SIP Presence Location Service

Wilson Wu, Aleksandar Radovanovic, William D. Tucker
Computer Science Department, University of the Western Cape, 7535, Bellville, Tel. No: (021) 959 2406
Fax No: (021) 959 3006, E-Mail: **wwu**, aradovanovic, btucker {@uwc.ac.za}

Abstract—This paper presents an innovative use of the Session Initiation Protocol (SIP) for the subscription and notification of geographic information in order to provide a privacy concerned location-based service. SIP is a signaling protocol used for establishing sessions in an IP network. It has been widely used for Internet conferencing and telephony. This research project aims to enhance the SIP presence model in order to protect sensitive geographic information. To achieve this goal, we thoroughly analyzed existing Location-Based Services (LBS), reviewed LBS designs' pitfalls and identified several key privacy requirements. Based on this research, we presented a SIP flow that meets the privacy requirements. This SIP message flow includes SUBSCRIBE, NOTIFY and PUBLISH messages. A data format to carry geographic location information has also been introduced. The data format is based on Presence Information Data Format (PIDF). We define it as Location-enhanced PIDF, or LPIDF. LPIDF contains geographical information objects. We hope that the outcome of this research project will provide rich, convenient, privacy concerned architecture for LBS. Because LPIDF is based on SIP, this approach can be easily integrated into IP telephony services. LPIDF enables personalization of the Location-Based services address user privacy concerns and hereby increase their satisfaction.

Index Terms— SIP, Privacy, Presence, Geographical Location

I. INTRODUCTION

THIS paper presents a new use of Session Initiation Protocol (SIP) [16] for subscription and notification of geographic information to provide a privacy concerned Location-Based Service (LBS). The approach was inspired by the outputs of the Internet Engineering Task Force (IETF) Geopriv working group. The main goal of this group is to select an already standardized format to recommend for use in representing location-based information [6].

H.323 and SIP are two standards of Voice over Internet Protocol (VoIP). H.323 is the more mature of the two, but problems may arise due to lack of flexibility. SIP is currently less defined, but has greater flexibility that can ease Internet application integration. Because of the SIP's flexibility, it provides more opportunity for personalized telecommunication services. In addition, SIP has the capability to support mobile users. Nowadays, wireless and Internet technologies are rapidly converging. Mobile commerce is expected to grow at seemingly incredible rates as the number of mobile users dramatically increases. Hence, the approach proposed in this paper improves SIP in order to support some location-based applications both on desktop and mobile devices. These new applications include privacy concerned location messaging and other location-based services.

The motivation of this work is to enhance SIP with spatial location capabilities for supporting personalized telecommunication services. In the age of significant telecommunications competition, network operators continuously seek new and innovative ways to create differentiation and increase profits. A suitable way to accomplish this is through the delivery of highly personalized services. An ideal way to personalize information services is to enable them to be location based.

An example of this is Find Friends. The Find Friends service provided by AT&T Wireless enables customers to find out where their friends are by using cell phones. The service enables cell phone users to retrieve information about the location of other phones. A customer's location usually appears in the form of a street address. After two people have located each other, they can use the service to find a convenient place to meet and get directions to that site. AT&T Wireless has taken steps to protect users' privacy. For Find Friends to work, each user has to give permission for the other person to track him/her. Once permission has been granted, a person can choose to be "invisible" to specific or to all users through easy-to-use menus. Moreover, every time a person requests to find a friend, a text message alerts the person being sought.

In this paper, we present a use of SIP for privacy concerned LBS and a data format used for carrying geographic location information. The data format is based on Presence Information Data Format (PIDF) [17]. We define it as Location-enhanced PIDF, or LPIDF. A user can subscribe to another user's LPIDF in order to get their geographic location information. LPIDF owners are able to decide which part of their LPIDF they want to expose.

II. BACKGROUND

To provide LBS, IETF Geopriv working group suggests enhancing an already standardized format and protocol, and to ensure that security and privacy methods are available to diverse location-aware applications. Possible enhancement targets include standardized data formats that incorporate fields directing the privacy handling of location information and methods of specifying variable precision of location [6]. This paper shows how the SIP Presence model and enhanced PIDF can be used to offer a new use of SIP for privacy concerned LBS.

The authors wish to acknowledge the Telkom/Cisco/THRIP Center of Excellence (CoE) at the University of the Western Cape for their financial support

RFC 2778 defines an abstract model for a Presence and Instant Messaging system [7]. The presence service accepts the presence information, stores it, and distributes it. A presence protocol is a protocol for providing a presence service over the Internet or any Internet Protocol (IP) network. RFC3265 describes an extension for providing an extensible framework by which SIP nodes can request notification from remote nodes indicating that certain events have occurred [14]. It defines two new SIP methods SUBSCRIBE and NOTIFY. Niemi defined another new SIP PUBLISH method [12]. RFC 3856 uses SIP as a Presence protocol to provide Presence services through these three SIP methods [15].

PIDF was defined by the IETF Instant Messaging and Presence Protocol (IMPP) Working Group in 2004. A PIDF object is a well-formed Extensible Markup Language (XML) document. SIP is a text-based protocol. SIP Presence can use PIDF, an XML format, to carry information. RFC3859 specifies the Common Profile for Presence (CPP) and presents PIDF as a common presence data format for CPP-compliant Presence protocols [13]. It also defines a new media type “application/pidf+xml” to represent the XML MIME entity for PIDF.

III. Related Work

A. Privacy concerns

Since the first indoor location system, Active Badge, was built by Want et al in 1992 [18], much subsequent work has been done in LBS area. LBS continue to attract more and more attention. We can illustrate this tendency from the history of Open Geospatial Consortium (OGC). OGC was founded with eight charter members on the first Board of Directors meeting on September 25, 1994. From 1994 to 2004, the membership has grown from 20 to more than 250 government, academic, and private sector organizations.

LBS is used to transfer highly personalized location information. Hence, it also presents the potential to reveal someone’s personal location information. At the forefront of LBS development, Active Badge did not take privacy into account. Active Badge detects the location of each user and broadcasts the information to everyone in the building. The system, as originally deployed, assumes everyone in the building is trustworthy. It therefore provides no mechanism to limit the dissemination of an individuals’ location information [3]. This ‘feature’ reduces user satisfaction and leads to the tendency of people not using it. As Want himself noticed, “There will always be some days when for whatever reason somebody does not wish to be located” [18]. The easiest option was to remove the badge and leave it on the desk when one does not want to be located

Obviously, concern about privacy is a potential risk threatening the uptake of LBS. In [19], Westin defined information privacy as “the claim of individuals, groups or institutions to determine for themselves when, how, and to what extent information about them is communicated to others”. Therefore, in this paper, location information privacy is one of the major concerns.

B. Presence and LBS

Quite a number of SIP related LBS research effort has made recently. In 2002, Costa and Tang used SIP as transport and the Spatial Location (SLO) as a data format inserted into the SIP payload [5]. In 2003, IBM China Research Laboratory did some research on Intelligent LBS by using a Spatial Publish/Subscribe model [4]. In 2004 Kanamaru and Yoshitsugu built fieldcast2, a peer-to-peer presence service, with the SIMPLE protocol [10]. SIMPLE is SIP for Instant Messaging and Presence Leveraging Extensions [20].

Presence services have been found very useful lately, and the notion of presence expands far beyond indicating user status as “Online” or “Offline”. Presence information today can include geographic location, personal and many other types of information. Basically, there are two presence protocols, SIMPLE and Extensible Messaging and Presence Protocol (XMPP) [2]. Both XMPP and SIMPLE are presence protocols that provide a presence service. XMPP is an open-source, XML-based presence protocol. An advantage of XMPP is that it can be extended across disparate applications and systems. Compared to XMPP, SIMPLE has additional capabilities for unifying voice, video, and data messaging.

The spatial location (SLO) format used by Costa and Tang is an XML structure defined by the IETF for representing a user’s geographic location information [5]. SIP presence uses PIDF to hold presence information. We propose an extension to PIDF, LPIDF, as a data format to include geographic information. IBM China Research Laboratory’s LBS can actively push location-dependent information to mobile users according to their predefined interests [4]. The successful development of push-based LBS applications relies on the existence of publish/subscribe middleware that can handle spatial relationships. In fact, the SIP presence provides a similar subscribe-notification model. A SIP presence context-awareness service, Fieldcast2, has been developed by NTT Information Sharing Platform Laboratories in 2004 [10]. Fieldcast2 uses a P2P architecture for presence information sharing. It uses SIMPLE as the protocols for conveying presence information. Basically, in this approach the SIP presence model is also used to share geographic information.

IV. Problem Statement and Methodology

A. Research Problem Statement.

The research question of this project is “How can SIP be used to transfer location information in a private manner?” The research question can be divided into several sub-questions:

1) In what format can the geographic information be enclosed?

In order to convey geographic information, we define LPIDF as an enhanced, PIDF based format. LPIDF can be inserted into the payload of SIP messages. More importantly, other SIP proxies and SIP Presence agents should be able to interpret LPIDF.

2) In what ways can SIP be used for LBS?

SIP is a protocol for creating, modifying, and terminating Internet telephone calls, multimedia distribution, and multimedia conferences. SIP has many extensions. SIP also provides a presence service and IM service. The SIP

Presence model has been chosen for this project.

3). How can SIP model meet privacy requirements?

A suitable mechanism is designed to fulfill the privacy requirements with respect to RFC3261, RFC3265 and RFC3856.

B. Research methodology

The methodology of this project is based on a proof of concept and prototype approach. A prototype is developed to investigate the feasibility of the concept. We use an exploratory prototype process to perform rapid development of a system, where an initial prototype is produced and refined through a number of stages towards the final system. Overall, the steps include: requirements analysis, rapid design and implementation, using and verification of the prototype, refine the prototype when the prototype is not adequate, and finally, deliver the system.

V. THE KEY PRIVACY REQUIREMENTS

A. LBS needs dynamic response to circumstance

With regard to geographic information disclosure, a Notifier's willingness to reveal his/her information primarily depends on who is requesting that information and why. Depending on the social relationship between a Notifier and a Subscriber, a response might be quite different from one user to another. As Roach pointed out, "while traditional approaches understand privacy as a state of social withdrawal" [14], Altman instead sees it as a dialectic and dynamic boundary regulation process [1]. Privacy management is not about setting rules and enforcing them. Rather, it is the continual management of boundaries between different spheres of action and degrees of disclosure within those spheres.

B.LBS needs a level of deniability built in

Hindus et al have suggested a social need to avoid potentially embarrassing situations, undesired intrusions, and unwanted social obligations [8]. A good example of this is with mobile phones. If a person does not answer a mobile phone call, it could be for technical reasons—such as being outside of the service range, not having the phone with him/her, or the phone was off—or for social reasons, such as being busy or not wanting to talk to the caller at that moment. The result is that the person being called has a simple model for protecting his/her privacy, while the caller cannot tell why that person is not answering. By default, it does "the right thing" without the end-user having to take any special action.

C. LBS needs coarse-grained control

LBS need coarse-grained control. A LBS user should have a way to stop or adjust the information disclosure to the level that users want to reveal to the others. Lederer and Hong suggest that ubiquitous computer systems that convey location information could incorporate both a precision dial (ordinal) and a hide button (binary), e.g. audio device volume and mute controls, so users can either adjust the precision at which their context is disclosed or decidedly halt disclosure [11]. This helps users to accommodate the controls and even co-opt them in ways that the designer may not have intended.

D. LBS needs feedback

It is important for a user to know his/her actual level of information disclosure. Users may have difficulty accepting a system into their privacy practice if the scope of its privacy implications is unclear. With feedback mechanisms, a system could provide social visibility to prevent misuse [9]. For example, Alice is less likely to repeatedly query Bob's location if she knows that Bob can see each of her requests. A user will feel comfortable with the capability to control his sensitive information and the ability to know the actual information disclosure.

E.LBS needs special exceptions for emergencies

In crisis situations, safety far outweighs privacy needs. An emergency should be given privilege to be treated in a special manner. IP telephony can support emergency situations as with E911 call services in USA, 110 in Germany, and 112 in the rest of Europe [5]. Hospitals, for example, may require up-to-date information about the location of patients, particularly when medical emergencies arise. Trusted proxies are sometimes used to handle these kinds of situations. People are willing to pay for this service. For example, the MedicAlert is a paid service that stores personal medical records and forwards it to emergency responders in the case of medical emergencies.

VI. SYSTEM DESIGN AND IMPLEMENTAION

A. System design

For our SIP-based approach to privacy and LBS, we use a Peer-to-Peer (P2P) architecture and authorization mechanism. In order to prevent unnecessary information from being revealed to a third party, we use SIP Back-to-Back User Agents (B2BUA) as end points [16]. A B2BUA processes incoming requests and generates outgoing requests to communicate with another B2BUA. Once a P2P connection has been built up, a proxy hands over the data transfer between the two nodes. Geographic location information is collected into a B2BUA where as much personal information about an end user is captured, stored, and processed on local devices owned by that end user.

RFC 3265 states: "Privacy concerns may require that Notifiers apply policy to determine whether a particular Subscriber is authorized to subscribe to a certain set of events. Such policy may be defined by mechanisms such as access control lists or real-time interaction with a user [14]." Whenever a B2BUA sends a Subscribe request to another B2BUA, it will trigger real-time authorization process with a user. On a peer-to-peer level, B2BUAs authorize one another personally.

1) Components

The system architecture is shown in Figure 1. It includes: SIP proxy, Domain Name System (DNS) server, Presentity and Watcher. The SIP proxy is used to forward a SIP message and to the desired Presentity. The DNS server is used to find the next-hop IP address. A Presentity is a presence model entity. It is the LPIDF owner that sends geographic information to Watchers. A Watcher is a Presence model entity that subscribes to receive the LPIDF from a Presentity in order to learn that Presentity's geographic information.

2) Routing the Request

SIP networks are capable of routing requests from any user on the network to the server that holds the registration state for a user [15]. SIP uses hybrid P2P architecture. Its features include:

Lookup centralized: SIP provides a mechanism for a User Agent (UA) to explicitly create a binding. This mechanism is known as registration. Registration entails sending a REGISTER request to a special type of User Agent Server (UAS) known as a registrar. A registrar acts as the front end to the DNS server for a domain, reading and writing mappings based on the contents of REGISTER requests. A proxy server that is responsible for routing requests for that domain typically consults this DNS server

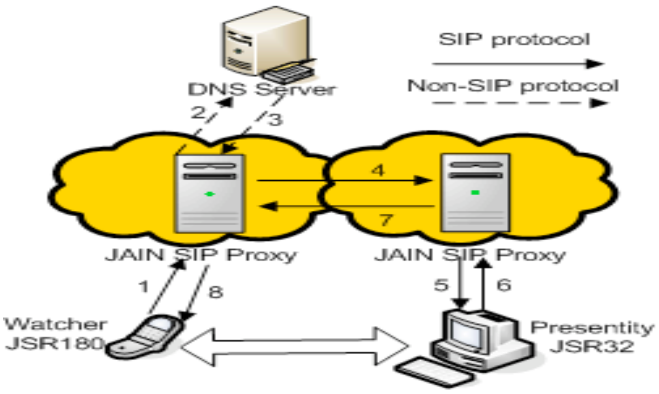


Fig 1. *Proposed system architecture*
Step1-5 A Watcher sends SUBSCRIBE Request Presentity through SIP proxies and DNS server.
Step6-8 Desired Presentity reply 200 ok back to Watcher.
Finally, a dialog is established between Watcher and Presentity for peer-to-peer message exchange.

Data exchange between peers: If a user wants to initiate a session with another user, SIP must discover the current host(s) at which the destination user is reachable. This discovery process is frequently accomplished by SIP network elements such as proxy servers and redirect servers that are responsible for receiving a Request, determining where to send it based on knowledge of a registrar and DNS server, and then sending it there. When a SUBSCRIBE message reaches the Presentity, it establishes a "dialog" with the presence agent. A dialog is defined in RFC 3261, and it represents the SIP state between a pair of entities to facilitate peer-to-peer (P2P) message exchanges [16].

B. Location-enhanced PIDF (LPIDF)

LPIDF, is a extension of PIDF, defined as a data format for containing geographic information. SIP, by itself, only provides call control. However, SIP accepts additional information inserted as a SIP payload for other applications. Geographic information in the LPIDF format can be inserted into a SIP message's payload. The basic function of LPIDF is to provide a common and extensible container where the user can place identifiers, security factors, location representation, and other parameters to manage the user's location information. The requirement for the LPIDF is to secure and self-contained. Furthermore, LPIDF has to fulfill user needs and meet the privacy requirements.

The basic unit of storage in an LPIDF document is the tuple. A LPIDF document might contain more than one tuple. A tuple is used to describe individual pieces of contextual data. For example, a LPIDF might contain static information, such as a name and email address, as well as dynamic information, such as current location and activity. A SIP Presence LBS application retrieves and manipulates LPIDF data to accomplish location-aware tasks through end users specify privacy preferences.

C. Proposed SIP flow meets privacy requirements

Figure 2 shows our proposed SIP message flow. SUBSCRIBE and NOTIFY methods are used to deal with most of presence location issues, and PUBLISH is used to deal with an emergency situation. The SIP authorization mechanism is applied to prevent sensitive information from being revealed. We can now examine our prototype in light of the key privacy requirements defined in section V.

1). Dynamic response to circumstance?

When a Subscriber wishes to subscribe to a particular state for a resource, it forms a SUBSCRIBE message. The SUBSCRIBE request will be confirmed with a final response. 200-class responses indicate that the subscription has been accepted, and that a NOTIFY will be sent immediately. A 202 response merely indicates that the subscription has been understood, and that authorization may or may not have been granted. Whenever a request comes, a Presentity should be able to accept or deny the request, and reveal part of the geographic location information to the Subscriber. SIP provides the authorization mechanism to dynamically accept or deny an incoming SUBSCRIBE request. The authorization

```
Subscriber (Alice)    SIP Proxy       Notifier (Bob)
Step 1  |----Subscribe----->|----Subscribe--->| Request state subscription
Step 2  |<-------202----------|<--------202--------| a level of deniability "pending"
Step 3  |<------------NOTIFY (pending)--------| Waiting for authorization
Step 4  |-------------------200 ok---------------->| Acknowledge notifying
Step 5  |<------------NOTIFY (active)----------| Grand city level information
Step 6  |-------------------200 ok---------------->| Acknowledge notifying
     PUA (Alice)       SIP Proxy       Watcher (Hospital)
Step 7  |------Publish----->|                    | update emergency information
Step 8  |<-----200 ok-------|                    | Acknowledge publication
Step 9  |                   |---------Notify----->| Inform emergency information
Step 10 |                   |<------ 200 ok------| Acknowledge notifying
```

Fig 2. Proposed SIP Message flow
Alice sends SUBSCRIBE Request to Bob asking for his geographic information. Notifier reply 202 Response indicates that the subscription has been understood, and that an authorization request needs to be approved by Bob. Bob authorizes the Request and decided to reveal his City level geographic information to Alice.
When Alice encounters an emergency situation, Presence User Agent (PUA) publishes her geographic information to SIP proxy, and SIP Proxy notifies hospital.

mechanism is used to provide real-time interaction. Hence, a user can give dynamic responses for the incoming requests. The current project offers three options for users: "authorize", "authorize with privacy concern" and "reject".

2) Level of deniability?

A NOTIFY request will be sent to a Subscriber after sending a 202 response. RFC 3265 specifies that s NOTIFY message is sent immediately after any 200-class response to a SUBSCRIBE request, regardless of whether the subscription has already been authorized. 200-class responses to SUBSCRIBE requests do not generally contain any useful information beyond subscription duration. Their primary purpose is to serve as a reliability mechanism. The NOTIFY requests must contain a "Subscription-State" header with a value of "active", "pending", or "terminated". The "pending" value indicates that the subscription has been received, but that policy information is insufficient to accept or deny the subscription at this time. This approach provides a degree of deniability, as a "Subscription-State" might be "pending" due to technical failures, lack of actual data, restricted access, or because some other possible reason.

3)Coarse-grained control?

When the authorization has been approved, a user can decide which parts of the LPIDF he/she wants to reveal. We define five levels: "country", "province", "city", "street" and "room". Meanwhile, another two parameters have been provided: "Duration" and "Interval". The user can decide how long he/she wants to reveal the geographic information (for instance, 2 hours), and the user can determine the interval for releasing the geographic information (for instance, once every 5 minutes).

4). User feedback?

The Notifier contains a dynamic subscription list. When a subscription is created in the Notifier, it stores the event package name and the "Event" header "id" parameter as part of the subscription information into the Notifier. A subscription is destroyed when a Notifier sends a NOTIFY Request with a "Subscription-State" of "terminated". According to the subscription list, our SIP Presence LBS is able to indicate who is getting geographic information and how much geographic information the Subscriber is getting. When a subscription is terminated, it is removed from the subscription list. Thus, the Presence LBS application will reflect that the Subscriber stopped getting geographic information from a Notifier.

5). How to deal with emergency situations?

A Presence User Agent (PUA) pushes data into the presence system, but it is outside of the system. In that way , the PUA does not receive SUBSCRIBE messages or send NOTIFY messages. [12] provides a method, PUBLISH, to push the geographic location information to a proxy server. PUBLISH is used to upload geographic information from the PUA to the SIP proxy. The SIP proxy can act as a re-distributor of that geographic information. The SIP Proxy can then notify the geographic information to public emergency response units like a hospital, fire department or police station.

D. Implementation

To investigate the feasibility of the proposed SIP Message flow (see Fig. 2), a prototype is developed according to the system architecture shown in Figure 1. The prototype solution uses SIP mechanism implemented with the Java SIP Application Programming Interface (API). The presence service has two distinct sets of clients. One set of clients, called Presentities, provides the presence information to be stored and distributed. The other set of clients, called Watchers, receives the presence information from the service. We use the JSR32 SIP API to develop the Presentity and use the JSR 180 SIP API to develop the Watcher for this prototype. The JAIN-SIP proxy is used to test the Presentity and the Watcher and to forward SIP requests. The Nokia S60 emulator was used to run Java 2 Micro Edition (J2ME) code. The prototype is shown in Figure 3.

Presentity is at the left hand side of figure 3

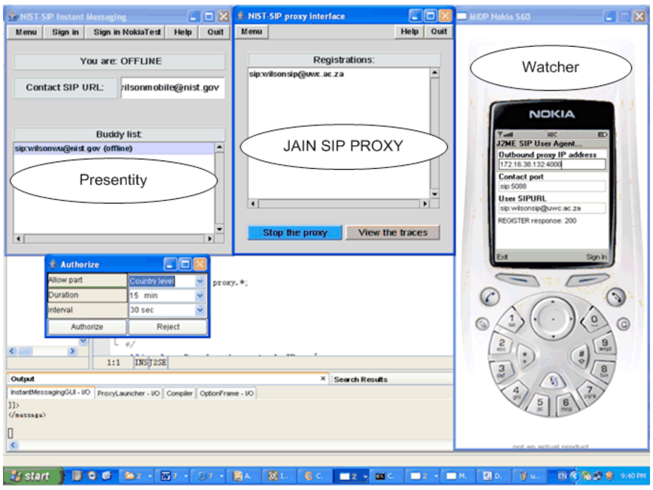
The Presentity capabilities are:

- Send and process NOTIFY and SUBSCRIBE requests.
- Support XML format "lpidf+xml".
- Register and unregister to a SIP proxy.
- Authorize mechanism for incoming SUBSCRIBE request.
- Modify LPIDF data for coarse-grained control

Watcher is at the right hand side of figure 3

The Watcher capabilities are:

- Send and process NOTIFY and SUBSCRIBE requests.
- Support XML format "lpidf+xml".
- Register and unregister to a SIP proxy.
- Send PUBLISH request to SIP proxy



You are: OFFLINE

Contact SIP URL: /ilsonmobile@nist.gov

sip:wilsonwu@nist.gov (offline)

sip:wilsonsip@uwc.ac.za

J2ME SIP User Agent...

Outbound proxy IP address: 172.16.38.132:4000

Contact port: sip:5088

User SIPURL: sip:wilsonsip@uwc.ac.za

REGISTER response: 200

Allow part: Country level

Duration: 15 min

interval: 30 sec

```
proxy.*;
 */
1:1   INS J2SE
]]>
</message>
```

Fig 3. Java Implementation

Watcher sends SUBSCRIBE Request to Presentity asking for geographic information. Authorization needs to be taken by Presentity. Presentity needs to decide the "level", "duration" and "interval" of geographic information disclosure.

VII. Conclusion

We presented an innovative use of SIP for the subscription and notification of geographic information to provide a privacy concerned location-based service. Because this approach is based on SIP, it can be easily integrated into IP telephony services for enabling personalization of telecommunication LBS while reducing a user's privacy concerns in order to increase user satisfaction. LPIDF enhances SIP with the required spatial location capabilities for supporting the personalized telecommunication services. Through the SIP Presence model and LPIDF, a SIP Presence Agent (PA) can convey geographic information to pass through any SIP network. An end user can subscribe to another user's LPIDF in order to get the other user's geographic location information. A LPIDF owner is able to decide the frequency and duration of information availability, and control which parts of the LPIDF to expose. A lot of work still lies ahead, as our prototype still needs to be refined and evaluated. A methodology needs to be developed to test the prototype. In order to carry out data collection and analysis, the LBS privacy concerns still need to be addressed through different methods. In the near future, we would like to provide some recommendations to the Geopriv working group regarding the use of SIP for privacy concerned LBS.

References

[1] I. Altman, *The Environment and Social Behavior: Privacy, Personal Space, Territory and Crowding*, Monterey, CA: Brooks/Cole, 1975.

[2] P. S. Andre, "Extensible Messaging and Presence Protocol (XMPP): Core", IETF, RFC3920, 2004.

[3] A. Beresford and F. Stajano, "Location Privacy in Pervasive Computing", *IEEE Pervasive Computing*, vol. 2 pp. 46-55, 2003.

[4] X. Y. Chen, Y. Chen and F. Y. Rao, "An Efficient Spatial Publish/Subscribe System for Intelligent Location Based Services", *In Proceedings of the 2nd International Workshop on Distributed Event-Based Systems,* San Diego, CA, USA, pp.1-6, 2003.

[5] J. Costa and H. Tang, "Application of Spatial Location Information to SIP", *ACM Cluster Computing*, pp. 399–410, 2002.

[6] J. Cuellar, J. Morris, D. Mulligan, J. Peterson and J. Polk, "Geopriv Requirements", IETF, RFC 3693, 2004.

[7] M. Day, J. Rosenberg and H. Sugano, "A Model for Presence and Instant Messaging", IETF, RFC 2778, 2000.

[8] D. Hindus, S. D. Mainwaring, N. Leduc, A. E. Hagström and O. Bayley, "Designing Social Communication Devices for the Home", *ACM Human Factors in Computing Systems*, pp. 325-332, 2001.

[9] J. Hong and J. A Landay, "Support for Location: An Architecture for Privacy Sensitive Ubiquitous Computing", *In Proceedings of Mobisys '04*, Boston, MA, USA, pp.177-189. 2004.

[10] A. Kanamaru and T. Yoshitsugu, "Fieldcast2: Flexible P2P architecture for presence information sharing", *The Second IEEE Annual Conference on Pervasive Computing and Communications Workshops*, pp.98-102, 2004.

[11] S. Lederer and J. Hong, "Personal privacy through understanding and action: five pitfalls for designers", *ACM Personal and Ubiquitous Computing*, vol. 8, pp. 440–454, 2004.

[12] A. Niemi, "Session Initiation Protocol (SIP) Extension for Event State Publication", IETF, SIP WG Internet-Draft, 2004.

[13] J. Peterson, "Common Profile for Presence (CPP)", IETF, RFC 3859, 2004.

[14] A. B. Roach, "Session Initiation Protocol (SIP)-Specific Event Notification", IETF, RFC 3265, 2002.

[15] J. Rosenberg, "A Presence Event Package for the Session Initiation Protocol (SIP)", IETF, RFC3856, 2004.

[16] J. Rosenberg, H. Schulzrinne, G. Camarillo, A. Johnston, J. Peterson, R. Sparks, M. Handley and E. Schooler, "SIP: Session Initiation Protocol", IETF, RFC 3261, 2002.

[17] H. Sugano, S. Fujimoto, G. Klyne, A. Bateman, W. Carr and J. Peterson, "Presence Information Data Format (PIDF)", IETF, RFC 3863, 2004.

[18] R. Want, A. Hopper, V. Falcao and J. Gibbons, "The Active Badge Location System", *ACM Transactions Information Systems*, vol. 10, pp. 91–102, 1992.

[19] A. F. Westin, *Privacy and Freedom*, Atheneum NY: Bodley Head, 1967.

[20] IETF SIMPLE Working Group, http://www.ietf.org/html.charters/wg-dir.html.

Authors

Wilson Wu is a Master student of Computer Science at the University of the Western Cape. His main research interests are SIP presence services, location based services and human privacy concern.

Aleksandar Radovanovic is Lecturer in Computer Science at the University of the Western Cape. His research interests include the general area of computer networks and protocols.

William Tucker is a Senior Lecturer in Computer Science at the University of the Western Cape. He is finishing a PhD at the University of Cape Town on Quality of Service and multi-modal semi-synchronous IP communications.