

# Socializing in the Mist: Privacy in Digital Communities

Jalal Al-Muhtadi<sup>1</sup>, Roy Campbell<sup>1</sup>, Apu Kapadia<sup>1</sup>,  
M. Dennis Mickunas<sup>1</sup>, Prasad Naldurg<sup>1</sup>

<sup>1</sup>Department of Computer Science, University of Illinois at Urbana Champaign,  
1304 W. Springfield Ave., Urbana, IL 61801.  
{almuhtad, rhc, akapadia, mickunas, naldurg}@uiuc.edu

**Abstract.** Ubiquitous computing with its ability to provide anytime, anywhere, and any platform access to services promises to revolutionize the way we interact, collaborate, and socialize with other people. While many ubiquitous tools for online collaboration, teleconferencing, and instant messaging exist, they often overlook and ignore privacy issues. We argue that privacy is an essential element in any collaboration or interaction tool, particularly in ubiquitous computing environments. Embedded sensors may be planted at every corner, in effect, creating a distributed surveillance system. We describe Mist, a protocol that can be used to provide an infrastructure for ubiquitous and private communication. We describe how Mist can be used to create digital communities where users can interact in an anonymous fashion.

## 1 Introduction

Ubiquitous computing promises to revolutionize the way we interact with computers, humans, and the surrounding physical spaces. In the *Gaia* project [1][2], we define a generic computational environment that integrates physical spaces and their ubiquitous computing devices into a programmable computing and communication system, called an *Active Space*. These technologies promise to boost productivity through seamless interactions, and allow anytime, anywhere access to applications and services and the construction of smart rooms and buildings. Ubiquitous computing has the potential to enable new generations of integrated services and multimedia applications. We believe that tools for online collaboration, instant messaging, chatting, and electronic socializing will be some of the most appealing and valuable applications for ubiquitous computing environments. People are fascinated by tools that allow them to communicate, socialize, and collaborate in effective ways in a manner that is no longer bound by time or location barriers. The various smart devices, sensors, and displays that populate an Active Space enhance such applications greatly. Instead of merely capturing the ongoing communication, a ubiquitous environment will be able to capture ambient effects, and achieve telepresence or simulation of physical embodiment. These tools allow leverage of inter-personal interactions and subsequently, promote diversity, tolerance, cultural awareness, and racial understanding.

However, many research projects try to make ubiquitous computing environments more active and “intelligent” by populating them with large numbers of embedded sensors that are able to identify and track users through the devices they carry or wear. These technologies severely threaten the privacy of users. The lack of location privacy when engaging in online collaboration hinders the system’s anytime, anywhere access capabilities. Further, while several research efforts tackle many social and collaborative aspects of ubiquitous computing, their proposed solutions come at the cost of personal privacy. Overlooking privacy issues, particularly in a ubiquitous computing environment, can transform the surrounding environment into an electronic stalking or surveillance system. We argue that all extensions or enhanced services introduced into these environments should be privacy-aware [3][4][5]. We also argue that in many scenarios, there is a strong demand for an effective, privacy-preserving method for socializing and interacting with others.

We describe a protocol that allows netizens, or “ubizens” to utilize ubiquitous computing services to socialize and interact while preserving their privacy. In effect, we create a virtual “mist,” in which people can utilize ubiquitous computing facilities and socialize while keeping their identities and location hidden.

Since the term *privacy* is often overloaded to mean different things, in this paper we use it to refer to two different things:

- *Location privacy*: Neither the system, nor other users of the system will be able to know the exact physical location of a user unless that user decides to disclose such information or if another person physically sees that user at that location.
- *Identity privacy*: Neither the system, nor the users of the system will be able to know the exact identity of a user unless that user decides to disclose such information (i.e. the user is anonymous).

The remainder of this paper is divided as follows. Section 2 talks about the importance of privacy. Section 3 describes Mist, a privacy-preserving communication protocol augmented with identity privacy. Section 4 describes our privacy-preserving socializing scheme. In Section 5, we discuss our implementation. Section 6 talks about related work. We conclude in Section 7.

## 2 The Need for Privacy in Digital Communities

An individual’s right to privacy is enshrined in the Universal Declaration of Human Rights that states: “No one shall be subjected to arbitrary interference with his privacy, family, home, or correspondence, nor to attacks upon his honor and reputation. Everyone has the right to the protection of the law against such interference or attacks [6].” We believe that this right extends to person-to-person communication in ubiquitous computing environments as well. In the context of Active Spaces, we define a *digital community* as a gathering of individuals across different administrative domains with an intention to socialize. These digital communities may use the Internet as the underlying communication infrastructure to link their users together. Extending the notion of ubiquity to encompass social

interactions, applications similar to Internet chat and bulletin boards will foster social interactions among participants by allowing people to communicate freely.

## **2.1 Socializing and Digital Communities**

We believe that socializing in ubiquitous computing environments will become immensely popular. The pervasive nature of ubiquitous computing technology will make it easier for people to keep in touch with each other. This trend will mirror what is happening in the context of the Internet today, exemplified by the proliferation and ubiquity of applications such as instant messaging, chat rooms, bulletin boards and email lists. In this sense, we believe that ubiquitous computing will influence the social revolution started by the Internet, and create a “global village” by putting more people in touch with each other across the world, and facilitating exchange of ideas and opinions among people from diverse backgrounds.

To many people, existing Internet-based digital communities have become virtual support groups where they freely discuss their thoughts and feelings. Studies have shown that people feel more comfortable in these forums to voice their concerns and problems, counting on their anonymity to overcome their shyness. In many cases, people have come to rely on their digital community to act in place of other supportive relationships. Users seek counsel from each other providing valuable therapy. Many substance-abuse rehabilitation programs have set up support groups [7] over the Internet. There are even groups to help people survive graduate school, deal with job and relationship problems, physical and emotional abuse, as well as financial, legal and tax problems.

## **2.2 Privacy Concerns**

In recent years, pedophiles and stalkers have used Internet chat rooms to get children and even adults to reveal addresses or phone numbers, leading to violent acts of physical and emotional abuse [8]. Such examples only amplify the need for stricter control over a user’s privacy in the context of ubiquitous computing. In many cases, digital communities are the only available outlets for individuals to voice their opinions and seek comfort in the company of other individuals. Anonymity and privacy play an important part in motivating discussions in these communities.

Many pervasive computing applications rely on infrastructure support to track users and services to make the experience of computing and communication transparent to the users. However, without adequate safeguards, the location and other private information about a user can become widely available to all users in the Active Space.

Protecting the privacy of an individual in this setting becomes extremely important, especially because these interactions expose users to emotional and physical abuse. The need to safeguard a naïve user against these types of attacks and exposures becomes acute, failing which it can turn an Active Space into a surveillance and monitoring system that can be exploited by malicious users to cause greater harm. Additionally, in extreme cases we would like to provide a legal recourse that links the

actions of an offender to his or her identity and location. This would prevent the misuse of a privacy preserving system by malicious groups such as terrorist groups and pedophiles.

### 2.3 Why Security is not enough

Existing security mechanisms, in the context of digital communities, do not address privacy issues adequately. Authentication and access control can restrict who can participate in a digital community, but cannot provide identity privacy. Secure multicasts using group keys and encryption cannot prevent legitimate members from attacking the privacy of their fellow members because the content of messages exchanged cannot be controlled. Users may inadvertently reveal private information even if the communication channels are secure. We argue that in digital communities, we need to strike a balance between privacy and security, depending on the context.

Instead, in the next section, we describe a privacy-preserving layer called Mist that forms the backbone of communication in these applications. This layer provides location privacy to the users of the system, in addition to pseudonymity. Attackers masquerading as legitimate users cannot deduce the physical location or the real name of other people in the community. However, our system provides mechanisms to trace back attackers or offenders who engage in illegal activities. In order to prevent users from revealing their location and name information accidentally, we believe that educating users about these risks will be an important component of any solution. In Section 5 we also discuss the design of special agents that can detect and warn users when they inadvertently reveal personal information.

## 3 Introducing Mist

In previous work, we introduced Mist [4] a general communication infrastructure that preserves privacy in ubiquitous computing environments. Mist facilitates the separation of location from identity. This allows authorized entities to access services while protecting their location privacy. We introduce the notion of identity privacy in this paper. Here, we just give a brief overview on how Mist works. Mist consists of a privacy-preserving hierarchy of *Mist Routers* that form an overlay network, as illustrated in Figure 1. This overlay network facilitates private communication by routing packets using a *hop-by-hop, handle-based routing* protocol. We employ public key cryptography in the initial setup of these handles. These techniques make communication infeasible to trace by eavesdroppers and untrusted middlemen.

A handle is an identifier that is unique per Mist Router. Every incoming packet has an “incoming handle” that is used by the Mist Router to identify the next hop to which to forward the packet. The incoming handle is replaced by an outgoing handle before the packet is transmitted to the next hop. This hop-by-hop routing protocol allows a Mist Router to forward the packet to the next hop, while hiding the original source and final destination. In effect, this process creates “virtual circuits” over which data can flow securely and privately. More details on how these virtual circuits are established and used can be found in [5]. Mist Routers keep a log of handles as

audit trails to trace back users in the case of illegal activity. This is not trivial and requires the coordination of all Mist Routers along the path. This logging information can only be disclosed upon request from law enforcement agencies. At the same time, we claim that it is infeasible for an intruder to gain access to all these logs. This trace back provides the location of the offender. However for tracing the identity, we rely on the surveillance logs of the Active Space, if available. Since these surveillance mechanisms do not interact with the communication infrastructure, location and identity privacy trace back mechanisms are disjoint.

Mist introduces “Portals” that are installed in the ubiquitous computing environment. These Portals are devices capable of detecting the presence of people and objects through the use of base stations or sensors. However, they are incapable of positively identifying the users. To effectively hide a user’s location, we introduce a special Mist Router referred to as a “Lighthouse.” A user registers with this Lighthouse, which allows packets to be routed to and from the user. The Lighthouse of a user exists at a “higher level” in the hierarchy, high enough not to be able to

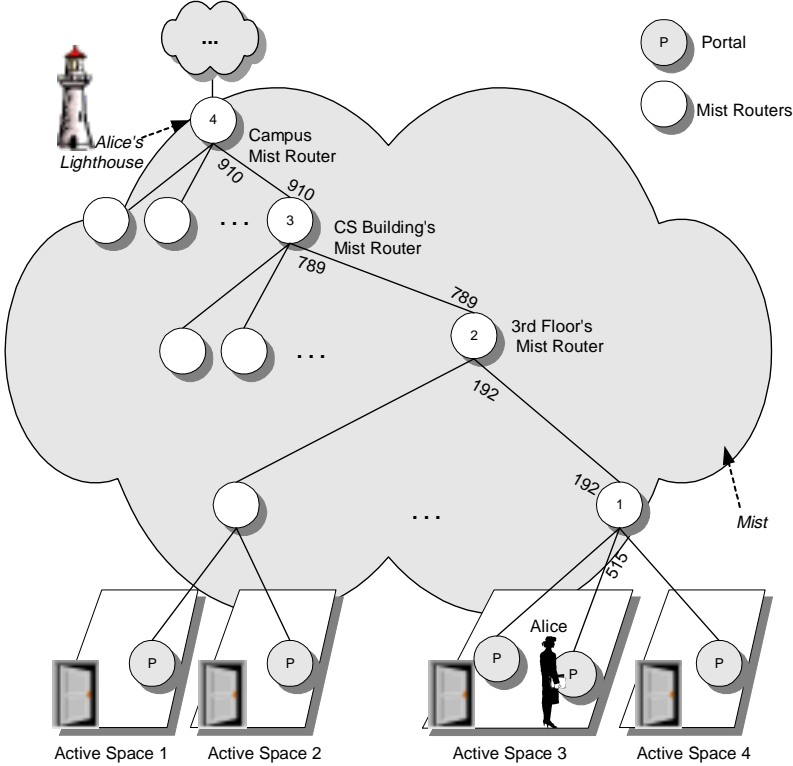


Fig. 1. The Mist communication protocol.

deduce the actual physical location of the user. However, the Lighthouse is kept in the dark about the actual physical location of the user (thanks to the hop-by-hop routing protocol). The term Lighthouse is used here, because this special Mist Router aids in navigating packets to its agents much like a conventional “lighthouse” that aids in marine navigation, particularly on “foggy” nights.

To illustrate, in Figure 1, Alice, who is in Active Space 3, is detected by the Portal in that space. The Portal only detects Alice’s badge ID (or other information embedded into other devices that Alice is carrying or wearing) however, this information alone is insufficient to indicate that this is actually Alice. The campus Mist Router is designated as Alice’s Lighthouse. A secure channel between Alice’s devices and her Lighthouse is established, going through the Portal, node 1, node 2, node 3, and finally node 4. To prevent private information from leaking, encryption is employed. The numbers over the links shown in the figure represents the handles. As depicted, the handles are valid only over a single hop. The intermediate nodes translate an incoming handle to an outgoing one (e.g. Mist Router 1 in the figure translates the incoming handle 515 to outgoing handle 192). Thus, intermediate Mist Routers can only route to the next hop correctly, but do not know the actual destination or source. Mist distributes the trust to better preserve the privacy. Only if enough intermediate Mist Routers collude, can the true location of Alice be found. Note that in the example, Alice’s Lighthouse can only infer that Alice is located somewhere within the campus. Mist provides a customizable level of privacy. A user can enjoy better location privacy if he or she chooses a Lighthouse that is higher in the hierarchy, e.g. choosing the campus Lighthouse as opposed to the CS building Lighthouse. Since users can register anonymously with Portals, their anonymity is preserved.

## 4 Socializing in the Mist

So far we have motivated the need for digital communities that preserve the privacy of their members. We have also briefly explained how Mist can be used to achieve privacy-preserving communication. In this section we show how the Mist framework can be used to build privacy preserving digital communities. We first introduce the concept of digital “masks” and then discuss how communities can be built using Mist. We discuss authentication mechanisms for restricted communities. Finally we discuss privacy monitors that warn users if they are about to voluntarily disclose private information.

### 4.1 Digital Masks

In a previous section we saw that users can register with Lighthouses that are lower or higher in the hierarchy. A Lighthouse that is higher up in the hierarchy offers greater privacy. We draw an analogy between a user registering with a Lighthouse, and a person hiding behind a mask. As we can see in Figure 2, some masks are better than others because they hide a person more effectively. Hence a user, who is registered with a Lighthouse higher in the hierarchy than another user, has a “better Mask” than

the other user. In Figure 2 we can see that when Alice is registered with the Campus Lighthouse, her Mask is much better than when she is registered with the 3rd floor Lighthouse. We also use this terminology to directly indicate the level of the Lighthouse a user is registered with; for example, a user has a “Campus Mask” if he or she is registered with the Campus Lighthouse.



**Fig. 2.** Digital Masks.

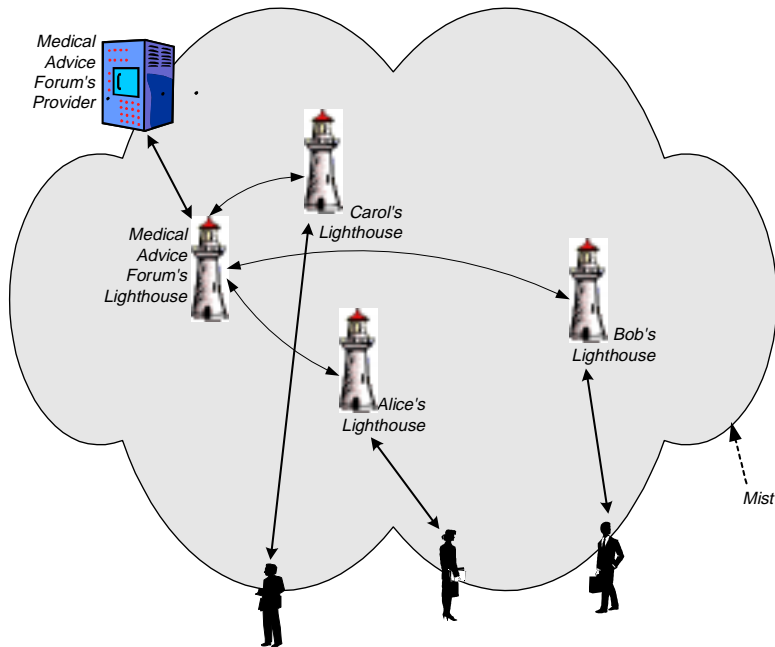
#### **4.2 Mistified Communities**

A “Mistified” community is an electronic chat forum that is built over the Mist infrastructure. As a result, all members of this community are given immunity against identity and location disclosure. Neither the Mistified community nor the Mist routers themselves can determine the identity and location of the members. No entity in the system can “peek behind” a member’s Mask.

A Mistified community may want to hide its own location to protect itself from groups opposed to its activities. Since Mistified communities are built over the Mist infrastructure, they are also Masked. When a member Alice wants to enter a community such as the “Medical Advice Forum,” she notifies her Lighthouse. The Lighthouse then looks up the Lighthouse of the community and establishes two-way communication with the community’s Lighthouse. Communication between Alice and the Medical Advice Forum now takes place through Mist, which is privacy preserving. Since communication takes place through both the Lighthouses, both Alice and the Medical Advice Forum are Masked from each other. All communication between members and the forum are broadcast to the other members by the Mistified community, similar to any well known chat implementation (e.g., IRC). Figure 3 illustrates this. The creation of Mistified communities is discussed in Section 5.

#### **4.3 Anonymous Authentication for communities**

Our architecture encourages open communities where users can participate anonymously. However, situations may arise where a community may want to restrict its membership, while preserving privacy for its members. For example, the Illinois College Board may create a Mistified community for discussing its teaching standards



**Fig. 3.** Mistified communities.

with students. In this case it is natural to want to restrict the membership to Illinois students only, while maintaining their anonymity.

In our system we rely on end-to-end authentication schemes for restricted communities, i.e., the community itself handles authentication. For example, the Illinois College Board can issue a group key to Illinois students. Likewise, a group password can be in effect to restrict access to the community. It is desirable to carry out end-to-end authentication at the application layer, as opposed to the Mist layer, since solutions already exist for the *anonymous authentication* problem [9][17]. Depending on the level of security desired, the community can employ an appropriate anonymous authentication scheme.

#### 4.4 Privacy-Awareness Agents

We propose to augment our chat application with special agents called privacy monitors. These privacy monitors will be integrated into the client end of our chat application. They will contain token-parsing algorithms, along with a customizable dictionary to identify proper names, addresses, credit card numbers, phone numbers, etc., and warn users that they are about to transmit personal information before they send their messages. These warnings will be unobtrusive (e.g., by underlining the

relevant words or phrases) and will prevent inadvertent disclosure of sensitive information. They will also act in educating users about their rights to privacy and improve awareness about privacy related issues.

## 5 Implementation

Our implementation consists of two components: Socializing Clients and Mistified Communities. These are implemented in Java. The Mist architecture is also implemented in Java and makes use of CORBA for communication. Administrative tools for building the Mist Hierarchy are also provided. Due to this design, Mist is readily deployable in ubiquitous computing environments such as Gaia [1][2].

### 5.1 Socializing Clients

Figure 4 shows a Socializing Client implemented in Java. The top left portion of the window displays the Lighthouses (or Masks) available to the user, e.g., Alice. These Lighthouses are obtained after the Socializing Client registers with a Portal. Once Alice is presented with a list of available Lighthouses, she clicks on a suitable

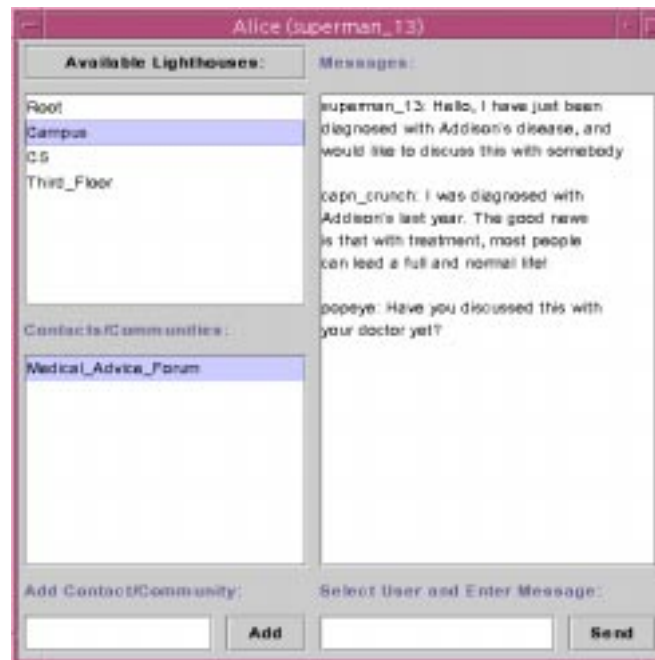


Fig. 4. A snapshot picture of the socializing client in Java.

Lighthouse to establish a Mask. Once Alice is Masked, she connects to a Mistified Community by using the “Add Contact/Community” feature. This creates a request message that travels to Alice’s Lighthouse. Alice’s Lighthouse contacts the lookup service with the Mistified Community’s name, and establishes two-way communication with the Mistified Community’s Lighthouse. A lookup service maintains secure bindings between Mist pseudonyms and their current Lighthouses, and is essential for looking up a Mistified Community’s Lighthouse. In Figure X we can see that the Medical Advice Forum has assigned Alice the pseudonym “superman\_13.”

Messages sent from the Socializing Client will now be “routed through the Mist” to the Mistified Community. The user can have multiple sessions established with other communities and contacts. Messages are sent to the appropriate parties by clicking on the relevant entry in the list of “Contacts/Communities.” Messages are displayed in the “Messages” window.

## 5.2 Mistified Communities

This is a server implementation in Java that combines some of the features of a Socializing Client and a generic chat server. The Mistified Community connects to a Lighthouse just like a Socializing Client does, and uses the same functionality of a Socializing Client for Portal registration and Lighthouse selection. The Mistified Community, however, differs from Socializing Clients in that it broadcasts messages received from any member to all other members in its list. Mistified Communities can be set up easily. If Bob wishes to create his own Mistified Community, he must run the Mistified Community component and supply it with a name, e.g., “Medical Advice Forum” and register it with a Portal. After this, he must Mask it with a suitable Lighthouse. The Lighthouse consequently registers the community with the lookup service. This lookup service maintains secure bindings between Mist pseudonyms and their current Lighthouses. Hence Mistified Communities are registered with the lookup service, and users can now connect to the community using their Socializing Clients as described in the previous section.

## 6 Related Work

In this section, we describe related work in the context of privacy preserving communications and privacy in ubiquitous computing. The need for privacy in ubiquitous computing is highlighted in Mark Langheinrich’s article [3]. He develops a strong case for privacy in ubiquitous computing by giving a background on the history of privacy, exemplifying the issues and summarizing them with a comprehensive set of guidelines for designing privacy aware ubiquitous computing. Our research is influenced by these guidelines and we pay careful attention to his suggestions with respect to pseudonymity, locality and social aspects of communication privacy.

In related research, the PISA project (Privacy Incorporated Software Agents) [10] is an initiative by the Dutch government to study the ramifications and threats to user

privacy in e-commerce, e-government and communications applications that use software agents. The author claims that intelligent agent technologies (ISAT) present a significant threat to a user's privacy. User-profiling can also expose an individual to threats from a user's own agents or foreign agents. This paper introduces the concept of an Identity Protector (IP) and PET-agents (Privacy Enhancing Technologies) that reduce the exposure of personal information to agents, protecting a user's privacy.

In the realm of privacy preserving communications, existing protocols focus on the Internet and aim to provide sender or receiver anonymity, and protection against traffic analysis. Crowds [11] is one approach to achieve anonymous communication by anonymizing a sender's request to web servers. The receiver of the web request cannot trace the IP address of the sender. All users in the Crowd are equally likely to generate messages with that address. In Onion Routing [12], packets are encrypted with multiple keys to form layers of hop-to-hop protection similar to layers in an "onion." In addition, the routing layer is oblivious to traffic analysis, maintaining a constant traffic rate by injecting noise traffic and padding packets to make all packets the same size, as well as controlling the inter-packet spacing. Onion routing provides complete sender and receiver anonymity at the price of performance. NetCamo [13] models the traffic patterns of nodes or networks and provides real-time rerouting and padding to hide communication patterns. In Mist, we provide sender and receiver anonymity and location privacy by building an overlay network on top of an existing network. We also include simple cryptography to make it infeasible to read packets to collect statistics without compromising all the keys on the path between a portal and a lighthouse. In order to analyze traffic in our scheme, all routers on a Mist path need to be compromised.

In addition to communication privacy, several research efforts have addressed other social aspects within the ubiquitous computing context. For example, GroupCast [14] introduces a method to aid in socializing by combining different types of content and user information and generating automatic content. By displaying this information on displays and consoles, it tries to provide opportunities for people who are physically close to interact and socialize. PRoP [15] introduces "tele-embodiment," where remote humans can project their presence into "tele-robots" known as PRoPs, in an attempt to capture the social aspects that result from the experience of being there. Similarly, the eTravel project [16] developed a tele-operated robot that substitutes for physical travel. Live video of the user's head is displayed on the head of the robot. These projects tackle the need for physical presence during communication, by including a virtual presence in place. We believe that Mist can augment these techniques to include anonymous communication with virtual presence, simulating the existence of people, while hiding their location and identity. Our focus however, is on applications such as group therapy sessions and free speech forums etc., that arise in context of digital socializing, where privacy plays a very important part in motivating and sustaining these interactions.

## 7 Conclusion

In this paper we make a strong case for preserving an individual's identity and location privacy while fostering meaningful social interactions in ubiquitous computing environments. We believe that digital communities are an important component of Active Spaces and will augment traditional mechanisms of socializing. Ubiquitous computing applications have the potential to revolutionize the way we interact with each other, by connecting people across the world and encouraging freedom of expression. Protecting privacy concerns and limiting the exposure of sensitive personal information in this context becomes extremely important. We argue that lack of privacy can expose ubizens to physical and emotional abuse, and create serious problems for law enforcement agencies. Hence privacy must coexist with security to protect users' interests. To prevent misuse by malicious users, we argue that law enforcement agencies will be able to force enough routers to cooperate and reveal the identity and/or location of the malicious user.

We describe a privacy preserving communication protocol called Mist, the details of which are elaborated in an earlier paper [4][5] that provides location privacy. We augment this protocol with identity privacy and describe an integrated solution for privacy preserving communication in digital communities. We also describe an implementation, similar to an online chatting application, which protects an individual from malicious users by preserving their privacy. We claim that the guarantees this provides make it easier for people to socialize, by directly addressing their physical security concerns effectively.

## References

- [1] M. Roman and R. Campbell, "GAIA: Enabling Active Spaces," *9th ACM SIGOPS European Workshop*, September 17th-20th, 2000, Kolding, Denmark.
- [2] M. Roman, C. Hess, A. Ranganathan, P. Madhavarapu, B. Borthakur, P. Viswanathan, R. Cerqueira, R. Campbell, and M. D. Mickunas, "GaiaOS: An Infrastructure for Active Spaces," Technical Report UIUCDCS-R-2001-2224 UILU-ENG-2001-1731, University of Illinois at Urbana-Champaign, 2001.
- [3] M. Langheinrich, "Privacy by Design – Principles of Privacy-Aware Ubiquitous Systems," *ACM UbiComp 2001*, Atlanta, GA, 2001.
- [4] J. Al-Muhtadi, R. Campbell, A. Kapadia, M. D. Mickunas, and S. Yi, "Routing through the Mist: Privacy Preserving Communication in Ubiquitous Computing Environments," to appear in the Proceedings of ICDCS '02.
- [5] J. Al-Muhtadi, R. Campbell, A. Kapadia, M. D. Mickunas, and S. Yi, "Routing through the Mist: Design and Implementation," UIUC Technical Report UIUCDCS-R-2002-2267.
- [6] Universal Declaration of Human Rights, Article 12, Adopted and Proclaimed by the United Nations General Assembly resolution 217 A (III) of 10 December 1948.
- [7] [http://dmoz.org/Society/Support\\_Groups/](http://dmoz.org/Society/Support_Groups/)
- [8] <http://www.cybercrime.gov/>
- [9] S. Schechter, T. Parnell and A. Hartemink, "Anonymous Authentication of Membership in Dynamic Groups," *Financial Cryptography '99*, Anguilla, British West Indies, February 1999.

- [10] J. Borking, Privacy Incorporated Software Agents (PISA): Proposal for Building a Privacy Guardian for the Electronic Age, Proceedings of the Workshop on Design Issues in Anonymity and Unobservability, ICSI, Berkeley, California, July 2000.
- [11] M. Reiter and A. D. Rubin, "Crowds: Anonymity for Web Transactions," *ACM Transactions on Information and System Security (TISSEC) Volume 1, Issue 1*, November 1998.
- [12] M. Reed, P. Syverson, and D. Goldschlag, "Anonymous Connections and Onion Routing," *IEEE Journal on Selected Areas in Communication, Special Issue on Copyright and Privacy Protection*, 1998.
- [13] Y. Guan, C. Li, D. Xuan, R. Bettati, and Wei Zhao, "Preventing Traffic Analysis for Real-Time Communication Networks," *Proceedings of The IEEE Military Communication Conference (MILCOM) '99*, November 1999.
- [14] J. McCarthy, T. Costa and E. Liongosari "UniCast, OutCast & GroupCast: Three Steps Toward Ubiquitous Peripheral Displays," *International Conference on Ubiquitous Computing (UbiComp 2001)*, 30 September - 2 October 2001, Atlanta.
- [15] E. Paulos and J. Canny, "PRoP: Personal Roving Presence," *ACM SIGCHI*, 1998.
- [16] <http://research.compaq.com/wrl/projects/eTravel/ET.html>
- [17] D. Boneh, and M. Franklin, "Anonymous authentication with subset queries," In proceedings of the *6th ACM conference on Computer and Communications Security*, pp. 113—119.