

A Strong-Relationship Relay Delivery Strategy for Mobile Social Networks Based on Markov Behavior Prediction

Chong Guo¹, Jiayi Zhang¹, Maojie Xue^{2*}, Jinming Zhu³

¹*School of Digital Economy and Management, Suzhou Vocational and Technical University, Suzhou, China*

²*School of Computer Science and Technology, Nanjing Tech University, Nanjing, China*

³*Chairman's Office, Jiangsu Zhengjin Accounting Co., Ltd., Suzhou, China*

**Corresponding Author. Email: 455379513@qq.com*

Abstract. Mobile social networks (MSNs) deliver messages through opportunistic store-carry-forward communication, where relay selection is strongly affected by intermittent encounters, limited node resources, and socially selfish behavior. In inter-community transmission, nodes with formal social ties are not always reliable relays, because some of them may show pseudo-affinity and refuse forwarding during actual encounters. To address this problem, this paper develops SRRN, a strong-relationship relay delivery strategy based on Markov behavior prediction. SRRN first identifies second-degree and third-degree strong-relationship nodes through the Open Strong Relationship First (OSRF) algorithm, and then predicts node activity states using a first-order Markov chain. A dynamic kinship trust model is further built from historical feedback and Beta distribution-based interaction evaluation to distinguish reliable relays from pseudo-affinity nodes. Relay candidates are selected according to their kinship indicators with the destination node. Experiments on the ONE platform using MIT Reality Trace show that SRRN achieves a higher delivery success ratio and lower transmission delay than SimBet and Bubble Rap, while keeping the average hop count within an acceptable range.

Keywords: Mobile social network, kinship index, kinship trust model, behavior prediction, pseudo-affinity node

1. Introduction

Mobile social networks (MSNs) support store-carry-forward communication through opportunistic encounters and have been extended to the Internet of Things, edge social networks, and vehicular social networks. In MSNs, inter-node communication is strongly affected by social attributes, including social relationships, interest similarity, encounter frequency, and trust [1-3]. However, under constrained energy, buffer, and computing resources, rational nodes may exhibit social selfishness by selectively forwarding messages to preserve their resources [4]. Recent studies have explored graph neural networks and reinforcement learning to extract social features for routing decisions, but such learning-based methods usually require sufficient trajectory data and incur additional computational costs, limiting deployment on resource-constrained mobile terminals [5].

In contrast, heuristic routing based on intrinsic social attributes, such as the kinship index, can be combined with lightweight probabilistic models to balance energy consumption and delivery performance [6-7].

Another challenge is pseudo-affinity, i.e., nodes maintain formal social ties but show limited forwarding willingness during physical encounters. Routing algorithms that rely only on static relationship strength may fail to evaluate actual forwarding intentions, leading to unreliable relay selection and increased delay under selfish or malicious behavior [8-9]. Hence, a strong formal tie should not be treated as sufficient evidence for relay selection. In this paper, SRRN uses strong social relations only as the initial screening condition rather than the only routing criterion. The OSRF procedure first locates second-degree and third-degree nodes that connect different communities. Their recent encounter patterns are then modeled by a first-order Markov chain to estimate short-term activity. For the remaining candidate relays, historical reports and direct interaction outcomes are further converted into a kinship trust value, so that pseudo-affinity nodes can be removed before message forwarding. In this way, SRRN keeps the routing process lightweight while making relay selection depend on both social position and observed forwarding behavior.

2. Methodology

2.1. Network model

The network follows a two-dimensional access point framework, and node relationships remain relatively stable per observation period. This study considers a social network with hierarchical classification based on the kinship index. As shown in Figure 1, nodes are connected through relationships such as family ties, friendship, and collegial relations. Nodes sharing the same relationship type are grouped into the same community, while some nodes may belong to multiple communities. A node shared by three communities is defined as a third-degree strong-relationship node, and a node shared by two communities as a second-degree strong-relationship node. Since this study focuses on inter-community transmission, nodes with second-degree or higher relationship strength are collectively regarded as strong-relationship nodes.

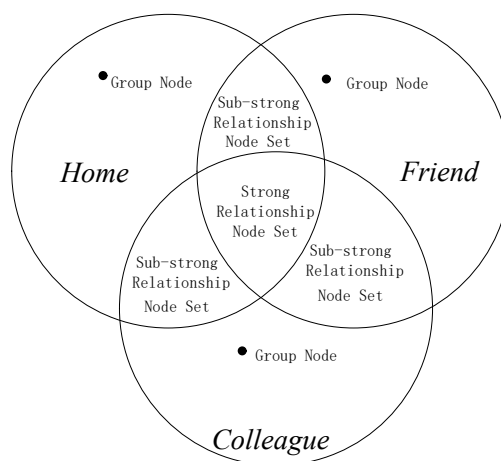


Figure 1. Social relationship model and node distribution

Each node is assigned a label B to indicate its social group. Single-relationship nodes are labeled as H, F, or C; second-degree strong-relationship nodes are labeled as HF, HC, or FC; and third-

degree strong-relationship nodes are labeled as HFC. For simplicity, the MSN is modeled as a graph with n nodes, where each node maintains a kinship array to record its relationship strength with neighboring nodes. The single kinship index $ksi_{m,i}^x = (ksi_{i,m}^x)$ denotes the kinship strength between nodes m and i under relationship type x , where x represents family ties, friendship, or collegial relations.

The comprehensive kinship index KSI_m^x is obtained by weighted aggregation of different single kinship indices. A valid kinship relationship is established when the corresponding ksi_m^x exceeds the predefined threshold Yx , with Y_H , Y_F , and Y_C denoting the thresholds for family ties, friendship, and collegial relations, respectively.

The model further considers both social selfishness and pseudo-affinity. Socially selfish nodes may selectively forward messages according to social ties, resource conditions, and their own utility, while pseudo-affinity nodes may refuse forwarding despite having formal social ties. Therefore, nodes are assumed to monitor neighbor forwarding behavior to support subsequent trust evaluation and relay selection.

2.2. Strong-relationship node identification and activity prediction

This study develops the Open Strong Relationship First (OSRF) algorithm to identify strong-relationship nodes by adapting the link-state concept of OSPF. In OSRF, kinship relationships between nodes are treated as shareable social link information. Each node periodically sends its social group label and kinship indices to neighboring nodes, and the received information is integrated into a local multidimensional kinship matrix, as shown in Equation (1).

$$\begin{bmatrix} y & i_1 & i_2 & \dots & i_n \\ i_1 & 999 & y_1^{12} y_2^{12} y_3^{12} & \dots & y_1^{1n} y_2^{1n} y_3^{1n} \\ i_2 & y_1^{21} y_2^{21} y_3^{21} & 999 & \dots & y_1^{2n} y_2^{2n} y_3^{2n} \\ \dots & \dots & \dots & 999 & \dots \\ i_n & y_1^{n1} y_2^{n1} y_3^{n1} & y_1^{n2} y_2^{n2} y_3^{n2} & \dots & 999 \end{bmatrix} \quad (1)$$

The first row and first column denote node labels, and the remaining elements represent the kinship indices between row and column nodes. The diagonal elements are set to 9, indicating the maximum self-kinship value.

Nodes are screened according to the predefined relationship thresholds. If a node pair satisfies the H, F, and C thresholds simultaneously, it is labeled as HFC and added to the third-degree strong-relationship node set. If only two thresholds are satisfied, the node pair is labeled as HF, HC, or FC and added to the second-degree strong-relationship node set. Since the kinship matrix is symmetric, only its upper triangular part needs to be checked, which reduces the computational cost of strong-relationship node identification.

To identify active nodes given limited computing, buffer, and energy resources, this study employs a first-order Markov chain for lightweight activity prediction. During network operation, each node records its encounter frequency in each time period and estimates its activity state accordingly. According to the Markov property, the activity state of node m in period $i+1$ depends only on its state in period i :

$M(n_{i+1} = S_a | n_i = S_b, n_{i-1} = S_{c,\dots}) = M(n_{i+1} = S_a | n_i = S_b) = h_{\theta,a}$. In the above equation, n_{i+1} , n_i , n_{i-1} describe the activity states of node m in consecutive periods, S_a , S_b , S_c represent possible activity states, and $h_{b,a}$ denotes the transition probability from state S_b to state S_a , satisfying $h_{b,\alpha} \geq 0$ and $\sum_{b=1} h_{b,\alpha} = 1$.

Based on the state transition matrix, the future state probability can be iteratively updated as $r_{i+j}(a) = \sum r_{i+j-1}(b)h_{b,a}$. The value $r_{i+j}(a)$ denotes the probability that node m will be in state S_a in the $i+j$ -th period. Nodes with higher predicted activity are added to the active node set. The active strong-relationship node set is then formed by taking the intersection between the strong-relationship node set and the active node set. HFC nodes are included in the third-degree active strong-relationship set $S' = [m, n, \dots]$, while HF, HC, or FC nodes are grouped into the second-

degree active strong-relationship set $E' = \begin{bmatrix} m_1, n_1, \dots \\ m_2, n_2, \dots \\ m_3, n_3, \dots \end{bmatrix}$. This screening keeps cross-community nodes with higher predicted encounter opportunities.

2.3. Interactive evaluation layer

Active strong-relationship nodes are not necessarily reliable relays, since pseudo-affinity nodes may still refuse to forward messages during actual encounters. SRRN therefore evaluates candidate nodes through a dynamic kinship trust model that combines historical feedback with current interaction records. The basic kinship trust value T_b reflects the historical reliability of a node. For inter-community forwarding, T_b is initialized by the comprehensive kinship index, namely $T_b = KSI_m^x$. In each update cycle, T_b is adjusted according to the verification result of reported forwarding behavior: correct reporting increases the value, while incorrect reporting decreases it. The update rule is defined as follows:

$$T_b^n \begin{pmatrix} n \end{pmatrix} = \begin{cases} T_b^0(i-1) + 0.5 \times |KSI_n^x - KSI_m^x|, l = 1 \\ T_b^0(i-1) \times \frac{1}{2}, l = 0 \end{cases} \quad (2)$$

Here, $T_b^n(i)$ denotes the basic kinship trust value of node n in cycle i , while $T_b^0(i-1)$ denotes the trust value in the previous cycle. $l = 1$ indicates correct reporting, and $l = 0$ indicates incorrect reporting. $|KSI_n^x - KSI_m^x|$ represents the difference in the comprehensive kinship index between the reporting node m and the reported node n .

To evaluate current interaction reliability, neighboring relationship nodes h , f and c monitor the forwarding behavior of node m . Following the Beta distribution-based reputation model, inter-node trust is measured by the expected value of successful and unsuccessful interactions^[8-9]. The direct trust $T_{d(h,m)}$ from relationship node h to node m is defined as $T_{d(h,m)}' = \frac{\alpha_{hm}+1}{\alpha_{hm}+\beta_{mh}+2}$, where α_{hm} and β_{mh} denote the numbers of successful and unsuccessful interactions between node m and relationship node h in the previous cycle, respectively. Considering that trust may decay over time, the single kinship index is introduced as a relationship-based attenuation factor to calculate the direct kinship trust value. The direct kinship trust values for relationship nodes f and c can be obtained in the same way.

Following the MoleTrust model, the comprehensive kinship trust value is obtained by weighted integration of basic trust and direct trust [10]. For third-degree strong-relationship nodes, the trust

value is calculated by integrating three relationship nodes, as defined in Equation (3):

$$TK_m = T_{b(m)} + \frac{T_{d(h,m)}[ksi_{h,m}^{x1} - T_{h(m)}] + T_{d(f,m)}[ksi_{f,m}^{x2} - T_{f(m)}] + T_{d(c,m)}[ksi_{c,m}^{x3} - T_{c(m)}]}{T_{d(h,m)} + T_{d(f,m)} + T_{d(c,m)}} \quad (3)$$

Here, $T_{b(m)}$ is the basic kinship trust value of node m . $T_{d(h,m)}$, $T_{d(f,m)}$ and $T_{d(c,m)}$ are the direct kinship trust values from relationship nodes h , f , and c to node m , respectively. $T_{d(h,m)}$, $T_{d(f,m)}$ and $T_{d(c,m)}$, together with $ksi_{h,m}^{x1}$, $ksi_{f,m}^{x2}$, and $ksi_{c,m}^{x3}$, denote the corresponding basic trust values and single kinship indices, where $x1$, $x2$, and $x3$ represent different kinship relationship types.

For second-degree strong-relationship nodes, which are associated with only two relationship nodes, the comprehensive kinship trust value is defined in Equation (4):

$$TK_m = T_{b(m)} + \frac{T_{d(u,m)}[ksi_{u,m}^x - T_{u(m)}] + T_{d(v,m)}[ksi_{v,m}^y - T_{v(m)}]}{T_{d(u,m)} + T_{d(v,m)}} \quad (4)$$

In Equation (4), $(u, v) \in \{(h, f), (f, c), (h, c)\}$, x and y denote different kinship relationship types.

Finally, the third-degree and second-degree active strong-relationship node sets are ranked in descending order according to the comprehensive kinship trust value, and the corresponding trusted active strong-relationship node sets are obtained for subsequent candidate relay selection.

2.4. Data transmission layer

The SRRN encounter delivery strategy uses the trusted active strong-relationship node set as the relay candidate pool and integrates the replica control mechanism of BSW for inter-community forwarding. To reduce blind diffusion in cross-community scenarios, SRRN prioritizes nodes that have strong kinship relations, active states, and high comprehensive kinship trust values with the destination node. The process is shown in Figure 2.

When node m receives a message, it first checks whether the destination node D is included in its neighbor set $|E_m|$. If $D \in |E_m|$, the message is forwarded directly to D . Otherwise, node m searches the second-degree trusted active strong-relationship set E for nodes with the same relationship type as the destination node and obtains the candidate set $M = |E_m| \cap E$. If M is not empty, candidate relays are selected in descending order according to the single kinship index. If no suitable relay is found, node m further considers the third-degree trusted active strong-relationship set S . When the activation condition is satisfied, the candidate set is updated as $K = |E_m| \cap S$, and nodes whose single kinship index is not lower than that of the current node are selected as candidate relays. If no suitable relay is available, node m retains the message and waits for the next encounter.

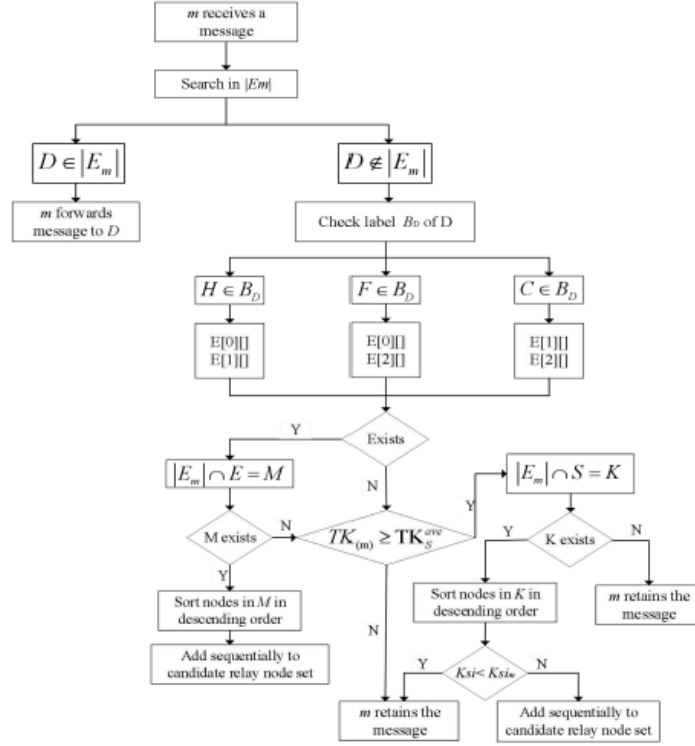


Figure 2. Flowchart of the SRRN encounter delivery strategy

2.5. Simulation and result analysis

2.5.1. Simulation settings and metrics

The simulation was conducted on the ONE platform with MIT Reality Trace as the mobility trace. A continuous 300-minute segment was extracted to represent real encounter patterns among mobile devices. Since the dataset does not contain explicit social relationship labels, the initial kinship indices were assigned according to the proposed network model. The experiment focuses on inter-community delivery, where J denotes the set of second-degree and higher strong-relationship nodes, and T/J represents the proportion of trusted active strong-relationship nodes in J . The main parameters are listed in Table 1.

Table 1. Parameter settings for ONE simulation

Parameter	Value	Parameter	Value
scene size	500m*500m	node cache	5MB
community Node	97	interface scope	10m
number of communities	3	simulation time	300min
T/J	0%~60%	mobile model	MIT Reality Trace

2.5.2. Comparative routing algorithms and evaluation metrics

SimBet and Bubble Rap are selected as baseline algorithms because they are representative social-aware routing methods in opportunistic networks. Three metrics are used for comparison: delivery

success ratio, transmission delay, and average hop count. The delivery success ratio refers to the proportion of generated messages successfully delivered to their destinations. Transmission delay measures the average delivery time of successful messages, while average hop count records the number of forwarding steps involved in each successful delivery.

2.5.3. Experimental results and analysis

Figure 3 compares the performance of SRRN, Bubble Rap, and SimBet under different T/J values. As shown in Figure 3a, the delivery success ratio of all three algorithms increases as more trusted active strong-relationship nodes become available, and SRRN shows the most evident improvement. This result indicates that combining kinship strength, predicted activity, and trust evaluation can reduce forwarding failures caused by pseudo-affinity nodes.

Figure 3b shows that transmission delay decreases with the increase of T/J . SRRN achieves lower delay than Bubble Rap and SimBet because its candidate relays are selected according to both their social position and their kinship indicators with the destination node. Compared with community- or similarity-based forwarding, this selection mechanism gives inter-community delivery clearer routing directionality.

Figure 3c reports the average hop count. SimBet has a slightly lower hop count, while SRRN remains within an acceptable range. This means that SRRN does not simply minimize the number of relays, but trades a limited increase in forwarding hops for higher delivery reliability and lower transmission delay.

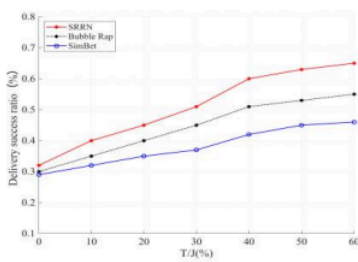


Figure 3a. Delivery success ratio under different T/J values

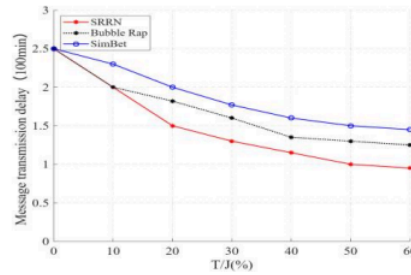


Figure 3b. Message transmission delay under different T/J values

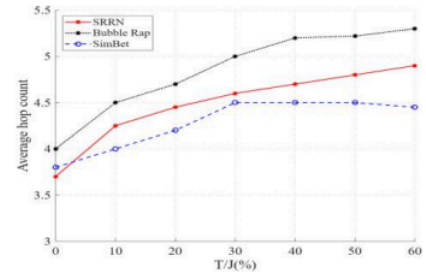


Figure 3c. Average hop count under different T/J values

Figure 3. Performance comparison of different routing algorithms

3. Conclusion

SRRN is designed for inter-community forwarding in mobile social networks, where strong formal ties do not always indicate reliable forwarding behavior. The strategy first uses OSRF to identify second-degree and third-degree strong-relationship nodes, then applies a first-order Markov chain to estimate their activity states, and finally evaluates kinship trust through historical feedback and direct interaction records. By combining relationship strength, activity prediction, and trust evaluation, SRRN can filter pseudo-affinity nodes before relay selection. Simulation results show that SRRN achieves a higher delivery success ratio and lower transmission delay than Bubble Rap and SimBet, while keeping the average hop count within an acceptable range.

The current study still has several limitations. The experiments mainly focus on delivery success ratio, transmission delay, and average hop count, while network overhead, energy consumption, node density, and buffer capacity have not been fully examined. Future work will further test SRRN

under more diverse network settings and explore incentive mechanisms for highly selfish nodes. In addition, edge-assisted behavior prediction and trust evaluation may be introduced to improve routing efficiency in larger-scale MSN scenarios.

References

- [1] Conti, M., & Giordano, S. (2014). Mobile ad hoc networking: Milestones, challenges, and new research directions. *IEEE Communications Magazine*, 52(1), 85–96.
- [2] Mtibaa, A., May, M., & Ammar, M. (2012). Social forwarding in mobile opportunistic networks: A case of PeopleRank. In M. T. Thai & P. M. Pardalos (Eds.), *Handbook of Optimization in Complex Networks: Communication and Social Networks* (pp. 387–425). Springer.
- [3] Li, F., Zhao, L. N., Zhang, C., Gao, Z. M., & Wang, Y. (2014). Routing with multi-level cross-community social groups in mobile opportunistic networks. *Personal and Ubiquitous Computing*, 18(2), 385–396.
- [4] Pan, H., Kuang, X., Li, V. O. K., et al. (2009). Selfishness, altruism and message spreading in mobile social networks. In *IEEE INFOCOM Workshops*.
- [5] Jiang, W., Han, H., Zhang, Y., Wang, J., He, M., Gu, W., Mu, J., & Cheng, X. (2024). Graph neural networks for routing optimization: Challenges and opportunities. *Sustainability*, 16(21), 9239.
- [6] Meng, X., Xu, G., Guo, T., et al. (2019). A novel routing method for social delay-tolerant networks. *Tsinghua Science and Technology*, 24(1), 44–51.
- [7] Shi, Y., Zhang, F., Xu, G., Wei, G., & Yuan, Z. (2024). A message routing algorithm based on the importance of node social relationships in opportunistic mobile networks. In *Wireless Artificial Intelligent Computing Systems and Applications* (pp. 229–240). Springer.
- [8] Singh, J., Dhurandher, S. K., Woungang, I., & Chao, H. C. (2024). Context-aware trust and reputation routing protocol for opportunistic IoT networks. *Sensors*, 24(23), 7650.
- [9] Hasan, A. A., Fang, X., Latif, S., & Iqbal, A. (2025). Context-aware trust prediction for optimal routing in opportunistic IoT systems. *Sensors*, 25(12), 3672.
- [10] Massa, P., & Avesani, P. (2007). Trust-aware recommender systems. In *Proceedings of the 2007 ACM Conference on Recommender Systems* (pp. 17–24). ACM.