

Disseminating Trust Information in Wearable Communities

JAY SCHNEIDER, GERD KORTUEM, JOE JAGER, STEVE FICKAS, ZARY SEGALL

Department of Computer and Information Science, University of Oregon, Eugene, OR 97403, USA

Email: {jay,kortuem,jager,fickas,zs}@cs.uoregon.edu

Abstract: This paper describes a framework for managing and distributing trust information in a community of mobile and wearable computer users. Trust information in the form of reputations are used to aid users during their social interactions with the rest of the community.

Keywords: *Wearable computing, social networks, social interaction, trust.*

Introduction

In our modern world, the use of communication technologies like phone, fax and email has become commonplace. Despite this fact, most social interactions between individuals still occur when we meet people face-to-face.

Many of our daily interactions are actually the result of a chance encounter, i.e. a situation in which we meet someone unexpectedly, for example in a hallway or an elevator. In most cases, the majority of the people we encounter every day we don't know and have never met before; however, some are familiar. Any encounter with another person, friend or stranger, is a chance for striking up a conversation and for exchanging information. Chance encounters play an important part in

our social life and they are vital for effective collaboration in the work place and for the coordination of work activities [1,2].

Mobile devices such as wearable computers and PDAs can help us form and maintain cooperative and interdependent relationships with the people we meet. Being small and unobtrusive, they have become our constant companions that are ready and available wherever we go. As we use them to store personal information about ourselves and others, our mobile companions become something more than just communication devices, they become our trusted confidants.

With the appearance of short-range wireless network technology like Bluetooth [3] our personal mobile devices gain the ability to assist us in our daily social encounters. This is the world of wearable communities.

Wearable Communities [4,5] is a project that investigates the use of cutting-edge mobile and wearable computing technology to assist people in the exchange of information during face-to-face social interactions in the real world: when people meet on the way to the office, in the elevator, or at the grocery store.

These social interactions are built around trust. We trust our friends to honor their word, we trust a doctor to give us medical advice and we often trust complete strangers to help us when we are lost or need assistance. Even more so, members of a wearable community need to be able to reason about trust, to facilitate their social interactions.

This leads to the question of how to evaluate the trustworthiness of a wearable community member. In this paper, we propose an approach based on user reputations. In the following, we describe a framework for managing trust information, i.e. reputations, in a decentralized manner that mimics the flow of personal recommendations in the real world.

Trust in Wearable Communities

Wearable Communities were first discussed in [5] to describe a protocol-based negotiation system that takes advantage of chance encounters between rational wearable computer users with the goal to trade errands from their to-do list. This system uses game theoretic techniques to maximize the benefits to the trading individuals and to the community [6].

As an example, let's consider what happens when two members of a wearable community meet. Let's assume the first member's to-do list contains the following two tasks: dropping off mail at the post office and making copies

at the local copy center. The second member's to-do list contains similar tasks: buying stamps at the post office and returning books to the public library. Using the negotiation protocol described in [5] these two users might optimize their tasks in a way that one of them goes to the post office to drop off the mail and buy stamps, while the other returns the library books and make copies.¹ This would lead to a net gain in efficiency for both parties and the community as a whole.

The trading of tasks in the described manner raises a number of trust related issues. For example, people might cheat by either not telling the truth about their task list or by not performing a task they received from someone else. In the real world, people use reputations to determine if and how to negotiate with other people. The difference between wearable communities and agent-based communities is the irrationality of the human partner in a wearable community. Actions in wearable communities are decided not solely by completely rational personal agents, but in a joint decision making process of human user and personal agent.

Related Work

The traditional solution to managing trust information is based on a centralized

¹ The optimal task distribution depends on the exact location of the encounter and the locations associated with the various tasks (post office, etc.). See [5] for a more detailed example.

reputation server. For example, the Internet auction site EBay.com uses a centralized reputation server to provide trust information (reputations) about potential buyers or sellers in their open market.

The centralized approach has many shortcomings. The most significant is its vulnerability to falsified information. A user with 10,000 good reports and only a relatively small number of bad reports looks like a legitimate trader unless the 10,000 positive reports have all been falsified.

Another problem with centralized reputation servers is the ability of anyone to know their exact reputation. This enables a mischievous trader to know when to “flush” his or her old identity and to start over with a clean slate.

Finally, there is the trustworthiness issue of a centralized reputation server. A centralized trust approach places a great deal of sometimes unsupported trust in the security of the centralized server: Can an on-line auction-house’s trust server trust information be trusted when they themselves are the buyers or sellers? What about the reputations provided regarding their advertisers? Can the security of their trust server be trusted?

The ineffectiveness of a centralized trust server is evident by the almost 10,000 cases of fraud relating to on-line auctions reported in 1999 to the National Consumer League. The National Consumer League also posts the following warning regarding online auction sites: *“Look at the auction site's feedback*

section for comments about the seller. Be aware that glowing reports could be "planted" by the seller”. [7]

Another approach to handling trust is the decentralized model used by PGP [8]. The PGP system does not rely on a centralized reputation server but it allows users to vouch for one another. For example: user A vouches for user B, and user B vouches for user C; thus someone who trusts user A will also trust user C based on the chain of recommendations. This is the basic transitive trust property that decentralized trust servers are based upon.

Abdul-Rahman and Hailes [9], and Marsh [10] have proposed trust models based up social models of interactions and real world social properties of trust. In both cases, the goal is to develop a formal model of trust while our main focus is the dissemination of trust information during chance encounters.

Disseminating Reputations in Wearable Communities

We have developed a decentralized reputation framework that uses opportunistic physical encounters to propagate trust data. Each member in the wearable community will store a database of reputation information on everyone with whom they have negotiated personally or about whom they have received negotiation information. This reputation database has the following structure:

- *userid*: unique identifier of the user the reputation entry is about.

- *personal opinion value*: personal opinion about user *userid* based on personal encounters.
- number of personal encounters with that person
- *community reputation value*: summarized opinions of other users about user *userid*.
- number of users who contributed to the community reputation value.

The opinion values range from -2.0 to 2.0 with 0.0 corresponding to no information.

Whenever members of a wearable community completes a negotiation and can evaluate how well their negotiating partner fulfilled their part of an agreement, they record their opinion of their negotiation partner in their local reputation database. This will be propagated whenever a social encounter in the wearable community occurs and local reputation databases are exchanged.

This exchange allows both parties to update their databases after reasoning about the information provided. Providing reputation information has the effect of telling every person you encounter “here are my feelings about the people I’ve traded with and here’s what I’ve been told about them.” This information may then be passed on during subsequent encounters and will eventually spread throughout the entire wearable community.²

² Exchanging reputations in Wearable Communities is similar to the data sharing approach in the Liveware system [11]. Like Wearable Communities, Liveware is

Reasoning about and applying reputation information involves several steps:

1. If there has been a recent exchange with the same user, then we assume that the information will only reinforce old views and should be discarded. This prevents any specific user from gaining too much weight.
2. If the user provides personal opinion values that are significantly divergent from the values of our own personal encounters, then the information provided is suspect and will be disregarded.
3. Otherwise, the values from the other users personal opinion and community opinion will be averaged in to the local users community information values. It is important not to base any reasoning on the number of recommenders or the number of encounters, as this could allow users to have a stronger “voice” in recommendations.

This system solves the key problem of the centralized reputation server as each person can only provide a single positive or negative feedback about any other individual in a category. To get 10,000 positive comments about an individual would require 10,000 different people to provide positive feedback.

based on the idea of information transmission as an unobtrusive side-effect of interpersonal communication during chance encounters. However, Liveware’s emphasis is on data consistency while reputations in Wearable Communities necessarily can be inconsistent.

This is as opposed to the centralized server where one person can say positive things 10,000 times.

The problem of an individual knowing their exact status in the eyes of the community also vanishes under this system. It is replaced with only a general knowledge of ones reputation. The distributed reputation server also solves the need for trust in a foreign server. Everyone maintains their own information and if part of the databases suffers due to negligence or intentional corruption it will be corrected by the valid information in the rest of the community.

By using social interactions to trade entire trust set data we gain the advantage of a rapid propagation of information from the numerous encounters in an environment, yet we maintain the advantages of a system that mirrors the way real world reputations spread – by word of mouth during daily encounters. In addition, a decentralized system does not suffer from the issues that occur with traditional reputation servers.

Current Status and Future Work

We are using a dual approach for investigating trust issues in Wearable Communities. First, we ported the task-exchange mechanism described in [5] to Handspring Visors and extended it to exchanging trust information from user to user during task negotiations as outlined above. Second, we have modified the

WALID simulator from [5] to examine how users' reputations spread throughout a wearable community.

Our future work involves determining the exact weights and values for the trust exchange system described in our approach to trust. We are comparing experimental results from WALID simulations with the actual flow of reputations between users in the real world.

References

1. Whittaker S., Frohlich D. and Daly-Jones O. Informal Workplace Communication: What Is It Like and How Can We Support It? In Proceedings of CHI 94, ACM Press.
2. Belotti V. and Bly S. Walking Away from the Desktop Computer: Distributed Collaboration and Mobility in a Product Design Team. Proceedings of CSCW '96, ACM Press
3. Bluetooth SIG home page www.bluetooth.com
4. Kortuem G., Segall Z., Thompson Th. G. C. Close Encounters: Supporting Mobile Collaboration through Interchange of User Profiles. In: Proceedings 1st International Symposium on Handheld and Ubiquitous Computing (HUC 99), 1999, Karlsruhe, Germany.
5. Kortuem G., Schneider J., Suruda J., Fickas S. Segall Z. When Cyborgs Meet: Building Communities of Cooperating Wearable Agents. In: Proceedings 3rd Int. Symposium on Wearable Computers (ISWC99), Oct. 1999, San Francisco.
6. Schneider J., Suruda J., Fickas S. Modeling Wearable Negotiation in a Opportunistic Task Oriented Domain. In: Proceedings 3rd International Symposium on Wearable Computers (ISWC 99), 1999, San Francisco.
7. National Consumer League Web Site: www.natlconsumersleague.org
8. Zimmermann P. The Official PGP User's Guide, MIT Press, 1995.
9. Abdul-Rahman A., Hailes S. Supporting Trust in Virtual Communities. In: Hawaii Int. Conference on System Sciences 33, Maui, Hawaii, January 2000.
10. Marsh S. Formalising Trust as a Computational Concept. Ph.D. Thesis, University of Stirling, 1994.
11. Thimbleby H., Greenberg S., Witten I.H., Coulouris G. F. Liveware: A New Approach to Sharing Data in Social Networks, International Journal of Man-Machine Studies, 34(3), pp337-348, 1991.