Message Transmission with User Grouping for Improving Transmission Efficiency and Reliability in Mobile Social Networks

Takuro Yamamoto, Takuji Tachibana,

Abstract—**Recently, due to the rapid spread of wireless devices such as cell phones, mobile social networks have attracted considerable attention. In the mobile social networks, privacy issues have to be addressed and messages have to be transmitted effectively. In this paper, in order to resolve both the issues for the mobile social networks, we propose a reliable message transmission method. In our proposed method, each user classifies other users into two groups; reliable group and unreliable group. This classification is performed based on the number of times each user is selected as a destination user by a source user. Based on this classification, all messages are forwarded to users in the reliable group. This can improve the reliability of message transmission. Moreover, this method utilizes the number of times a user encountered other users. This can decrease the number of hops for the message transmission, resulting in the efficient message transmission. We evaluate the performance of our proposed method with simulation. In numerical examples, we compare the performance of our proposed method with those of other methods. Numerical examples show that our proposed method can transmit messages reliably and effectively.**

Index Terms—**Mobile social networks, Reliability, User grouping, Message transmission, Performance evaluation**

I. Introduction

SOCIAL networks are one of the latest and most interesting revolutions in network technology. In the social networks, users with common interests can connect each other and exchange information [1]. Currently, several kinds of applications such as Facebook, Twitter, MySpace, and LinkedIn have been utilized worldwide. Moreover, due to the rapid spread of wireless devices such as cell phones, mobile social networks have attracted considerable attention recently. Mobile social networks are social networks that can be utilized in mobile environments [2], and mobile social network services have gained popularity among users nowadays [3].

In vehicle environments, [1] has considered an innovative solution for providing mobile social network services. In the solution, IMS (IP multimedia subsystem) and M2M (machine to machine capabilities) have been utilized. In [3], authors have proposed and implemented a new application called CenceMe. In this application, the presence of individuals is inferred by using a mobile phone, and the information about the inference is shared through social networking applications such as Facebook and MySpace. The implementation of this application has been discussed for the Nokia N95 mobile phone. Moreover, in [4], an opened mobile social networking system has been proposed for university students and faculties in a university campus. For the campus mobile social networks, some future applications have also been discussed.

Here, in mobile social networks, a connectivity between two mobile devices (users) can be obtained only when one device gets into the transmission range of the other device. Moreover, each user does not know the state of the whole networks and have little information about the state of the partitioned network [5]. Due to such intermittent connectivity and lack of continuous end-to-end path [6], in mobile social networks, a message routing is one of the challenging problems. Hence, a lot of methods have been studied and proposed in the literature [2], [5], [7], [8].

In addition, for future mobile social networks, privacy issues have to be addressed [9]. Some studies have considered the privacy issues of location disclosure and guidelines on protecting privacy [10], [11], [12]. For the mobile networks, the utilization of security key management has been proposed to restrict user's access [12]. However, the key distribution and management are not easy in mobile social network environments [13]. Therefore, a reliable message transmission should be performed for the mobile social networks without the security key management.

In this paper, we propose a reliable message transmission in mobile social networks. In our proposed method, a source user classifies other users into two groups; reliable group and unreliable group. This classification is performed by the source user based on the number of times each user is selected as a destination user. Based on this classification, all messages are forwarded to users in the reliable group. This can enhance the reliability of message transmission. Moreover, this method utilizes the number of times an user encountered other users. This can decrease the number of hops for the message transmission, resulting in the efficient message transmission. The performance of our proposed method is evaluated with simulation. In numerical examples, we compare the performance of our proposed method with that of other methods.

The organization of this paper is as follows. Section II describes some routing methods for mobile social networks as related work. In Sect. III, we explain our proposed reliable message transmission in detail, and Sect. IV denotes numerical results. Finally, conclusions and future work are denoted in Sect. V.

II. Related Work

In this section, we explain two message routing methods for mobile social networks as related work.

T. Yamamoto is with Graduate School of Engineering, University of Fukui, Fukui 910-8507, Japan. Email: takuro-y@network.fuis.u-fukui.ac.jp
T. Tachibana is with Graduate School of Engineering, University of Fukui, Fukui 910-8507, Japan. Email:takuji-t@u-fukui.ac.jp

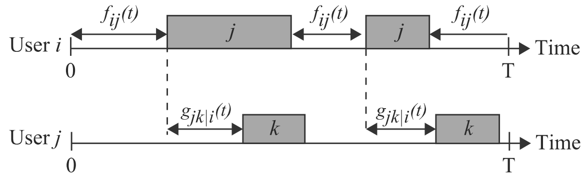


Fig. 1. Encounter history among users i, j, and k.

A. Epidemic Routing

In order to resolve intermittent connectivity, [7] has proposed a flooding-based routing called *Epidemic routing*. In the epidemic routing, a message is copied in each user before the user transmits it to other users. Then, the message is transmitted from the user to all users that are within a transmission range. Therefore, a destination user can receive its corresponding message with a high probability. On the other hand, in this routing, the number of hops becomes large and many users tend to have the same message. As a result, this routing is inefficient due to redundant message transmission.

B. Friendship Routing

In [2], authors have proposed a routing method called *Friendship routing* in order to transmit a message from a source user to a destination user effectively. In this method, the source user utilizes the information about the frequency of encountering other users.

Now, $f_{ij}(t)$ denotes the remaining time at time t until user i encounters user j. Moreover, let $g_{jk|i}(t)$ be the remaining time at time t until user j encounters user k after user i encounters the user j. Figure 1 shows an example of $f_{ij}(t)$ and $g_{jk|i}(t)$. With $f_{ij}(t)$ and $g_{jk|i}(t)$, two indexes SPM_{ij} and $CSPM_{jk|i}$ are derived from the following equations:

$$SPM_{ij} = \frac{\int_{t=0}^{T} f_{ij}(t)}{T}, \quad (1)$$

$$CSPM_{jk|i} = \frac{\int_{t=0}^{T} g_{jk|i}(t)}{T}. \quad (2)$$

From these indexes, the user i determines whether it forwards a message to the user j when the user k is its destination user. By using this routing method, messages can be transmitted to those destination users effectively.

III. Proposed Method

In this section, we propose a reliable message transmission in mobile social networks. Our proposed method does not utilize security key management due to its complexity. Our proposed method consists of three parts: user grouping, encounter counting, and transmission algorithm. In the following subsections, we explain each part in detail.

A. User grouping

In our proposed method, each source user classifies other users into two groups; reliable group and unreliable group. Throughout this paper, we assume that a source user has strong relationship with a destination user and that such a destination user is reliable for the source user. Therefore, in this case, the reliability between two users can be considered for the message transmission with the above classification.

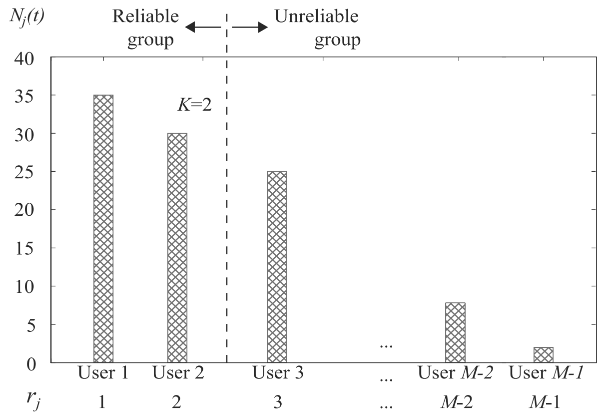


Fig. 2. Proposed rule of user grouping.

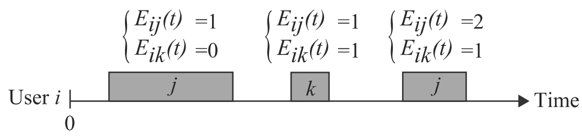


Fig. 3. Number of encounters among users i, j, and k.

Now, let M be the number of users in a mobile social network and let $N(t)$ be the number of messages that have been generated before time t by user i ($i = 1, \cdots, M$). Moreover, let $N_j(t)$ denote the number of messages whose destination user is j. In this case, $\sum_{j=1}^{M} N_j(t) = N(t)$ is satisfied.

Here, the user i ranks $M-1$ users based on the number $N_j(t)$ of times the user j is selected as the destination user. Let $r_j(t)$ ($j = 1, \cdots, M, j \neq i$) be rank of user j at time t for source user i. The rank $r_j(t)$ of the user j and the rank $r_k(t)$ of the user k are determined from the following inequalities:

$$\begin{cases} r_j(t) < r_k(t), & \text{if } N_j(t) < N_k(t), \\ r_j(t) > r_k(t), & \text{if } N_j(t) > N_k(t), \\ r_j(t) = r_k(t), & \text{otherwise.} \end{cases} \quad (3)$$

The user i arranges $M-1$ users in descending order of the rank, and Fig. 2 shows an example of the user's ranking.

With the ranks, the user i classifies those users into the reliable group and the unreliable group according to the following rule:

Rule: A user whose rank is smaller than K ($K = 1, \cdots, M-1$) is included in the reliable group. Otherwise, the user is included in the unreliable group.

Figure 2 also shows how users are grouped according to this rule. In Fig. 2, K is set to 2. Note that the user's ranking changes dynamically.

B. Encounter counting

In our proposed method, an user estimates the frequency of encountering each user. This estimation is utilized to avoid redundant message transmission. As shown in Sect. II-B, the friendship routing utilizes two indexes called SPM and CSPM to estimate the frequency of encounter. These indexes

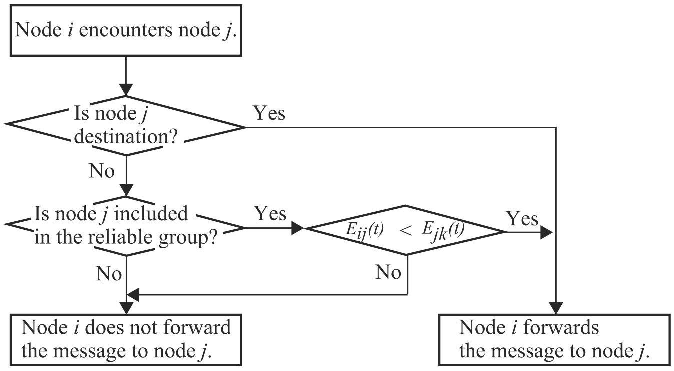


Fig. 4. Proposed message transmission algorithm.

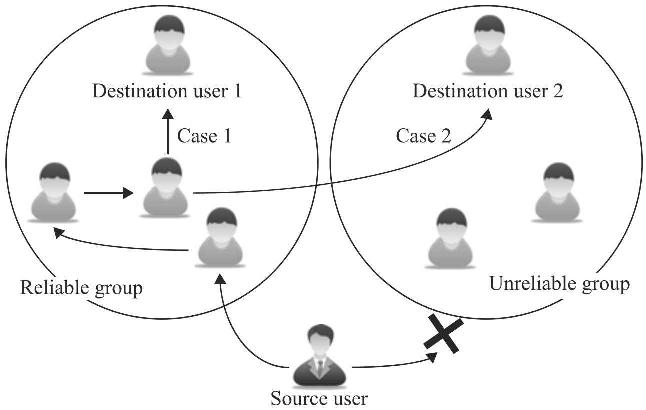


Fig. 5. An example of message transmission with our proposed transmission algorithm.

are derived based on the remaining time until the next encounter. However, this estimation is somewhat difficult because the user has to store the remaining time for each user.

In our proposed method, on the other hand, each user counts the number of encounters for other users. Here, let $E_{ij}(t)$ denote the number of encounters between user i and j until time t. Figure 3 shows an example among users i, j, and k. Moreover, as is the case with [2], an user exchanges the information about the number of encounters with other users.

C. Transmission algorithm

Finally, we explain our proposed message transmission algorithm.

In our proposed method, in order to keep the reliability, a source user forwards the information about reliable group along with its corresponding message to an intermediate user. The intermediate user also forwards both the message and the information to the next user. When the destination user is k, user i determines whether the message is forwarded to user j according to the following algorithm (see Fig. 4).

1) If user j is the destination user k, user i forwards the message to the user j. Otherwise, go to step 2.
2) The user i checks whether the user j is included in the reliable group or not. If the user j is included in the reliable group, go to step 3. Otherwise, go to step 4.
3) The user i compares $E_{ik}(t)$ with $E_{jk}(t)$. When $E_{jk}(t)$ is larger than $E_{ik}(t)$, the user i forwards the message to the user j. Otherwise, go to step 4.
4) The user i does not forward the message to the user j.

Figure 5 shows an example of our proposed transmission algorithm. As shown in this figure, a message is forwarded to users in the reliable group except for the destination user.

As shown in the previous subsections, the user's ranking changes dynamically. Therefore, the determination about the message transmission for each user also changes dynamically.

IV. NUMERICAL EXAMPLES

In this section, we evaluate the performance of our proposed method with simulation. In this simulation, the number of users is M, and the M users move within a square whose size is 1000 $\times$ 1000. The initial position of each user is randomly selected and the direction of movement is also randomly selected. Moreover, the speed of movement is selected randomly from a uniform distribution [0, 3.0]. The direction of movement of a user is randomly selected again just before the user cuts across the square. In this case, the speed of movement does not change. We assume that the transmission range of each user is 20 and each message can be forwarded to users within the transmission range.

Here, a message is generated for user i $(i = 1, \cdots, M)$ per 50 unit time and user j is selected as the destination user of the message with probability p_{ij}. In the following, p_{ij} follows a zipf distribution as follows:

$$p_{ij} = \frac{1/f(j-i)^s}{\sum_{n=1}^{M} 1/n^s},$$

where $f(j-i) = j-i$ when i is smaller than j and otherwise, $f(j-i) = M-i+j$. The generated message is disappeared after 5000 unit time.

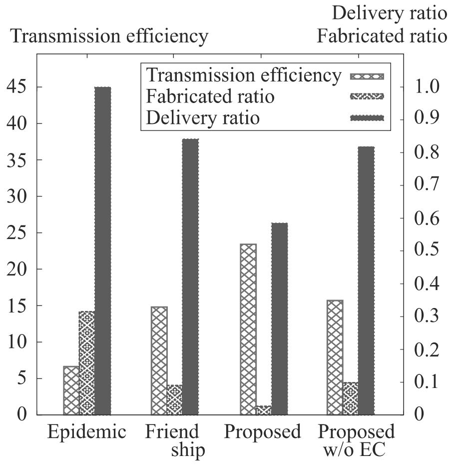
Moreover, we assume that a message that is generated by user i is fabricated by user j with probability $q_{ji} = p_{ji}$. That is, a message is fabricated by a user with a high probability q_{ji} when the user is selected as a destination user with a low probability p_{ji}.

In the above situation, we evaluate the performance of our proposed method, the epidemic routing, and the friendship routing. For the performance comparison, we calculate three performance metrics; delivery ratio, transmission efficiency, and fabricated ratio. Those metrics are calculated as follows:

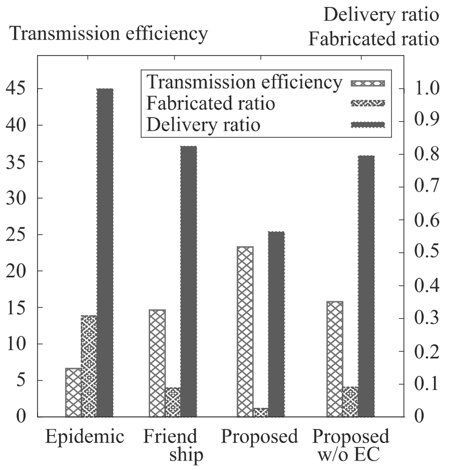
$$\text{Delivery ratio} = \frac{\text{Number of messages delivered to destination user}}{\text{Number of transmitted messages}}, \quad (4)$$

$$\text{Transmission efficiency} = \frac{\text{Delivery ratio}}{\text{Number of transmission hops}}, \quad (5)$$

$$\text{Fabricated ratio} = \frac{\text{Number of fabricated messages}}{\text{Number of transmitted messages}}. \quad (6)$$

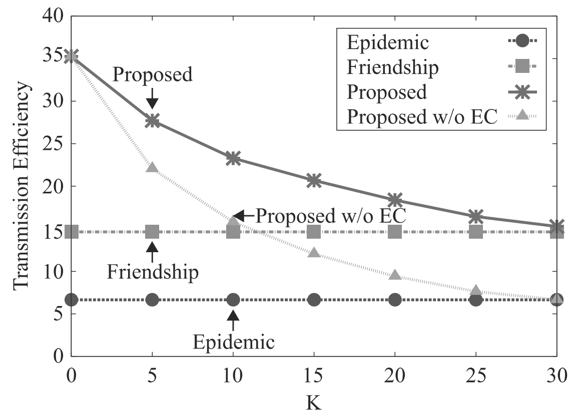


(a) A case where s is equal to 0.001.

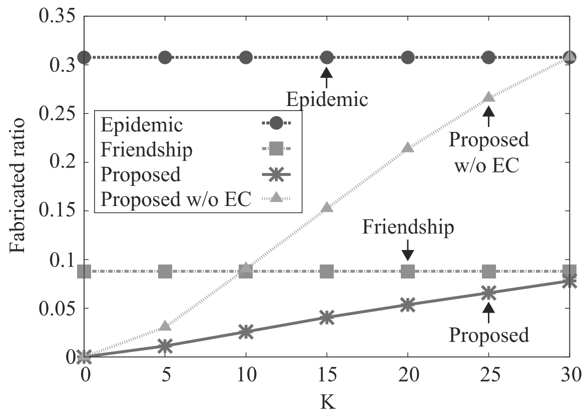


(b) A case where s is equal to 1.1.

Fig. 6. Performance of each method when probability p_{ij} changes.



(a) Transmission efficiency.



(b) Fabricated ratio.

Fig. 7. Performance of each method vs. parameter K.

A. Impact of probability p_{ij}

First, we investigate the impact of probability p_{ij} with which user j is selected as a destination user by user i. Figures 6(a) and (b) show the performance of each method when p_{ij} changes from 0.034451 to 0.034568 ($s = 0.001$) and p_{ij} changes from 0.007126 to 0.28938 ($s = 1.1$), respectively. Here, the number M of users is equal to 30. For our proposed methods, K is equal to 10. We also evaluate the performance of our proposed method without the encounter counting process shown in subsection III-B. This result is denoted as *Proposed w/o EC*.

From these figures, we find that the delivery ratio for the epidemic routing is the highest. This is because for this method a message is forwarded to all users within the transmission range. However, in the epidemic routing, the number of hops becomes large. Therefore, the transmission efficiency is the smallest. By using the friendship routing, the transmission efficiency is increased significantly by reducing the number of hops, as expected.

On the other hand, for our proposed method, the transmission efficiency is larger than that for the friendship routing. This is because messages are forwarded to users in the reliable group and the number of hops is much small. Moreover, we find that the encounter counting process is effective to improve the transmission efficiency regardless of its simpleness. Moreover, the fabricated ratio for our proposed method is much smaller that for than other methods. This represents that our proposed method can transmit message reliably, as expected.

B. Impact of parameters K

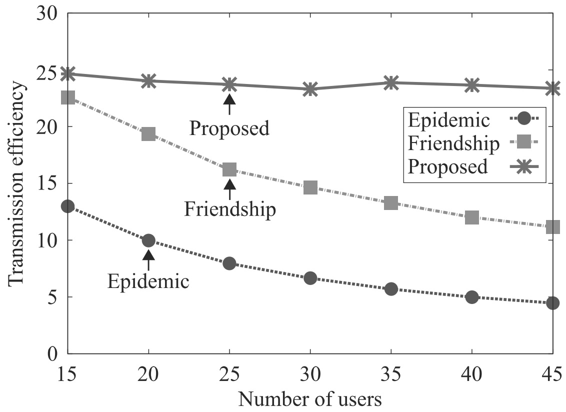
Next, we investigate the impact of setting parameter K on the performance of our proposed method. Here, M is equal to 30.

Figures. 7(a) and (b) show the transmission efficiency and the fabricated ratio against K, respectively. Note that the results for the epidemic routing and the friendship routing do not change because these methods do not utilize the parameter K. From both the figures, we find that the transmission efficiency and the fabricated ratio of our proposed method decreases and increases as the parameter K increases, respectively. This is because the number of users in the reliable group becomes large. Our proposed method is more effective than other methods regardless of K. From the above results, our proposed method can increase the transmission efficiency and decrease the fabricated ratio significantly by changing K.

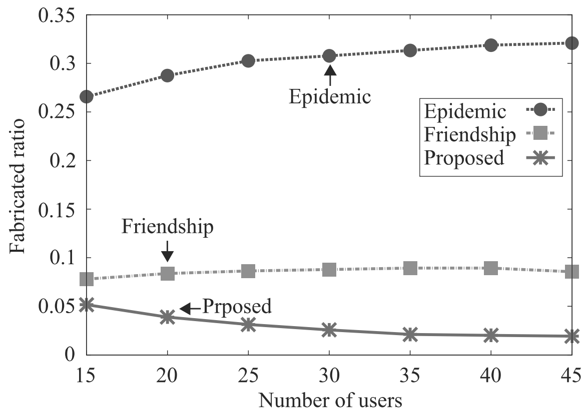
C. Impact of number of users

Finally, we evaluate the performance of each method when the number M of users changes. In the following, K is set to 10.

ISBN: 978-988-19253-3-6
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)



(a) Transmission efficiency.



(b) Fabricated ratio.

Fig. 8. Performance of each method vs. number of users.

Figures 8(a) and (b) show the transmission efficiency and the fabricated ratio, respectively. From Fig. 8(a), we find that the transmission efficiency decreases as the number of users becomes large expect for our proposed method. Moreover, the fabricated ratio also is decreased by our proposed method. Therefore, our proposed method is effective regardless of the number of users.

V. Conclusions and Future Work

In this paper, we proposed a reliable message transmission for mobile social networks. In our proposed method, users are classified into two groups and messages are forwarded to users in the reliable group. Moreover, the number of encounters for each user is counted, and this information is utilized to transmit messages effectively. For this method, we also considered a transmission algorithm. We evaluated with simulation the performance of our proposed method with a grouping rule. Numerical examples have shown that our proposed method is effective to avoid the fabrication of message, enhancing the reliability. Moreover, we found that the transmission efficiency is not degraded by using our proposed method. For our future work, we will extend this proposed method so that the other information such as community can be included.

Acknowledgement

This work was supported partly by MIC SCOPE.

References

[1] I. Lequerica, M.G. Longaron, and P.M. Ruiz, “Drive and Share: Efficient Provisioning of Social Networks in Vehicular Scenarios,” *IEEE Communications Magazine*, vol. 48, no. 11, pp. 90–97, Nov. 2010.

[2] E. Bulut and B.K. Szymanski, “Friendship Based Routing in Delay Tolerant Mobile Social Networks,” in *Proc. IEEE Globecom 2010*, Dec. 2010, pp. 1–5.

[3] S.B. Eisenman, X. Zheng, and A.T. Campbell, “Sensing Meets Mobile Social Networks: the Design, Implementation and Evaluation of the CenceMe Application,” in *Proc. the 6th ACM Conference on Embedded Networked Sensor Systems (SenSys 2008)*, Nov. 2008.

[4] J. Zhou, W. Wang, and L. Ge, “Constructing Campus Mobile SNS Based on FOAF,” in *Proc. 2011 Second International Conference on Networking and Distributed Computing*, Sept. 2011.

[5] J. Burgess, B. Gallagher, D. Jansen, and B.N. Levine, “MaxProp: Routing for Vehicle-Based Disruption Tolerant Networks,” in *Proc. IEEE INFOCOM 2006*, Apr. 2006.

[6] S. Chan, P. Hui, and K. Xu, “Community Detection of Time-Varying Mobile Social Networks,” in *Proc. In Proc. of the First Int. Conf. on Complex Sciences: Theory and Applications*, Feb. 2009.

[7] A. Vahdat and D. Becker, “Epidemic Routing for Partially-Connected Ad Hoc Networks,” Technical report, Duke University, 2000.

[8] T. Spyropoulos, K. Psounis, and C.S. Raghavendra, “Spray and wait: an efficient routing scheme for intermittently connected mobile networks,” in *Proc. ACM SIGCOMM workshop on Delay-tolerant networking 2005*, pp. 252–259.

[9] G. Chen and F. Rahman, “Analyzing Privacy Designs of Mobile Social Networking Applications,” in *Proc. the 2008 IEEE/IFIP International Conference on Embedded and Ubiquitous Computing*, Dec. 2008.

[10] J.I. Hong, J.D. Ng, S. Lederer, and J.A. Landay, “Privacy Risk Models for Designing Privacy-Sensitive Ubiquitous Computing Systems,” in *Proc. the 5th Conference on Designing Interactive Systems: Processes, Practices, Methods, and Techniques*, Aug. 2004.

[11] M. Langheinrich, “Privacy by Design - Principles of Privacy-Aware Ubiquitous Systems,” in *Proc. the 3rd International Conference on Ubiquitous Computing (Ubicomp 2001)*, Sept. 2001.

[12] C. Boldrini, M. Conti, and A. Passarella, “Exploiting Users’ Social Relations to Forward Data in Opportunistic Networks: The HiBOp Solution,” *Pervasive and Mobile Computing*, vol. 4, no. 5, pp. 633–657, 2008.

[13] I. Parris, G. Bigwood, and T. Henderson, “Privacy-enhanced social network routing in opportunistic networks,” in *Proc. the 8th IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom 2010)*, Mar./Apr. 2010.