SocioNet: A Context-Aware Approach for Lowering the Communication Barrier

Igor Pernek[1] and Karin Anna Hummel[2]

[1] Faculty of Electrical Engineering and Computer Science, University of Maribor, 2000 Maribor, Smetanova 17, Slovenia
igor.pernek@uni-mb.si
[2] Institute of Distributed and Multimedia Systems, University of Vienna, 1080 Vienna, Lenaugasse 2/8, Austria
karin.hummel@univie.ac.at

Abstract. Social networking platforms, such as Facebook and Twitter, foster new social interactions. Following this vision, we introduce SocioNet, a context-aware and rule-based system for mobile devices that finds best matching persons in proximity and therefore establishes contacts. The system architecture is a hybrid central server and P2P architecture supporting matchmaking.

As concerns for social platforms arise mainly in terms of usability and privacy, SocioNet proposes *(i)* the use of existing personal information for matchmaking to avoid tedious filling-in of user profiles and *(ii)* preservation of privacy by not storing personal data on the SocioNet server if not wanted by the user. We demonstrate the feasibility of SocioNet by a prototypical implementation based on .NET CF and WLAN. To rate user satisfaction, we performed a user survey. First results show, that privacy is still a major cause not to use social networking platforms when physical presence is involved.

Keywords: Context-awareness, Personal Information Data, Privacy Preservation, Social Communication Barriers.

1 Introduction

Social networks supported by Internet services are experiencing a tremendous popularity all over the world. Building social networks and sharing experiences, like videos and photos, has become very easy, although privacy concerns remain. Huge databases hold private and personal information of various kinds which can be maliciously exploited as well. However, many people rate the benefit of these IT based social networks higher than their threats to privacy.

We experience that everyday life becomes more and more supported by networked computing technologies such as everywhere wireless connectivity, mobile smart devices, and sensors to determine orientation, acceleration, and location, e.g., supported by GPS receivers. As a consequence, IT based social networks can also be extended to situations of physical presence and interaction with the physical world.

We expect that IT based social networks of the future will combine both virtual and physical social interactions. In this work, we propose SocioNet, which aims at

R. Meersman, P. Herrero, and T. Dillon (Eds.): OTM 2009 Workshops, LNCS 5872, pp. 444–453, 2009.

establishing contacts in the physical world by matching a user's personal data with personal data of others in proximity. In other words, SocioNet fosters physical interactions based on social relationships known in the virtual world, but possibly not known in the physical world. A possible use case is a situation in a big mall, where a person would like to find the best shop for digital cameras, but also a shop that can be trusted, etc. Instead of just proposing all the shops around, SocioNet provides the user with links to persons who might be of help (and are currently willing to interact). If the system provides a good match, a short conversation might help to find out which shop to prefer and the searching person might also get additional hints during this conversation.

To provide these features, SocioNet integrates location sensors, like GPS receivers for outdoor positioning, uses personal information already stored on the mobile smart device of the user, and introduces several roles of others to search for (e.g., friend of a friend). By using personal information already stored on the device, such as contacts and calendar entries, SocioNet avoids cumbersome entering of preferences and other personal data. The matchmaking further relies on the availability of wireless networking (ad-hoc and infrastructure WLAN, 3G networks, etc.). Here, SocioNet allows keeping personal data local to increase the level of privacy, but allows also to store it on a central server. The server is in any case used to identify who is participating in SocioNet. Depending on where the data is stored, either a Peer-to-Peer (P2P) connection is suggested between the two user devices for exchanging personal information and matchmaking is done at the clients, or the server performs matchmaking. (Note, that the information is encrypted before sending.)

The research questions we want to answer are: *(i)* Can we propose a system that avoids tedious filling-in of user profile data? *(ii)* What are the performance and privacy tradeoffs between storing SocioNet information on a central server and exchanging information in P2P manner? *(iii)* How does a user rate the benefits of SocioNet, e.g., is it useful and preserves privacy good enough?

In the remainder of the paper, we will address these questions after introducing related work in Section 2. How SocioNet approaches to lower communication barriers is summarized in Section 3 followed by a presentation of the prototypical implementation for PDAs (Personal Digital Assistants) based on .NET CF and WLAN in Section 4. In Section 5, we present performance reflections and the results of a user survey which has been carried out to rate user acceptance.

2 Related Work

After the rapid growth of Internet based social network services the same phenomena is happening in the area of mobile computing. Over the last years various mobile social networks have been established and it is to expect more of them to arise as mobile smart devices are spreading equipped with multiple wireless networking facilities (3G, WLAN, Bluetooth, etc.). According to a recent forecast [1], half of the new connections to the Internet in 2009 will be mobile and the mobile device will become the primary Internet connection tool for most people in 2020.

Besides the ability to maintain social groups and to connect with a social network's members, mobile social networking is also often used as a means, which helps the mobile users to hook-up with friends, friends-of-friends, or other people in proximity [8], [15],

[10], [3], [11]. The continuous appearance of new tools for facilitation of face-to-face interaction with the help of electronic personal assistants is reflecting the potential of systems combining physical and virtual world. For example, using the Short Message Service (SMS) often leads to face-to-face communication and PDAs can promote social interaction [14]. Depending on the mobile device's operating system, like Android, Symbian OS, Windows Mobile, applications are written in J2ME, C++, or based on .NET CF. We have chosen .NET CF for the prototypical implementation of SocioNet.

Existing mobile social networks use different system architectures on top of wireless networks, such as WLAN or 3G. While the general architecture of mobile social networks is centralized [6], a lot of them are using P2P architectures [12], [4], [2] to exploit the fact that only the peers nearby should be contacted and no additional infrastructure is needed. Each system architecture paradigm is accompanied with a set of advantages and disadvantages. Although processors of mobile devices are getting faster, they are still not able to perform real-time matchmaking on a larger set of profile data. On the other hand, the central server approach solves the problem of matching large data sets but privacy concerns are raised.

Different data provisioning patterns are used to perform matchmaking between the users. While in the past user predefined profiles were used to perform pairing of users with similar interests, nowadays context information is becoming a valuable source of profile information [9]. It is expected that context-awareness will become even more important as trends in mobile computing are converging to smarter approaches.

Besides usability, the main factor that makes or breaks a mobile social platform is trust in the system. Different studies have been carried out evaluating the way privacy is handled in existing mobile social applications and mobile social system architectures. In [7], the Bellotti and Sellen's feedback and control framework [5] is used to analyze existing mobile social applications. The conclusions drawn are, that privacy designs are usually weak, as they are not offering enough control over the user's personal data and are not providing enough feedback about where the data is stored.

SocioNet incorporates the insights and beneficial design principles concluded by related work on social networks by considering performance, privacy, and usability issues at the same time.

3 SocioNet Concept

In this section, we will describe design decisions and the concepts included in SocioNet answering the question how to derive profiles for matchmaking. Additionally, we will discuss the system architecture of SocioNet.

3.1 Functions and Features

The design of SocioNet aims at making the application unobtrusive, transparent, and simple to use, to make it suitable to a broad range of different users. The prototype installation of SocioNet can be controlled using the mobile device main window, which results in a gently sloped learning curve for inexperienced users. Additionally, we have eliminated the phase of entering long and cumbersome user profile and preference data. Instead of fostering users to enter these data, SocioNet uses personal information already stored on the device, like contact data and calendar entries. The

control over the data used in the matchmaking process lies in the hands of the user and can be selected via a profile data control interface.

As both the P2P and the central server architecture have advantages and disadvantages, we have decided to combine them into a hybrid system architecture (Fig. 1a) to select between different configurations for storing profile data for matchmaking. In this system architecture approach, the P2P network is an unstructured network and the server is in any case responsible for providing links to clients (names, IP addresses of clients). We have decided not to use any structured P2P network approach (like Distributed Hash Tables) mainly because we may exploit the hybrid architecture and therefore can avoid costly searches in the P2P sphere.

Using a central server also for matchmaking leads to decreased privacy, but also better performance in terms of matchmaking execution time and data transfer in particular of large scale profiles (load and delays) necessary prior to matchmaking. The P2P sphere avoids storing private data centrally but requires more resources on the mobile devices since matchmaking is performed by a mobile peer.

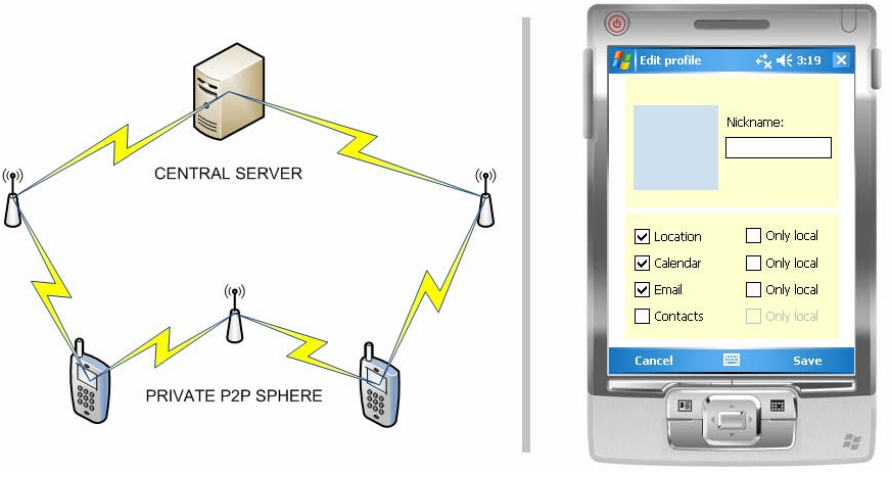

Fig. 1. a) Hybrid network architecture and b) Profile data control screen

The central server acts as a tracker of online clients able to perform matching of the data stored on the server (if any). In any configuration, the server's responsibility is to provide link information to all clients. The server is also ready to store optionally the most frequently used matchmaking data, if allowed by the user's privacy settings. Fig. 1b shows how the user may select different types of personal data for matchmaking and whether the data should be used only local in the P2P sphere. After a user issues a matching request, data available on the server is matched on the server to avoid additional network traffic. If client data is not available, a list of nearby clients is forwarded to the client device which then pushes the necessary data to the clients residing nearby for matchmaking. Finally, matching results are returned either from the server or the peer client devices – or both – and joined to a final result set, which is presented to the user. Using the approach described, we are able to adapt the

communication style to privacy, performance, and cost considerations. Hence, the user remains not only in control which data to share for matchmaking, but also where the data should be stored.

To summarize, all design steps were taken to reach the main goal of the application, i.e., to find the best matching persons in proximity of the user and to promote face-to-face interaction in an urban area where wireless networks are available. Matches are based on location and personal information (contact and calendar data) provided by state-of-the-art mobile devices.

3.2 Roles and Rules

While the main matchmaking criterion is the proximity of users, SocioNet uses the roles presented in Table 1 to reflect social relationships in the SocioNet community. Different roles further allow the user to pick a person matching his or her personality or current mood. If the user would like to get in contact with a person he or she knows or is partly familiar with, the user can pick a result annotated with the *friend* or a *friend-of-friend* tag. If the person would like to socialize with an unknown person who shared interests with the user or even with a total stranger nearby, he or she can easily pick a match tagged with the *interests match* or a *stranger* tag and possibly expand his or her social network.

Table 1. Description of the SocioNet roles

Role	Description [all persons in proximity]
Friend	A person with whom the user is acquainted.
Friend-of-friend	A person with whom a friend of the user is acquainted.
Interest match	A person with same interests, taking part in the same social activities.
Stranger	A person, who is not a friend, neither a friend-of-friend nor an interest match.

All of the roles used by the SocioNet application are based on simple classification rules as explained in Table 2. With respect to the described classification rules, different roles are not necessarily mutually exclusive, as the friend or a friend-of-friend could also have interests in common with the user and therefore lead to an interest match. For determining the roles, different profile sources are used.

Table 2. Description of the main SocioNet rules

Role	Profile section	Classification rule
Friend	Contact-book	A person whose telephone number is stored in the user's contact-book.
Friend-of-friend	Contact-book	A person with whom the user is sharing one or more contacts.
Interest match	Calendar	A person with whom the user is sharing social events in the calendar.
Stranger	Contact-book, calendar	A person having nothing in common with the user, but residing nearby.

In more detail, optimized matchmaking at the server introduces new complexity to the basic concept. After a match is accepted, the match's role is determined and the corresponding user-role match counters are increased for the matched persons. If a match counter for a role meets a pre-configurable threshold, profile reorganization is performed. E.g., if a user regularly accepts interest matches the system predicts that it is more likely that the next match accepted will be an interest match. As a consequence, if allowed by the user's privacy settings, profile data used to recognize interest matches (e.g., calendar data) will be stored on the server to decrease network traffic.

4 Implementation

The SocioNet mobile social network prototype is built as a hybrid P2P and central server solution, which allows matchmaking being done on the central server or directly on the mobile client device (here, a peer). While the server is implemented in the .NET Framework 3.5, the PDA client prototype is based on the Pocket PC .NET Compact Framework 3.5 platform and tested on a DELL AXIM X51V. Although WLAN and IP are used in the prototype implementation, the network layer is abstracted and can easily be exchanged by, e.g., GPRS or a 3G network. The system architecture was successfully implemented, meaning that clients can connect to a server and/or other peers directly to perform matchmaking, as well as the role concept.

To achieve a higher level of modularity, the server solution is implemented as host application and a library of XML Web services, which could be upgraded or replaced without much effort. Clients contact servers on a specific socket port to invoke a Web service and listen then for notifications of the service. With the use of transparent privacy settings and a rule-based profile storing approach, we expect that a good performance-trust tradeoff will result. Relationships between two contact book or calendar entries are stated by full-text match. We have decided to obfuscate the data with a one-way hash function and transform the text into a form not readable by humans, while still preserving enough information to perform full-text matching. Although original data could be restored with a simple rainbow attack [13], an additional step is needed to abuse the personal data.

To optimize matchmaking at the server, rule-based profile storing as described in Section 3.2 is implemented together with profile caching to reduce network traffic. Rather than transmitting locally stored profile data for each matching attempt, profile information is stored in the server's volatile memory for the time of a session. After the user logs out or is inactive for a pre-configurable amount of time (timeout), his or her profile is removed from the cache.

5 Performance Reflections and User Questionnaire

The prototype has been evaluated with respect to performance measurements for comparing the messaging load to the analytically expected load and user acceptance. With respect to performance, the important question was about the costs to expect

when preserving privacy using the P2P sphere for matchmaking in comparison to the central server solution. User acceptance is evaluated by means of a user survey. In this section, we will briefly summarize first results of these investigations.

5.1 Performance Reflections

We now evaluate the impact of matchmaking placement by taking a look at the network traffic caused (bytes transferred) of two configurations: *Central server only* and *peer-side*. We present here the analytical calculations useful for determining trade-offs between privacy and overall network load L in bytes (additionally, response time could have been investigated experimentally based on the used WLAN IEEE 802.11g). By comparing the analytical numbers with our measurements, we discovered no significant deviations (as expected from a correct implementation of messaging). The experiment carried out was simulating $N_u = 100$ mobile user devices in proximity, each one holding $C_u = 100$ contact-book entries; each of $size = 32$ bytes after obfuscation. Each user requests matchmaking to take place $Mf_u = 10$ times in the simulation period.

The *peer-side* approach, where client profiles are stored in the P2P sphere only, resulted in $C_u \; x \; size = 3200$ bytes transferred $(N_u - 1) \; N_u = 9900$ times to the matchmaking mobile device (note, that the whole profile has to be transferred for each request). After $Mf_u = 10$ matchmaking requests, resulting number of bytes transferred are calculated as $L = C_u \; x \; size \; x \; (N_u - 1) \; N_u \; x \; Mf_u = 316.800.000$ bytes.

For the *central server only* system configuration, the size of the initial data transfer of $N_u = 100$ clients is $L = C_u \; x \; size \; x \; N_u = 320.000$ bytes. Additionally, due to changes in the contact book, incremental synchronization with the server will be required causing additional load.

As can be seen, the pure P2P solution is reasonable in case small amounts of data have to be exchanged, N_u is small, or frequent updates of personal data occur. With the use of a central server, there is only one initial data transfer and incremental updates (e.g., a new contact is added to the contact-book). Matchmaking is then performed by the server and no additional data transfer is needed.

Since our approach allows to store profile data partially on the central server and in the P2P sphere (on the mobile device), the rule-based profile can be used to generate arbitrary hybrid configurations, which allow to store some information of lower privacy protection level (e.g., calendar entries) on the server while leaving others on the mobile device (e.g., contact data). Network load will be reduced while keeping the user in the loop of controlling where his or her profile data is stored. The performance increase depends here linearly on the amount of data kept at the central server.

5.2 Questionnaire Based User Survey

After a short demonstration of the features of SocioNet, we conducted a user questionnaire to find out the answers to the following crucial questions with respect to user acceptance of SocioNet in terms of usability and privacy:

i. Do the participants think that SocioNet will open new communication options and which roles do they like to interact with (friends, friends-of-friends, persons sharing interests, strangers)?

ii. Do the participants think that privacy is assured by keeping data local?
iii. Do the participants think that their mobile personal information is rich enough to lead to good matches?

We evaluated the answers of 40 participants in the age ranging from 18 to 48 years. The *Computer Proficiency (CP)* self-estimate of the participants was either *high* (*CP*=3), *medium* (*CP*=2), or *low* (*CP*=1). The average proficiency was calculated as 2.6 and is rather high. Table 3 summarizes the results of the questionnaire.

Table 3. Results of the user survey [in %]

Classes [# of participants]	**CP < 3 [15]**	**CP = 3 [25]**	**All [40]**
Opens new communication options	73	76	75
Use SocioNet to contact a			
friend	53	64	60
friend-of- friend	33	52	45
interest match	46	68	60
stranger	13	24	20
Privacy			
feeling in control	20	56	43
local storage	93	72	80
PI-data sufficient	53	52	53

We can state some observation based on the results of the questionnaire:

- More than 70% of both computer proficient participants and participants not that familiar with computing technology think that SocioNet opens new communication possibilities.
- When asked about the type of contacts which should be fostered via SocioNet, it is remarkable that higher proficiency generally comes with a higher likelihood of using SocioNet for establishing (social) contacts.
- Generally, 60% of the participants would use SocioNet to contact their friends and persons with similar interests, while only 45% would contact friends-of-friends, and 20% of the participants would also like to use SocioNet to contact strangers. These first results show that the participants base their contacts on *existing* close relationships or on *existing* similar interests.
- It is remarkable, that only 20% of low and medium proficient participants think they are in control of their privacy, while 56% of the highly proficient participants feel in control. Here, we see a general lack of mental models of where digital personal data is best stored and how unauthorized access can be prevented which may be a cause for this feeling.
- On the other hand, 93% of low and medium computer proficient participants felt that storing the data not on a central server helps to increase privacy, while participants with high proficiency were more reluctant (72%). Here, computer proficient participants have most likely considered several remaining threats to privacy (like, men-in-the-middle, not trustworthy P2P system, etc.).

- SocioNet tries to avoid entering of boring user profiles, but many participants think that personal information stored on their mobile devices will not be sufficient to identify persons to contact. Here we see that our alternative approach requires further (positive) evaluations (e.g., a longer field study with real-life personal information data) before users might trust the solution.

Finally, the participants were asked why they would *not* use SocioNet to contact others. Some participants thought that they do not need technology to contact friends or friends-of-friends. Additionally, missing trust in the system was a major issue.

6 Conclusions

In this work, we have introduced SocioNet, a social networking platform dedicated to mobile smart devices to support social interactions among persons in proximity. While addressing performance and trust issues, SocioNet provides pointers to other persons willing to interact and help in particular every-day situations. SocioNet follows the vision that human-to-human interaction allows for better problem solving due to the richness of human social interactions when compared to a solely database based recommender system. To find best matching persons, we introduced an extended role model representing social relationships.

Due to privacy issues, we provided a solution where personal information does not have to be stored on a central server but may be exchanged directly between the participating mobile devices. The prototypical implementation showed that this peer-to-peer solutions results in significant messaging overhead, which could be reduced by adding rules resulting in partial central storage of personal data.

To evaluate the usefulness of SocioNet and the privacy enhancing solutions, we performed a questionnaire. 75% of the 40 participants (computer proficiency high) rated the prototype as capable of establishing new communication options, which was our general aim. SocioNet would be more likely used to establish communication channels with friends and persons of similar interest than with unknown persons (even if they are friends-of-friends). When it comes to privacy, we investigated that the loss of control over private data is felt more intensive by low and medium computer proficient participants. A mental model for digital data and data privacy might help to improve this situation.

The questionnaire also pointed out that it is not yet clear to the user whether personal information retrieved from the databases available on mobile smart devices is sufficient to perform good matchmaking. In future work, we plan to address this issue by a wider field study.

References

1. Anderson, J.Q., Rainie, L.: Future of the Internet III, Pew Internet & American Life Project (2008),
`http://www.pewinternet.org/Reports/2008/The-Future-of-the-Internet-III.aspx`

2. Arb, M., Bader, M., Kuhn, M., Wattenhofer, R.: VENETA: Serverless Friend-of-Friend Detection in Mobile Social Networking. In: WIMOB 2008, IEEE International Conference on Wireless and Mobile Computing, pp. 184–189 (2008)
3. Axup, J., Viller, S., Maccoll, I., Cooper, R.: Lo-Fi Matchmaking: A Study of Social Pairing for Backpackers. In: Dourish, P., Friday, A. (eds.) UbiComp 2006. LNCS, vol. 4206, pp. 351–368. Springer, Heidelberg (2006)
4. Belle, S.K., Waldvogel, M.: Major Domus Redux: Privacy in Mobile Social P2P Networks (2008), http://www.ub.uni-konstanz.de/kops/volltexte/2008/5495/
5. Bellotti, V., Sellen, A.: Design for Privacy in Ubiquitous Computing Environments. In: ECSCW 1993: Third European Conference on Computer-Supported Cooperative Work, pp. 77–92 (1993)
6. Chang, Y.-J., Liu, H.-H., Chou, L.-D., Chen, Y.-W., Shin, H.-Y.: A General Architecture of Mobile Social Network Services. In: ICCIT 2007: International Conference on Convergence Information Technology, pp. 151–156 (2007)
7. Chen, G., Rahman, F.: Analyzing Privacy Designs of Mobile Social Networking Applications. In: EUC 2008: IEEE/IFIP International Conference on Embedded and Ubiquitous Computing, pp. 83–88 (2008)
8. Jambo Networks, http://www.jambo.net/
9. Joly, A., Maret, P., Daigremont, J.: Context-Awareness, the Missing Block of Social Networking. International Journal of Computer Science and Applications 4(2), 50–65 (2009)
10. Kern, S., Braun, P., Rossak, W.: MobiSoft: An Agent-Based Middleware for Social-Mobile Applications. In: On the Move to Meaningful Internet Systems 2006: OTM 2006 Workshops, pp. 984–993 (2006)
11. Konomi, S., Thepvilojanapong, N., Suzuki, R., Pirttikangas, S., Sezaki, K., Tobe, Y.: Askus: Amplifying Mobile Actions. In: Pervasive 2009: Pervasive Computing, pp. 202–219 (2009)
12. Mani, M., Nguyen, A.-M., Crespi, N.: What's Up 2.0: P2P Spontaneous Social Networking. In: PERCOM 2009: IEEE International Conference on Pervasive Computing and Communications, pp. 1–2 (2009)
13. Oechslin, P.: Making a Faster Cryptanalytic Time-Memory Trade-Off. In: Boneh, D. (ed.) CRYPTO 2003. LNCS, vol. 2729, pp. 617–630. Springer, Heidelberg (2003)
14. Olson, G.M., Olson, J.S.: Human-Computer Interaction: Psychological Aspects of the Human Use of Computing. Annual Review of Psychology 54(1), 491–516 (2003)
15. Playtxt, http://www.playtxt.net/