Environmental Context Aware Trust in Mobile P2P Networks

Upendra Rathnayake[†*], Vijay Sivaraman[†*], Roksana Boreli[*†]
† School of Electrical Engineering & Telecommunications, UNSW, Sydney, Australia
∗ NICTA, Sydney, Australia
Email: [Upendra.Rathnayake, Vijay]@unsw.edu.au, Roksana.Boreli@nicta.com.au

***Abstract*—With the growing popularity and capabilities of mobile devices, peer-to-peer networking among such devices is increasingly of interest for mobile content sharing. One of the major challenges in practical use of Mobile Peer-to-Peer networks (MP2P) is the trust among peers. Traditionally, solutions in the state of the art have focused on a peer's past experience in evaluating trust of other peers, based on direct interactions. Previously unknown peers (with no history of direct interactions) are assessed based on third party recommendations, yet again requiring a peer to evaluate and find trustworthy recommenders. This reveals the fundamental need to find peers with honest intentions before any interaction. It becomes challenging when no known peers are in the vicinity, which is highly likely in an MP2P scenario.**

For a general mobile user, the probability of encountering trustworthy peers in particular situations or environmental contexts may be higher than in other contexts, e.g. in office than on the road while traveling. Further, observed peers which are co-located over a number of environmental contexts may have more in common and thus resulting a higher mutual trust. These facts can be utilized to enrich the trust derivation process in a decentralized manner. In this paper, we propose a generalized and a novel distributed mechanism to estimate the trust for peers using their encounter history in different environmental contexts, and a way to prioritize contexts depending on the level of association with them. When evaluated against real user data of the reality mining dataset, the results of the proposed mechanism show a significantly improved accuracy of trust evaluation compared to the state of the art.

***Index Terms*—Mobile P2P, Context Based Trust, MP2P Trust**

I. Introduction

Modern mobile devices are getting more and more advanced, both in terms of processing power and storage/memory capacity. This enables the widespread use of highly celebrated Internet services such as peer-to-peer networks on such devices, known as mobile peer-to-peer networks or MP2P in short. One of the major challenges against the practical use of MP2P is the trust among devices, which provides self-protection for a device by enabling it to choose which devices to interact with in a given situation. Trust can be briefly separated into three categories in an MP2P context, namely *social trust*, *similarity trust* and *QoS trust* [1], [20]. The social trust determines whether a user is genuine with honest intentions (unmalicious), while the similarity trust finds whether another peer has similar opinions or taste. On the other hand the QoS trust captures the property that whether the intended peer will perform an action (e.g. forwarding packets to a destination) with the required quality of service. These three matrices are orthogonal to each other and can be combined with different weights according to different requirements. In the state of the art, there are a number of various proposals primarily aimed at evaluating QoS trust [1], with some proposals addressing social and similarity trust [20], [21].

In an MP2P network, before initiating an interaction with another peer, a peer needs to first evaluate the social trust for the encountered peer, i.e. to find out whether that peer is genuine and non-malicious. Therefore, social trust primarily assists a peer to avoid interactions with malicious peers who might compromise it's privacy and/or pose a security threat. Subsequently, the QoS trust i.e. the capability estimation of peers needs to be evaluated. Traditionally QoS trust in MP2P environments has been addressed using mechanisms where trust of a device is determined by the direct experience from previous interactions [4]. For devices with no previous history of interactions, proposed reputation systems assess trust using third party recommendations [10], [25]. These third parties include devices which have had a direct experience with devices being evaluated for trustworthiness. Finally, the similarity trust which helps to identify recommenders with similar opinions is evaluated. As an example, a peer may find another peer transferring a file with a 1 Mbps speed (e.g. compared to a peer offering 100 Kbps) has *good QoS*, and recommenders with similar opinions may help to identify other peers who provide that *good QoS*. Most importantly, a peer needs to find genuine and non-malicious recommenders before evaluating their similarity of opinions, as the recommenders themselves may pose a security risk, in interactions or in providing false recommendations. This reveals the fundamental need to find peers with honest intentions as a starting point, either for the purpose of interacting with such peers, or for obtaining recommendations about others (i.e. the derivation of social trust). This becomes infeasible when there are no peers with direct interaction experience present in the vicinity. Even when known peers are present, the peer may still want to interact with a larger number of peers due to different requirements, such as the need to find different content, to obtain recommendations from greater number of recommenders etc.

In a typical MP2P environment, it is unlikely that a peer may always find sufficient number of other peers with previous direct interaction experience. Therefore, it is desirable to have a mechanism to derive social trust for a peer, which does not require previous interaction experience. State of the art addresses this by a) allowing a user to name his/her social friends manually [20], b) by importing social friendships from social networks or e.g. from a phonebook [15] and considering transitivity of trust through friendship chains [7], and c) by finding familiar people by looking at the encounter times or similarity scores [21]. The first two approaches need the user's manual intervention. They are also limited in their capacity, as the number of social friends of a person is limited and it is unlikely to always find friends or friend's friends in a specific locality. On the contrary, the last approach evaluates the trust of the peers who are already in the same locality, and therefore it is possible to find suitable peers to interact with in the vicinity using their co-location history. Please note that the *interaction* and *co-location* are different concepts. An interaction suggests e.g. a file transfer from a peer device. A co-location means that two peers were in the same location (not necessarily at the same time), but may not have interacted, and the amount of time two peers were *simultaneously co-located* (co-located at the same time) is identified as the *encounter time*. However, in the latter approach, the proposed solutions to date [20], [21] determine the trust solely based on either the amount of encounter time or the similarity score, i.e. the extent to which two users have been in the same locations. When determining the similarity score, they neither consider whether the two peers were co-located at the same time, nor any difference in importance of different locations.

If we consider a general case, an MP2P user may regularly encounter different people even though he/she may have no direct interaction experience with them: the *frequent strangers* [14]. This indicates that the amount of encounter time does play a role in determining trust and that those frequent strangers can be treated as more trustworthy than a randomly encountered person. However, he/she may find more trustworthy peers in particular environments than in others. As an example, a university student may find more trusted peers in the university campus, than on the road while traveling. As a consequence, those strangers who may be frequently seen in environmental contexts such as the campus may be considered more trustworthy than those strangers frequently found in other situations such as on the road. We pursue the argument that in environments which a peer inhabits more frequently and for a greater amount of time (e.g. campus, office), there is a higher chance that even the strangers are more trustworthy than those found in other environments. Moreover, if two peer have been co-located (present at the same time, as opposed to similarity trust where simultaneous co-location is not considered) in a larger number of different contexts in the past, it is likely that these peers may have more in common than other general peers. This logic can be exploited to assess the trustworthiness of a peer when no direct interaction experience is available. To the best of our knowledge, this work is the first to exploit the encounter context history of peers in establishing social trust in MP2P environments. In doing so, this paper makes the following contributions.

- We present a generalized mechanism which combines the encounter time and the co-location history of peers in different environmental contexts together with different weights for those contexts to assess the social trust, without using any direct interaction experience,
- We further show with real user data that with the use of context information, trust derivation can be improved significantly compared to purely encounter time based models.

The rest of the paper is organized as follows. In the next section, we describe the background and related work. Then, in section III we provide the model details. Section IV shows results when evaluated against the reality mining dataset, followed by a discussion of the results and models in section V. We conclude the paper in section VI.

II. Background and related work

As Veijalainen emphasized, the trust in an MP2P environment is an important issue to be addressed for the practical use of MP2P, which is closely related to privacy, security and autonomy [23]. There are numerous approaches in the state of the art which mainly target QoS trust, and [1] provides a comprehensive survey of existing work addressing trust in MANETs, a closely related area to MP2P. It provides related research papers in the areas of delay, packet dropping rate, throughput, goodput etc and also highlights papers which talk about different attacking methods such as DoS, collusion, new comer, selectively misbehaving, sybil etc.

Trifunovic et al. [20] specifically talked about *social trust* together with *environmental trust* and *similarity trust* in MP2P environments, where the *environmental trust* necessarily is a component of *social trust*. They proposed to use friend ties for explicit social trust derivation which requires a user intervention, and the use of encounter durations to find the environmental trust. The larger the encounter duration, the more the trust in that peer. Further, they suggest that trust can be estimated with the exchange of information about familiars, however the exchange of information can be forged. This proposal does not give any importance to distinct environmental contexts as we do. The importance of strangers and frequent strangers is discussed in [14] and presents the results that people do have familiar strangers in their day to day life: those who are seen frequently but do not have any interaction. It is these strangers that we look for according to their encounter history in different contexts, which allows a peer to find trustworthy counterparts for interaction. SPATE [9] describes a system which allows peers to interact with each other in a secure way. However, their trust model is primitive that the users have to manually verify (i) both mobiles are in the same place and (ii) the messages displayed on both screens are identical. The work of Lenders et al. [8] has considered location in deriving trust, but in a different perspective. That is the trust in content by *geaotagging* them, and not in the users.

Context information consideration in MP2P trust is not new in the literature. However, the context considered in most of the approaches is the service context. That is the trust of a user for a service. For example, Uddin et al. proposed CAT, a context aware trust model which defines trust for different contexts (services), and also a way to infer trust from one context to another through a context-similarity parameter [22]. Similarly, the proposal in [16] suggests a *context aware agent providing a service selection mechanism*. Wang et al. also considered location in their context definition in establishing and mapping trust over different contexts [24]. However, the implications of the location is not viewed in terms of social trust but only in QoS trust, meaning *"different environments may have significant effect on an agent's service quality"*. The work of Rehak et al. [17] also describes context based trust; however, their way of weighting observations in different contexts depend on the distance between those abstract contexts. Whereas our approach considers different contexts with different weights which are not necessarily dependent on the distance between contexts, but on the user's level of association in those environmental contexts. As an example, a person may highly trust those peers found in "home" context and "office" context, where both contexts may not necessarily be close to each other. On the other hand, this work does not specifically consider environmental context for the purpose of deriving social trust in mobile MP2P environments. Other work such as [13] have also considered context in their trust systems, but again do not specifically consider environmental context for deriving social trust.

Research in (mobile) social networking and delay tolerant networking has also some implications in tracking social relationships and thereby trust. For example, [12] and [18] discuss the importance of trust in social networking systems and emphasizes the importance of a mechanism which does not require previous interaction experience for trust formation. The latter further proposes to use "Neighbourhood Reputation" which considers the neighbors of a target agent and their relations, but does not consider the environmental context as we do. Manweiler et al. extend these concepts for mobile social networks and describe a mechanism which uses previous encounters to assess the trust of a stranger [11]. However, only the co-location (not necessarily at the same time) of two users is considered and locations bear similar weights. This inevitably amounts to *similarity trust* than *social trust*, because according to this model, even though two users share the same locations, they may haven't even seen each other as the sharing of locations is not necessarily at the same time, and hence may have only a similarity in taste. Meanwhile Hui et al. proposed community detection algorithms which consider the accumulated encounter time or the frequency of being in close proximity [5]. However, they neither consider different environments differently nor derive any kind of trust, and the community detection is solely used for efficient forwarding purposes in Delay Tolerant Networks [6].

III. Context Aware Social Trust

Trust has numerous definitions. Gambetta defines it as "*Trust (or, symmetrically, distrust) is a particular level of the subjective probability with which an agent assesses that another agent or group of agents will perform a particular action, both before he can monitor such action (or independently of his capacity ever to be able to monitor or enforce it) and in a context in which it affects his own action*" [3]. As described in the introduction section, the most fundamental form of trust, the social trust, has to be derived in a distributed manner in an MP2P environment before any interaction. A user has no choice other than to interact with the peers who are in the locality anyway, and the need is to rank them according to their perceived social trust. For this purpose, together with the encounter times, the history of environmental contexts where they were seen can be combined with some weights to those contexts, depending on the user's level of association or the familiarity with those contexts. How this information amounts to social trust than to similarity trust is, if a peer has *seen* another peer in a particular context as opposed to both peers *sharing* the same context not necessarily at the same time (as in the case of similarity trust), there is a good change that both peers may know each other to some extent. On top of that, if both peers have seen each other in a number of different contexts, and if those contexts are considered to be more important to them (e.g. office context than on road while traveling), the trust in each other may be more. This form of knowledge inevitable hints about the acquaintance of each other, the *social trust*, than the similarity in taste, *the similarity trust*. For a peer to find this, it has to first observe the co-located times of other peers and also where they were seen, together with its own stay times in those environmental contexts over a period of time. Then it can estimate the social trust in other peer as described in the following section.

Before introducing the trust models, let us explain what the *environmental context* means. The environmental context distinguishes between different surroundings of a user at a point in time and it can consist of anything which identifies the associated environment of the user distinctly. For example, information such as the geographical location or the location in terms of GSM cell IDs or WLAN access point names, whether it is a densely populated place or not, whether the user is mobile or not etc. can be combined to identify different environmental contexts for a user. An interesting point to note is that the context should not necessarily be confined only to the location [19], but can contain any information that can differentiate the environment, so that a user can distinctly identify many different environments he associates with.

A. Trust Model

A peer needs to record the amount of time that the other peers have been in close proximity to him, together with the associated environmental contexts where they were observed to be in. Let the total stay time of a user in the context j be t^s_j, for all j=*1...n* contexts. Then the fraction of time the user spent in context j, F_j is,

$$F_j = \frac{t^s_j}{\sum_{j=1}^{j=n} t^s_j} \tag{1}$$

This measure portrays the importance of the context *j* for this user in some way, as the higher the amount of time the user spent there, the higher the value of F_j for him. If the user spent more time in that context, then he knows more about and is more familiar with that context. Hence he may trust those found in that context more. In estimating trust for a peer, these F_j's can be combined with different weighs to raise different aspects such as the importance of co-located times or the importance of contexts and the co-location over a multitude of contexts, as described below.

1) Encounter time based trust (state of the art): Now for this user, let the accumulated encounter time (co-located time) with a peer *i* in context *j* be denoted by ${t^e}_{i,j}$. Then, let the weight W_i be defined as in equation 2.

$$W_{i,j} = \frac{t^e_{i,j}}{t^s_j} \tag{2}$$

$$T_i = \sum_{j=1}^{j=n} W_{i,j} \times F_j = \frac{\sum_{j=1}^{j=n} t^e_{i,j}}{\sum_{j=1}^{j=n} t^s_j} \tag{3}$$

Now the trust quantity T_i towards peer *i*, defined in equation 3, is precisely the accumulated co-located times of a peer in all of the contexts over the total stay time of the user in all of the contexts. This is the traditionally defined *encounter time based* trust [20] where no consideration is given to the importance of the contexts where the other peer was seen, or to the number of different contexts where the peer was seen. Instead, it evaluates peers whose accumulated co-located time is the maximum irrespective of where the co-location happened, to be the most trustworthy peers. Let this state of the art model be named as *encounter trust model*.

2) Context based trust: Here we propose our environmental context based novel trust model. As described in the introduction section, it is important to consider different contexts with different weights in deriving trust, where the weights should be dependent on the amount of association of the user with those contexts, as defined in equation 1. In introducing the model, let us define an indicator function $I_{i,j}$ as in equation 4. This indicator function returns *one* if the peer *i* was seen in a context *j* irrespective of for how long that encounter lasted. If the peer was not seen in that context, it results in a *zero*.

$$I_{i,j} = \begin{cases} 0 & \text{if } t^e_{i,j} = 0 \\ 1 & \text{if } t^e_{i,j} > 0 \end{cases} \tag{4}$$

$$T_i = \sum_{j=1}^{j=n} I_{i,j} \times F_j \tag{5}$$

Then the trust quantity T_i defined in equation 5 gives the trust value estimated only considering in which contexts the user was seen, of course assigning different weights to different contexts. It does not give any importance to for how long the encounters lasted, but to the extent two peers simultaneously co-locate in different environmental contexts. We identify this model as *context trust model* here onwards.

3) Combined context aware hybrid trust model: Here we are going to devise a novel and an improved trust model which is tunable. Both of the above models prioritize only a single aspect of trust, one considering the encounter times and the other considering the amount of co-location in different environmental contexts. However, if we consider a general user population, for some users and some environments, stay time based trust might suffice. For others, context should also be considered. As an example, an office worker may stay in the office for a higher amount of time, apart from his house. As he has only a very few number of important contexts (importance depends on his stay time in those environments), context history would not suffice to identify his trusted peers. Because most of his peers can be found in the office context but there is no way to distinguish between them using the context history alone. Therefore, co-location times should also need be considered in this case. For other environments like campuses, context also plays a major role in trust and should be considered in the trust calculations. For example, a campus student may stay co-located with many unknown peers in a lecture theater for a long time. For these peers, the encounter model will assign the same trust value even though encounter time alone does not imply trust in this case. Instead, if a peer is found to be simultaneously co-located in the *canteen* context as well, then there is a higher chance that the user has more in common with that peer, than any other peer found in the lecture theater alone. Therefore, to get a hybrid weight in aggregating F_j's introduced in equation 1, let us combine the previous weights as in the equation 6 with a tunable parameter α $(0 \leq \alpha \leq 1)$. The parameter α in this novel, generalized trust model allows us to fine tune the trust derivation mechanism according to different circumstances. By setting α to zero, equation 6 will result in the encounter trust model's weight whereas α equal to one will give the context based trust model's weight.

$$W^h_{i,j} = ((1-\alpha) \times W_{i,j} + \alpha \times I_{i,j}) \tag{6}$$

$$T_i = \sum_{j=1}^{j=n} W^h_{i,j} \times F_j = \sum_{j=1}^{j=n} ((1-\alpha) \times W_{i,j} + \alpha \times I_{i,j}) \times F_j \tag{7}$$

The trust quantity given in equation 7 provides the hybrid trust for a peer *i*. This is know as the *hybrid trust model* here onwards. From the encounter history of different peers in different contexts, these encounter times, context weights and indicator functions can easily be calculated and hence the overall trust for a peer for a given α.

IV. Performance Evaluation with Real User Data

In this section, we evaluate our social trust derivation model with real user data. We change α from zero to one and compare the results with each other where the $\alpha = 0$ case happens to be the conventional method proposed in the state of the art.

A. Real User Data

MIT Reality Mining project has collected data of 106 users over a 6 month period [2]. The recorded data includes periodic Bluetooth scans done every 5 minutes where the record contains all of the Bluetooth IDs which could be seen in the vicinity of the recording device. The time stamp provides the absolute time at which the scan was performed. It also contains records of GSM location areas and cell IDs when a location change happened. This enables identifying the corresponding GSM area and cell ID when a Bluetooth scan was performed, a valuable piece of information which helps to formulate a context when a Bluetooth scan was performed. That means, these GSM location area and cell ID combinations can be considered as different environmental contexts. However, it is possible that more than one area/cell ID may cover the same environment due to overlapping of the coverage. They can be identified by analyzing the ping-pong effects in location changes. That means, within a short period of time, the phone changes its attached cell to a different one and then back to the initial one. Therefore, we grouped those area and cell ID combinations together, where the ping-pong effect happens within 30 seconds, so that a single context can be derived for such instances. Hence the pre-analysis of the data produced the time stamp, bluetooth IDs in the vicinity, and the context (GSM location area + cell ID clusters).

In the middle of the time span where the data was collected, a survey has been performed among users. It lists whether any other participating user is a friend of that user or not. Even though friendship/non-friendship does not necessarily imply trust or distrust precisely, it enables identifying trusted peers of a particular user to a reasonable extent. Therefore, this information was used to evaluate and validate the trust models. The more the number of friends captured in the highly trusted peer set of a user by a model, the better that model is in general.

For the evaluation, we took two months of data around the month where the survey was performed. If the data was not available for a particular user in that time period, the data files whose dates are closest to that time period were selected for analysis. Moreover, the number of friends listed by each user can be found from the survey. We analyzed data of users who listed at least 4 friends or more, and at least 3 friends or more appearing in the records of that user in that period. Altogether, we were left with 11 users from the dataset to be analyzed. Further, we considered 20 different contexts which are clusters of GSM location areas plus cell IDs for each user.

We have also evaluated our models against a dataset collected in NICTA, which consists of 12 users' data over 3 weeks period, and similar results were found to be held true in general. However, we provide the results against the more comprehensive dataset, the reality mining dataset, in this presentation.

B. Results

With the records created from the pre-analysis as described in the section IV-A, we can identify the Bluetooth IDs around a user at a particular time, and the environmental context at which the scan was performed. By analyzing all the records together, it is possible to find the co-located times of other peers and the associated environmental contexts where they were seen. Moreover, the stay times of a particular recording user in each such context can also be calculated. From these figures, we can calculate and assign trust values to each peer seen in that recording time period using the models given in equation 7. We changed α from zero to one (0, 0.5 and 1) and found the corresponding trust values assigned by each model to other peers. $\alpha = 0$ case corresponds to the model where only the aggregated co-location time is considered irrespective of the contexts where they happened, which is identified as "encounter model" that is proposed in the state of the art (section III-A1). $\alpha = 1$ is the case where no consideration is given to the co-location times but to the contexts where they happened, the "context model" we proposed in this paper (section III-A2). The generalized model we proposed where α is 0.5 in this case, is identified as "hybrid model", which is a blend of both the above.

One such trust calculation for a user is depicted in figure 1 where the Bluetooth IDs are sorted according to the trust values resulted with the hybrid model, in the decreasing order. The X axis gives the Bluetooth ID number, starting from 1 to 40 (depicted for only first 40 peers). The Y axis is the trust value derived by each model. All the trust values are normalized with respect to the maximum trust value resulted in each model. From this figure where the Bluetooth IDs 2, 3, 10 and 18 are friends according to the survey data, it appears that the results with each approach are better to a varying degree in capturing different friends. For example, the friend 2 is given the highest trust value by the hybrid and context models but not by encounter model. The third Bluetooth ID is given a comparably higher trust value by the encounter model. However, this is based on the data of a single sample user on a single day. To see the overall performance of models, let us apply the metrics described below on all of the 2 months data of all 11 users.

1) Trust ratio of friends to non-friends: In this metric, we first take the average trust value of all of the friends out of all of the *n* number of peers who were found to have encountered with this user, as given in the equation 8 where *m* denotes the total number of friends. Then we sort the peers according to the trust values resulted with a model in the decreasing order. So the first or the top most in the list has the highest trust value, and the next possesses the next highest and so on. A friend may appear anywhere in the list depending on its assigned trust value. The higher the trust values given to the friends and hence the more the friends are towards the top of the list, the better the model is, as it can identify friends (who are the really trusted peers of the user) and push their trust values up. To estimate this, we take the average trust value of

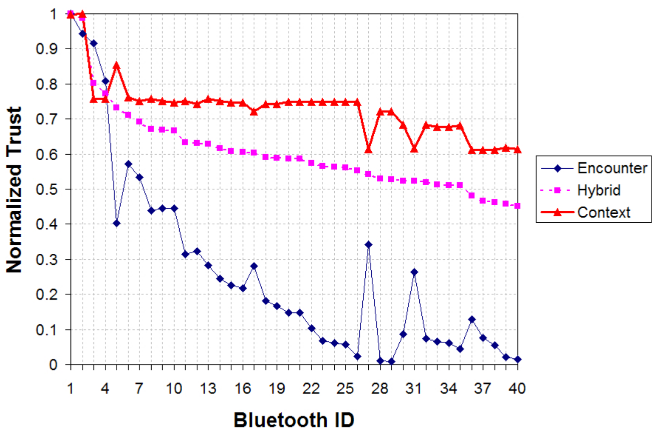

Fig. 1. Normalised trust values using the three trust models: encounter time based, context based and hybrid, for a sample user. Note the Bluetooth IDs 2, 3, 10 and 18 are friends.

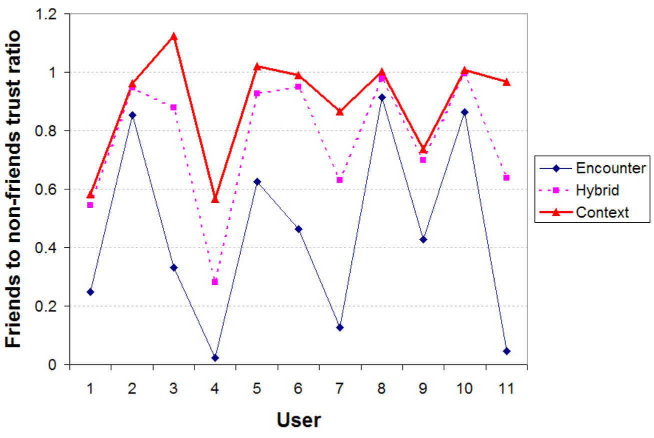

Fig. 2. The trust ratio of friends to non-friends; the highest trust values for the non-friends have been used to derive the average trust values, with the number of non-friends used equal to the number of friends.

a similar number of non-friends from the top of the sorted list as given in equation 9. The ratio of average trust of friends to the average trust of similar number of non-friends who are given the highest trust values, $R_{N(1)}$ given in equation 10, provides to what extent the model gives higher trust values to the actual friends. If the ratio is more than one, the model is clearly able to filter and pick up friends and give them higher trust values than to non-friends. Even when a model gives a less than (but close to) one trust ratio where another model gives a ratio which is further low, the former model can be considered to be better in tracking friends. Because it has been able to place the friends still higher in the derived trust list. However if the ratio is close to zero with a model, it means that the model is incapable of capturing friends by any means. The results are shown in figure 2.

$$T^F = \frac{\sum_{i=1}^{i=m} T_i}{m} \ , \ i \in friends \tag{8}$$

$$T^{N(1)} = \frac{\sum_{j=1}^{j=m} T_j}{m} \ , \ j \in nonfriends \ , \ T_j \geq T_{j+1} \tag{9}$$

$$R_{N(1)} = \frac{T^F}{T^{N(1)}} \tag{10}$$

From Figure 2, it can be observed that the context model performs the best. That means, the peers who get the highest trust values mostly constitute of friends. That is why the ratio is close to 1 in a number of users with that model. It has gone down only to 0.6, for the fourth user for whom, performance of the encounter model is the worst. Overall, if we consider with respect to a few number of peers from the top of the sorted list of trust, it can be concluded that the context model is able to pick up friends more than any other model, at least in a campus environment where the dataset was collected. This reveals the validity of our reasoning that, it is not the stay time alone that matters most, but the contexts and to what extent two users simultaneously co-locate in a number of environmental contexts. If they do, then there is a higher chance that both peers have more in common. Especially in a campus environment, there may be a lot of unknown/untrusted peers who are co-located with a user for a long time, for example in a lecture theater. As the encounter model considers only the co-location times irrespective of the contexts where they met, it probably would fail to identify trusted peers. On the other hand, the hybrid model provides a combination of both, which might be suitable in other environments than a campus, where co-location times also play a significant role in trust. So a proper value for α has to be found for such environments as discussed in section V.

Further, it is interesting to identify out of 11 users analyzed, the cumulative number of users who got trust ratio of more than 1, than 0.8 etc. The figure 3 shows these results which further establishes the strength of the context model. The number of users who got a trust ratio of more than 1 with the context model is 4, whereas for other models it is zero. If the ratio is one or more, that means the friends' trust average is higher than the top non-friend's average, meaning friends are clearly separated from non-friends. This shows that the context model surpasses other models in distinctly separating the friends who are the actually trusted peers, from non-friends.

The same metric $R_{N(5)}$ where the number of non-friends is five times the number of friends was also calculated (equations 11 and 12) for the purpose of taking a larger sample of non-friends. However, when the sample size of friends gets larger, the importance of the trust ratio becomes low, as now it does not compare against fewer top most peers who are given the highest trust values. These results are given in figure 4.

$$T^{N(5)} = \frac{\sum_{j=1}^{j=5m} T_j}{5m} \ , \ j \in nonfriends \ , \ T_j \geq T_{j+1} \tag{11}$$

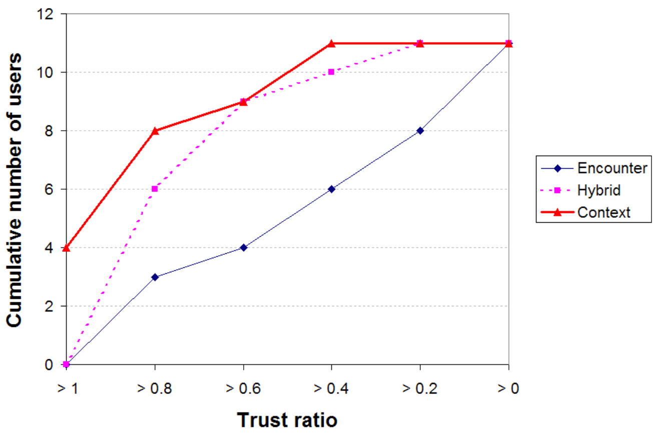

Fig. 3. Cumulative number of users possessing a trust ratio of more than x; the number of non-friends used in deriving the average trust values is equal to the number of friends.

$$R_{N(5)} = \frac{T^F}{T^{N(5)}} \tag{12}$$

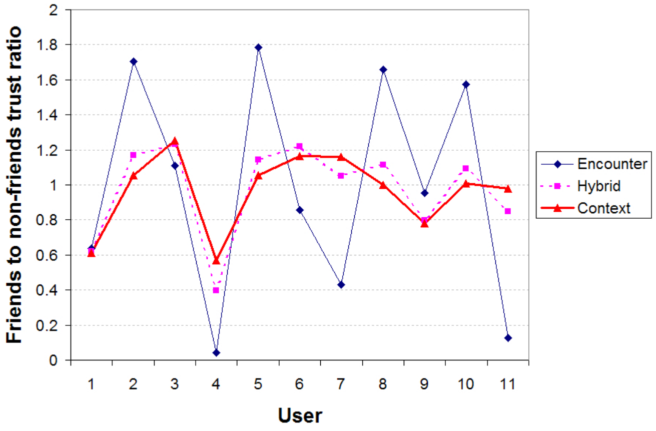

Fig. 4. The trust ratio of friends to non-friends for a larger sample of non-friends; the highest trust values for the non-friends have been used to derive the average trust values, with the number of non-friends used equal to five times the number of friends.

According to the Figure 4, the context model (and also the hybrid model) results in lower trust ratios than the encounter model for some users such as user 2, 5, 8 and 10. However, the interesting point to note is that even for those users, the ratio with context and hybrid models are still above or close to one. That means the friends' trust values are larger compared to non-friends trust values on average, which suggests that the encounter model has not gained much in comparison. On the other hand, the ratio with the encounter model is very low for the users 4, 7 and 11 where the context model performs better with close to 1 ratio (except for the fourth user). The apparent discrepancy in the results for the fourth user is because his/her listed friends neither have spent much time together nor have shared different multitude of contexts, than any other peer. Anyhow, still this suggests that even when compared to a larger set of non-friends, the context based trust provides fairly good results in general.

The reason for the comparably low ratios for some users with the context model than the encounter model in Figure 4 is due to its inherent weakness that when several peers were found to be co-located with the user in the same set of contexts, they are assigned the same trust values which happens sometimes. If these trust values happen to be higher values, the ratio becomes less even if the sample size of non-friends is large, because there are non-friends with not so low trust values in that sample. Moreover, this model produces only a limited number of trust levels, which is equal to the number of contexts considered. If several peers were co-located in the same set of contexts, there is no way to distinguish between them. In comparison, the encounter model produces a trust value which can be any between zero and one, depending on the total co-location time. As the hybrid model, where α is between zero and one, encompasses both extremes' qualities, it can produce varied trust values between zero and one. Also it is able to distinguish between peers who share the same set of contexts, depending on the co-location times of those peers. Therefore if the scenario is more towards a case where the number of prominent contexts of a user is low, a model with α less than one has to be used than a pure context based trust model where α is one.

2) *Friends positions in the sorted trust list:* Another metric which can be used to evaluate a model is finding at what positions friends are placed in the list of peers sorted according to the trust values in the decreasing order. Note that in the sorted list, the first peer has the highest trust value, next possessing the next highest etc. If friends can be found in the initial positions, then the model is capable of picking up friends and giving high trust values to them more (who are the actually trusted peers) and hence, the trust derivation appears acceptable with that model. Therefore, in this section, we show the first friend's position found in the sorted list when we traverse from the beginning of the list. We also find the average position of a friend, for each model and both results are shown in the figures 5 and 6.

Figure 5 shows that when the trust values are assigned to the peers and sorted decreasingly, the position of the first friend found from the beginning of the list is low with the context model. That means this model picks friends, at least few of them, in the top of the list where trust is highest for them. There are two exceptions. First, the inconsistency in the results for the fourth user for whom, as described in section IV-B1 also, neither the friends are co-located with him for a considerable amount of time nor are seen in a number of different contexts. The next one, the ninth user, contains a number of peers with the same trust values in the top of the list, which happens with this model due to reasons described in the section IV-B1. If several peers happen to posses the same trust level, we take the median of all of them as the position for each one of them, which happens to be the case here. Hence, the first friend's position is high, even

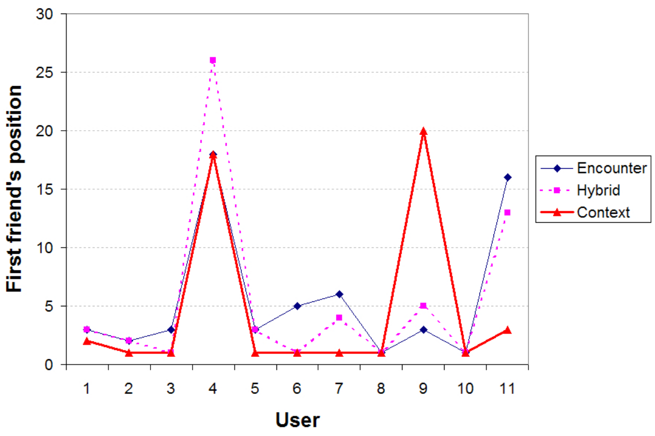

Fig. 5. The position of the trust value for the highest ranked friend in the sorted list of trust values for all peers.

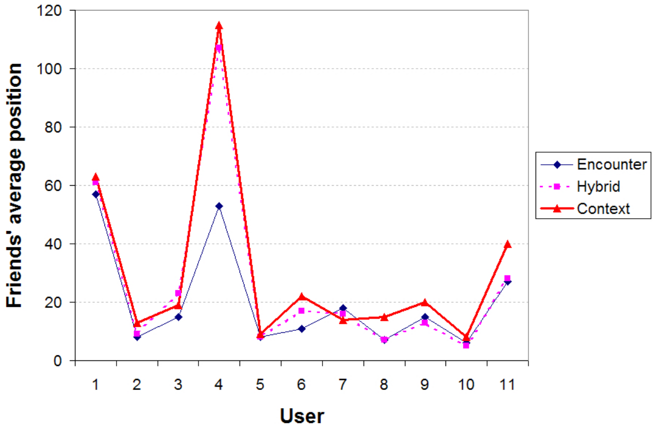

Fig. 6. The average position of the trust value for all friends in the sorted list of trust values for all peers.

though that batch with the same trust level starts from position 7. Overall, the context model seems to surpass encounter model's performance whereas the hybrid model gives results in between in general.

However, when we consider the Figure 6 where the average position of friends are shown, the reverse seems to be true. Here, the performance of the context model appears to be the worst, whereas hybrid model is behaving in between. The apparent reason is the weakness of the context model which assigns only a limited number of trust levels, which is equal to the number of environmental contexts considered. Therefore, it happens that more than one peer posses the same trust level. Hence, there is no way to distinguish a friendly peer who has co-located for some greater amount of time with the user, than other peers who have shared the same set of contexts with the user. However, with a hybrid model where α is in between zero and one, it is possible to remove this weakness and give peers with distinct ranks which depend not only on the location history, but on the encounter time as well.

V. Discussion

The results clearly demonstrate the value of environmental context in assigning trust to peers. That is why the context and hybrid models over-perform than the encounter model in most of the cases. However, there are inherent weaknesses in the context model as described in the above section. The endeavor should be to get a proper value for α which, while preserving the importance of environmental contexts in the trust derivation process, still emphasizes the importance of co-location times in it. With $\alpha = 0.5$, we saw that it performs in between encounter and context models. However, as the context model performs better in most of the cases for this dataset, it is likely that α close to one would pick more strength of the context model, and some from the encounter model. But that is for this dataset which is in a campus environment.

How about a different setting where a user may not spend a lot of time in settings like lectures together with others who are considered to be non-friends? In that case, if a peer is seen in a number of contexts, there is a good chance that they both have more in common and may trust each other as also the case in a campus environment. On the contrary, if a peer is observed to be co-located for a long time, that may also suggest that both have more in common than any other peer who is encountered only lightly. A model with $\alpha = 1$ would only capture the strength of the context history in those situations whereas α in between would make use of both. We can argue that if the user has a very few number of important contexts, then it is likely that α not equal to one will most probably represent such situations accurately. Because for him, there is a higher chance of finding the peers only in those contexts as the user spends most of the time there, and the context history alone would not be able to distinguish between them, as also shown in section IV-B2. The suitable value for α, of course, has to be found by analyzing the results generated with several distinct values for α. To do this without the intervention of the user, phone books, call detail records etc, can be used for validating the trust relationships, as are used for identifying social relationships as in [2]. Moreover, when to trust a peer after deriving trust values is another important question. It probably needs further investigations for example using some survey data, as to find beyond what trust values a peer can really be trusted. We leave these studies for future work.

When it comes to the weaknesses and limitations of the models, it is apparent that if an attacker can stay close to a peer in most of his trusted contexts, it is possible for that malicious attacker to gain trust. However, it is arguable that an attacker may find it practically impossible to stay close to a peer in most of his/her trusted contexts such as office or home, particularly for a considerable amount of time. Hence, provided the targeted peer considers the encounter times in the trust calculation (α not equal to one), it is possible to significantly reduce the effect of this attack. To complement this, the trust calculation may be enriched with data such as direct inputs from the user in regards to trusted peers, information on who are the friends (likely from social profiles), details of call records, SMS records etc. whenever these may be available. All of this additional information will assist to filter out the truly trusted peers if the user is more vulnerable to attacks. Another weakness of the models is the reliance on a context which can be formed using different factors such as GSM cell IDs and location areas etc. If the derived contexts are too coarse, then they cannot distinctly identify different disjoint contexts of a user and indicates a vulnerability. Therefore, it is desirable to use fine grained variables, so that the environmental contexts can be uniquely and distinctly identified. Moreover, in our models, we did not specify a timeliness factor for the data to be used for trust calculation. Additionally, it is evident that more recent data plays a more significant role in deriving trust than older data. In our evaluation, we have used two months of data close to the time the friendship survey was performed (section IV-A), so that we could utilize the most relevant data for the evaluation. To formally include the timeliness of data, a *sliding window* approach for data selection can be used, so as to ensure that the old data expires after a specific period of time.

VI. Conclusion

For mobile peer to peer networks to be a success, trust issues between devices have to be resolved in a distributed and efficient manner. The fundamental form of trust, social trust, must be derived with minimal information before any interaction. In this paper, we proposed an environmental context based social trust derivation mechanism which is enriched with information such as past encounters of peers and in which contexts they were seen, while still considering the overall contact durations as in the state of the art. With the reality mining dataset, we showed that the proposed mechanism performs better than purely contact time based models and improves the accuracy significantly with the use of context information. We also discussed possible ways to adapt the model to different situations.

Acknowledgment

This project is funded by NICTA, a research organization funded through the Australian Government's Backing Australia's Ability initiative, in part through the Australian Research Council.

References

[1] J.-H. Cho, A. Swami, and I.-R. Chen, "A survey on trust management for mobile ad hoc networks," *In press IEEE COMMUNICATIONS SURVEYS & TUTORIALS*.

[2] N. Eagle, A. Pentland, and D. Lazer, "Inferring social network structure using mobile phone data," in *Proceedings of the National Academy of Sciences (PNAS)*, vol. 106 (36), 2009, pp. 15 274–15 278.

[3] D. Gambetta, *Can We Trust Trust? Trust: Making and Breaking Cooperative Relations*. Basil Blackwell, Oxford, 1990.

[4] C. M. C. L. Han Yu, Zhiqi Shen and D. Niyato, "A survey of trust and reputation management systems in wireless communications," in *Proceedings of the IEEE*, vol. 98, 2010, pp. 1755 – 1772.

[5] P. Hui, E. Yoneki, S. Y. Chan, and J. Crowcroft, "Distributed community detection in delay tolerant networks," in *Proceedings of 2nd ACM/IEEE international workshop on Mobility in the evolving internet architecture (MobiArch)*, 2007, p. 18.

[6] P. Hui, J. Crowcroft, and E. Yoneki, "Bubble rap: Social-based forwarding in delay tolerant networks," in *Proceedings of the 9th ACM International Symposium on Mobile Ad Hoc Networking and Computing (MobiHoc)*, 2008, p. 241250.

[7] A. S. Jin-Hee Cho and I.-R. Chen, "Modeling and analysis of trust management for cognitive mission-driven group communication systems in mobile ad hoc networks," in *International Conference on Computational Science and Engineering*, Vancouver, Canada, August 2009.

[8] V. Lenders, E. Koukoumidis, P. Zhang, and M. Martonosi, "Location-based trust for mobile user-generated content: Applications, challenges and implementations," in *HotMobile*, Napa Valley, CA, USA, February 2008.

[9] Y.-H. Lin, A. Studer, H.-C. Hsiao, J. M. McCune, K.-H. Wang, M. Krohn, P.-L. Lin, A. Perrig, H.-M. Sun, and B.-Y. Yang, "Spate: Small-group pki-less authenticated trust establishment," in *MobiSys*, Krakw,Poland, June 2009.

[10] J. Liu and V. Issarny, "enhanced reputation mechanism for mobile ad hoc networks," *iTrust*, vol. 2995, pp. 48–62, 2004.

[11] J. Manweiler, R. Scudellari, and L. P. Cox, "Smile: Encounter-based trust for mobile social services," in *Proceedings of ACM CCS*, NY, USA, November 2009, p. 246255.

[12] P. D. Meo, A. Nocera, G. Quattrone, D. Rosaci, and D. Ursino, "Finding reliable users and social networks in a social internetworking system," in *Proceedings of the International Database Engineering & Applications Symposium*, Cetraro - Calabria, Italy, 2009, pp. 173–181.

[13] M. Moloney and S. Weber, "A context-aware trust-based security system for ad hoc networks," in *Workshop of the 1st International Conference on Security and Privacy for Emerging Areas in Communication Networks*, Athens, Greece, Sep. 2005, p. 15360.

[14] E. Paulos and E. Goodman, "The familiar stranger anxiety, comfort, and play in public places," in *CHI*, Vienna, Austria, April 2004.

[15] Y. Raivio, "Mobile peer-to-peer in cellular networks," in *HUTT-110.51 Seminar on Internetworking, Helsinki Institute of Technology*, 2005-04-26/27.

[16] N. Razavi, A. M. Rahmani, and M. Mohsenzadeh, "A context-based trust management model for pervasive computing systems," *International Journal of Computer Science and Information Security*, vol. 6, no. 1, p. 137142, 2009.

[17] M. Rehak and M. Pechoucek, "Trust modeling with context representation and generalized identities," in *CIA*. Springer, 2007, pp. 298–312.

[18] J. Sabater and C. Sierra, "Social regret, a reputation model based on social relations," in *Proceedings of the 4th Int. Workshop on Deception, Fraud and Trust in Agent Societies, in the 5th Int. Conference on Autonomous Agents (AGENTS01)*, Montreal, Canada, 2001, pp. 61–69.

[19] A. Schmidt, M. Beigl, and H. Gellersen, "There is more to context than location," *Computers & Graphics Journal, Elsevier*, vol. 23, no. 6, December 99.

[20] S. Trifunovic, C. Anastasiades, and F. Legendre, "Social trust in opportunistic networks," in *Second IEEE International Workshop on Network Science For Communication Networks (NetSciCom'10)*, San Diego, CA, USA, Mar 2010.

[21] A. H. Udayan Kumar, Gautam Thakur, "Protect: Proximity-based trust-advisor using encounters for mobile societies," in *Proceedings of the 6th International Wireless Communications and Mobile Computing Conference (IWCMC '10)*, 2010.

[22] M. G. Uddin, M. Zulkernine, and S. I. Ahamed, "Cat: A contextaware trust model for open and dynamic systems," in *SAC*, Brazil, March 2008.

[23] J. Veijalainen, "Autonomy, heterogeneity, trust, security, and privacy in mobile p2p environments," *International Journal of Security and Its Applications*, vol. 1, no. 1, July 2007.

[24] Y. Wang, M. Li, J. Xue, J. Hu, L. Zhang, and L. Liao, "A context-aware trust establishment and mapping framework for web applications," in *International Conference on Computational Intelligence and Security*, 2007.

[25] X. Wu, J. He, and F. Xu, "A group-based reputation mechanism for mobile p2p networks," in *4th International Conference of Advances in Grid and Pervasive Computing (GPC)*, Geneva, Switzerland, May 2009, pp. 410–421.