Building Common Ground for Face to Face Interactions by Sharing Mobile Device Context

Vassilis Kostakos, Eamonn O'Neill, and Anuroop Shahi

Department of Computer Science,
University of Bath,
Bath BA2 7AY, UK
{vk, eamon}@cs.bath.ac.uk, anu.shahi@gmail.com

Abstract. We describe an application used to share context and build common ground between nearby users. Our application runs on mobile devices and allows users securely to exchange the contents of their address books. This exchange reveals only which entries are common to the two users. We explore the use of our application using both Bluetooth and NFC as an underlying technology. Finally, we present the results of a small user study we have conducted.

1 Introduction

A frequent activity amongst people who meet for the first time is the establishment, and subsequent refinement, of common ground [3]. When we meet someone we do not know, we often try to establish whom and what we have in common. This shared knowledge, referred to as common ground, is used to frame our communication. In this paper we describe a mobile application that facilitates the process of sharing and establishing common ground between people within physical proximity.

A number of similar systems have previously been developed, but we feel they are overambitious in their design; they try to replace, rather than assist, the human ability to communicate with other humans within physical proximity. Our system does not aim to strengthen the social bonds within communities, nor to provide its users with new friends; these are things that still need to be done by humans. Our aim is to assist users in building common ground by means of identifying shared context. There are of course many different elements of common ground or shared context. For our purposes in this paper, the shared context is already stored in users' address books: whom they know. Using our application, two users can identify their common address book entries.

In this paper we explore the implementation of our system with two proximity-based technologies: Bluetooth and Near Field Communication (NFC)[1]. Because of their differences, these two technologies offer distinct social affordances to users, and allow for different uses of our application. Specifically, Bluetooth systems can act as a first point of contact, while with NFC this is not the case. We also present our

[1] See http://www.nfc-forum.org

M. Hazas, J. Krumm, and T. Strang (Eds.): LoCA 2006, LNCS 3987, pp. 222 – 238, 2006.

findings from a small user study. Our results point to the perceived utility of our application, and highlight the differences in the underlying technologies as a crucial factor in shaping users' experience and use.

In Section 2 we present related work in this area, and in Section 3 we describe the motivation and theoretical background which informed the development of our system. In Section 4 we describe two different versions of our system, based on Bluetooth and NFC respectively. Here we describe the implementation process, and highlight the technical implications of our theoretical motivation. Finally, in Section 5 we discuss the results of a small user study we carried out to compare the two systems, and the feedback we obtained from users.

2 Related work

A number of systems have been developed that aim to socially engage and connect their users. Most common are online web portals such as Friendster.com and Match.com. Such systems typically allow users to upload their profile and search for others with similar profiles or specific criteria. These portals are only available online, and are thus suitable for computer-mediated communication rather than face-to-face, co-located interactions.

An interesting category of systems is based on the notion of familiar strangers [12]. One such example is Jabberwocky [15]. This application continuously scans the environment for other Bluetooth devices, and gradually builds a visual map of the familiar strangers that the user encounters. Although Jabberwocky mainly shows graphical information about nearby devices, users can gradually get a feel for the environment around them, and the people next to them. The Telelogs application [6] takes a further step in allowing for interactions between familiar strangers. This system allows profiles in the form of auditory blogs to be shared between familiar strangers. If two people encounter each other more than once, they obtain access to each other's most recent voice blog entry. This information allows strangers to gradually get to know each other. The information delivered with this system depends on the sender or broadcaster of the Telelogs. Crucially, this means that the information could potentially be irrelevant to the recipients. Additionally, users need to record new audio blogs daily in order to keep their profile up to date.

An interesting application which makes use of implicit user input is ContextContacts [16]. This application allows for presence and context cues to be shared between users over the network. ContextContacts is used between people who already know each other. Information such as location, time spent there, state of the phone (ringer, vibrator), and number of friends or strangers nearby is shared via servers over the network. This application acts very much like instant messaging applications, and is aimed at enhancing the communication between friends across distances.

A system which tries to bridge the gap between online services and local interactions is BlueAware [8]. This system runs on mobile devices and scans every 5 minutes for nearby Bluetooth devices. When it detects a new device, it sends the device's BTID to an online server. The server carries out a comparison between the two users' profiles. If there is a match, the server sends both users an alert, along with the photo of the other user, their commonalities, as well as contact information. An issue with this system is the need for establishing communication links with an online server and service. Also, the recipients of an introductory message are not informed whether or not the other user has been made aware of the receiving message, or if in fact the other person is still in their vicinity. This system, however, remains an interesting adaptation of online dating services to local situations.

The need for an online third party is overcome with Nokia's Sensor[2] system. This system allows users to broadcast their profile locally using Bluetooth. Users can actively search for Sensor-enabled phones around them, and can view others' profiles as well as engage in text-based conversation. With Sensor, users engage in direct and live interactions, but the problems of the broadcast model associated with Telelogs apply here. Also, Sensor relies on explicit input for providing an up to date profile of its user. Despite its commercialisation, Sensor does not appear to have successfully penetrated the market.

A similar system is Bluedating [2], which works by storing dating profiles on users' mobile devices and then uses Bluetooth to discover and transfer profiles found on nearby devices. All matching is performed on the mobile device therefore avoiding the need for a central matching service. Similar to Nokia Sensor, this system relies on users' explicit input for updating their profile. Additionally, the broadcast nature of this system leaves room for potential abuse by users. Finally, the system does not guarantee that both users will be aware of the matching.

Many interesting systems have been developed to date, but we feel that most of them fall short of their own expectations. A number of factors contribute to the apparent difficulty in socially engaging friends or strangers via the use of technology. These factors include:

- the complexity of the technology involved, which can act as a barrier rather than an enabler
- the sometimes irrelevant information being broadcast by users
- the potential for abuse
- the outdated information presented in users' profiles
- the possibly inconsistent levels of awareness between the users
- the social awkwardness of being introduced to a nearby person via a non-human entity.

These are issues which we have attempted to address in the design of our application. We now proceed to describe the motivation and background to our application.

3 Motivation and Background

3.1 Building Common Ground

Part of the work of getting to know someone is in determining and constructing shared knowledge, assumptions and beliefs. Stalnaker [18] coined the term common ground to include shared or mutual knowledge, assumptions and beliefs, while Clark [3] presents an extensive body of work on the construction of common ground in

[2] See http://www.nokia.com/sensor

language use. However, Clark [4] identifies language use, and its reliance on common ground, as just one example of the more general notion of a joint activity. Other examples of joint activities are playing music together, working on a shared drawing, dancing, playing games, and using technology together. Successful collaborative activities both depend on and contribute to the construction of common ground.

Clark and Marshall [5] proposed that "very often mutual knowledge is established by a combination of physical or linguistic copresence and mutual knowledge based on community membership" (p.41). Later, Clark [4] refined this proposal to two main types of evidence used in constructing common ground:

(i) evidence of common membership of cultural communities;
(ii) joint perceptual experiences and joint actions.

Evidence of common membership of cultural communities and associated assumptions (such as universality of particular knowledge within the community) leads to communal common ground, while joint perceptual experiences, joint actions and associated assumptions (such as rationality and shared inductive standards) leads to personal common ground. Personal common ground is specific common ground established amongst people who share a joint experience. However, their assumptions of rationality and shared inductive standards depend ultimately on their previously established communal common ground.

Our premise is that effectively to facilitate co-located social interaction, it is best to assist, rather than to replace, human capabilities. This is a well established HCI principle [e.g. 7]. Our fine-tuned human communication capabilities can only be hindered if we introduce cumbersome devices and mechanisms aimed at carrying out communication on behalf of humans. This is evident in the numerous systems already developed. Fundamentally, we still need to establish eye contact, body language and verbal communication [9, 13]. Technology, we maintain, should be focused on assisting where the advantages over "manual" mode are clear.

In this respect, the construction of common ground is an aspect of social interaction that may lend itself to technological assistance. The most important basis for the construction of common ground, *evidence of common membership* of cultural communities, is often difficult to establish. Every day, we implicitly and explicitly provide such evidence to others through our appearance, the ways we dress, our language and accent, and in many other ways. Yet there are no such commonly used indicators for one critical aspect of our membership of cultural communities: whom we know. Often, this evidential basis for communal common ground is built up serendipitously and we may take moments or years to discover that we have a friend in common.

3.2 Locally Sharing Address Book Information

Our application uses Bluetooth, NFC and mobile device address books as a means of locally sharing context for a number of reasons. Increasingly, through our use of mobile devices such as smartphones, we carry around with us a large body of evidence of our membership of cultural communities, in a form that is accessible by us and potentially by others. A contacts or address book on a mobile device stores details about the people we know and often includes implicit and explicit information about which cultural communities we share with them. The information stored in address books describes our family, friends, colleagues and institutions that have been meaningful enough to us that we have stored them.

Our use of mobile device address book data seeks to provide the first of Clark's [4] evidential bases of common ground: *common membership of cultural communities*. Our use of Bluetooth and NFC as the data sharing technologies seeks to provide the second: *copresent joint actions and joint perceptual experiences*. In Figure 1 we show how our system relates to the identification of communal common ground, and the generation of personal common ground.

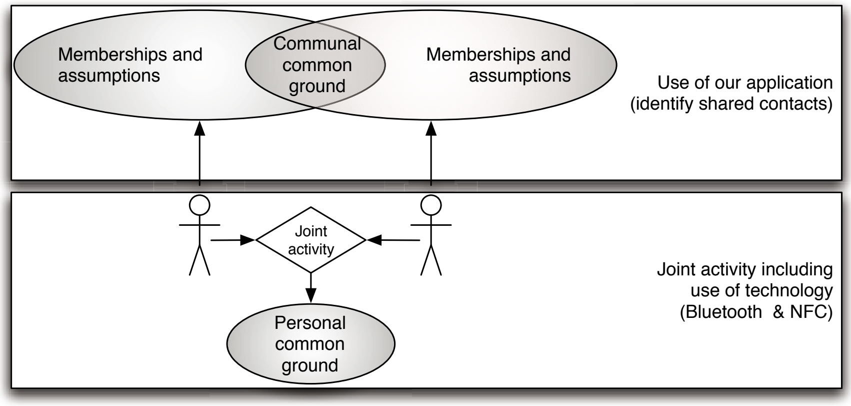

Fig. 1. Our application helps users identify their communal common ground (top half) by helping them identify whom they know in common. The copresent use of the enabling technology (Bluetooth and NFC) supports the creation of personal common ground (bottom half).

Both Bluetooth and NFC rely on physical copresence for communication – they are proximity-based, rather than location-based, communication channels – and both rely on enabling actions performed by the users. However, both the physical range of communication and the joint enabling actions are very different between Bluetooth and NFC. These differences and their influences on the utility, usability and acceptability of our application is an exciting research issue raised by this work.

There are other advantages to our choice of mobile device address books. Particularly in the case of mobile phones, address books are used extensively and frequently. Hence, address books are typically well maintained by users. By drawing on address book information, we are making use of implicit user input, reducing the burden of having explicitly to enter and update information specifically for our application. Thus, we overcome the problem of outdated profiles that seems to deter the use of similar systems.

Also, the information stored in address books (i.e. telephone numbers and email addresses) is effectively unique in identifying a person or entity. This feature lends itself to comparison and matching. Furthermore, our encryption scheme is based on this uniqueness.

Because users share common information only with others who are physically local, this is a convenient way of addressing the problems associated with a broadcast model (swamping users with irrelevant information).

Finally, we felt that this application could potentially be controversial; after all, advertising and broadcasting one's own address book is not commonplace. We are interested in developing such provocative applications as a vehicle for probing and better understanding users' attitudes towards social technology and pervasive computing.

3.3 Security and Privacy Concerns

From the outset of this research, we were aware of potential privacy concerns. In our system, we decided to address two main privacy concerns in relation to exchanging address books:

- Can others gain access to all of my address book entries?
- Even though I have a contact in common with another user, I may want to hide this fact.

The first concern relates to the fact that our application transmits the whole address during an exchange process. This raises the issue of how much of this information can be read by the receiving party. We address this concern by employing a one-way hash function using an SHA-1 algorithm (as defined in FIPS PUB 180-1)[3]. This generates a digest for each entry in the address book, which cannot (easily) be reverse engineered to retrieve the original piece of information. An exchange, therefore, involves generating digests for each entry in the address book (name, phone, email) and transmitting every digest. On the receiving end, the device generates digests for each of its local entries, and compares the local digests to the received digests. Since local digests can be traced back to their source, the receiving party can associate local information with received digests.

The result is that if both Alice and Bob have Peter's phone number, Alice will be shown only her local information about Peter (e.g. "Peter (Husband)"), which may be different to what Bob sees (e.g. "Peter (Coach)"). This encryption scheme, therefore, can reveal the common entries (such as a phone number) with another user, while displaying to each user only the information that user already had about the entry.

Another concern relates to the fact that a user may wish to hide their relationship with certain individuals. Sharing "too much" context could lead to potentially awkward, or even harmful situations. We addressed this issue by drawing on the information classification presented in [14]. Based on this work, users can classify entries in the address book as belonging to the public or private sphere.

In our system, private entries are completely hidden from all operations of our system. This means that private entries are neither transmitted nor used locally to check for matches with received digests. On the other hand, public entries are always used in the exchange process. By default, new entries are private.

[3] For the SHA-1 standard, see http://www.itl.nist.gov/fipspubs/fip180-1.htm

3.4 Technological Affordances

There are a number of technologies that could be used for carrying out the digest exchange. Such technologies include SMS, MMS, Infrared, HTTP/Web, GPRS, WiFi, Bluetooth and NFC. We decided to implement our application using Bluetooth and NFC for a number of reasons.

First, both Bluetooth and NFC are proximity-based technologies; thus, communication taking place with these technologies has to be between nearby users. This was an important feature, as we were interested in supporting the construction of common ground between users having copresent interactions. Additionally, both of these technologies support true peer-to-peer interactions, as opposed to server-based interactions. This aligns the technological interactions provided by our system more closely to the copresent interactions of users.

Despite their similarity in being proximity-based technologies, Bluetooth and NFC support very different social interactions. Bluetooth, on the one hand, allows for interacting with someone across the room or train carriage. Depending on the class of the Bluetooth device, this can be up to 10, 100 or 250 metres. On the other hand, NFC requires that the two devices are physically within 2 cm of each other. This difference in range plays a crucial role in the affordances of the technologies, and the interactions they can support. This is a dimension we were interested in exploring, and these differences were observed in our study.

With Bluetooth, two people can use our application without having established prior physical communication (in the form of eye contact, body language, or verbal communication). On the other hand, the use of NFC requires that the users and devices enter each other's "intimate zones" [10]. For this to take place, users will almost certainly have established some form of previous physical communication. Thus, although Bluetooth and NFC are both proximity-based peer-to-peer technologies, their affordances in relation to our application are very different. With Bluetooth, our system may be used without prior physical communication. In this case, communication will be between strangers. With NFC, our system almost certainly will not be the first point of contact. In this case, communication will be between people who have already communicated at least to the extent of allowing intrusion into their intimate zones.

Also, the different ranges of Bluetooth and NFC create two different models of interaction between the users. Using Bluetooth, users need verbally to negotiate and coordinate their efforts to exchange data. With NFC, users have the cue of physically touching their phones. This tangible interaction is an explicit action which synchronises both the data exchange between devices and the coordination process between the users.

3.5 Interaction Design

In addition to the restrictions imposed by technology, the interface of our system enforces certain rules in the underlying social interaction model. These rules are consistent between both the Bluetooth and NFC versions of our system. These are:

- An exchange is always two-way.
- No exchange can take place without explicit input from both users.
- The received digests are discarded after the comparison.

The first feature is used to ensure reciprocity in the social interactions. Reciprocity has been shown to have a positive effect on human-human and human-computer interaction [e.g. 17]. By requiring both users to exchange address book digests, we ensure the presence of reciprocity.

The requirement for explicit user input is used to ensure that both parties are aware of the exchange taking place. This avoids the problems inherent in systems like BlueAware where users may not be aware of the interaction taking place. Additionally, it also avoids unwanted interactions and potential privacy breaches. In the case of Bluetooth, this could be a potential threat of unwittingly broadcasting information. In the case of NFC, this could accidentally happen in situations such as in a crowded bus, where people stand close to each other and have their phones in their pockets.

Finally, by discarding the received digests, our application reflects the ephemeral nature of social interaction. This is a concern which has been shown to be of importance to users [1]. Obviously, this restriction can easily be lifted, as one could develop a similar system that actually records the received digests. These could potentially be used for future reference — for example, being alerted that the contact you just added exists in a previously received digest. Additionally, by collecting a large number of digests, one could start building up a model of the social network represented in the digests. Despite these potential uses however, we felt that the perceived ephemeral nature of social interaction is a key aspect, and so we opted to preserve it in the current version of our application. Not recording the digests also avoids potential problems of received digests becoming outdated. As noted in Section 2, our use of implicit input in the form of address book entries addresses the problem of keeping information up to date. But this is undermined if digests are kept by a receiving user since updates made in the sender's address book after the synchronisation will not be reflected in the digest.

4 The Address Book Application

Our system runs on mobile devices with J2ME, such as phones and PDAs, and allows users to encrypt and exchange address book information. This includes names, phone numbers, and email addresses stored in users' mobile devices. For our prototype, these were stored directly in our application instead of tapping into the phone's native address book. Accessing the phone's native address book was not possible across all the devices for which we were developing, but is becoming increasingly achievable as J2ME is upgraded and phones are changed. Before a data exchange takes place, our system performs a one-way encryption (digest) of every entry in the address book. This ensures that the two-way exchange can reveal only information that is common to the users. Additionally, users have the option of identifying certain entries as "Private" (as opposed to "Public") thereby withdrawing them from the exchange process.

The functionality of our system is shown in Figure 2. We developed two versions of our system - one using Bluetooth (on a Nokia 6680) and one using NFC (on a Nokia 3220 with NFC shell). Unfortunately a phone with both Bluetooth and NFC

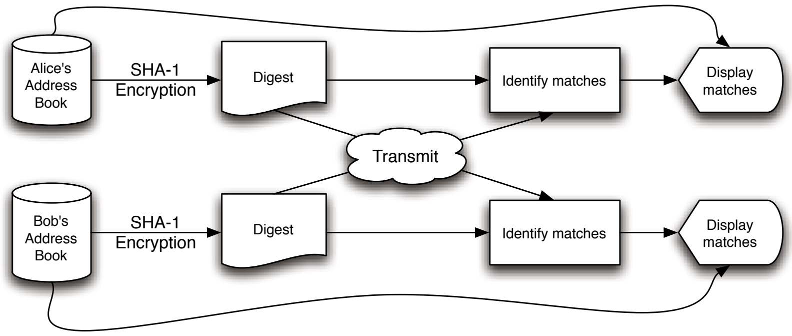

Fig. 2. Alice and Bob exchange digests of their address books. They then compare the received digests with their local digests to identify matches. Alice is then shown her local information linked to the matches, and so is Bob. The displayed information is not necessarily identical.

is not yet available. The interface functionality was the same across both systems, but each device rendered the interface components differently. This is a feature of J2ME over which we had no control.

4.1 The Encryption Scheme

We utilised the SHA-1 algorithm for generating the digests. Our implementation was based on Sam Ruby's port of SHA-1 to J2ME[4]. Our encryption scheme works as follows. Each device generates digests of all its address book entries. These digests are locally concatenated into one long string which is exchanged with the other device. Each device then generates a digest for each local entry, and searches for it in the received digest. If the local digest is found in the received digest, this means that the local entry also exists on the remote device. At the end of this process, the device displays a summary of the matched entries.

One obvious problem with this scheme is that string matching needs to be exact. For instance, a telephone number such as +1 123 1234567 would not match the number 123 1234567. This is because the digests of each number would be different. This issue can be addressed by a filter which turns phone numbers into a uniform format before encryption. The same problem applies to names. For instance, "Dr. Alice" would not match "Alice". This, however, is not such a problem with email addresses, as they tend to be recorded without variations.

A brute-force attack could decrypt the transmitted digests. This is because the full strength of the encryption algorithm is not utilised, as the input strings are actually smaller than the generated digests. Prior to encryption, each string is appended with padding bits, as described in the SHA-1 standard. The number of combinations that would have to be tried are in the range of 35^(length-of-data). Thus, a digest of a 10 digit number would require approximately 2.75e+15 comparisons. Effectively, critical information should not be shared using our application (either by not including it in the address book, or by marking it as Private).

4 See http://www.intertwingly.net/blog/2004/07/18/Base64-of-SHA1-for-J2ME

4.2 The Bluetooth Implementation

The Bluetooth and NFC versions of our application have the same hashing and matching functionality. Their differences lie in the communication protocol, and the required user actions to initiate the communication. Our Bluetooth application (Figure 3) runs as a multi-threaded application. It can serve and respond to Exchange requests from nearby peers, together with performing exchange requests on behalf of the user. Our application exposes a proprietary Bluetooth service for carrying out the address book exchange. Note that private entries are indicated with an exclamation mark.

To perform an exchange over Bluetooth, the user first selects the "Exchange" option causing the application to perform a Bluetooth inquiry scan that discovers all Bluetooth devices situated within close proximity to the user. Once discovered, all devices are listed by their Bluetooth defined names. The user can then select the desired device name to initiate the exchange process. This name identifies who the user

Fig. 3. Using Bluetooth, a user needs to activate the exchange mechanism (photos 1 to 4). The other user is alerted to the request for exchange (photo 5). If the user agrees, the phones carry out a two-way exchange of digests. Upon successful completion of the exchange, the phones present the common entries (photo 6).

will interact with. This name is customisable by the owner of the device, and sample names include "John's phone" and "Nokia 6680".

Once a connection has been established, the application determines whether the proprietary service is available on the target device; if so, an exchange is attempted causing an alert message to appear on the remote device. Essentially, this message acts as a prompt allowing a user to participate in an exchange with the requesting device; if the user accepts, a mutual exchange of the address books is performed over Bluetooth based RFCOMM channels. Upon a successful exchange, both devices display the matches.

4.3 The NFC Implementation

Near Field Communication (NFC) is an RFID based communication protocol targeted at mobile devices. A number of companies are members of the NFC Forum, and NFC-enabled devices are beginning to emerge in the market. NFC allows for communication between devices and tags with a range of approximately 2-3 cm. Envisioned applications for this technology include mobile ticketing, physical hyperlinking, secure purchasing, and service discovery.

The initial concept behind NFC was for devices to establish a trusted connection due to the physical limitation of the protocol's range. This connection would then be used to negotiate a long-range protocol, such as Bluetooth or WiFi. Thus, it was envisioned that two users could physically touch their laptops to establish a trusted WiFi connection (via an NFC negotiation), or touch two phones to establish a trusted Bluetooth connection (again via an NFC negotiation). The other proposed use of NFC was for users to touch their phones on a tag in order to receive information about an artefact or service associated with the tag. Our use of NFC for peer to peer device communication is quite different to the intended uses of NFC, and in this sense is novel.

We developed our application on a Nokia 3320 NFC-enabled phone. Development was done using the Nokia J2ME NFC SDK. Additionally we used the Nokia UI API Extension For Nokia 3220 Lights to employ the lights and vibrator of the phone as a means of user feedback. The hashing and matching functionality is identical to that used with the Bluetooth system.

The first obstacle we had to overcome with NFC was that users could not easily use their phone's keypad while touching another phone. This meant that our system could not ask for user input while an NFC communication was taking place. Additionally, we found that users could not easily read the phone's screen while touching another phone; this meant that we had to use the phone's lights and vibrator to notify users of the progress and status of the exchange.

A minor problem was the fact that when the battery level dropped below approximately 20 percent, the operating system did not allow for connections to the NFC hardware. This caused inexplicable behaviour by our software, as exceptions were raised for no apparent reason.

Another problem we faced was that, currently, NFC does not allow for a direct communication channel between devices. Existing phones have an NFC reader which can also emulate a tag. Therefore, two-way communications are made slow because to switch from receiving to sending data, a device must alter its hardware configuration from acting as a reader to emulating a tag, and wait for the partner device to read the information. This means that, effectively, two-way protocol exchanges are slowed.

One way of carrying out the two-way digest exchange would be to have two interface options: “Send information” and “Receive information”. This would make the NFC exchanges themselves very fast, but would require extra user input as well as physically separating and retouching the phones.

Our solution was to have only one interface option — “Exchange”. Both users had to select “Exchange”, and then touch the devices. At this stage, both devices would be attempting to send as well as receive information. What happens in practice is that, apparently randomly, one of the two devices succeeds in transmitting the data first. At this stage, the devices have to rediscover each other (whilst still touching) and carry out the second part of the exchange.

In short, the use of our NFC system is as follows: both users issue the exchange command. At this stage the phone lights glow orange to indicate the discovery stage. The users then touch their phones for 5-7 seconds, during which time the phone lights blink red to indicate communication. Finally, the users are notified by a vibration and green blinking lights that the exchange was successful. Any matches then appear on the phones’ displays.

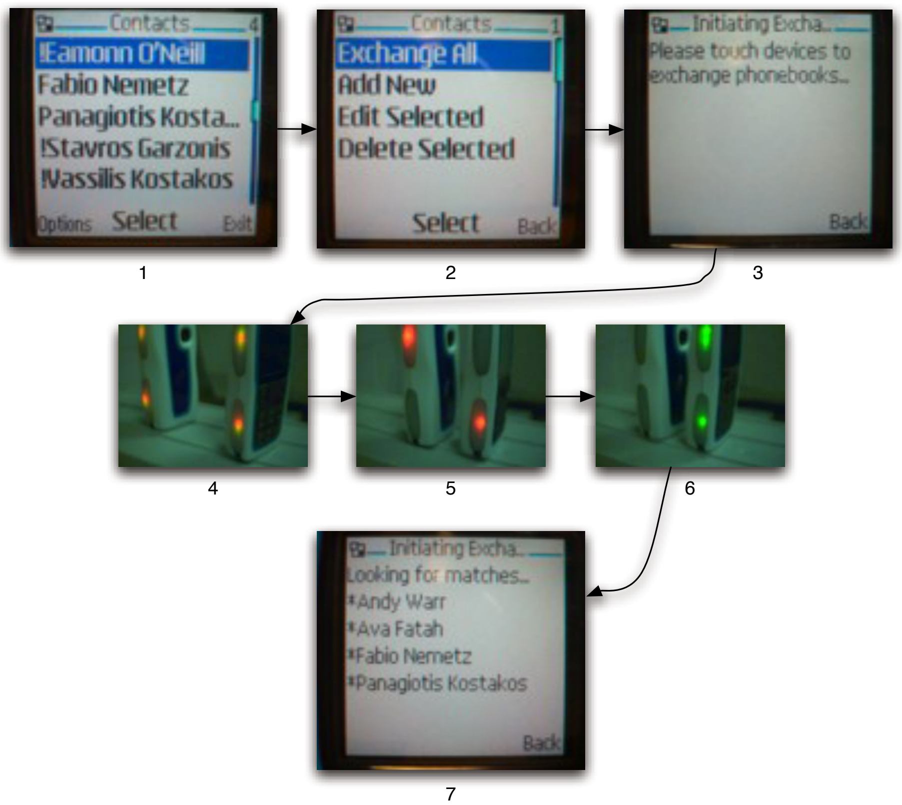

Fig. 4. Using NFC, both users need to activate the exchange mechanism (photos 1 to 3). The users place the phones next to each other, and wait for the exchange to take place (photos 4 to 6). The phones then display the common entries (photo 7).

5 Results of a User Study

We have so far carried out a limited user evaluation of our application with five participants. Our study was a probe aimed at getting some initial reactions and feedback from users. Specifically, we were interested in observing instances of joint activities, which in turn could lead to the establishment and construction of common ground.

Each trial involved one participant and one of the authors, and all participants used both the Bluetooth and NFC systems. The participants were undergraduate students at our university, aged 18-24, and they did not receive any financial compensations. All participants previously owned mobile phones for more than one year.

We gave each user a phone and explained to them how the system works. For training purposes, we asked them to enter some names, numbers and emails into our application. This helped users get acquainted with the phone itself as well as our application. We then carried out the exchange of digests. We repeated the same process with the second system. We observed users during the trials, and all users were asked open-ended questions about the systems and their impressions and attitudes.

With the NFC system we observed limited usability of the phone during NFC communication. This observation confirmed our predictions during the design process. Additionally, we had to explain to the participants that the purpose of our system was *not* to exchange phone numbers. All our participants commented that the NFC technology would be very useful for simply exchanging phone numbers. This appears to be a user requirement which currently is not effectively addressed by mobile phones.

All participants mentioned that identifying common contacts is something they often do with new acquaintances. They claimed that our system could help them in this process. Two claimed that the trial setting was not very realistic, and that they would have liked to try the system with their full address books, as well as trying it out with their friends. This suggests that in addition to exploring common contacts with new acquaintances, users would try to do the same with people they already know well. This reflects our observation that without this kind of technological aid we may take years to discover that we have a friend in common.

Participants appeared to prefer the NFC application for face to face interactions. When asked to elaborate on this, they claimed that it was easier to carry out the exchange using the NFC system because it involved fewer steps. One participant preferred the Bluetooth system, claiming that it would be useful in getting to know new people. However, one participant claimed that she would be very reluctant to respond to Bluetooth exchange requests from someone unknown. She claimed that with Bluetooth everyone could "see" her, while with NFC only friends could "see" her.

Our trials highlighted the importance of the underlying technology in establishing common ground. In Section 3.1 we identified joint experiences as a primary basis for the construction of common ground. Our observations suggest that NFC provides a much stronger joint experience because of the physical act of touching the phones. This is symmetric between users, and they receive the same feedback from the phones. With Bluetooth, the joint experience is not so strong; Bluetooth technology imposes a request-reply model, which makes the experience asymmetrical. Furthermore, there is little or no physical interaction using Bluetooth.

From our discussions with participants, we conclude that both systems can be useful in certain situations, their usefulness relating to the affordances and limitations of the two technologies. The choice of Bluetooth or NFC for exchanging address books depends on the type of experience that a user wants. Bluetooth will be preferred in situations where the user wants to meet or "discover" someone new. Another potential benefit of Bluetooth is that it does not give away strong physical cues, so users seeking to remain "hidden" will prefer Bluetooth. NFC may be preferred if the users are having a face to face conversation and are close enough to touch their phones. Additionally, the joint physical experience and ease of interaction when using NFC makes it preferable to use when the users are very proximate and have already established the common ground necessary to permit intrusion into one's intimate zone of very close proximity.

Crucially, however, the technology itself has an effect on the joint action experienced by users. NFC provides a much more engaging physical experience, which is reinforced by the symmetry of users' physical actions. This fosters the establishment of common ground. Conversely, Bluetooth's weak and asymmetrical physical user actions contribute less to the construction of common ground. In Table 1 we provide a summary of the lessons learned from the evaluation of our system.

Table 1. Lessons learned from our evaluation of the address book application

Bluetooth	NFC
• Could be useful for getting to meet strangers	• Limited usability when using the phone
• Users reluctant to respond to requests from unknowns	• Participants initially thought the system would exchange numbers
• Does not give away physical location of user	• Preferred for face to face interaction
• Weak joint experience	• Strong joint experience
• Request - reply model	• Symmetric model

6 Conclusions and Ongoing Work

In this paper we describe a system that enables the sharing of context between users in physical proximity. Drawing on our survey of existing systems, we identified a number of problems which we addressed in our design. We utilise users' address books as the source of context. Using our application, two users are made aware of the common entries in their address books. This informs the users of part of their shared context and reveals a critical aspect of their communal common ground. We have implemented our system with two proximity-based technologies: Bluetooth and NFC.

Our user study suggested a preference for NFC over Bluetooth for interactions with friends. This is due to a combination of the affordances of each technology. NFC offers synchronous reciprocity – making the same interface actions at the same time, simultaneously reaching out to each other, getting the same kind of feedback at the same time. NFC also requires that the users feel comfortable with coming into each other's intimate zones of very close proximity. Bluetooth interaction is less synchronous and less reciprocal and requires no intimate proximity or tangible interaction. With Bluetooth you may not even be able to see or hear the other user.

Conversely, our user study suggested a preference for Bluetooth over NFC for interactions with strangers. In this case, the very same affordances of the technologies make Bluetooth more appropriate than NFC to supporting the social processes involved. Strangers typically do not appreciate our intrusion into their intimate zones.

Interesting distinctions appeared in relation to our theoretical motivations of supporting the construction of common ground through evidence of shared community membership and joint actions and experiences. The mutual identification of common contacts was intended to provide users with evidence of shared community membership. This is effective in the face to face situation (required by NFC and possible with Bluetooth) partly because the users are likely already to have some established communal common ground that has brought them together in the first place. It is also effective in a face to face situation because the users enjoy mutual knowledge that the contacts are common to both users. In other words, each user not only knows that he shares contacts with the other, copresent user. In addition, he knows that the other user knows that they share these contacts, and so on *ad infinitum*. This mutual knowledge is the cornerstone of common ground [4, 11, 18].

In contrast, it can be less effective with Bluetooth when the users are not face to face, since the users may be completely unknown to each other and therefore lack previously established communal common ground. It is also less effective when users are not face to face since they may not know with whom they have established a Bluetooth connection. In this case, each user simply knows that he has common contacts with someone in reasonably close proximity. He has no knowledge of which nearby people actually have the common contacts. In turn, there can be no mutual knowledge, so a key component of common ground is missing.

Our system has taken into account issues raised by previous "social software" applications. Our user study has suggested some user preferences for one technology or the other depending on the situation and user desires, and indicates that users may find our system useful, although an extensive evaluation study is required to make any more definitive statements. We are currently planning such a study. We are interested in exploring the use of our system in a more realistic environment, where users are shown actual matches from their own address books. This would allow us to assess the impact of actual common ground between two users of our system.

Another dimension we wish to explore is a comparison of the use of our system between friends versus new acquaintances versus strangers. We are interested in identifying situations were two friends or two strangers will feel comfortable enough to carry out a phonebook match. Such an evaluation will have to take place in the field, in a setting such as a cafeteria or restaurant. We also wish to explore further the impact of the two different technologies on the use of our application, and gain a better understanding of the strengths and weaknesses of both Bluetooth and NFC in relation to face to face and proximate communication and interaction.

Finally, the address book application can be augmented to handle additional types of information. For instance, by including company or university names, our system would indicate that the two users know people from the same organisation.

Furthermore, our matching system can be adapted to handle different types of data which can also serve as indicators of common context. For example, we can utilise schedule and calendar data to identify common free slots between users. Another example would be to identify common preferences, common Internet bookmarks or music that both users listen to.

Acknowledgements

The authors' research is funded by the UK Engineering and Physical Sciences Research Council grant EP/C547683/1 (Cityware: urban design and pervasive systems). We thank Vodafone Group R&D and Nokia Insight & Foresight for their support of this work. We also thank Stavros Garzonis, Andy Warr, Kharsim Al Mosawi, Tim Kindberg and Danaë Stanton Fraser.

References

1. Adams, A. and Sasse, M. A. (1999). Privacy Issues in Ubiquitous Multimedia Environments: Wake Sleeping Dogs, or Let Them Lie? In proceedings of INTERACT 1999, pp. 214-221.
2. Beale, R. (2005). "Supporting social interaction with the smartphone – designing pervasive systems", IEEE Pervasive Computing, 4(2): 35-41.
3. Clark, H.H. (1992). Arenas of language use, Chicago, University of Chicago Press.
4. Clark, H.H. (1996). Using language, Cambridge, Cambridge University Press.
5. Clark, H.H. and Marshall, C.R. (1981). Definite reference and mutual knowledge. In A.K. Joshi, B.L. Webber and I.A. Sag (eds) Elements of discourse understanding, Cambridge, Cambridge University Press, pp. 10-63.
6. Davis B. and Karahalis, K. (2005). Telelogs: a social communication space for urban environments. In proceedings of the 7th interantional Conference on Human Computer interaction with Mobile Devices & Services (MobileHCI '05), pp. 231-234.
7. Dix, A., Finlay, J., Abowd, G. D. and Beale, R. (2003). Human-computer interaction. 3rd Edition, London, Prentice Hall Europe.
8. Eagle, N. and Pentland, A. (2005). Reality mining: sensing complex social systems. Journal of Personal and Ubiquitous Computing, December 2005, pp. 1-14.
9. Grayson, D. M. and Monk, A. F. (2003). Are you looking at me? Eye contact and desktop video conferencing. ACM TOCHI, 10(3): 221-243.
10. Hall, E. T. (1969). The hidden dimension. Man's use of space in public and private. Bodley Head, London.
11. Lewis, D.K. (1969). Convention: a philosophical study, Cambridge, MA, Harvard University Press.
12. Milgram, S. (1977). The individual in a social world: essays and experiments. Reading, Mass.: Addison-Wesley Pub. Co.
13. Nardi, B. (2005). Beyond bandwidth: Dimension of connection in interpersonal interaction. The Journal of Computer-supported Cooperative Work, 14: 91-130.
14. O'Neill, E., Woodgate, D. and Kostakos, V. (2004) Easing the wait in the Emergency Room: building a theory of public information systems. In proceedings of the ACM Designing Interactive Systems (DIS '04), Boston, MA., pp. 17-25.
15. Paulos, E. and Goodman, E. (2004). The familiar stranger: anxiety, comfort, and play in public spaces. In proceedings of CHI '04, pp. 223-230.

16. Raento, M., Oulasvirta, A., Petit, R., Toivonen, H. (2005). ContextPhone - A prototyping platform for context-aware mobile applications. IEEE Pervasive Computing 4(2): 51-59.
17. Salvador, T., Barile, S., and Sherry, J. (2004). Ubiquitous computing design principles: supporting human-human and human-computer transactions. In Extended Abstracts of CHI '04, pp. 1497-1500.
18. Stalnaker, R.C. (1978). Assertions. In P. Cole (ed.) Syntax and Semantics 9: pragmatics, New York, Academic Press, pp. 315-32.