of the number of nodes, simulation time, and node caching on simulation results. Among them, the experimental parameters are set as follows: We choose Stanford University real map area is 1070 m × 810 m. The simulation time is from 1 to 12 h. The simulation node is set to 120–900, and the node cache is set to 5–40 M. The speeds of pedestrians, cars, and trams are 5 km/h, 100 km/h, and 60 km/h, respectively, the channel bandwidth is 250 kb/s, and the bandwidth of high-speed transmission interfaces is 10 m/s. In addition, the node's mobility model is Shortest Path Map Based Movement [1]. The node's transmission mode is a social model. The default number of nodes is 300. Each node's

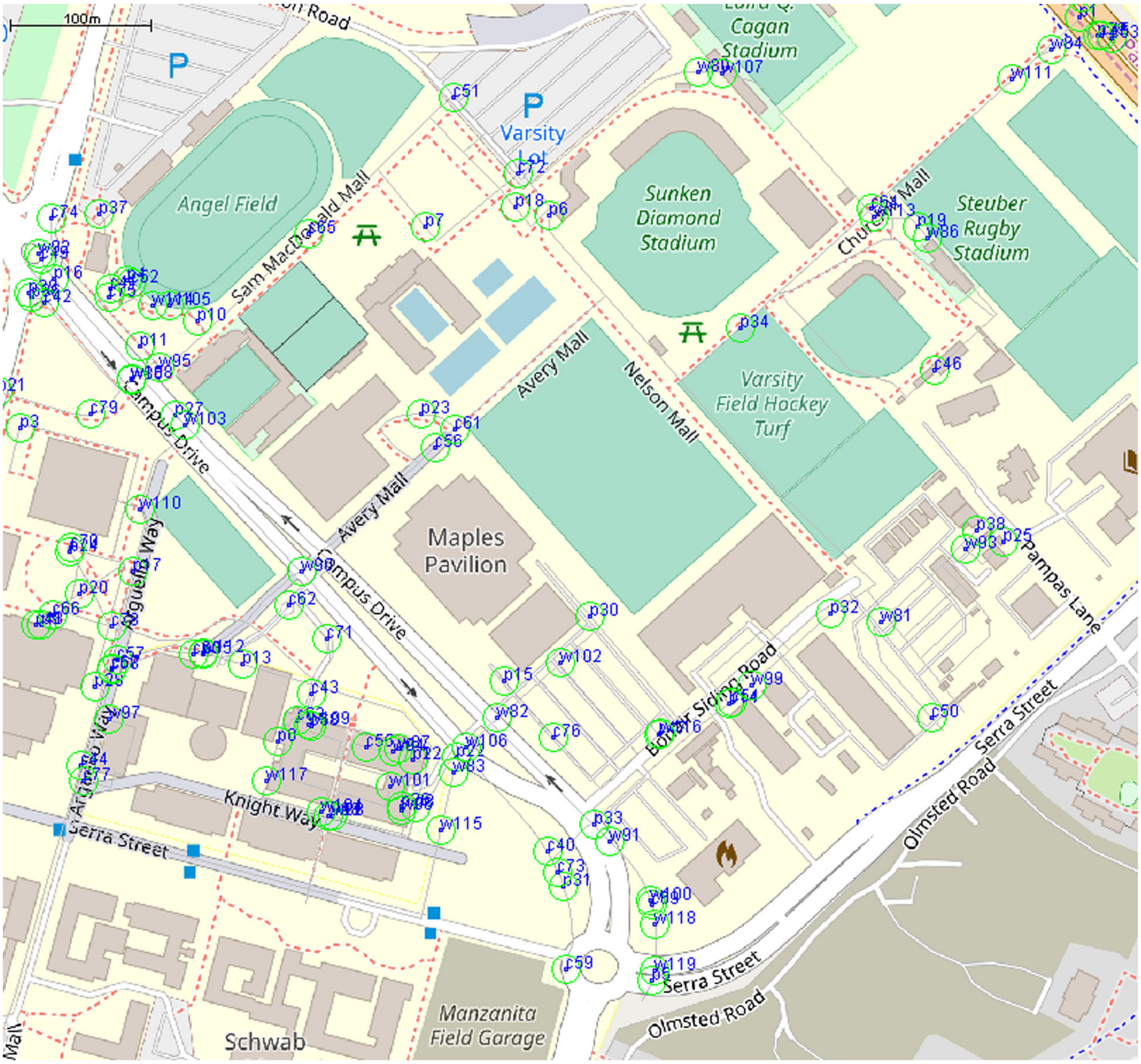


Fig. 2 Simulation scene diagram

cache is 8M. The maximum transmission area of each node is 10 m^2. The frequency ranges from 25 to 35 HZ and the packet type is a random array. The topology of the simulation experiment is shown in Fig. 3.

In the model simulation experiment proposed in this paper, we simulate the real data set in The One, in which the wired connection node is the trusted node selected by the source node. It can be seen that the trust node is filtered by the model. With the increase of time, the transmission connection established between the nodes is reduced, which means that the number of cooperative nodes is reduced by the model selection, and the nodes that can cooperate are changed from high density to low density. The screening of trusted nodes is more and more accurate. It not only avoids the insecurity of data flooding, but also improves the transmission efficiency of the network, reduces the probability of network congestion, and enhances the robustness of the network structure.

5.2 Experimental results

The experiment mainly analyzes the algorithm's performance in transmission success rate, transmission delay, and routing cost by adjusting parameters. The model is mainly evaluated from two aspects: (1) effectiveness analysis: experiments were conducted to compare the difference

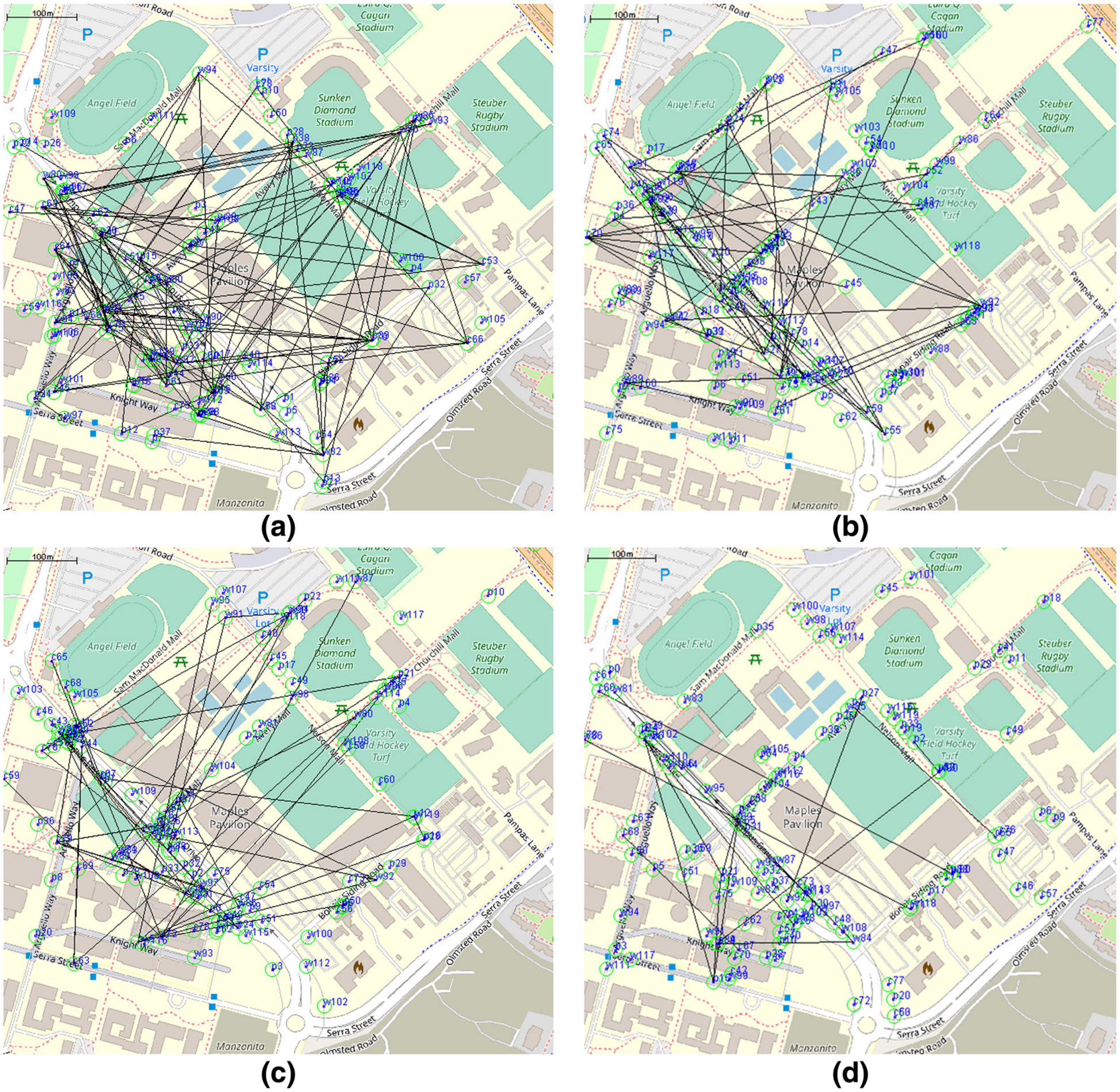


Fig. 3 Simulation experiment topology

between the model and other existing models in optimizing the network structure and increasing the success rate of information transmission and (2) adaptability analysis: through the process of dynamic changes in various uncertainties, the trusted nodes are selected to send data, which reduces the amount of information on the network and improves information transmission capabilities. Because our information transmission concept is still the classic way of probabilistic routing. The difference is that we form a quantitative probability value based on the social characteristics of the node, and the nodes are filtered by this value. Furthermore, we have made great improvements to the method of filtering nodes of the Prophet algorithm. Therefore, by comparing with other classical transmission methods applied in opportunistic social networks, we demonstrate the advantages and importance of node social characteristics and probabilistic transmission. As a reference, the algorithm of this paper is compared with Epidemic [27], Spray and wait [28], First Contact [29], and MaxProp [30] routing algorithm to analyze and compare the characteristics of each algorithm. It is proved that the proposed algorithm is more effective.

Figure 4 shows the relationship between the transmission success rate and simulation time. We can see that the algorithm's transmission success rate gradually increases as the simulation time increases. First Contact and Epidemic routing algorithm have the lowest transmission success rates, only 0.2 and 0.18, respectively. The reason is that Epidemic algorithm uses flooding to transmit information in nodes. Each node has too many message information. When the node cache is small, it is easy to cause a large amount of information data to be lost. However, First Contact is based on the forwarding strategy. It does not duplicate the information in the node and only transmits one copy of the message in the network. Therefore, the transmission success rate is low. Spray and wait routing algorithm improves information transmission success rate while reducing the number of information copies. However, the node of the MaxProp algorithm maintains a packet queue according to the transmission cost to the target node and determines the replication order according to the priority of the packet, which not only avoids network congestion, but also avoids waste of resources by blindly copying message information between nodes. Therefore, the transmission success rate of the spray and wait routing algorithm is lower than that of the MaxProp algorithm. The NSFRE algorithm has the highest transmission success rate, reaching 0.68. Precisely, it uses a combination of features to calculate the social network trust relationship to select trusted nodes, which reduces network congestion and information replication and improves the efficiency of the selected node and the reachability of the destination node. It also effectively improves the algorithm's transmission success rate.

Figure 5 shows the relationship between routing overhead and time. From the figure, we can see that the routing overhead of the NSFRE algorithm is not affected by the time. In the early stage, like the MaxProp routing algorithm, the routing overhead has a sharp downward trend, and the cost of the later routing is maintained between 12 and 26. The reason is that, as time increases, the number of nodes filtered by the algorithm will gradually decrease. Because the selection of nodes for

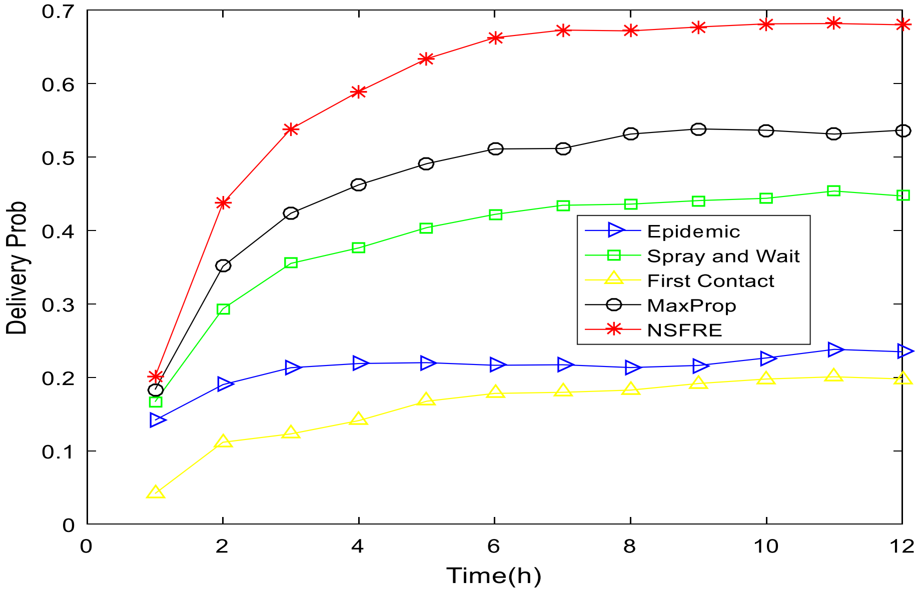


Fig. 4 The relationship between transmission success rate and simulation time

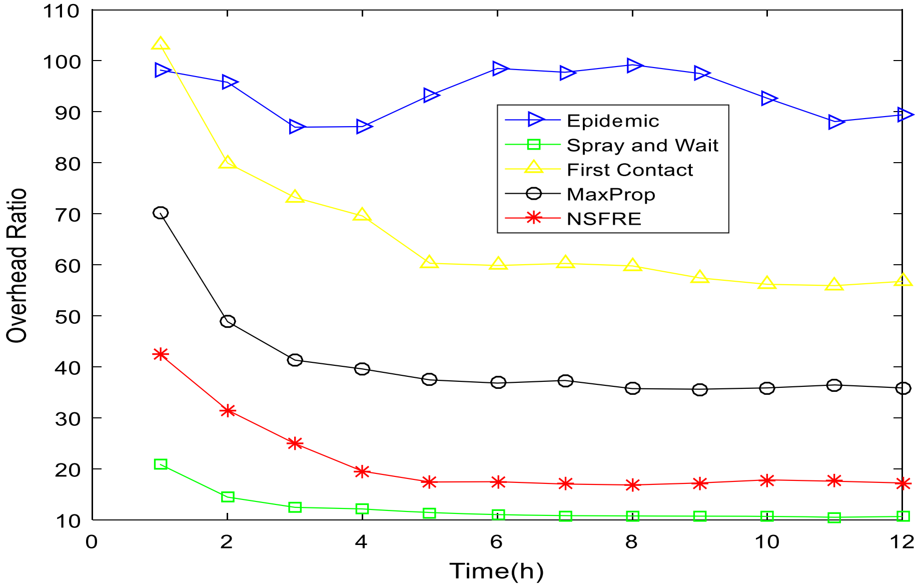


Fig. 5 The relationship between routing overhead and time

information transmission will be more accurate and the number of nodes sharing information transmission tends to be stable, the routing overhead can be kept stable. Spray and wait routing algorithm is similar to the algorithm in this paper. Compared with other algorithms, the routing overhead is relatively small, and as the time increases, the routing overhead decreases. This is because the Spray and wait routing algorithm reduces the amount of data transmission in the network and has good scalability. However, the route overhead of the Epidemic routing algorithm is relatively large, and the fluctuation is relatively large. This is because the algorithm maximizes the success rate of packet transmission. Each node carries a copied packet, and a large number of packet copies exist in the network. The network performance is degraded and the network structure is unstable.

Figure 6 shows the relationship between the average transmission. From the figure, the MaxProp algorithm determines the packet priority based on the transmission

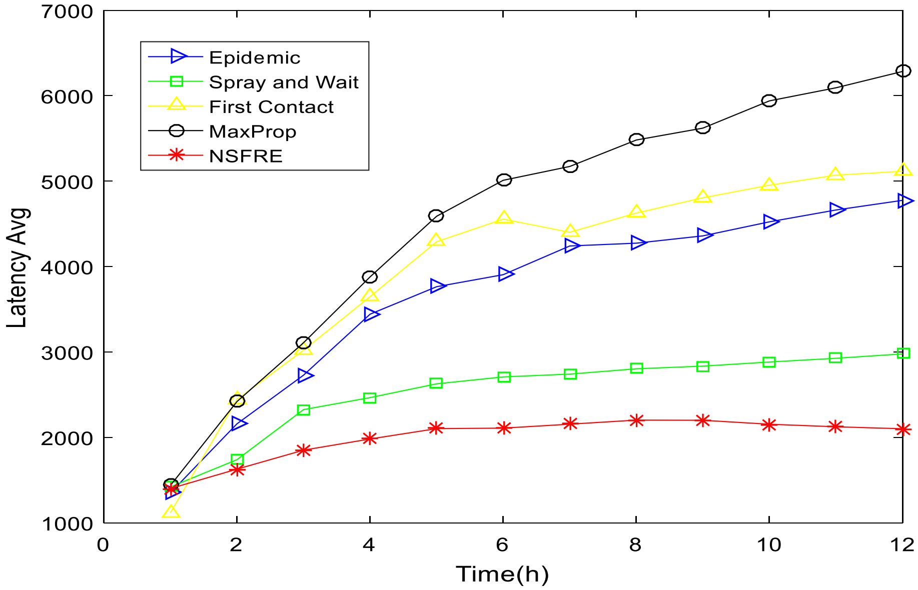


Fig. 6 The relationship between average transmission delay and time

cost, and the transmission cost is an estimate of the probability that the packet is successfully transmitted to the target node, which is estimated by the incremental averaging method. Because each transmission message must be calculated, the algorithm has the highest transmission delay. Because the First Contact algorithm only sends a copy of the message to the node that met for the first time, and the probability of the first node meeting with the destination node is very small, the algorithm has a higher propagation delay. The Epidemic routing algorithm uses flooding to deliver packets. As time increases, more and more packets are transmitted on the network. The resources in the network are consumed in large amounts. It is easy to cause network congestion, resulting in a high transmission delay. The average delay of the Epidemic algorithm reaches 4000. The NSFRE algorithm's delay is similar to the Spray and wait routing algorithm. This is because the algorithm uses resources to filter the nodes according to different factors, causing delays. However, as the NSFRE algorithm increases with time, the transmission delay tends to be flat, which proves that the algorithm has good stability and the information transmission delay does not increase exponentially with time.

Figure 7 shows the relationship between the transmission success rate and the number of nodes. We can see that the transmission success rates of the First Contact routing algorithm and the Epidemic routing algorithm are the lowest. With the increase in the number of nodes, the success rate of these two algorithms does not change much, only 0.24 and 0.18, respectively. The reason is that the Epidemic routing algorithm uses the form of flooding to carry out the information transmission to the nodes, causing a great deal of information data loss. The First Contact routing algorithm only transmits one replication message. With the increase of the number of nodes, the transmission success rate is stable at 0.24. The Spray and wait routing algorithm copies a certain amount of information for each message. With the increase of the number of nodes, the number of nodes receiving the copied message information increases, and the probability of encountering the node and the target node also increases, so the transmission success rate has increased, reaching 0.8. The transmission success rate of the MaxProp routing algorithm and the NSFRE algorithm is high, exceeding 50%. The MaxProp routing algorithm sends packets based on the calculated routing overhead, which improves the transmission and reception of valid information. Therefore, the transmission success rate reaches 0.51–0.82. The NSFRE algorithm has the highest transmission success rate, reaching 0.53–0.93. This is because the NSFRE algorithm takes into account the reachability of the destination node to calculate and filter the transmission of trusted mobile nodes. With the increase of nodes, the nodes are more closely connected and the reachability between nodes is higher, which effectively improves the transmission success rate of the algorithm.

Figure 8 shows the routing overhead and the number of nodes. In the figure, the routing overhead of the NSFRE

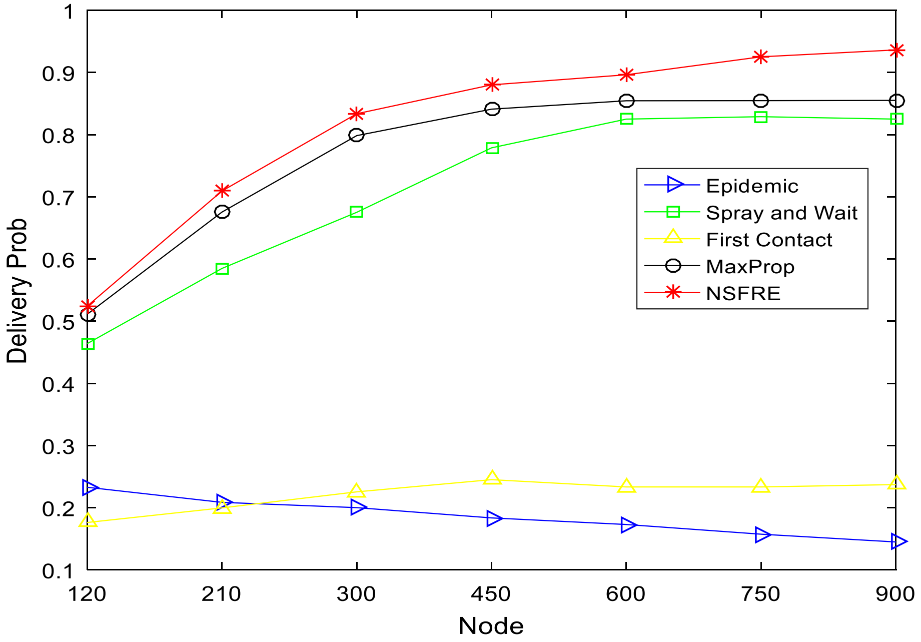


Fig. 7 The relationship between transmission success rate and number of nodes

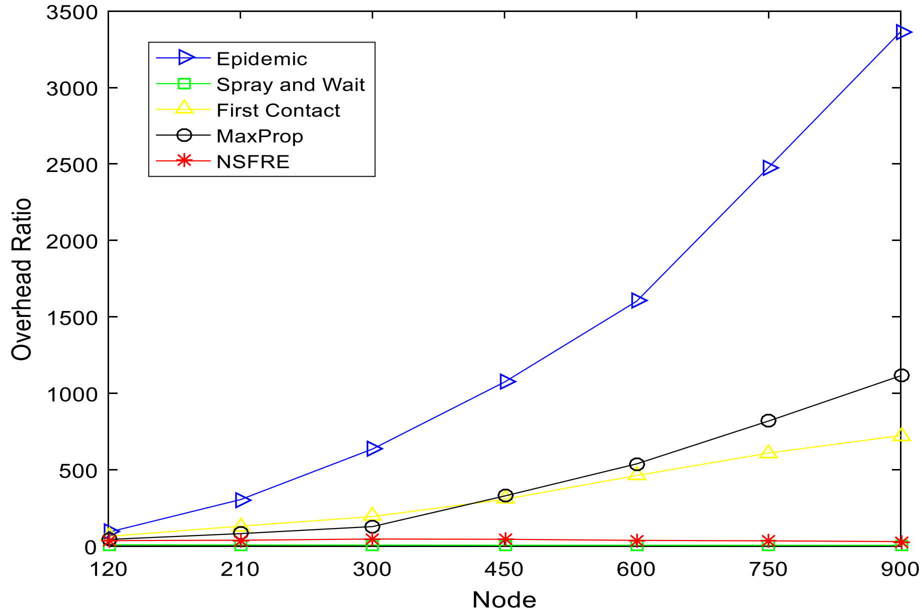


Fig. 8 The routing overhead and the number of nodes

and Spray and Wait algorithms is basically independent of node density. For the NSFRE algorithm, as the number of nodes increases, the connections between different communities will become closer. The energy consumption of the nodes filtered by the algorithm will not affect the information transmission overhead of the entire network, and the algorithm has good stability. For the other three algorithms, the routing overhead increases sharply when the node density reaches a certain level, which will lead to a significant increase in node energy consumption, thus limiting the scope of application of these routing algorithms. Among them, based on the flooding method of the Epidemic routing algorithm, as the number of nodes increases, the routing overhead approaches exponential growth, indicating that the Epidemic algorithm consumes network resources as the number of nodes increases, so the routing overhead of this algorithm is the largest. For First Contact algorithm and MaxProp algorithm, as the number of nodes increases, the number of hops the node takes to reach the destination node also increases. Therefore, the increase in the number of nodes increases the routing overhead of the network, but the increase is not significant.

Figure 9 shows the relationship between the average transmission delay and the number of nodes. We can see that the transmission delay of the NSFRE algorithm is low, and the trend of the relationship between the transmission delay of the algorithm and the node density is obviously different from other algorithms. As with the propagation delay trend of the MaxProp algorithm, it does not increase significantly with the increase in the density of nodes but decrease. This is because the NSFRE algorithm is not limited to a single social relationship. As the number of nodes increases, the number of social relationships existing between nodes increases. Therefore, the increase of social relations will make the calculation of trust values between nodes more accurate. Consequently, as the number of nodes increases, the transmission delay tends to decrease. Among them, the First Contact routing algorithm has the highest transmission delay. Because the number of nodes increases, the number of nodes from the source node to the target node increases. The Spray and wait routing algorithm has a low transmission delay. The initial phase is similar to the NSFRE. However, as the number of nodes increases, the reachability of randomly dispersed packets to the destination node decreases, and the transmission delay increases. The main reason why the NSFRE algorithm is superior to other algorithms is that the nodes that transmit the message information are filtered, which can reduce some nodes with low cooperation, reduce the network overhead, improve the reachability of the destination node, and reduce the transmission delay.

Figure 10 shows the relationship between the transmission success rate and the node cache. Node cache has different effects on the transmission success rate of each routing algorithm, and the effect is relatively significant when the node cache is relatively small. From the trend point of view, increasing the node cache can improve the transmission success rate. As can be seen in the figure, the NSFRE routing algorithm has the highest transmission success rate. When the number of nodes is set to 210 and the node cache reaches 8, the transmission success rate is gradually stable. The trend of the

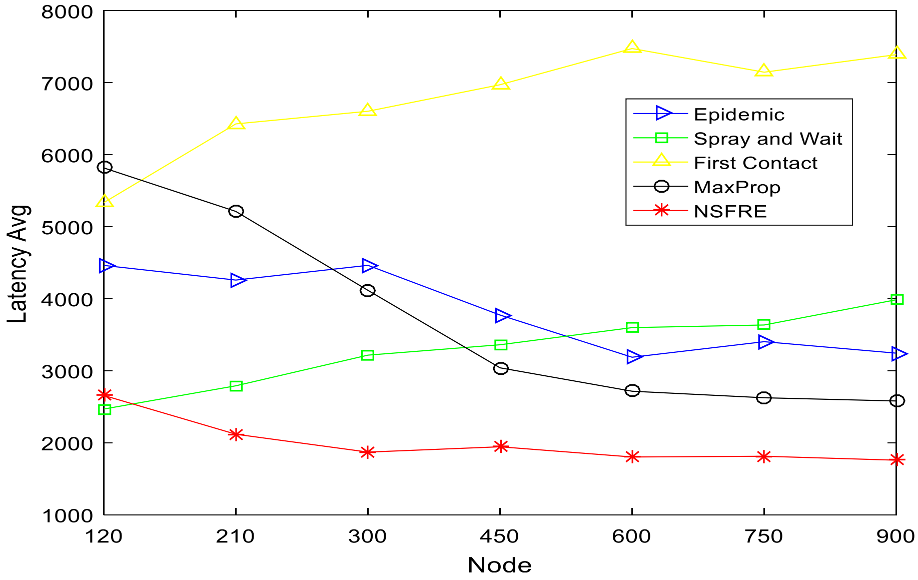


Fig. 9 The relationship between the average transmission delay and the number of nodes

algorithm curve is the same as Spray and wait and MaxProp routing algorithm. This is because the feature considered by the nodes selected by the NSFRE algorithm is the characteristic information between the nodes and the nodes themselves, regardless of the node cache size. When the node cache reaches a certain value, it will not have a great impact on the transmission success rate. The Epidemic algorithm uses a large amount of cache for the flooded message information. As node caching increases, more information can be delivered. Therefore, as the node cache increases, the transmission success rate increases. The First Contact algorithm's transmission success rate is still small, and the node cache is stable at 15. Because only the information is passed to the node that meets the first time, the encounter node has randomness, which will reduce the reachability of the destination node. Therefore, the increase in node cache does not significantly increase the transmission success rate.

Figure 11 shows the relationship between routing overhead and node caching. In the figure, the node cache has a large impact on the routing overhead of the

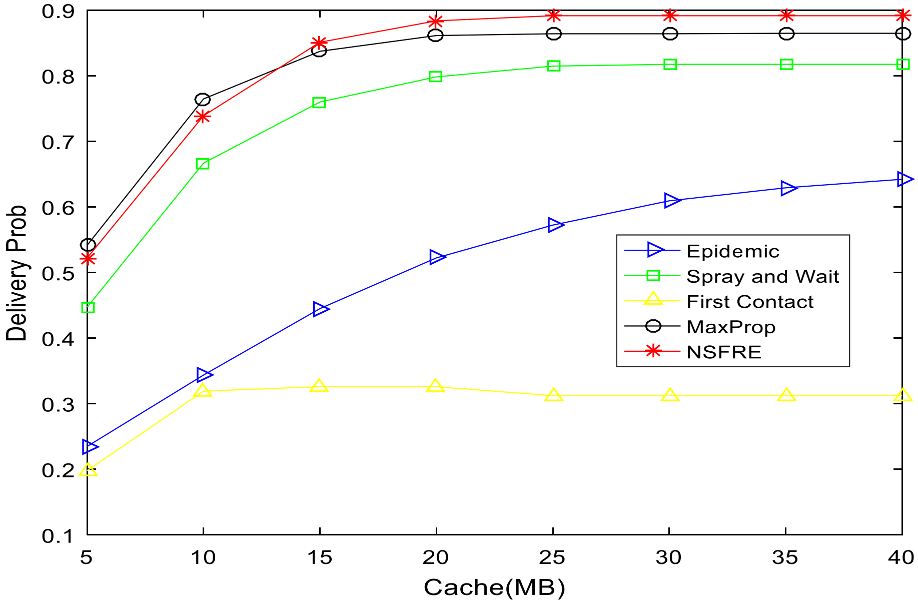


Fig. 10 The relationship between transmission success rate and the node cache

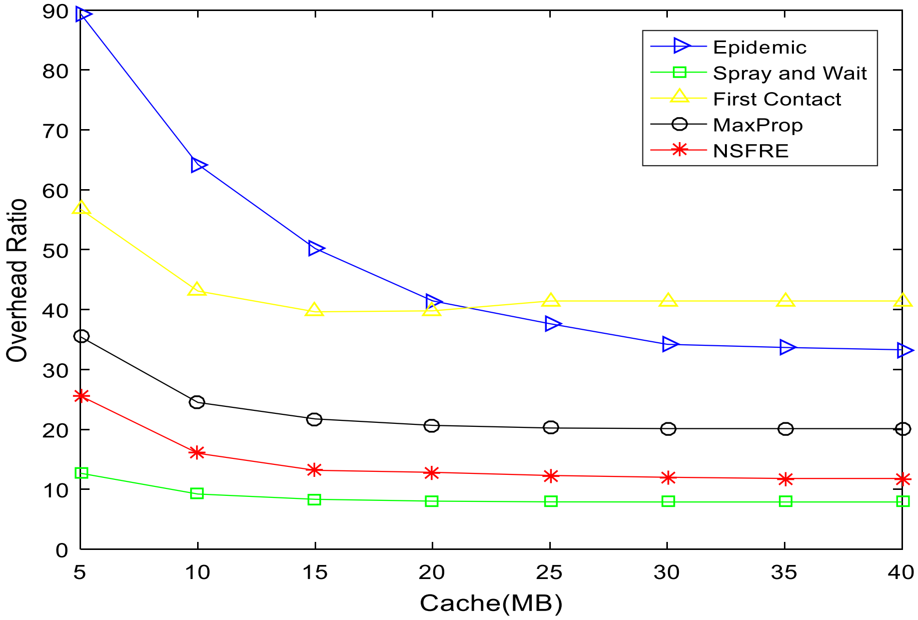


Fig. 11 The relationship between routing overhead and node caching

epidemic routing algorithm. The impact on each routing algorithm is relatively significant when the node cache is relatively small. From a trend point of view, increasing the node cache can reduce the routing overhead. When the node cache is small, the epidemic algorithm has the highest routing overhead. With the increase of node caches, the information that can be carried by a node increases, which makes it difficult to cause network congestion and information loss. Therefore, the routing overhead is significantly reduced. Because the First Contact algorithm only transmits one copy of the message at a time in the network, the routing overhead increases with the node cache and decreases significantly when there is less node cache. After that, the routing overhead does not change much, and it ranges between 40 and 57. As can be seen from the figure, the routing overhead of the NSFRE algorithm is larger when the node cache is smaller. As with the Spray and wait routing algorithm, as the node cache is increased, the routing overhead is gradually reduced, and finally, it becomes stable. The NSFRE algorithm's routing overhead is stable in the 11–13 range. This is because both algorithms are copying information to a part of the node, so the trends of the two algorithms are the same. However, because the NSFRE algorithm filters out some cooperating nodes to send message information according to the feature information, there is a certain consumption in the screening process, and the expenditure in the process of information transmission is small. Therefore, the routing overhead of the NSFRE algorithm is much less than that of the Spray and wait routing algorithm.

Figure 12 shows the relationship between the average transmission delay and the node cache. In the figure, in addition to the MaxProp algorithm, increasing the cache of other nodes to a certain extent will increase the transmission delay, especially when the cache is relatively small. It can be seen in the figure that the first contact algorithm is still the highest transmission delay. When the node cache is small, the propagation delay of the NSFRE algorithm and the Spray and wait routing algorithm is relatively small. With the increase of node cache, the trend of the curve tends to be stable, and the transmission delay of the NSFRE algorithm is still minimal. This is because the nodes selected to transmit information are filtered out according to the network structure and node characteristics, and the access to the destination node is more accessible than the random filtering of nodes by the spray and wait routing algorithm. Therefore, in this process, the transmission delay is smaller. The Epidemic algorithm has a smaller transmission delay when the node cache is small. With the increase of node cache, the amount of information in the network increases dramatically, which makes the transmission delay increase exponentially. Therefore, there is still not much advantage under other algorithms.

The relationship between the three indicators and the time, the node cache, and the number of nodes can be concluded. The NSFRE algorithm is superior to other algorithms in terms of transmission success rate, transmission delay, and energy consumption. And it has less advantage in routing overhead than the Spray and wait routing algorithm. In the real environment, NSFRE

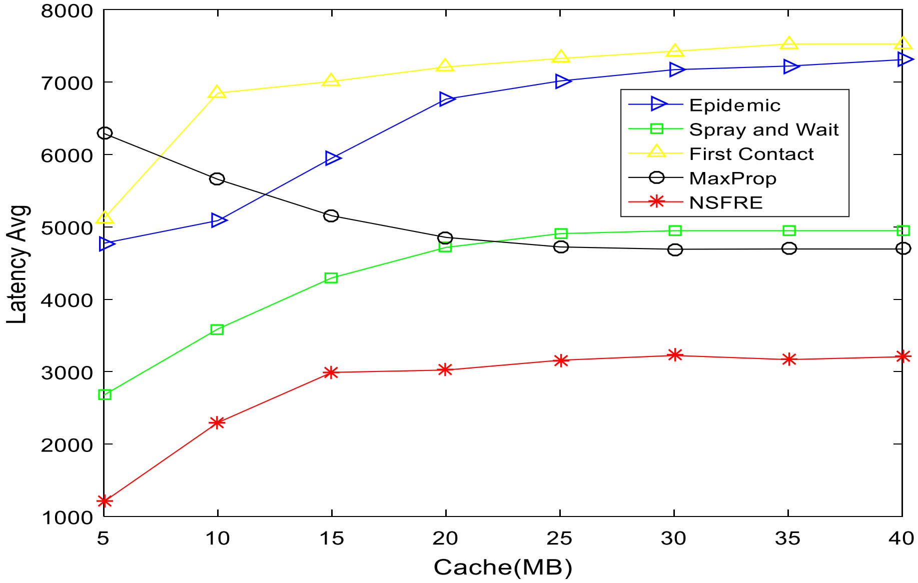


Fig. 12 The relationship between the average transmission delay and the node cache

algorithm is superior to other algorithms for long time information transmission.

6 Conclusions

In this paper, a decision-making method of opportunistic social network routing based on trust mechanism social relations is proposed, NSFRE. The algorithm calculates the trust degree of the forwarding node according to the forwarding path of trust message and message delay time collected by the destination node. Firstly, it analyzes the social elements of the impact of mobile node social relations and the characteristics of nodes and combine the features of network structure to extract location characteristics, interaction quality characteristics, trust quality characteristics, and social relationship feedback characteristics as the decision feature of social relations quantified. Secondly, through the introduction of rough set and information entropy theory, the different attributes of the mobile node are deeply studied, and the law of social attribute changes is excavated to dynamically and adaptively allocate the weights of different attributes. Finally, experimental verification of the proposed social relationship quantification model to screen trusted nodes as the next-hop nodes for data transmission has good results. The model allows data to be transmitted along the trusted cooperative nodes in the network, and at the same time, the uncooperative nodes gradually active participate in the data forwarding in the network. In the process of information transmission, the model has better dynamic adaptability, higher transmission success rate, and lower average transmission delay, so that the negative effect of uncooperative nodes on the network is minimized and the overall performance of the network is improved.

In the future, we will conduct in-depth research on the node's trusted interactions based on the characteristics of nodes through machine learning. According to the selected nodes build trust routing tables, the timestamp mechanism is used to prevent the routing table from being tampered with by malicious nodes in the feedback process, thereby further improving the stability and security of information transmission.

Abbreviation

NSFRE: Node Social Features Relationship Evaluation

Funding

This work was supported in The National Natural Science Foundation of China (61672540); Hunan Provincial Natural Science Foundation of China (2018JJ3299, 2018JJ3682); China Postdoctoral Science Foundation funded project (2017M612586); Foundation of Central South University (185684); Major Program of National Natural Science Foundation of China (71633006). Also, this work was supported partially by "Mobile Health" Ministry of Education-China Mobile Joint Laboratory.

Availability of data and materials

Data sharing not applicable to this article as no datasets were generated or analyzed during the current study.

About the authors

GengHua YU received the Master Degree Candidate in School of Computer science and engineering at Central South University, Chang-sha, Hunan, P.R.China, in 2017. She is the 2017 outstanding graduate of Nanchang University. Her research interests include wireless communications and networking, big data research, wireless network, data mining.

Zhigang Chen received the BE, the MS and PhD from Central South University in China in 1984, 1987 and 1998. He is currently a Professor, Supervisor of PhD and chair in School of Computer Science and Engineering, Central South University. He is also director and advanced member of China Computer Federation (CCF), and member of pervasive computing committee of CCF. His research interests cover the general area of cluster computing, parallel and distributed system, computer security, wireless networks.

Jia WU received the Ph.D. Degrees in software engineering Central South University, Chang-sha, Hunan, P.R.China, in 2016. He is engineer in "Mobile Health" Ministry of Education-China Mobile Joint Laboratory and assocate professor in School of information science and engineering Central South University. Since 2010, he has been Algorithm engineer in IBM company in Seoul, Republic of Korea and in Shang-hai, P.R.China. He is a senior member of CCF(China Computer Federation), a member of IEEE and ACM. His research interests include wireless communications and networking, wireless network, big data research, mobile health in network communication.

Jian Wu Currently he is a student in School of Computer Science and Engineering of Central South University, China. His research interest is network computing.

Authors' contributions

GY, ZC, and JW conceived the idea of the paper. GY, ZC, JW, and JW drafted the manuscript and collected the data, wrote the code, and performed the analysis. ZC contributed reagents/materials/analysis tools. GY wrote and revised the paper. All authors read and approved the final manuscript.

Competing interests

The authors declare that they have no competing interests.

Publisher's Note

Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Received: 22 November 2018 Accepted: 5 March 2019
Published online: 02 April 2019

References

1. W.U. Jia, Z. Chen, Z. Ming, Effective information transmission based on socialization nodes in opportunistic networks. Comput. Netw. **129**, 297–305 (2017).
2. W. Jia, Z. Chen, Z. Ming, Information cache management and data transmission algorithm in opportunistic social networks. Wirel. Netw. (8), 1–12 (2018).
3. H. Zhou, V.C.M. Leung, C. Zhu, S. Xu, J. Fan, Predicting temporal social contact patterns for data forwarding in opportunistic mobile networks. IEEE Trans. Veh. Technol. PP (99), 1–1 (2017).
4. H. Zhou, H. Wang, X. Chen, X. Li, S. Xu, *Data offloading techniques through vehicular ad hoc networks: a survey, IEEE Access* (2018).
5. W. Jia, Z. Ming, Z. Chen, Small data: effective data based on big communication research in social networks. Wirel. Pers. Commun. **99**(3), 1391–1404 (2018).
6. C. Huang, Y. Chen, S. Xu, H. Zhou, The vehicular social network (VSN)-based sharing of downloaded geo data using the credit-based clustering scheme. IEEE Access (2018).
7. G. Yu, Z. Chen, J. Wu, J. Wu, A transmission prediction neighbor mechanism based on a mixed probability model in an opportunistic complex social network. Symmetry (2018).
8. R. Ju, G. Hui, C. Xu, Y. Zhang, Serving at the edge: a scalable IoT architecture based on transparent computing. IEEE Netw. **31**(5), 96–105 (2017).
9. X.J. Wu, J.K. Xiao, J.B. Shao, *Trust-based protocol for securing routing in opportunistic networks* (2015), pp. 434–439.
10. S. Bansal, M. Baker, Observation-based cooperation enforcement in ad hoc network. Comput. Sci. (2003).
11. L. Li, X. Zhong, Q. Yang, in *IEEE International Conference on Communication Systems*. A secure routing based on social trust in opportunistic networks (2016).
12. L. Chen, J. Zhuo, A trust management scheme based on behavior feedback for opportunistic networks. China Commun. **12**(4), 117–129 (2015).
13. E.K. Wang, Y. Li, Y. Ye, S.M. Yiu, L.C.K. Hui, A dynamic trust framework for opportunistic mobile social networks. IEEE Trans. Netw. Serv Manag. PP (99), 1–1 (2017).
14. G.K. Wong, Y. Chang, X. Jia, W.Y. Hui, in *International conference on computing*. Performance evaluation of social relation opportunistic routing in dynamic social networks (2015).
15. N. Palaghias, N. Loumis, S. Georgoulas, K. Moessner, in *IEEE International Conference on Communications*. Quantifying trust relationships based on real-world social interactions (2016).
16. R. Atat, L. Liu, J. Wu, G. Li, C. Ye, Y. Yi, *Big data meet cyber-physical systems: a panoramic survey* (2018).
17. H. Chen, L. Wei, Z. Wang, X. Feng, On achieving asynchronous energy-efficient neighbor discovery for mobile sensor networks. IEEE Trans. Emerg. Top. Comput. **6**(4), 553–565 (2018).
18. C. Zhu, V.C.M. Leung, J.J.P.C. Rodrigues, L. Shu, L. Wang, H. Zhou, *Social sensor cloud: framework, greenness, issues, and outlook. IEEE Network* (2018).
19. H. Chen, W. Lou, Z. Wang, Q. Wang, A secure credit-based incentive mechanism for message forwarding in noncooperative DTNs. IEEE Trans. Veh. Technol..
20. J. Wu, G. Song, H. Huang, W. Liu, X. Yong, Information and communications technologies for sustainable development goals: state-of-the-art, needs and perspectives. IEEE Commun. Surv. Tutorials (99), 1–1 (2018).
21. J. Wu, G. Song, L. Jie, D. Zeng, Big data meet green challenges: big data toward green applications. IEEE Syst. J. **10**(3), 888–900 (2016).
22. X. Peng, R. Ju, S. Liang, D. Zhang, L. Jie, Y. Zhang, BOAT: a block-streaming app execution scheme for lightweight IoT devices. IEEE Internet Things J. (99), 1–1 (2018).
23. W. Tang, K. Zhang, R. Ju, Y. Zhang, X.S. Shen, Flexible and efficient authenticated key agreement scheme for BANs based on physiological features. IEEE Trans. Mob. Comput. (99), 1–1 (2018).
24. R. Ju, Y. Zhang, R. Deng, Z. Ning, X. Shen, Joint channel access and sampling rate control in energy harvesting cognitive radio sensor networks. IEEE Trans. Emerg. Topics Comput. (99), 1–1 (2016).
25. Z. Chen, Y. Song, X. Huang, L. Yang, in *International Conference on Cyber-Enabled Distributed Computing & Knowledge Discovery*. An adaptive feedback timing control algorithm of delay-constrained data aggregation in wireless sensor networks (2009).
26. J. Yi, M. Yin, Y. Zhang, X. Zhao, in *IEEE international conference on computational intelligence and applications*. A novel recommender algorithm using information entropy and secondary-clustering (2017), pp. 128–132.
27. A.Y. Lokhov, M. Mézard, H. Ohta, L. Zdeborová, Inferring the origin of an epidemic with a dynamic message-passing algorithm. Phys. Rev. E Stat. Nonlinear Soft Matter Phys. **90**(1), 012801 (2014).
28. G. Wang, B. Wang, Y. Gao, in *International conference on communications & mobile computing*. Dynamic spray and wait routing algorithm with quality of node in delay tolerant network (2010).
29. S. Jain, K. Fall, R. Patra, in *SIGCOMM'04: Proceedings of the 2004 Conference on applications, Technologies, Architectures and Protocols for Computer Communications*. Routing in a delay tolerant network (ACM, New York, 2004), pp. 145–158.
30. J. Burgess, B. Gallagher, D. Jensen, B.N. Levine, in *IEEE International Conference on Computer Communications*. MaxProp: routing for vehicle-based disruption-tolerant networks (2006).