POSITION INFORMATION FOR VOIP EMERGENCY CALLS
Originating from a Wireless Metropolitan Access Network

J. Barceló, B. Bellalta, C. Macián, M. Oliver and A. Sfairopoulou
Technology Department, Universitat Pompeu Fabra, Passeig de Circumval.lació 8, Barcelona, Spain

Keywords: Location, WiFi, VoIP, Emergency Calls.

Abstract: This article describes a mechanism to provide location information about users of a wireless metropolitan access network to trusted and authorized third parties. A case of particular interest is that of providing emergency centers with the location of the VoIP caller. The location information is obtained from the wireless access points using SNMP polling, and stored in a location server. The outbound SIP proxy server requests the user's location and includes it in the SIP invite message when the callee is an emergency center.

1 INTRODUCTION

VoIP communications appear as a new channel to reach emergency call centers. However, they usually fail to provide the position of the caller.

The provision of the position to the emergency center consists of two steps; first, obtaining the position of the user, and second, transmitting this information to the emergency center.

The proposed solution focuses on a scenario in which the caller is connected to a Wireless Metropolitan Access Network. This is a level-2 network, or a Internet Attachment Provider (IAP) in the terminology of the Internet draft that addresses emergency SIP calls (Schulzrinne and Marshall, 2006). The other supposition is that the emergency call is actually an end-to-end IP call. In other words, that it terminates in a IP-capable emergency center.

The second section of the article references some related work. The third section addresses the problem of collecting caller's position in a Wireless Metropolitan Access Network based on IEEE 802.11 technology. In the fourth section the distribution of such information to third party web applications is explored. Section 5 is devoted to the inclusion of caller location information in emergency calls. The last section concludes this preliminary work.

2 RELATED WORK

In our approach the location of the user is approximated by the position of the access point to which the wireless terminal is associated. There are different alternatives to find that association detailed in(Clementi, 2005).

The accuracy might be increased by compiling radio measures from the user's device and comparing them with a radiomap that reflects the propagation characteristics of the environment (Bahl and Padmanabhan, 2000).

For practical purposes, a network-assisted approach is much more desirable. In this case the information is obtained from network devices rather than networked devices. This would allow to find the position of any kind of terminal, no matter whether it is a laptop, a PDA or a telephone.

Once the user is located, the position information has to be attached to the call, and the call has to be routed to the corresponding emergency center. (Rosen et al., 2006) covers these aspects in a general way.

The recommendations for position information management are described in (Cuellar et al., 2004). (Peterson, 2005) defines the position object, called Presence Information Data Format - Location (PIDF-LO).

(Polk and Rosen, 2006) proposes a mechanism to convey position information in a SIP message. It in-

Barceló J., Bellalta B., Macián C., Oliver M. and Sfairopoulou A. (2007).
POSITION INFORMATION FOR VOIP EMERGENCY CALLS - Originating from a Wireless Metropolitan Access Network.
In *Proceedings of the Third International Conference on Web Information Systems and Technologies - Internet Technology*, pages 393-396
DOI: 10.5220/0001277203930396

volves the inclusion of a new SIP header, the Geolocation header, either with the PIDF-LO in the body or as a location-by-reference URI. Since in our proposal the terminal is not aware of its own position, and body parts may not be inserted by a proxy server, the only applicable solution is specifying a location-by-reference URI.

Current work at the IETF mainly supports the idea that the user terminals obtain their own position at boot time (e.g. using DHCP) and then include this information in the SIP message that initiates the call. This approach has two main shortcomings. The first is that the UAs that are available nowadays do not include emergency call and location functionality. The second is the assumption that the terminal has not moved since boot time (or last DHCP renewal). For this reason, this article suggests a network-oriented approach, that will work with existing SIP phones.

3 OBTAINING THE POSITION INFORMATION

Every wireless access point maintains a table that contains the associated terminals' addresses. This information can be collected to roughly determine the position of a user, since the coverage area of an access point is limited, specially indoors (typically less than 100m).

This kind of position information is called *cell tower/sector*. This is one of the types of location information supported by the IETF and is intended for mobile networks (sectorial) towers. The others are *civic* and *geospatial* (WGS84 coordinates). The tower (in our case the access point) position is expressed as a point, and might include an irregularly shaped polygon of geospatial coordinates reflecting the coverage footprint.

The entity that collects and re-distributes location information is called location server. A database is created in the location server, containing a table with the IP address of each access point, together with the position of the access point (coordinates), the size of the cell, and type of access point (i.e. the manufacturer, model and firmware version). Based on this table, an SNMP poll is conducted periodically to obtain the association tables from the Management Information Base (MIB). These tables contain the MAC addresses and IP addresses of the wireless terminals associated to the polled access point.

After polling all the access points the location server can store in a database the association between terminal address (MAC and IP) and access point address (IP). And knowing this association, the position of the terminal can be inferred.

The time granularity depends on the frequency of the polls. The design decision in our implementation is to perform polls every 30 seconds. More polls would offer more accuracy, but also generate more network traffic. A solution to increase time accuracy that does not have such an impact in network traffic consists on combining SNMP polls with SNMP traps. Some access points can be configured to issue an SNMP trap (a message to the network management service) after IEEE802.11 events (association or de-association of terminals) occur. A solution based only on traps is undesirable, because the traps (UDP packets) can be lost on their way to the location server, specially on wireless links.

4 MAKING THE LOCATION INFORMATION AVAILABLE TO TRUSTED THIRD PARTIES

Previous work in this area (Hong et al., 2003) already recognized the importance of mechanisms to distribute the position information only after user consent. Our proposal differs from the previous ones in that it is completely web-based. The user does not need to install any special software in her wireless terminal to manage the position information.

In our testbed, the access network is owned and managed by an entity called the Neutral Operator. This entity would be in charge of running the location server. If this location information has to lead to a plethora of new and original services, it should be available to third parties. Being position information tightly related to privacy, only trusted parties should be provided with such information, and always after user consent. We propose that the location server offers this data via a Web Service interface in the public Internet. Any organization interested in providing position-aware content should apply to the Neutral Operator. If the organization is considered trusted, the Neutral Operator will provide it with credentials that allow identification in subsequent transactions.

The reason to choose Web Services is to make the position information available to the broadest variety of position-aware applications. Mobile operators have already chosen this mechanism to provide cell-related position information to their commercial partners. Making the position provision for WiFi network operators similar to the one offered by mobile operator would simplify the implementation of position-aware applications that act as consumers from both sources. The implementation uses Axis' native JWS

(Java Web Services) files.

A well defined process has been established to guarantee that the position information is offered only after user authorization. It consists in a number of steps that are illustrated in figure 1.

During the authorization process, a user that is browsing a location aware website is redirected to an interface of the location server that is connected to the same access (level 2) network as the user. Then the user is going to be back-redirected to the position-aware website.

Every time that the position-aware application contacts the location service, it has to provide a user name and a password for authentication purposes. This detail has been obviated in the explanation that follows for the sake of simplicity.

Another aspect that should be highlighted from figure 1 is that the location server needs two physical interfaces. The first interface is connected to the access network where the user resides. Usually, the wireless terminals use private addressing, and therefore the first interface of the location server probably has a private address. In any case it needs an address in the same subnet as the user's terminal.

The second interface connects the location server to the Internet. This interface is used to communicate with third party position-aware applications and is configured with a public Internet address.

This is a step-by step explanation:

1. The user browses to a position-aware website.
2. This site wants to obtain the position of the user, in order to provide that user with position tailored content. The position-aware website needs to contact the location server to ask for that information, but explicit authorization from the user is needed. To obtain that permission, the position-aware website contacts the location server and sends a user identifier (*user_id*). This *user_id* must be unique in the position-aware-website. The back-redirect URL (which is going to be used again in step 7) is also sent.
3. As an answer the location server sends an url pointing to an interface of the location server that is situated in the access network.
4. The position-aware website redirects the user to the url indicated in the previous step, delivering the application name and the *user_id* as parameters attached at the URL.
5. At this point, the location server receives the HTTP request from the user. It captures the user MAC address and associates it to the position-aware website and *user_id* in the database.

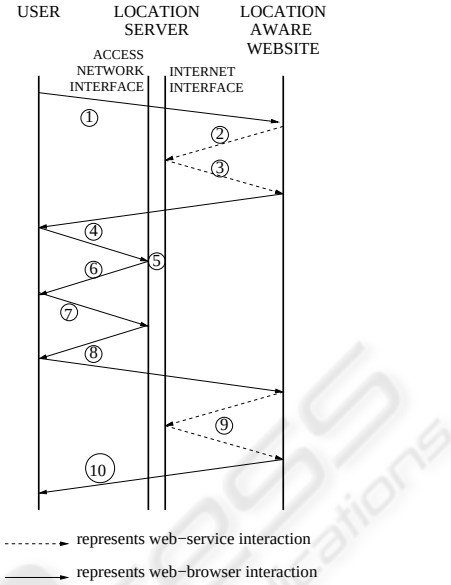

Figure 1: Steps to authorize the provision of position information to trusted third parties.

The MAC value is the key value that allows to search for a user in the position database, since it is the value that appears in the access points association tables.

6. The location server presents a form to the user asking if she or he wants to be located by the position-aware website for a given period of time (e.g one hour).
7. The user agrees.
8. The user is back-redirected to the location-aware website, using the url mentioned in step 2.
9. Now the position-aware website can request position information.
10. And deliver the position-tailored content to the user.

The Web Services transactions contain sensitive information such as credentials and the position of the user and therefore they should be appropriately secured (TC, 2006).

The described protocol offers position information to trusted third parties without revealing any further information about the user. Usually, the position-aware website does not even know the IP address of the wireless terminal, since the terminal is probably assigned a private address that is converted using NAT/PAT. However, a user might decide to provide its identity (by any means, out of the scope of this work) and its position to the same position-aware application. In this case, this pair of items have severe

privacy implications and should be protected consequently.

5 PROVIDING EMERGENCY CENTERS WITH LOCATION INFORMATION

When adding position information to calls, it makes sense to use SIP mechanisms instead of Web Services. Thus the *Geolocation* header is used as proposed in (Polk and Rosen, 2006) containing location-by-reference. This header is introduced by the SIP proxy server. That means that both the SIP proxy and the emergency center will need to contact the location server to obtain the position of the terminal. The dialogs with the location server will benefit from the Web Services interface described in section 4 but will skip the user authorization web-based mechanism.

```
INVITE sip:112@emergency.cat SIP/2.0
Via: SIP/2.0/UDP sipproxy.voipow.com
  ;branch=z9hG4bK77ef4c2312983.1
Via: SIP/2.0/UDP pc33.voipow.com
  ;branch=z9hG4bK776asdhds
Max-Forwards: 70
To: 112 <sip:112@emergency.cat>
From: Victor <sip:victor@voipow.com>
  ;tag=1928301774
Call-ID: a84b4c76e66710@pc33.voipow.com
CSeq: 314159 INVITE
Contact: <sip:victor@pc33.voipow.com>
Resource-Priority: wps.0
Geolocation: sips:3sdefrhy2@lis.voipow.com
Supported: geolocation
Content-Type: application/sdp
Content-Length: 142
```

In the proposed example, Victor is in trouble and calls to the emergency center. Victor is a client of the *voipow* VoIP over Wireless service provider and therefore the SIP phone sends the requests to its outbound proxy called sipproxy.voipow.com[1]. The proxy realizes that the destination of the call corresponds to an emergency center and contact the location server to obtain the position of the user.

The SIP proxy knows both the IP and the MAC address of the terminal initiating and emergency call and it is considered a trusted third party by the location server and therefore is allowed to obtain the position of the user. In this special case, the SIP proxy does not need explicit authorization from the user to get the position information.

[1]It has to be noted that this proxy needs direct connection to the wireless metropolitan access network, and therefore the solution outlined in this paper is not general, but restricted to this scenario

The position information is included in the form of a header called Geolocation. This header has to be de-referenced by the emergency center to obtain the user position in the form of PIDF-LO object.

In addition to the position header, the highest Resource-Priority header is included in the request, in accordance to (Schulzrinne and Polk, 2006)

6 CONCLUSION

This article presents ongoing work for collecting information about the position of the users of a Wireless Metropolitan Access Network and storing it in a location server. After user authorization, this location information can be offered to trusted third parties that provide location tailored content.

A VoIP service provider operating in that network, can incorporate intelligence in the outbound proxy to interact with the location server. Then the location information can be conveyed in SIP invite messages in emergency calls. The location information is used to route the call and is presented to the emergency center operator.

REFERENCES

Bahl, P. and Padmanabhan, V. N. (2000). Radar: an in-building rf-based user location and tracking system. In *IEEE INFOCOM*, volume 2, pages 775–784.

Clementi, L. (2005). Infrastrutture di supporto per il progetto di servizi dipendenti dalla locazione. M. eng. thesis, Università degli Studi di Bologna, Italy.

Cuellar, J., Morris, J., Mulligan, D., Peterson, J., and Polk, J. (2004). Geopriv Requirements. RFC 3693 (Informational).

Hong, J. I., Boriello, G., Landay, J. A., McDonald, D. A., Schilit, B. N., and Tygar, J. (2003). Privacy and security in the location-enhanced world wide web. In *UBICOMP*.

Peterson, J. (2005). A Presence-based GEOPRIV Location Object Format. RFC 4119 (Proposed Standard).

Polk, J. and Rosen, B. (2006). Session initiation protocol location conveyance. Internet draft.

Rosen, B., Schulzrinne, H., Polk, J., and Newton, A. (2006). Framework for emergency calling in internet multimedia. Internet draft.

Schulzrinne, H. and Marshall, R. (2006). Requirements for emergency context resolution with internet technologies. Internet draft.

Schulzrinne, H. and Polk, J. (2006). Communications Resource Priority for the Session Initiation Protocol (SIP). RFC 4412 (Proposed Standard).

TC, O. W. S. S. (2006). Web services security v1.1.