2010 10th IEEE International Conference on Computer and Information Technology (CIT 2010)

A Framework for Building Trust Based Communities in P2P Mobile Social Networks

Basit Qureshi, Geyong Min and Demetres Kouvatsos
School of Computing, Informatics and Media
University of Bradford, Bradford BD7 1DP, United Kingdom
{b.qureshi, g.min, d.kouvatsos}@bradford.ac.uk

Abstract: **Trust management in applications for peer-to-peer (P2P) mobile networks has recently gained enormous interests. In a P2P mobile social network, users interact with each other to share information without relying on a centralized infrastructure. Users with similar interests establish groups or communities thus encouraging sharing of information such as interest profiles, personal information, documents, audio or video files etc. Gaining membership in a group/community in a mobile social network is based on recommendation from a pre-existing member of a group; revoking membership of a user from a group could be a challenging task without the existence of a central authority. In contrast to the existing implementations of social networks based on a client/server paradigm, we propose a decentralized (P2P) framework for trusted information exchange and social interaction among users based on the Dynamicity Aware Graph Relabeling System (DA-GRS). The proposed framework utilizes a light weight trust model for identifying trustworthy users and aims at creating communities of trusted users while isolating and reducing interactions with untrustworthy users. Simulations in three different environments show the effectiveness of the framework compared to the original DA-GRS algorithm.**

Keywords: Trust models, Peer to peer networking, Mobile Social Networks, Delay Tolerant Networks

I. INTRODUCTION

Recently with the increase in mobile internet users, access to various mobile applications and services on the Internet has been growing at an enormous rate. Popular mobile web browsers such as Opera mini that run on mobile devices, show an exponential growth in terms of number downloads [5]. Great interest is also being shown in Mobile Social Networking (MSN) service [1] that is being offered by online social networking sites such as facebook, mySpace, twitter etc. Smart phones and personal digital assistants have become a popular choice for social networking with the help of Email, Short messaging or by subscribing to a social networking service provider. Typical user of a social network would have a personal public profile advertised on the network including information such as personal interests, photos, videos etc. Any user with common interests would subscribe to share in the social environment.

Mobile social networking provides various challenges at two levels. At the network communications level, there are many limitations of providing social networking service to users connected to a mobile network. Frequent disconnections due to power exhaustion, poor signal quality and mobility hinders the quality of service for any mobile application. Knowing the network features ahead of transmission, such as throughput and delay, can help mobile social networks classify users based on best performance routes. This leads to the so-called wireless-aware social networks. Much work has been done in providing quality of service and performance evaluation of routing protocols for Mobile Ad Hoc Networks (MANETs) [13, 15, 16, 28]. At the second level, there are also social-aware or social inspired wireless networks where the knowledge of social network users is exploited for the benefit of wireless network design. Daly and Haar [10] presented a social network analysis for routing in disconnected delay tolerant MANETs. The methods for detecting community behavior in delay tolerant networks, exploiting the benefit of store and forwarding data in socially interactive users were reported in [4, 22]. Hui, Yoneki, Chan and Crowfort [11] proposed a novel technique determining the impact of human mobility on the design of opportunistic forwarding algorithms in delay tolerant networks.

Traditionally social networks have been implemented in a client/server environment. In MSN, users socially interact with each other with handheld mobile devices while on the move, membership in a group / community in a MSN is granted by a pre-existing member of a group; revoking membership of a group is a challenging task without the existence of a central authority. Recent advances in semi de-centralized P2P social networks have been proposed [2, 3]. These techniques rely heavily on encryption protocols in client to server communication but provide no security between P2P interactions. Trust management in a de-centralized peer to peer network is a challenging task in the absence of global knowledge for all users; any trust and reputation parameters for a user have to be computed locally [14, 30]. Given the existence of trust models for distributed systems, there is a need of a framework for trust management in MSNs. The goal of this framework is to identify trustworthy users and allow secure transmissions while isolating untrustworthy users from the community.

This paper presents a trust based framework for membership management in a mobile social network. We utilize the Dynamicity Aware Graph Relabeling System (DA-GRS) presented in [6, 8] to label nodes in the network with a trust level indicator. These trust labels are used to compute individual level trust ratings as well as community/group level trust ratings. A group of users utilize these trust-level indicators to communicate with new users and invite them to become members. The goal is to create communities/groups of users with high trust ratings while identifying untrustworthy users and isolating them from the community thus revoking their membership. This method of community based trust management is more effective in reducing the amount of computations required at a local level in a distributed environment. We present algorithms based on greedy concept using the DA-GRS system. Two cost functions to measure the trust-ability of a group of users in a network were also presented. Simulation results show that the trust based greedy algorithms create a much better quality of trusted groups compared to the standard DA-GRS algorithm.

978-0-7695-4108-2/10 $26.00 © 2010 IEEE
DOI 10.1109/CIT.2010.119

This paper is organized as follows; in Section 2, we discuss the related work followed by mobile social networking trust requirements in Section 3. The proposed algorithms for MSN trust management are described in Section 4. Section 5 presents the various simulation parameters and analysis of our results followed by conclusions in Section 6.

II. RELATED WORK

A trust based, decentralized mobile social networking service implies that users participate in a delay tolerant mobile ad hoc network topology. The related literature review is presented below.

A. Delay Tolerant Networks

A Mobile Ad-hoc Network (MANET) is a wireless network set up temporarily without a wired infrastructure (routers, switches, servers, cables, access points, etc.) [12]. The wireless nodes in a MANET may move around and each of them may need to forward packets for other components in the network. Since they can be deployed quickly, MANETs could be used for disaster rescue, battle field communication, sensor networks, etc. Routing protocols for MANETs focus on establishing routes to the destination. The route is maintained until the destination is accessible or until the route is no longer used. This assumption makes MANET routing protocols unsuitable for environments where disconnections are frequent and potentially long term [10].

Delay tolerant networks are a type of MANET that is characterized by long delay paths and frequent disconnections and network partitions [13]. In a DTN information may be carried by a mobile node and forwarded opportunistically across partitions, therefore allowing communication between areas of the network that are never connected by an end-to-end path. Recently, this type of opportunistic forwarding scenarios became popular in the research area of delay tolerant networks (DTN). Mobile nodes enable indirect data exchange among disconnected portions of the overall network, typically using a store-and-forward approach and some form of opportunistic forwarding [16]. Fall [15] presented the architecture for Delay Tolerant Networks consisting of an overlay called bundle. A bundle is defined to be a number of messages to be delivered together. DTN nodes implement the bundle layer which forms an overlay that employs persistent storage to overcome network interruptions. Leguay, Friedman and Conan [18] proposed a protocol for routing in DTNs based on mobility patterns of nodes. More recently a review of challenges of disconnected delay tolerant networks has been presented in [17].

B. Mobile social networking

Social networks are personal or professional sets of relationships between individuals. MSNs are technology-enabled services that adopt wireless and mobile communications to increase the closeness of social relationship. Some applications of social network services on the Internet have grown famous and recruit significant number of members. Twitter, Myspace, Facebook, Friendster and Dodgeball [1] are just a few examples of commercialized applications. Plazes [23] is a location-aware interaction system that helps mobile users hook up with friends or other like-minded people anywhere on the globe. Jambo Networks [24] uses Wi-Fi-enabled laptops, cell phones, and PDAs to match people within walking distance who have similar interests and would like to meet face to face. It is worth noting that most of these online applications are based on centralized client server architecture.

Due to the popularity of online social networks, most service providers have started to extend this service to mobile devices. Most approaches simply extend the web interface of the social network to the mobile device; i.e. a user can view the social network through his mobile phone without considering the issues in mobile communication. Problems such as low battery, poor communication signal, moving out of communication range, interoperability, etc can cause disconnections to the service provider. Efforts into implementation of decentralized mobile social networking have been discussed in [7, 9 and 26]. In [3] users connect to a centralized server to authenticate themselves and later can communicate in a P2P fashion. Implementation of mobile networking applications based on P2P communication model has been discussed in [12] and [14].

C. Trust Management

In human society, trust has become the basis of almost all activities, such as communications, work, etc. People gradually form mutual trust and refer to opinions of the third-party in assessing the trust [22]. Trust can be regarded as a criterion for making a judgment under complex social conditions and can be used to guide further actions [32]. In the early stages of trust and security on MANETs several researchers relied on authentication, cryptographic encryption and decryption techniques. These schemes for security were shown to be effective; however these are based on centralized certification authorities. Significant communication overheads from both preprocessing and during processing periods, as well as energy consumption were major challenges thus rendering these approaches to be poor for delay tolerant networks. It has been shown recently that reputation based techniques are more effective in de-centralized mobile networks [25]. In [20] researchers present a trust model based on fuzzy recommendation for mobile ad-hoc networks. Also a novel approach for trust and recommendations in MANETs has been presented in [21].

D. Dynamicity Aware – Graph Relabeling System

The Dynamicity aware Graph Labeling System (DA-GRS) [6, 8] is an adaptation of the Graph Relabeling Systems to the paradigm of dynamic and self-organizing networks. The main characteristics of the DA-GRS model, that are locality and dynamicity, make it a suitable tool to represent the core mechanisms that an application has to deal with in order to handle an unpredictable changing context.

The DA-GRS algorithm guarantees to maintain anytime a spanning forest that strives for a spanning tree, using only one-hop context information (*i.e.* it is a purely localized algorithm). The algorithm is composed of four rules, *i.e.* R = {r1, r2, r3, r4}. The algorithm is based on

three operations on a token: circulation, merging and regeneration. Initially, each node has a token J, meaning that each node is a spanning tree in itself, containing exactly one node (itself), and being its own root. When two nodes meet each other, applying rule r3, the two spanning trees merge. Labels 1 and 2 on an edge in the graph mean that it is a part of the spanning tree. The use of two different labels allows a node to know the local route to the token. When rule r3 applies, one of the two tokens is deleted and one of the nodes is relabeled N, that guarantees that there is at most one token per tree. Rule r4 codes the circulation of the token in a tree of the forest. When a communication link is broken, *i.e.* when an edge is deleted, the node that is on the token side has nothing to do regarding the token maintenance, and simply applies rule r2. The node that had the deleted edge label to 1 has lost the route to the token, and is the only one of its remaining

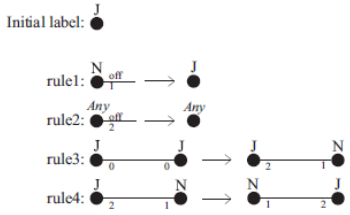


Figure 1. Four rules for the DA-GRS algorithm [6]

piece of tree to know that. It then regenerates a new token using rule r1. Figure 1 shows the four rules for the DA-GRS algorithm.

In the context of mobile social networking in P2P topology we discovered that DA-GRS is an excellent way of constructing and maintaining a decentralized spanning forest of numerous trees of nodes based on a rule based token management. The network is considered essentially as a directed graph where edges connect nodes. Each node has a token that is used to make a cluster of nodes by merging with other nodes. The process of creating clusters of node is further explained in Section 4.

III. MEMBERSHIP IN MSN

Most of the online social networking services rely on a challenge/response authentication based on centralized certification authorities. Membership in a P2P mobile social network must rely on a decentralized reputation based configuration where nodes participate in labeling other nodes with a trust level. Trust management within a partition of a delay tolerant network is very difficult because of its dynamicity, decentralized nature and non-permanent connection that can break up into two or more partitions at any moment. Although cooperative working manner among nodes/users within a DTN can be assumed, any trust management algorithm has to work at local level as global knowledge of the network is scarcely available and cannot be acquired.

A. Trust Requirements

We assume that each node in the network is assigned with a unique identification, a token for labeling and a trust level indicator. The token is an essential part of the DA-GRS labeling system and is primarily used to randomly merge a node into a group. We consider trust requirements to be a combination of human social trust factors and the quality of service in a delay tolerant disconnected MANET.

1) Social Trust and reputation: Trust is one of the most crucial concepts for decision in making relationships in human societies. Trust is indispensible when considering interaction among users in online societies such as e-commerce, e-government etc. Many trust based schemes have been presented in the literature, however for de-centralized applications or networks, trust is defined to be based on a history of a user's encounters with other users [27, 28, 30]. Reputation based systems however compute trust based on recommendations from other users of the system [27, 29]. In this paper we utilize the concept of computing trust for an individual user as well as a group of users based on reputation. Section 3.2 shows detailed method for computing the trust values for both individual users and user as a part of a group.

2) Trust as a quality of service metric in MANETs: We also define trust level for a particular node to be a measure of its quality of service. It is based on criterion such as low battery, node being out of range, poor communication signal, etc. The trust level of a user is decreased if the user's device encounters one of the above problems. Users with a higher trust level have the luxury to stay connected for the longer periods of time and communicate with a large number of users. Such users are able to store and forward data from adjacent nodes while serving as an intermediate router. Nodes with lower trust level should not be permitted to store and forward data from other users due to the higher probability of a failed delivery, therefore must be isolated from the group.

3) Gaining membership: We utilize the DA-GRS [6] algorithm to discover and merge a node with others. Assuming users A and B have discovered each other and are willing to communicate. User A is already a member of a group X, where as B seeks membership of this group through A as shown in Figure 2(a). In this case user B can merge with the group X if the tokens of A and B, i.e. T_X and T_Y can merge. If B was a part of a trusted group Y, then the groups X and Y can merge into a larger group Z such as shown in Figure 2(b). It has to be noted that the new group Z now posses only one token T_Z.

4) Trust labeling: A node's trust level can be assigned in a cooperative manner by the trusted adjacent nodes based

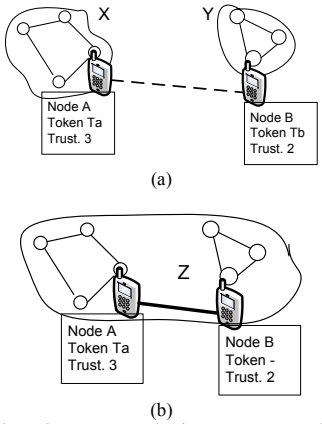


Figure 2: Nodes A in group X and B in group Y merge in to group Z

on its degree of connectivity (number of connections) and threshold for remaining uptime. This threshold is determined by a set of factors such as running out of battery, node being out of range, poor communication signal or at user's discretion. The purpose of introducing the threshold is to discourage connections to intermediate nodes that have a lower remaining uptime, thus reducing the number of connections to nodes with high degree. Nodes with higher trust levels can connect to a larger set of nodes and share information where as nodes with lower trust levels are isolated. Trust for a group of nodes is computed using two cost functions, group_cost function and isolation_cost function as detailed in section 3.2.

5) Membership revocation: If a node's trust level falls to 0, consequently it is detached from the group and the membership of that user is effectively revoked. All members of the group remove the untrustworthy user from their respective list of trusted users.

B. Trust Computation

We define trust level of a node to take values from 0 (lowest) to 3(highest). Typically a node with a trust level 3 can be connected to a large number of nodes (higher degree) and have a low possibility of disconnection (high threshold) and therefore is more likely to complete its task. Alternatively a node with low trust level such as 1 is considered to be an isolated node and must therefore be marginalized. Table 1 shows a comparison of various trust levels.

TABLE I. DEFINITION OF TRUST LEVELS IN NODES OF THE NETWORK

Trust Level	Degree	threshold	Example
3	High	High	Trustable store & forward intermediate node
2	Low	High	Trustable intermediate node
1	High	Low	Isolated node
0	Low	Low	Nodes membership is to be revoked

1) Computing Trust for a single user: To compute the trust for a user we utilize the recommendations from other users who have recently been in contact with the intended user. Each user maintains a list of users with which they had a direct interaction. Every user has an opinion about another user and labels it as trustworthy, unknown or untrustworthy, taking the values +1, 0 and -1 respectively. Typically a user may trust another user or distrust him; a new user having no previous encounters with a trusted user is labeled as unknown, i.e. 0. Trust of a user is computed by the following equations

$$T(x) = \frac{\sum_{i \in t\_list} (Trust(i) * opinion_i(x))}{\sum_{i \in t\_list} Trust(i)} \quad (1)$$

Whereas *x* is the node whose trust is to be computed, *i* is a node in the list of trusted users (*t_list*) and the function $opinion_i(x)$ indicates the opinion of user *i* towards user *x*. Value for *T(x)* is always in the interval (1, -1), i.e. a Trustworthy user will obtain a positive value, whereas a negative value indicates a untrustworthy node. *Trust(x)* labels the node *x* with a trust value based on the value of *T(x)* given by

$$Trust(x) = \begin{cases} 3 & 1 \geq T(x) \geq 0.5 \\ 2 & 0.5 > T(x) \geq 0 \\ 1 & 0 > T(x) \geq -0.5 \\ 0 & -0.5 > T(x) \geq -1 \end{cases} \quad (2)$$

The trust values for all users in contact are stored in the t_list and are updated frequently. If a trust rating is requested for a particular user, the latest value stored in t_list is forwarded to the requesting user.

2) Computing Trust for a group of users:
If a user A requests to join a group X and gain its membership, based on the DA-GRS algorithm, its token T_A is to be merged into group X's token T_X. When a token is to be merged, the group trust level is computed by the user possessing the token T_X. Trust level for a group is computed by two cost functions group_cost() and isolation_cost(). The trust level for the whole group indicates the quality of the trusted group therefore a higher value indicates a desirable trusted group. We compute the values of these cost functions to compare the trust values of groups in various environment settings.

- *Group_cost() function*: This function computes the cost of trust for the group. The cost of group G is determined by two factors, degree of trusted connections and trust level for each node in G. It is given by

$$Group\_cost(G) = \sum (trust(x) * t\_conn(x)) \quad (3)$$

Where t_conn() for a node x is the number of trustable connections to other nodes and trust(x) indicates the trust level of node x. As an example, the Group_cost() for the group shown in Figure 3(a) is 15. Similarly for the group in Figure 3(b) the group cost computed is 21. This shows that the group of users in Figure 3(b)

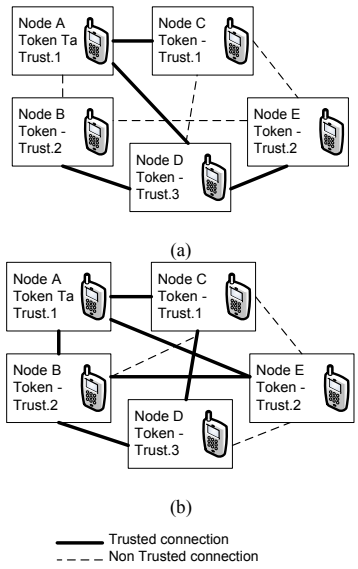


Figure 3: Examples of a group in a MSN

has a higher trust ability compared to group in Figure 3(a). Having connections with nodes that have a higher trust level is desirable for long term communication. Node D in Figure 3(a) has a trust level of 3 and has 3 active trustable connections therefore is more trust able than node A in Figure 3(b) having a trust level of 1 and 3 active connections. To have an optimal trust-level in a group, nodes with lower trust levels should be isolated with minimum number of connections while higher trust level nodes should be allowed to establish more connections.

- *Isolation_cost() function*: To create better quality trusted groups we try to isolate nodes with low trust levels (trust level <=1) and low number of connections. We simply compute the group_cost() for low trust nodes in the group and subtract this from the group_cost of that group. As an example the isolation_cost for group G in Figure 3(a) would be 12 , where as in Figure 3(b) it is 16.

IV. ALGORITHMS FOR TRUST MANAGEMENT

Due to the decentralized nature of mobile social networking in a delay tolerant environment maintaining a trust management in groups of nodes at a global level is very difficult. Instead a trust management algorithm must work at a local level. We utilize the dynamicity aware graph labeling system algorithm presented in [6] to construct groups of nodes in the MSN. The proposed algorithms modify the DA-GRS to compute trust in the network.

A. DA-GRS

We slightly modify the DA-GRS algorithm for trust management. Trust level of a group is computed whenever a user / node seek to communicate to another user in a group, i.e. the tokens of the two nodes willing to communicate are compared. If the trust levels and the group_cost() and isolation_cost() values are acceptable the merger is completed and a larger group is formed. As an example consider Figure 4. Node A in group X has a trust level 3 while the group_cost() value being 27 and isolation_cost() value being 21. Node B is group Y has a low level of trust while the group_cost() is 15 and isolation_cost() is 6. Node A has a higher trust level in a group X that has a higher group trust level as compared to node B in group Y. Also in group Y, the ratio of group_cost() versus isolation cost() is 15 to 6 indicating a high percentage of nodes that have a low level of trust and are isolated in the group. The DA-GRS algorithm in this case would allow groups X and Y to merge. It must be noted that this algorithm does not consider trust of individual nodes or the group trust level while merging.

B. Greedy Labeling

The Greedy DA-GRS algorithm is an improvement of the DA-GRS algorithm by adding the greedy algorithm concept. The idea behind this concept is to select a group from a set of groups that has the highest group trust level and merge with it. In Figure 4, the greedy labeling algorithm would merge node B with group X containing node A. Node B with a trust level 2 would prefer to merge with node A with a higher trust level of 3 instead of node C

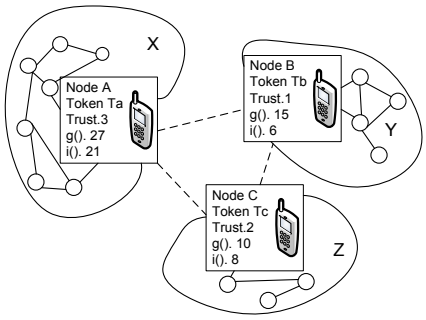


Figure 4: Merging of Groups. Each node in a group has a token, a trust level, the group trust cost g(x) and isolation trust cost i(x).

with a trust level of 1. The greedy labeling algorithm improves the overall group trust level.

C. High Group Trust Labeling

The High Group Trust (HGT) labeling algorithm focuses on group level trust rather than merging node's trust level. A group with a higher level of group_cost() value can be considered as a robust trusted group with a long duration of time to live, i.e. the group in terms of performance has the longest available connection time and therfore is more reliable. As an example, in Figure 4, node B prefers to merge with group X with a group cost of 27 rather than group Z with a group cost of 10. Larger groups with higher group trust cost can be considered most reliable. This algorithm is essentially a greedy algorithm based on DA-GRS where group_cost of a group is considered for comparison instead of individual node trust level.

D. Optimal Group Trust Labeling

The Optimal Group Trust (OGT) labeling algorithm focuses on quality of group trust. A group with lowest

```
1: void greedy(Tb){
2:   //Tb is the best trust value token in one hop
neighborhood
3:   if (Tb != NULL)
4:     Merge_with_group(Tb, Tx);
5:   else Move_token(Tx);
6: }

1: void HGT(Tb,Gb){
2:   int g_cost;
3:   g_cost=compute_g_cost(x);
4:   if (Tb != NULL && g_cost < Gb)
5:      Merge_with_group(Tb, Tx);
6:   else
7:      Move_token(Tx);
8:  }

1: void OGT(Tb,Gb,Ib){
2:   int g_cost, i_cost;
3:   g_cost=compute_g_cost(x);
4:   i_cost=compute_i_cost(x);
5:   if(Tb != NULL && (g_cost - i_cost) < (Gb-Ib))
6:      Merge_with_group(Tb,Tx);
7:   else
8:      Move_token(Tx);
9:   }
```

Figure 5: Proposed Algorithms for Trust Management

TABLE II PROPERTIES OF THREE SETS OF EACH CATEGORY OF NETWORKS (CAMPUS, SHOPPING MALL AND CITY STREET). TOTAL NUMBER OF USERS IN EACH NETWORK IS 100.

	Campus1	Campus2	Campus3	Mall 1	Mall 2	Mall 3	Street 1	Street 2	Street 3
Max no. of connections	20	40	60	20	40	60	50	70	90
Min no. of connections	0	0	0	1	1	1	2	2	2
Avg. no. of connections	5.8	19.1	33.2	4.2	17.3	28.6	9.2	11.6	12.8
Total no. of connections	708	1045	1389	688	943	1073	322	379	437

percentage of isolated nodes is preferable to larger groups with a high percentage of isolated nodes. As an example in Figure 4, group X has a ratio of 21 to 27; group Y has a ratio of 6 to 15 and group Z has a ratio of 9:10, this indicates that group Z has the highest optimal trust value, i.e. least number of isolated nodes. This algorithm is also a greedy algorithm based on DA-GRS. It focuses on quality of trusted groups in terms of group trust coherence. Figure 5 shows the three proposed algorithms.

V. SIMULATION & RESULTS

We assume in a mobile social network each user is equipped with a mobile device. Each device has a Omni directional transmission range. Users are mobile and can communicate and stay connected while on the move. Simulation in this work considers three real-world environment categories. The categories are selected in terms of mobility and concentration of users. Users in the University campus and Shopping Mall networks are considered to be less mobile. Users in a city street are considered to be highly mobile. The networks used in this work are generated in the Madhoc simulator [19]. To ensure validity of simulations we generate three different networks for each category of environment (9 networks in total). Table 2 shows the properties of each of these networks. We consider each network consisting of 100 users. The total duration for each simulation was 20 seconds with 40 simulation steps taken at 0.5 seconds intervals.

The simulation duration was selected carefully to reflect changes in networks that have higher mobility (street network). Changes in the city street network are more frequent than in campus or shopping mall networks. Figure 6 shows an example of each of the three types of networks.

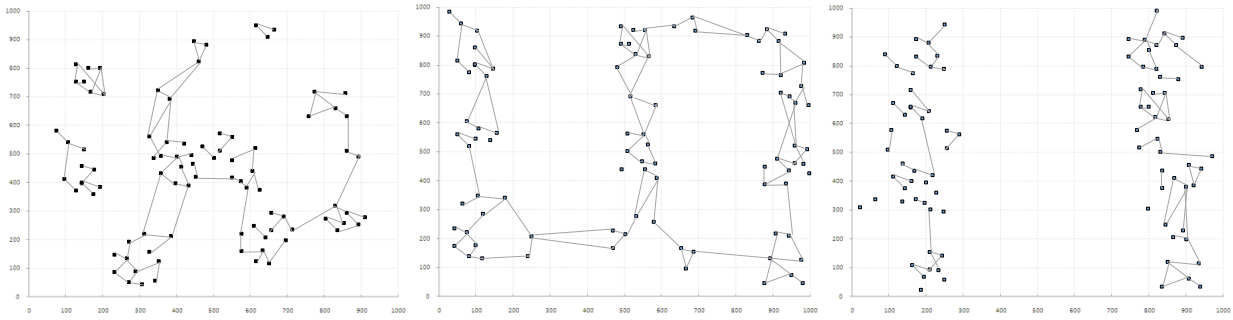
As stated before determining an optimal trusted group for a decentralized dynamic network is extremely difficult. However since networks used in this study were generated using Madhoc simulator, the configuration of a network can be pre-determined. Therefore the robustness of suggested algorithms can be evaluated by calculating the group_cost function and the isolation_cost function of each of these networks. For each of these networks we ran the simulation 400 times. The average percentage of trusted nodes ($T(x) > 1$) was 30, in this simulation. We also compare the number of untrustworthy nodes ($trust(x) <= 1$) and whether these are successfully isolated from groups. It must be noted that a node with a *trust(x)* values less than one is considered untrustworthy and its membership is revoked from the group.

A. Results for Campus Networks

Table 3 shows results for the average values of group and isolation cost functions for the suggested algorithms. The campus network is chosen due to its low mobility and high connectivity feature. From the results it can be seen that Greedy labeling algorithm yields the highest group cost thus resulting in most number of trustable groups. The percentage of successfully isolated nodes with *trust(x)* less than 1, is 83%. The isolation cost for High Group Trust (HGT) algorithm is higher than greedy algorithm therefore resulting in a better quality group. It must be noted that the group cost for Optimal Group Trust (OGT) algorithm is lower than both greedy and HGT algorithms but it provides the best isolation cost thus creating the best quality trust groups. The OGT provides the highest percentage of successfully isolated untrustworthy nodes.

B. Results for Shopping Mall Networks

Results for the averages of group and isolation cost functions for shopping mall networks can be seen in Table 4. The shopping mall networks have slightly higher degree of mobility compared to campus networks. Due to higher mobility the average numbers of connections are lower. It can be seen from the results that Greedy labeling algorithm performs better compared to HGT and OGT algorithms in



a) Campus (b) Shopping Mall (c) City Street

Figure 6. Examples of Networks used (a) Campus Network, (b) Shopping Mall and (c) City Street

creating trustable groups. The ratio of group cost and isolation cost indicates that OGT performs better in terms of creating high quality trusted groups. It can also be seen that the group cost function for HGT yields almost similar values for OGT.

C. Results for City Street Networks

Results for the averages of group and isolation cost functions can be found in Table 5. Users moving in a city street are considered to be highly mobile compared to the earlier defined networks. Results show that the dynamicity of the network yields fewer trusted connections therefore the average cost functions values are lower compared to campus and mall networks. An interesting fact observed in simulation indicates that due to higher mobility the group cost for OGT is not similar to HGT. A possible reason could be decrease in performance due to the cost of computing the ratios. Apart from this issue, OGT still performs better in terms of creating better quality trusted groups.

VI. CONCLUSIONS

Mobile social network services implemented by popular online social networking organizations simply extend the user interface to mobile devices without realizing the inherent problems of mobile communication. To date very few de-centralized MSNs have been implemented due to the enormous challenges posed by a dynamic nature of the networks. Trust management in dynamic decentralized mobile networks is receiving attention due to its immense application. This paper has presented algorithms for decentralized trust management in mobile social networks based on a dynamicity aware graph relabeling system. The proposed algorithms are based on greedy concept and the results affirm the benefits of using this approach.

Although simulating human behavior for trust and reputation assignment is unpredictable, we presented a method to compute trust of users based on a reputation model where users recommend their opinion about other users. Two cost functions to measure the trust-ability of a group of users in a network were also presented. The simulation results show that the trust based greedy algorithms create a much better quality of trusted groups compared to the standard DA-GRS algorithm. Extensive simulations also show the quality of proposed algorithms when tested in scenarios such as Campus, Shopping Mall and City Street. The proposed solution helps identify users with low trust ratings, isolate untrustworthy users and effectively revoke their membership. In future we intend to study the effects of using adaptive learning to measure trust for users in a dynamic mobile network.

REFERENCES

[1]. Ziv, N.D., Mulloth B, “An Exploration on Mobile Social Networking: Dodgeball as a Case in Point, Proceedings of the International Conference on Mobile Business, ICMB '06. 26-27 June 2006. pp.12 – 21.

[2]. Wolfgang Kellerer, Zoran Despotovic, Maximilian Michel, Quirin Hofstatter, Stefan Zols, "Towards a Mobile Peer-to-Peer Service Platform," IEEE/IPSJ International Symposium on Applications and the Internet Workshops, (SAINTW'07), 2007.Hiroshima, Japan, 15-19 January, 2007. pp. 2-10

[3]. Flora S. Tsai, Wenchou Han, Junwei Xu, Hock Chuan Chua , “Design and development of a mobile peer-to-peer social networking application”, International Journal of Expert Systems with Applications, Vol. 36, No. 8, pp. 11077-11087, October 2009.

[4]. Pan Hui, Jon Crowcroft, Eiko Yoneki, “BUBBLE rap: social-based forwarding in delay tolerant networks”, Proceedings of the 9th ACM international symposium on Mobile ad hoc networking and computing, Hong Kong, China, pp. 241-250, 2008.

[5]. Opera Mini website http://www.opera.com/mini/

[6]. A. Casteigts and S. Chaumette, “Dynamicity aware graph relabeling systems (DA-GRS), a local computation based model to describe MANET algorithms,” International Conference on Parallel and Distributed Computing Systems, pp. 231–236, November 2005.

[7]. Lugano G. and Saariluoma P., “To Share or not to share: Supporting the user decision in Mobile Social Software applications,” Proceedings of the International User Modelling conference (UM 2007; Corfu, Greece). Lecture Notes in Computer Science, volume 4511. Berlin: Springer. pp. 440–444, July 2007.

[8]. A. Casteigts, “Model driven capabilities of the da-grs model,” ICAS ’06: Proceedings of the International Conference on Autonomic and Autonomous Systems, p. 24, 2006.

[9]. Yao-Jen Chang, Hung-Huan Liu, Li-Der Chou, Yen-Wen Chen, Haw-Yun Shin, “A General Architecture of Mobile Social Network Services”, Proceedings of the 2007 International Conference on Convergence Information Technology, Ggyeongju, South Korea, pp 151-156, November 2007.

[10]. Elizabeth M. Daly, Mads Haahr, “Social network analysis for routing in disconnected delay-tolerant MANETs**”,** Proceedings of the 8th ACM international symposium on Mobile ad hoc networking and computing (MobiHoc), pp. 32 – 40, July 2007.

[11]. Pan Hui, Eiko Yoneki, Shu Yan Chan, Jon Crowcroft, "Distributed community detection in delay tolerant networks", Proceedings of ACM SIGCOMM workshops, 2007.

[12]. J. Wu (eds), “Peer-to-Peer Overlay Abstractions in MANETs”, *Handbook on Theoretical and Algorithmic Aspects of Sensor Ad Hoc Wireless, and Peer-to-Peer Networks*, Auerbach Publications, pp 857-874, 2005.

[13]. Sushant Jain, Kevin Fall and Rabin Patra, “Routing in a Delay Tolerant Network”, Proceedings of ACM SIGCOMM ‘04, Portland, OR, August 2004.

[14]. J. Sabater, C. Sierra “Review on computational trust and reputation models,” Artificial. Intelligence review., Vol. 24, No. 1, pp. 33–60, 2005.

[15]. K. Fall. A delay-tolerant network architecture for challenged internets. In Proceedings of SIGCOMM’03, August 2003.

[16]. Zhensheng Zhang, Qian Zhang, “Delay/disruption tolerant mobile ad hoc networks: latest developments”, Wireless Communications and Mobile Computing, Vol. 7, No. 10, pp. 1219 - 1232, 2007.

[17]. Elizabeth M. Daly, Mads Haahr, “The challenges of disconnected delay-tolerant MANETs”, Ad Hoc Networks, Vol. 8, No. 2, pp. 241-250, March 2010.

[18]. Leguay, J., Friedman, T. and Conan, V., “Evaluating Mobility Pattern Space Routing for DTNs”, Proceedings of the IEEE INFOCOM’06, Vol. 5, pp. 2540-2549, April 2006.

[19]. L. Hogie, P. Bouvry and F. Guinand, “The MADHOC simulator”, [Online] http://agamemnon.uni.lu/~lhogie/madhoc/

[20]. Junhai Luoa, Xue Liub, Mingyu Fana, "A trust model based on fuzzy recommendation for mobile ad-hoc networks", Computer Networks, Vol. 53, No. 14, pp. 2396-2407, September 2009.

[21]. Venkat Balakrishnan, Vijay Varadharajan, Udaya Kiran Tupakula and Phillip Lucs, “Trust and Recommendations in Mobile Ad hoc Networks “, Proceedings of the Third International Conference on Networking and Services, pp. 64 -70, 2007.

[22]. Raento M. and Oulasvirta A., “Privacy management for social awareness applications,” Proceedings of 1st Workshop on Context Awareness for Proactive Systems — CAPS’05, Helsinki, Finland, pp. 105–114, 2005.

[23]. Plazes. [Online]. Available: http://www.plazes.com

[24]. Jambo Networks. [Online]. Available: www.jambo.net/website/Home.html

[25]. J. V. D. Merwe, D. Dawoud, and S. McDonald, “A survey on peer-to-peer key management for mobile ad hoc networks,” ACM Comput. Surv.,Vol. 39, No. 1, pp. 1, 2007.

[26]. Beach, A. et al, "WhozThat? evolving an ecosystem for context-aware mobile social networks", IEEE Network, Vol. 22, No. 4, pp.50-55, July-Aug. 2008

[27]. L. Mui, M. Mohtashemi, and A. Halberstadt, “A computational model of trust and reputation for e-businesses,” in HICSS ’02: Proceedings of the 35th Annual Hawaii International Conference on System Sciences (HICSS’02)-Vol. 7, pp. 188, 2002.

[28]. Barbosa L., Siqueira I., Loureiro A.A., "Evaluation of ad hoc routing protocols under a peer to peer application", Proc. of IEEE Wireless Communications and Networking Conference, WCNC 2003, Vol.2. pp1143-1148, March 2003.
[29]. B. Yu and M. P. Singh, "A social mechanism of reputation management in electronic communities," in CIA '00: Proceedings of the 4th International Workshop on Cooperative Information Agents IV, The Future of Information Agents in Cyberspace. Springer-Verlag, pp. 154–165, 2000.
[30]. C.-W. Hang, Y. Wang, and M. P. Singh, "An adaptive probabilistic trust model and its evaluation," in proceedings of AAMAS, Vol 3. pp. 1485–1488, 2008.
[31]. A. Chaintreau et al. "Impact of human mobility on the design of opportunistic forwarding algorithms". In *Proc. INFOCOM*, April 2006.
[32]. A Piyatumrong and P Bouvry, F Guinand, K Lavangnananda, "Trusted Spanning Trees for Delay Tolerant Mobile Ad Hoc Networks", Proceedings of IEEE/IFIP International Conference on Embedded and Ubiquitous Computing, 2008. EUC '08. Shanghai, China, Vol. 2, pp. 293-299, 17-20 Dec. 2008.

TABLE III. AVERAGES OF GROUP AND ISOLATION COST FUNCTIONS FOR CAMPUS NETWORKS

	Campus Network		
	Group_cost	Isolation_cost	Percentage of Isolated nodes
DA-GRS	559.2	455.3	30%
Greedy labeling	683.3	581.4	83%
High Group Trust (HGT)	635.6	588.1	92%
Optimal Group Trust (OGT)	621.0	603.9	97%

TABLE IV. AVERAGES OF GROUP AND ISOLATIONS COST FUNCTIONS FOR SHOPPING MALL NETWORKS

	Shopping Mall Network		
	Group_cost	Isolation_cost	Percentage of Isolated nodes
DA-GRS	433.8	327.4	25%
Greedy labeling	592.5	497.7	81%
High Group Trust (HGT)	549.0	511.3	91%
Optimal Group Trust (OGT)	544.9	529.2	97%

TABLE V. AVERAGES OF GROUP AND ISOLATION COST FUNCTIONS FOR CITY STREET NETWORKS

	City Street		
	Group_cost	Isolation_cost	Percentage of Isolated nodes
DA-GRS	315.8	201.6	13%
Greedy labeling	483.2	311.7	74%
High Group Trust (HGT)	422.5	351.9	89%
Optimal Group Trust (OGT)	404.8	378.1	94%