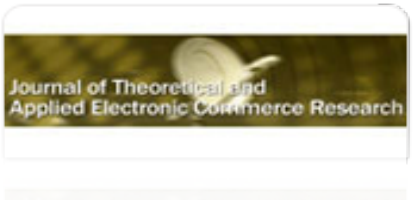


Journal of Theoretical and Applied Electronic Commerce Research

E-ISSN: 0718-1876

ncerpa@utalca.cl

Universidad de Talca

Chile

Bessler, Sandford

A system for locating mobile terminals with tunable privacy

Journal of Theoretical and Applied Electronic Commerce Research, vol. 2, núm. 2, august, 2007, pp. 82-91

Universidad de Talca

Curicó, Chile

Journal of Theoretical and Applied Electronic Commerce Research
ISSN 0718–1876 Electronic Version
VOL 2 / ISSUE 2 / AUGUST 2007 / 82 - 91

This paper is Available online at
www.jtaer.com

A System for Locating Mobile Terminals with Tunable Privacy

Sandford Bessler

Telecommunications Research Center Vienna (ftw.), bessler@ftw.at

Received 14 January 2007; received in revised form 13 May 2007; accepted 25 May 2007

Abstract

A number of approaches for capturing and processing location information of mobile users have been proposed in the past; however, only with the latest advances in the handset technology, a terminal-based positioning approach, using overlay SIP signaling on top of a packet switched bearer and area notification as basic functionality becomes feasible for mass applications. Especially in electronic commerce scenarios, in which users often interact with non-trusted services and shops, any location-based solution has to consider privacy aspects as well. The terminal-centric model presented in the paper leads to a simple and efficient way to achieve tunable privacy: mobile users define own "zones" and selectively disclose them to their buddies and to external services. As a result, localization can be performed only in the allowed places and by the allowed watchers, both parameters being configured by the user herself on her mobile terminal. We describe the system architecture, protocols and present representative technical scenarios.

Key words: Location, zones, privacy, SIP, GPS, presence, notification events, GML, IETF Geopriv, m-advertising

Journal of Theoretical and Applied Electronic Commerce Research
ISSN 0718–1876 Electronic Version
VOL 2 / ISSUE 2 / AUGUST 2007 / 82 - 91

This paper is Available online at
www.jtaer.com

1 Introduction

The Location Based Services (LBS) in operation nowadays provide added value mainly by using the physical position of mobile users. This location data may consist of geographical coordinates, access point cell IDs, or civil location in form of postal addresses.
Some of the privacy problems arising through disclosure of location information have been solved in the past through anonymity and pseudonymity [22], [4] achieving unlinkability between user identity and position data, and between successive locations of the same user [6], [19]. Location privacy should to be protected also when the interacting parties and services trust each other: however, for communicating friends or even within the family, hiding the identity behind pseudonyms does not make much sense [15]. The same applies for trusted services run by the employer of the user in the health or logistics sector, for emergency or insurance services. For example, in case of an emergency service the business model could be the following: as a part of an insurance contract, the user allows the service provider to subscribe to location events restricted to the visited zone (e.g. ski region, mountaineering, safari, etc). In the following, we mention some more application examples:

- A mobile user wants to localize any other user from her address book.
- A health worker visits patients at home. The locating service operated by the employer would help answer queries about the worker's time schedule and delays (from Myles et al. [17]).
- An advertisement service responsible for several shopping or entertainment locations, would push information to the users passing nearby
- A service provider operates an emergency service in a ski region and needs to know and communicate with all users present in a certain area in case of an avalanche or of other accidents.

The scheme described in this paper applies for all the applications mentioned above and delivers user tunable privacy.

1.1 Architectural prerequisites

At the core of location based services are positioning techniques. Küpper [14] categorizes them along three dimensions into terminal- and network-based positioning, satellite, cellular and indoor positioning, stand-alone vs. integrated infrastructure. For our approach we advocate the terminal-based positioning architecture since it allows processing the location information at its source, at the user terminal itself. The superiority in accuracy and performance over the cellular network-based positioning becomes relevant in the triggered location update (or notification) mode: instead of repeatedly polling the current position of the target terminal, the watching entity subscribes to events triggered when the target enters or leaves a certain circular or rectangular area. This mode of operation doesn't work efficiently with the current GSM network-based positioning infrastructure. Based on simulations, we have shown [25] that the signaling overhead is about 15% lower in triggered mode than in the polling mode. The most used terminal-based positioning technology is based on satellite (GPS), although the initial position determination is slow and it doesn't work well in buildings. Other positioning methods suited also for indoor spaces are based on WLAN, RFID and Bluetooth beacons and will be subject of future work.

The realization possibilities for the triggered location update narrow down when it comes to connecting mobile terminals via a packet bearer such as GPRS. The session initiation protocol (SIP) [26] is probably the best choice, since it has been selected by the 3GPP as the fundament for the IP Multimedia Subsystem, and as a consequence the SIP stack will be found soon in all next generation mobile phones. Thus, the location system described in previous works (NILS - Native IMS location system [19], [24], [25]) has nice properties: it is IMS-aware and it is completely independent of the current GSM/UMTS network-based location system. The solution described in more detail in the next sections requires implementing in each mobile terminal a component similar to an edge presence server. Slightly modified SIP/SIMPLE subscribe messages are received by this miniature presence server and processed to deliver immediate location information or a notification, triggered by the conditions mentioned in the subscription.

1.2 Contributions of this work

An efficient location service based on triggered location updates is the prerequisite for the location privacy work. Our main contribution is the design of a simple system that allows mobile users to define own location zones and to manage their disclosure to buddies, groups and external watching applications.

The presented model has several benefits with respect to the achieved privacy:

- the user discloses geographically isolated zones making tracking more difficult
- in many supported scenarios the location information is abstracted to a name instead of real geographical data, limiting the usage of the data by the watcher for further processing
- by selecting the zones and their size, the localized user has a fine control of his privacy towards individual watchers: that is what we mean by tunable privacy
- finally, the usability is increased, since it is easy for the user to understand the effect of his configuration actions

Journal of Theoretical and Applied Electronic Commerce Research
ISSN 0718–1876 Electronic Version
VOL 2 / ISSUE 2 / AUGUST 2007 / 82 - 91

This paper is Available online at
www.jtaer.com

The rest of the paper is organized as follows: Section 2 describes the discrete zone model, Section 3 explains in details the interactions and the standards used, Sections 4 presents different model extensions for external both trusted and non-trusted services and discusses possibilities for performance optimization, section 5 reviews related work, and finally section 6 presents conclusions and considerations for future work.

2 Location semantics and zone management

With the exception of pure tracking applications, useful location information consists of the name of the place the user is in. Our model is therefore based on discrete location areas we call "zones", between which the user moves in his daily life, for example home, office, gym, parents-home, supermarket, etc. For community applications, the names of these zones are meaningful only for the person herself, for her friends and family, or denote public places such cinemas or shops. The main idea of tunable location privacy is the fact that a user defines a number of "zones" and decides to disclose them selectively to trusted users from his address book (buddies). Outside these zones, the user cannot be localized.

Besides the discrete character of zones, the location accuracy varies with the size of the circle or polygon around that location: for example a zone can be defined as fuzzy as the whole city area in which the person lives. Even this information is sufficient since it allows colleagues to know whether the user is traveling or not, and it enhances his privacy !

In order to exchange location information two users have to establish a trust relationship. Technically, this leads to following two steps:
First, he has to add the other user to his contact list (similar to the popular VoIP and IM systems). Second, he has to associate a number of previously defined zones to that contact, meaning that the latter can query or be notified whenever our user reaches any of these places. It is a simple metaphor the user can understand and verify anytime.

Each place has a name, center coordinates and a radius. Alternatively, rectangular zones can be defined. Making the continuous location space to a discrete one can lead to the extreme case in which for a certain watcher user, only two states of the target user are available for example: "in the office" and "not in the office" achieving exactly the degree of privacy a person needs for some partners or customers at work. In any case the target user is always in control of the disclosure of every single zone he has defined.

In [17] the authors foresee the formation of a tree of hierarchical location areas starting for example with a region, town, working company, office, room, etc. , and a reasoning process to define the desired accuracy, corresponding to a node in the tree; our approach is simpler: we define a linear list of locations to be disclosed to each user:
The relationship between two zones can be: a) disjoint, b) overlapping or c) contained. Only in cases b) and c) several zones may be returned by a certain coordinate pair: the overlapping case b) is considered as not intended by the user, therefore one of the zones is selected. In case c) a zone is contained in another zone (both being disclosed to an asking watcher), the place with the smallest area is selected. Containment check is very simple especially for rectangular defined zones.
Creating a new zone is a very simple user action: the current user position is stored with a predefined size (radius or rectangle) around the coordinates, and then the user enters a name to identify that location.

Comparing the semantics of location and presence information we see that they are quite different: geographical location expressed in coordinates has practically a continuous value range, whereas rich presence information (standardized by the IETF as RPID [31]) consists of several attributes, each having a discrete number of values. In our model however, through the definition of discrete zones, the location becomes similar to the rich presence attribute "location_type": it has a number of discrete values, the user defined zones. Though, we cannot completely reuse the RPID presence model because of the following reasons: it doesn't trigger a notification when the attribute "location_type" attains a certain value (corresponding to a zone in our model), and it standardizes the values of this attribute instead of leaving them to be freely defined by the user. Therefore, the protocol presented in the next section reuses parts of the SIP presence event package, but defines also new messages.

3 Location service architecture and protocol

In Fig. 1 we summarize the proposed system architecture variations. They all use a SIP overlay network and are therefore independent of the GSM/UMTS network positioning infrastructure. We will use throughout the paper the user roles defined by IETF in their presence work: watcher is the user or application that consumes location information and presentity is the entity that provides it. In Fig. 1 we distinguish between four scenarios: in a) both watcher and presentity are user terminals; in b) the watcher is an application, but the underlying protocol is still SIP; in case c), the location function is mediated by a so called service enabler that serves several terminals and exposes a web service interface such as Parlay X [21] to 3rd party applications, whereas case d) is using a server component to reduce the radio traffic (see section 3.3). The servers in cases c) and d) may provide network-based positioning in case the localized terminal is not equipped with a GPS receiver or cannot temporarily receive GPS information from

Journal of Theoretical and Applied Electronic Commerce Research
ISSN 0718–1876 Electronic Version
VOL 2 / ISSUE 2 / AUGUST 2007 / 82 - 91

This paper is Available online at
www.jtaer.com

satellites. The use of a geographical information system (GIS) server as discussed in section 3.1 and 3.2 arises when applications define the zones instead of the presentity

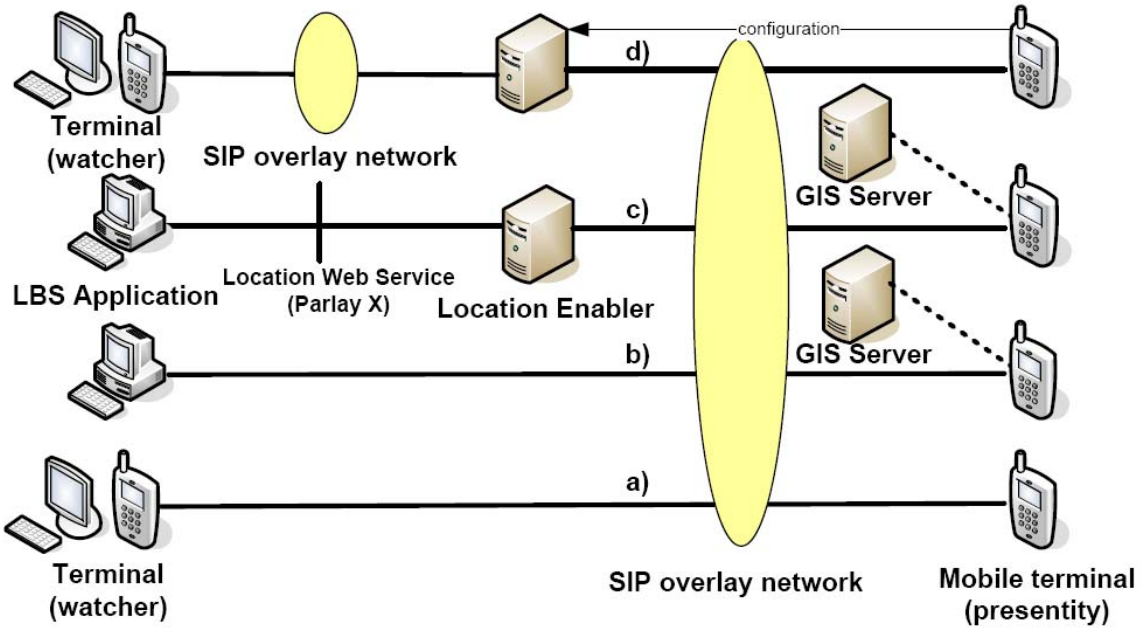


Figure 1: Variations of the proposed location architecture

The signaling between mobile terminals is based on the Session Initiation Protocol (SIP, RFC 3261 [26]) and the presence event package (SIMPLE RFC 3856 [28]). This family of standards is fundamental for VoIP, instant messaging, presence and IMS and starts to be available in an increasing number of mobile terminals such as the current Nokia models E60, N71, etc.

The SIP presence event package has basically two types of messages that form a so called SIP dialog: SUBSCRIBE and NOTIFY, and is used to convey presence information. In general, the standardization of our approach to provide location in addition to presence services requires the definition of a new event package and an own standardized URI distinct from the presence one, called location presence (this has been done in a IETF Draft [20]), and by doing that to make possible to address both a presence and a location user agent on the same terminal. Another possibility we use in our implementation is to convey both presence and location information in the same PIDF (presence document), transported in the NOTIFY message.

In the SUBSCRIBE message, the watcher expresses the request to either receive immediately the information whether the user is in the mentioned zone, or to subscribe to an event issued when the presentity enters or leaves the mentioned zone. Alternatively, the watcher can ask for location in raw geographical coordinates (if allowed). The coding of these requests into the SUBSCRIBE payload is done similar to the presence notification, using an IETF standardized XML structure called location filter [16], [11]. Each filter XML document can contain the description of one or several events that would trigger a notification: for example the presentity moves a specific distance since the last notification, or exceeds a different speed, or an element of its civic address changes. We use in our system mainly the event created when the presentity enters or leaves (also called containment triggers) a 2-dimensional area described in the GML language [18]. Simply stated, we have in the filter description a piece of XML code describing a circle with a pair of geographic coordinates as center and a radius, or a rectangle with two pairs of coordinates. Relevant for privacy in our approach is however, that instead of the area description, the filter contains only one of the zone names the watcher is allowed to monitor. The area description, at least in the user-to-user scenario of Fig. 1a, does not leave the presentity terminal.

In the NOTIFY message, the presence document PIDF is extended in RFC 4119 [23] to encapsulate location information. For containment triggers, the names of the zones and the attribute values “inside” or “outside” are returned. The structure of the two SIP messages is summarized in Figure 2.

Journal of Theoretical and Applied Electronic Commerce Research
ISSN 0718–1876 Electronic Version
VOL 2 / ISSUE 2 / AUGUST 2007 / 82 - 91

This paper is Available online at
www.jtaer.com

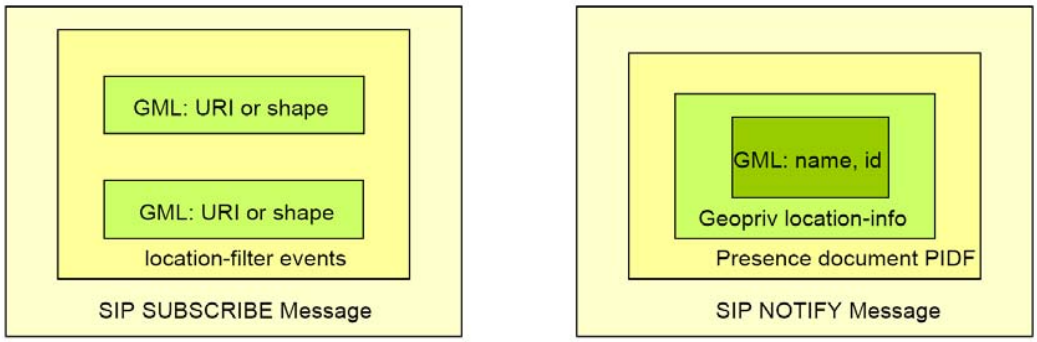
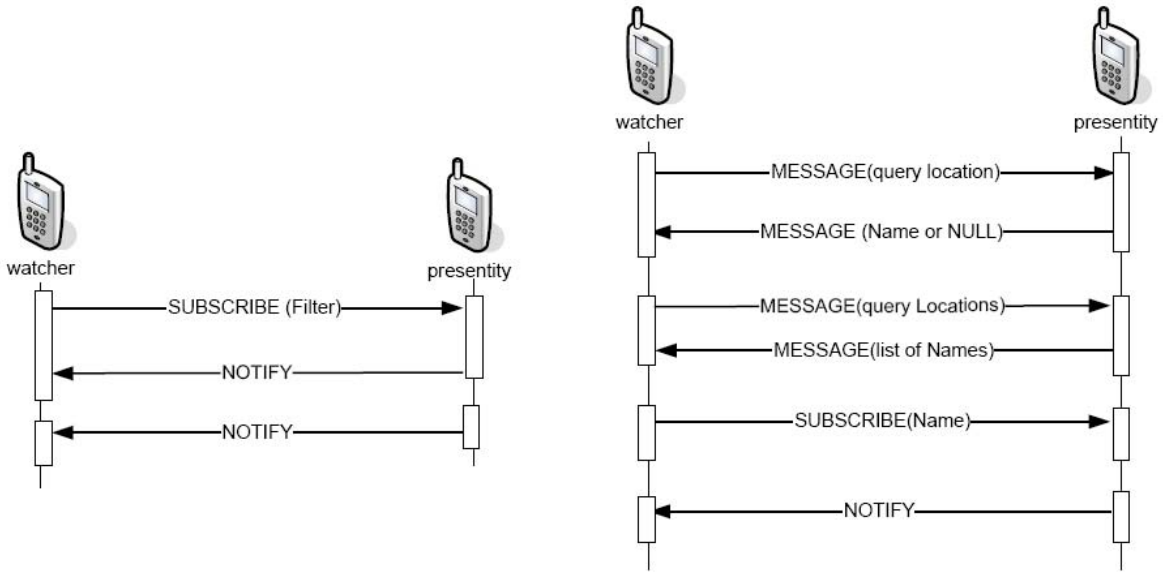


Figure 2: SIP Message structure

The protocol interactions for the location polling and notification cases are similar to SIP presence (see Figure 3). The message “200 OK” that always acknowledges a SUBSCRIBE, NOTIFY or MESSAGE message is omitted to improve the clarity of the diagrams. In the usual case a), the watcher has to send the zone description using GML in the filter. The notification takes place immediately in case the presentity satisfies the trigger conditions, e.g. is within the zone. Our proposal for the scenario from Fig. 1a is depicted in Fig. 3b: the watcher knows the presentity and understands the zone names, so she requests first the zones she is allowed to query or subscribe. This interaction is implemented using a SIP MESSAGE message. Once the list is returned, the watcher can query or subscribe any of them. The location filter contains therefore a name instead of the GML polygon or circle description. The method has also the side effect that it secures the association of names to the correct GML descriptions (done only by the presentity).



a) watcher defined zones b) presentity defined zones

Figure 3: Personal localization protocol interactions

3.1 System extensions to support watcher applications

Until now, we have described how a user can achieve tunable location privacy through the management of own defined zones, in interaction to other users or services.

In some scenarios (see Fig. 1b) the "zones" are however defined by the watcher and have to be "pushed" to the presentity, assumed the latter trusts the watcher. Such use cases arise for example when an employer needs to localize his service-persons, or when a user subscribes in advance to an emergency and information service covering a certain geographical region.

The main requirements for extending the system so it can support the applications above are:

- to be able to inter-operate with the terminal-to-terminal mode,

Journal of Theoretical and Applied Electronic Commerce Research
ISSN 0718–1876 Electronic Version
VOL 2 / ISSUE 2 / AUGUST 2007 / 82 - 91

This paper is Available online at
www.jtaer.com

- to provide the application with a flexible tool to define zones,
- to maintain the control of the presentity over the localization,
- to provide a single interface that ca be used by all applications.

To illustrate the design spectrum of the system, we present two alternatives:

1. The presentity user registers at the application, so the latter can contact her. The presentity can login in the application anytime, select the location zones and downloads them (as GML descriptions). A zone viewer that allows the presentity to verify the locations on a map is available. The application subscribes to the locations checked out by the presentity sending the names in the SUBSCRIBE message as in the former case. This alternative has the disadvantage that it requires the presentity to initiate the dialog and download the zone data. It can however manage the downloaded zones as described in the terminal to terminal case.
2. The presentity registers at the application and basically allows the application to "push" zone information to it. The application uses a third party GIS server to find zones corresponding to public points of interest or defines zones by postal address and name-ID. The name ID is sent in the SUBSCRIBE together with the URI to access the GIS server. The presentity needs to go to the GIS-server, fetch the GML code and eventually check the location visually. The GIS server insures the integrity of the zone information in the location filter. The geo server can be used by many applications, but stores application specific data (zones). The interactions are described in more detail in [7] and are sketched Figure 4 below:

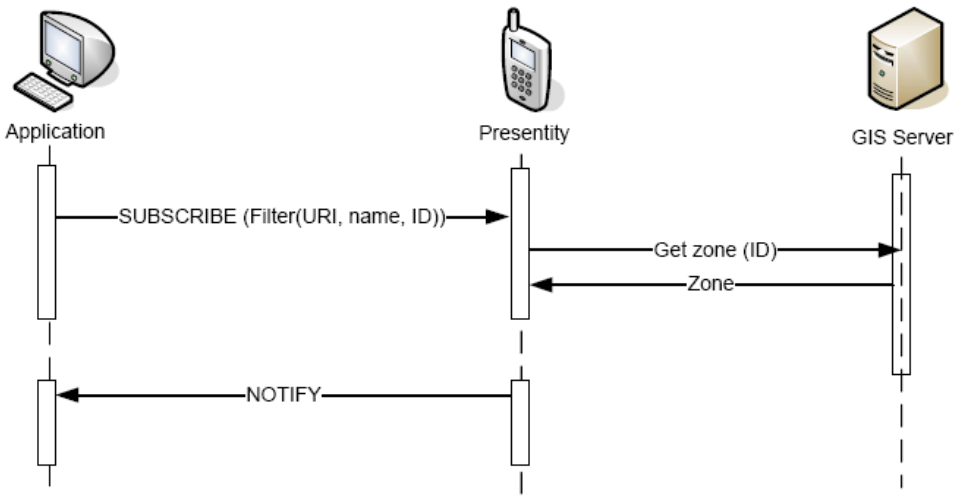


Figure 4: Terminal localization by an application (alternative 2)

According to the second alternative, the user may revoke a subscription anytime or remove zones like in the terminal to terminal case.

3.2 System extensions to support non-trusted applications

A whole class of services related to m-advertising [12] need to push messages to users located in proximity to shops. We cannot directly use the system above because any query or subscription message initiated by the service needs the address of the mobile terminal, thus making the privacy obsolete and opening the way to spam and tracking threats. The basic scenario corresponds to Fig. 1c. To solve this problem we propose to extend the system as shown in Fig. 5. We can identify now three actors: the mobile user, the non-trusted applications (e.g. shops) and a set of trusted services (advertisement, location, messaging) that could be hosted by the network operator. The advertisement service mediates between shops that publish messages associated to certain location zones and between the consumers that first have to register in order to obtain the advertisement service. This procedure is consistent with the permission marketing principle adopted in m-advertising [5]. In the same way the advertisement service hides the identity of mobile users (represented by contact addresses) from the shops.
The shops publish their advertisement messages and the respective locations at the advertisement server, specifying a validity period as well, similar to a broadcast message (see Fig. 5). The trusted advertisement server, having the addresses of the users interested in the shop, initiates the location subscriptions to the corresponding zones. The mobile user has at any time the control over the shops and zones that trigger notifications and can remove them or revoke the subscriptions. The shops can collect statistical data about the subscriptions or the forwarded advertisements, but not about individual users and their behavior.

Journal of Theoretical and Applied Electronic Commerce Research
ISSN 0718–1876 Electronic Version
VOL 2 / ISSUE 2 / AUGUST 2007 / 82 - 91

This paper is Available online at
www.jtaer.com

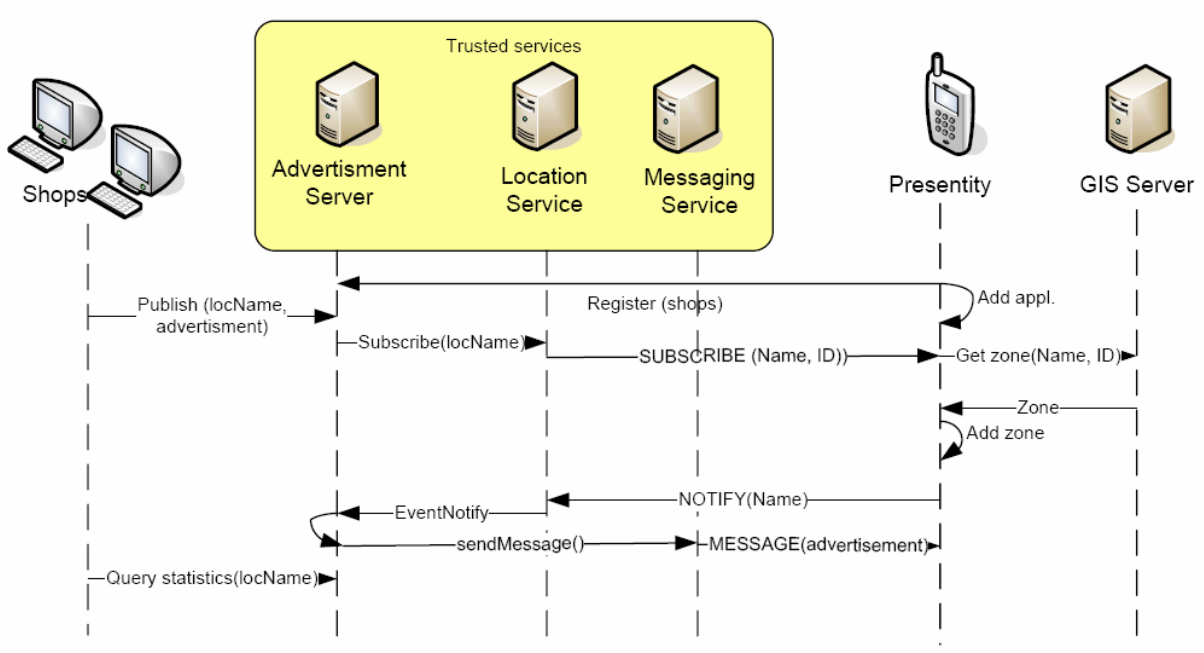


Figure 5: Architecture for an m-advertisement service based on zones

3.3 A server-based solution to reduce the radio traffic

A user that operates the location service in terminal to terminal mode (Fig. 1, a) has local control over the locations and address books available in his mobile terminal. Another alternative is to keep user contact lists and other personal on a server. One advantage of such an architecture (see Fig. 1d) is that the contact lists and other personal data are available from another personal or public terminal or when the terminal is lost or stolen. Another reason for the server solution is to reduce the data traffic: teenagers for example have often more than hundred buddies in their address books: if all buddies would subscribe to the same zone “home” of the user, then 100 notifications would be sent from the presentity over the air interface.
The traffic reduction suggested above becomes first feasible in our zones approach, through the discretization of the location space: similar to the presence case, all the zones defined by a certain user (we can extend this restriction to external locations defined by applications and agreed by the user) are maintained on a location server (see Figure 6). The presentity uses the SIP PUBLISH message as soon as an event caused by entering/leaving of ANY of these zones is triggered at the terminal. In contrast to the former discussed cases, the watcher subscriptions messages terminate now at the location server and the notifications are generated as well by the server. In order for the presentity to know who has subscribed which location zone, we use another mechanism standardized for the presence case, called WatcherInfo [27] notification. The presentity subscribes to WatcherInfo events and receives notifications every time a watcher subscribes to any zone belonging to that user. The main drawback of the server based solution is that the configuration of address books, new zones and the assignment of zones to buddies are done remotely (e.g. using the IETF defined XCAP protocol [29]), raising availability and trust concerns. The server could be part of the centralized solution deployed by the network operator or a home server owned by the user.

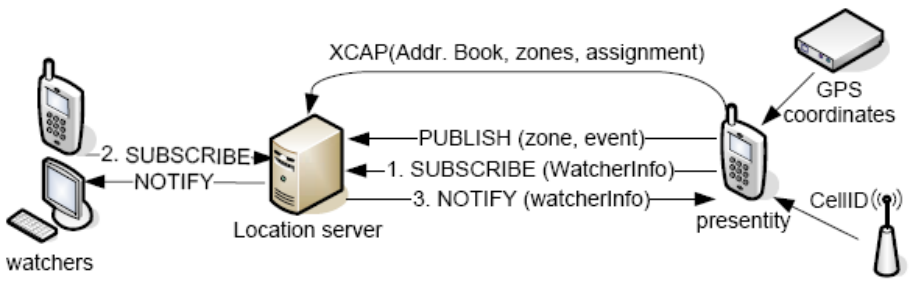


Figure 6: Server-based architecture to optimize the traffic on the air-interface

Journal of Theoretical and Applied Electronic Commerce Research
ISSN 0718–1876 Electronic Version
VOL 2 / ISSUE 2 / AUGUST 2007 / 82 - 91

This paper is Available online at
www.jtaer.com

4 Prototype realization

For the prototype realization we selected a GSM/UMTS mobile terminal running the mobile platform for Java (J2ME), a built-in SIP stack and API according to the JSR 180 [9] and a Bluetooth location interface according to JSR 179 [10] to connect to an external GPS receiver (SiRF Star III Chip). The existing address book function on the mobile has been extended to store SIP addresses of the contacts and each contact is associated to a subset of the places the user has defined and where he can be localized by that contact (for more details on the terminal-side prototype realization, see [7]). Besides the terminal to terminal mode, a location server and application prototype has been built using a SIP application server (BEA/WebLogic). Operated from a browser, the application is able to define location “zones” for different users (integrating Google Maps) to view them, “push” the zones to the users and subscribe to them. The application communicates with the SIP location server via the standardized Parlay X web service API. Finally, the application displays and logs the received notifications. The configuration corresponds to Fig. 1c, however without the GIS server.

One of the practical problems encountered when using area notification was to infer the correct state "inside" or "outside", since the GPS signal fluctuates in urban areas or even disappears when the user enters a building. The outcome from the measurement sequence had to be stabilized through a hysteresis filter. We made experiments that started with "tagging" a place, mostly at the entrance of a building and then accessing this place from different directions and streets. The radius of the area has been varied between 30 and 75 meters and we measured a success rate of 85% in triggering correctly the entering and leaving conditions at different times of the day at walking speed. Figure 7 shows a map-based notification that pops-up when the presentity user enters the zone marked with the circle.

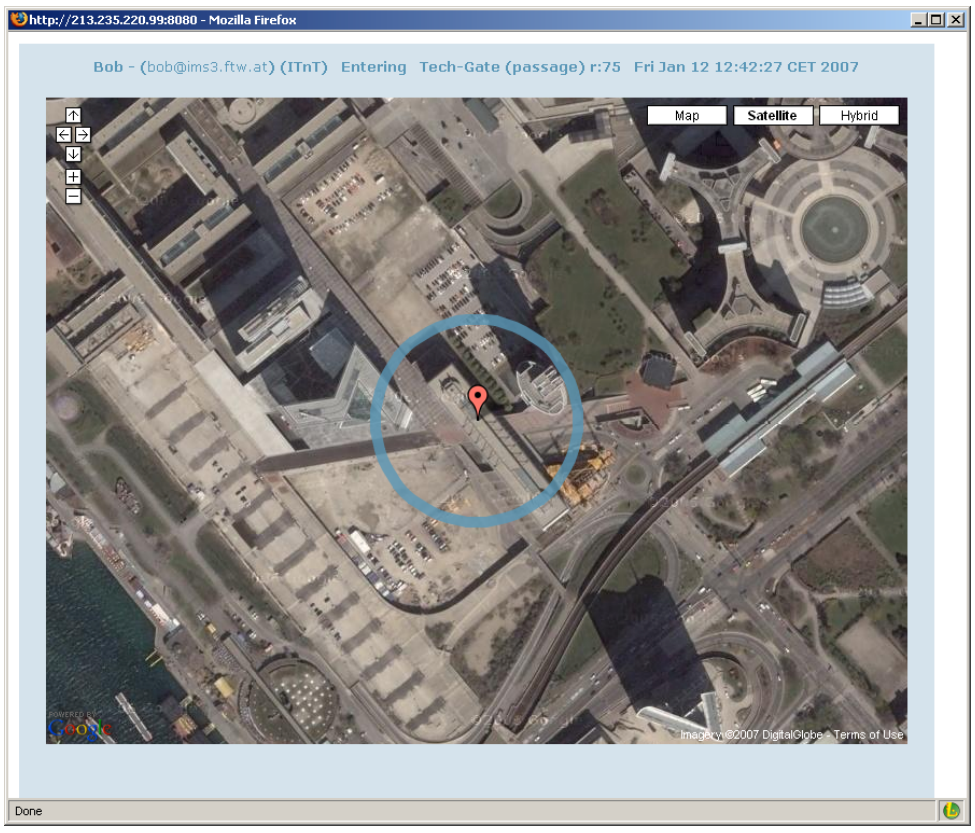


Figure 7: A watcher application (using Google Maps)

5 Related work

Location privacy mechanisms are a part of larger research topic, that of privacy enhancement techniques (a good overview of real privacy scenarios and mechanisms can be found in the deliverables of the IST PRIME project [8]). The work of the Geographic Location/Privacy (Geopriv) working group at IETF provides a quite generic and flexible framework in which our special mechanisms could fit as well (for a recent paper see [32]). Especially the selection of SIP as the “using protocol” between different entities of the Geopriv architecture (location server, location recipient, location generator) and the reuse of mechanisms encountered in the handling of presence are similar to our work.

Journal of Theoretical and Applied Electronic Commerce Research
ISSN 0718–1876 Electronic Version
VOL 2 / ISSUE 2 / AUGUST 2007 / 82 - 91

This paper is Available online at
www.jtaer.com

Geopriv basically defines a Location Object capable to carry both location information and the policy rules for the distribution of this information. However, instead of general policies and authorization rules, we have described a simple zone notification mechanism with tunable privacy that covers many practical scenarios.

At the Columbia University, the use of SIP for location services has been investigated in several publications. Shacham et al. [30] describe different scenarios for location sensing and tracking, device control, emergency calls using the SIP protocol. Küpper and Treu [13] propose complex location update strategies in the mobile terminal in order to realize scalable Location Based Services.

Instead of regarding access control mechanisms to protect location information, Beresford [19] focuses in his Dissertation on a class of location applications, where privacy can be realized through anonymity and pseudonymity, and investigates the degree of anonymity a user still has if he moves in a so called mixed-zone, i.e. between zones in which applications may track him.

Finally, a group of works investigate the use of policies and policy languages such as XACML, P3P etc. to express more complex rules for the protection of user privacy in general and location privacy in particular. Marc Langheinrich [15] describes pawS, a privacy awareness system for ubiquitous computing environments. In paswS, when the user enters an environment in which services are collecting privacy relevant data, a privacy beacon announces the privacy policies of each service, and the interaction with the user privacy policy is similar to that specified in P3P. Myles et al. [17] describe a location server in which so called validators check privacy policies and preferences against application requests to disclose user location and in this way automate the privacy management.
Most of the scenarios mentioned (tracking location by the employer, calling a cab, warning the user of traffic holdups and friend-finder services) can be however realized by our zone concept as well.

6 Concluding remarks and further research

The terminal based location system has major advantages versus the network based one in terms of the performance when using triggered location, scalability and easy distribution beyond the borders of a local network. These advantages are conditioned by solving the privacy problem. The scenarios we address vary from the community service of type "find your friend", the emergency-based scenario up to the m-advertising scenario saying for instance "when I pass the coffee shop, advertise discounted coffee prices".

Tunable privacy with a zone concept can be realized in principle with any overlay protocol, but we intended to show that it can be done with today's (SIP) technology and it complies with the NGN/IMS architecture. Using SIP, we still had to introduce minor extensions [20], mainly for addressing a location user agent and by defining a location event package and its content (in the SIP publish, subscribe and notify messages).

In order to improve the applicability of the zone model in places where GPS does not perform satisfactorily, more research has to be done in combining different positioning methods. For indoors positioning, RFIDs can be placed in the environment, map them to the defined zones and could be deployed as soon as the mobile terminals have a built-in the RFID reader. Bluetooth or WLAN beacons can also identify location zones. In cases where lower location accuracy is acceptable, cell-ID maintained by the network operator could also be used in the following way: the subscription to a location zone defined by a civil address is passed to the presentity terminal and from there, a network provider database is contacted to return the cell-ID corresponding to that location. The trigger occurs in the terminal as in the other cases. There are however two obstacles for this method: first, the actual cell-ID information can be read by client applications only in a few symbian mobile terminals. Second, the network operators are reluctant to disclose cell-ID information to terminals and applications, an attractive business model remains to be found to change this situation.

The presented zone model can be applied to a broad range of location based applications although no particular approach can fit all the applications and this applies to our solution as well. For example in continuous location tracking applications, as discussed in [6], [2] or for tracking remote monitored patients, we recommend the use pseudonyms instead of the zone model, because the position has to be available anytime. However, when the location problem is stated "where is person X?", the identity has to be revealed and our approach that allows a controlled disclosure of zones is preferable to other methods.

Acknowledgements

This work has been funded by the Austrian Government Kplus program. The author would like to thank Oliver Jorns, Rene Gabner, Joachim Zeiss, Marco Happenhofer, Rudolf Pailer and Joachim Fabini from the SIMS project team for fruitful discussions and for helping to realize the location system with tunable privacy.

Journal of Theoretical and Applied Electronic Commerce Research
ISSN 0718–1876 Electronic Version
VOL 2 / ISSUE 2 / AUGUST 2007 / 82 - 91

This paper is Available online at
www.jtaer.com

References

[1] A.R. Beresford, Location privacy in ubiquitous computing, Technical report, UCAM-CL-TR-612. University of Cambridge, 2005.
[2] A.R. Beresford, F. Stajano, Location Privacy in Pervasive Computing IEEE Pervasive Computing, vol. 2, no. 1, pp. 46-55, 2003.
[3] S.Bessler, R.Pailer, Verfahren zum Lokalisieren einer Mobilstation in einem Telekommunikationsnetz, European Patent pending: 02018 ftw, 2006.
[4] S. Bessler, O. Jorns, A Privacy Enhanced Service Architecture for Mobile Users, IEEE International Workshop on Pervasive Computing and Communication Security, PerSec'05 , Kauai Island, Hawaii, USA, March 2005.
[5] S. Godin, Permission marketing: Turning strangers into friends, and friends into customers: Simon and Schuster, 1999.
[6] M. Gruteser, D. Grunwald, Anonymous Usage of Location-Based Services through Spatial and Temporal Cloaking, The 1st Intl. Conference on Mobile Systems, Applications and Services, MobiSys, San Francisco 2003.
[7] M. Happenhofer, Eine Architektur für Positionsbestimmung im IP Multimedia Subsystem, Diplomarbeit, IBK, TU Wien, 2006.
[8] PRIME, Privacy and Identity Management in Europe, Architecture v2 [Online], Available: https://www.prime-project.eu/prime_products/reports/arch/pub_del_D14.2.c_ec_WP14.2_v1_Final.pdf.
[9] JSR 179, Expert Group, Location API for Java 2 Micro Edition, Java Community Process.
[10] JSR 180, Expert Group, SIP API for J2ME, Java Community Process.
[11] H. Khartabil, E. Leppanen, M. Lonnfors, J. Costa-Requena An Extensible Markup Language (XML) Based Format for Event Notification Filtering draft-ietf-simple-filter-format-05, Internet Engineering Task Force.
[12] B.Kölmel, S. Alexakis, Location based advertising, M-Business-The First International Conference on Mobile Business, 2002.
[13] A. Küpper, G. Treu, From Location to Position Management: User Tracking for Location-based Services, in Kommunikation in Verteilten Systemen (KiVS) Kurzbeiträge und Workshop 2005.
[14] A. Küpper, Location-based Services: Willey, 2005.
[15] M. Langheinrich, "A Privacy Awareness System for Ubiquitous Computing Environments," Proc. Ubicomp, LNCS 2498, Springer-Verlag, 2002, pp. 237–245.
[16] R. Mahy, A Document Format for Filtering and Reporting Location Notifications in PIDF-LO draft-mahy-geopriv-loc-filters-01.txt, Internet Engineering Task Force, 2006.
[17] G. Myles, A. Friday, N. Davies, Preserving Privacy in Environments with Location-Based Applications, IEEE Pervasive Computing, vol. 2 , no. 1, 2003.
[18] Open Geography Markup Language (GML) Implementation Specification, OpenGis 02-023r4, Jan 2003.
[19] R. Pailer, F. Wegscheider, S. Bessler, A Terminal-Based Location Service Enabler for the IP Multimedia Subsystem, IEEE Wireless Communications & Networking Conference, Las Vegas (NV), USA, April 3-4, 2006.
[20] R. Pailer, A Location Presence Event Package for the Session Initiation Protocol (SIP), draft-pailer-locpres-00.txt, Internet Engineering Task Force, 2007.
[21] ParlayX White Paper, Available: http://www.parlay.org/imwp/idms/popups/pop_download.asp?contentID=7103.
[22] A. Pfitzmann, M. Hansen, Anonymity, Unlinkability, Unobservability, Pseudonymity, and Identity Management, In Hannes Federrath, ed., Designing Privacy Enhancing Technologies, Proceedings of the International Workshop on Design Issues in Anonymity and Unobservability, vol. 2009 LNCS Springer, 2000. Available: http://dud.inf.tu-dresden.de/literatur/Anon_Terminology_v0.28.pdf.
[23] J. Peterson A Presence-based GEOPRIV Location Object Format RFC 4119, Internet Engineering Task Force.
[24] P. Reichl, S. Bessler, J. Fabini, R. Pailer, J. Zeiss Implementing a Native IMS Location Service Enabler over a Prototypical IMS Core Network Testbed, The 3rd IEEE International Workshop on Mobile Commerce and Wireless Services, San Francisco (CA), USA, June 26, 2006.
[25] P. Reichl, S. Bessler, J. Fabini, R. Pailer, A. Poropatich, N. Jordan, R. Huber, H. Weisgrab, C. Brandner, I. Gojmerac, M. Ries, F. Wegscheider, Practical Experiences with an IMS-Aware Location Service Enabler on Top of an Experimental Open Source IMS Core Implementation, Journal of Mobile Multimedia (JMM), Journal of Mobile Multimedia, vol. 2, no. 3, pp. 189 – 224, 2006.
[26] J. Rosenberg, H. Schulzrinne, G. Camarillo, A. R. Johnston, J. Peterson, R. Sparks, M. Handley, and E. Schooler. SIP: session initiation protocol. RFC 3261, Internet Engineering Task Force, June 2002.
[27] J. Rosenberg, A Watcher Information Event Template-Package for the Session Initiation Protocol (SIP), RFC 3856, Internet Engineering Task Force, 2004.
[28] J. Rosenberg, A Presence Event Package for the Session Initiation Protocol (SIP), RFC 3856, Internet Engineering Task Force, 2004.
[29] J.Rosenberg, The Extensible Markup Language (XML) Configuration Access Protocol (XCAP), draft-ietf-simple-xcap-12, Internet Engineering Task Force, 2006.
[30] R. Shacham, H. Schulzrinne, W. Kellerer, and S. Thakolsri, An architecture for location-based service mobility using the SIP event model, in Mobisys, Workshop on Context Awareness, Boston, 2004.
[31] H. Schulzrinne, V. Gurbani, P. Kyzivat, J. Rosenberg, RPID: Rich Presence Extensions to the Presence Information Data Format (PIDF), RFC 4480, Internet Engineering Task Force, July 2006.
[32] H. Tschofenig, H. Schulzrinne, A. Newton, J. Peterson, A Mankin, The IETF Geopriv and presence architecture focusing on location privacy, Position paper at W3C Workshop on Languages for Privacy Policy Negotiation and Semantics-Driven Enforcement, Ispra, Italy, 2006.