Role(s) of a Proxy in Location Based Services

20th February 2002

Alberto Escudero-Pascual
<aep@kth.se>

Gerald Q. Maguire Jr.
<maguire@kth.se>

TSLab - IMIT
Royal Institute of Technology (KTH)
Stockholm, Sweden

Wireless@KTH
Royal Institute of Technology (KTH)
Stockholm, Sweden

Abstract

We examine a number of roles that a proxy server can play in Location Based Services and how it can be used to provide protection of personal identifiable information. Location data, service requests, and privacy policies are encoded in XML by the mobile terminal and forwarded to a proxy server placed between the mobile terminal and the location based service(s). We will show that by a suitable architecture in the mobile client and in the proxy that we can hide the network location of the mobile device, hide the identity of the user of the mobile device, and in some cases even provide misleading physical location(s) for the mobile device. We will illustrate a number of different functions which can be provided by examining some scenarios.

In order to illustrate our approach, we have applied our privacy model to location information obtained from a Global Positioning System receiver. Among the different methods to obtain a mobile's position the GPS-based method was chosen as being the only method, available today, where the Positioning Calculation Function (PCF) is fully under the user's control, since the position is calculated within the GPS-equipped mobile terminal; while other technologies rely on the network infrastructure and hence some or all of the position data is outside the control of the user.

A proof of concept was implemented using Fastrax's iTrax02 GPS receiver. The iTrax02 is an ultra-low power consumption receiver, roughly the size of a stamp and specifically designed for small portable devices. In one of the scenarios, the location information is encrypted using a public key encryption scheme (with multiple private keys), embedded in a XML message and transmited to a proxy that runs a secure DNS update module. This location privacy solution allows a mobile terminal to publish its location as an encrypted DNS location record via the proxy, while concealing from eavesdroppers and third parties the relation between the location information and the identity of the mobile terminal and its user.

1 Introduction

Location-based services (LBS) can be described as applications that exploit knowledge about where an information device (user) is located. For example, location information can be used to provide automobile drivers with optimal routes to a geographical destination or a group of friends with the names and coordinates of Spanish's restaurants in the neighborhood open on a Saturday night.

Location information can be used as external input for applications, but can also be used by lower layers in combination with link level information in mobile networks to optimize network performance for example in assisting in handover decisions for MobileIP [3].

When talking about cellular networks, location-based services exploit any of several technologies for determining where a network user is geographically located. ETSI has issued a specification [2] that deals with different methodologies to obtain location information of a mobile station as follows: Time Advance (TA), Time of Arrival (TOA), Enhanced Observe Time Difference (E-OTD), Angle of Arrival (AOA) and Global Positioning System (GPS).

Depending on where the information is gathered and the position calculation function (PCF) is computed the different methods to obtain the position can be divided in four categories: network based, network based-mobile assisted, network assisted-mobile based, and mobile based [2].

This paper deals with the situations when then the position is computed in the terminal (i.e., mobile based) with or without assistance from the network. In these scenarios the user is in control of the location information associated with the mobile device. However, problems arise when the user needs to provide that information in order to obtain a service and at the same time doesn't want to reveal more personal identifiable information that is strictly necessary [1]. For example, a mobile user may want to inform to only a certain number of people for a certain period of time about his or her position or, to learn the position of the nearest catholic church without revealing his or her personal identity.

The paper is divided as follows:

SECTION 2 contains the description of our Location Based Services Architecture and the role of the proxy server.

SECTION 3 describes some technologies that can be integrated in some of the modules and will empower users to control their personal information.

SECTION 4 introduces GPS positioning, NMEA messages, and the iTrax02 GPS receiver

SECTION 5 illustrates a number of different services which can be provided by examining some scenarios.

This is followed by conclusions and the bibliography .

2 Location Based Services Architecture

We propose a privacy enhanced location based service (PE-LBS) architecture composed of six functional modules which allows a mobile node to request location based services via a proxy server. Once the basic functionalities are described, we will show that by using our architecture in the mobile client and in the proxy that we can hide the network location of the mobile device and hide the identity of the user of the mobile device.
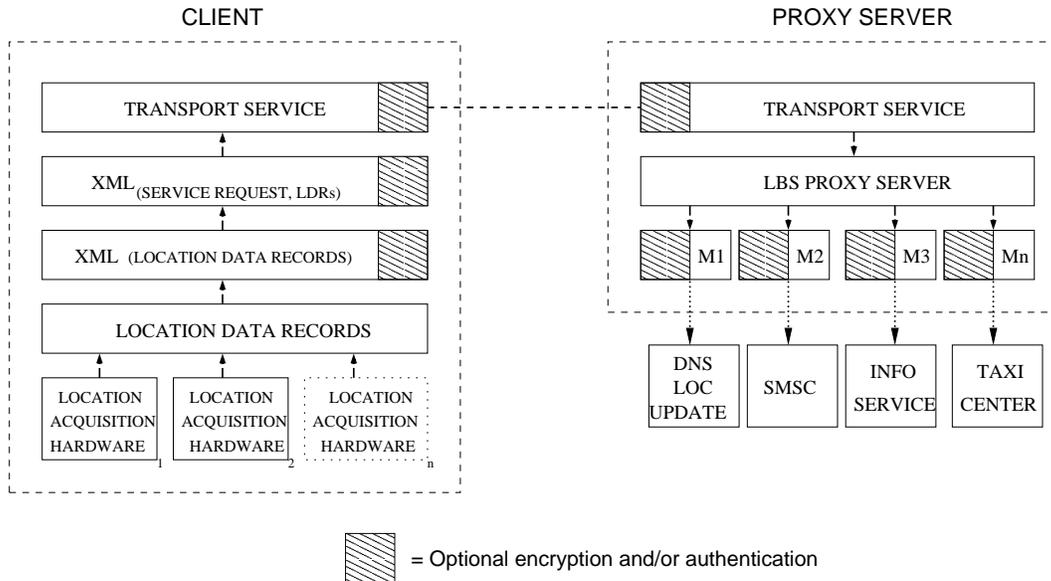
Figure 1: PE-LBS Architecture

2.1 Location Acquisition Hardware

The location acquisition hardware is responsible for calculating the position of the mobile device based on a set of data inputs that can vary from GPS radio signals or infrared beacons to an enhanced tape measure. The output is a set of coordinates based on a reference system. For example, most GPS receivers use a global reference system named WGS 84 (World Geodetic System 1984).

Location information records obtained from the hardware can include: latitude, longitude, altitude, velocity, horizontal error, vertical error, global error, orientation, etc.

2.2 XML Location Data Record

The format of the location records provided by the hardware or multiple pieces of hardware can be of very different nature. The XML Location Data Record module is reponsible for creating XML output based on location information provided by the location acquisition hardware. An example of a XML location data output encoded based on [5,6] looks like:

```
<?xml version = "1.0" encoding = "UTF-8"?>
<loc:SLO xmlns:loc="http://www-nrc.nokia.com/ietf-spatial/2001/05/08/location"
        xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
        xsi:schemaLocation="http://www-nrc.nokia.com/ietf-spatial/2001/05/08/location
        http://www-nrc.nokia.com/ietf- spatial/2001/05/08/location.xsd">
  <POS>
    <LAT>N59.40.54</LAT>
    <LONG>E017.94.36</LONG>
  </POS>
  <ALT>+12.99</ALT>
  <ALT_MSL>010</ALT_MSL>
```

```
    <H_ACC>50</H_ACC>
    <V_ACC>2.5</V_ACC>
    <TIME>2001-13-11T12:00:01+02:00</TIME>
    <G_SPEED>2.0</G_SPEED>
    <V_SPEED unit="knot">1</V_SPEED>
    <DIR>M240</DIR>
    <COURSE>M30</COURSE>
    <H_ORIENT>T25</H_ORIENT>
    <V_ORIENT>179</V_ORIENT>
</loc:SLO>
```

2.3 XML Service Request

The XML service request module will take the location information from the XML location data record and build a service request. In our architecture the service request uses Simple Object Access Protocol (SOAP) [4] to encapsulate and exchange RPC calls using the extensibility and flexibility of XML. SOAP can potentially be used in combination with a variety of other protocols; however, the most common use of SOAP is in combination with HTTP, the experimental HTTP Extension Framework, or SNMP.

```
POST /Temperature HTTP/1.1
Host: www.lbs-proxyserver.com
Content-Type: text/xml
Content-Length: 357 SOAPAction: "http://weather.org/query#GetTemperature"

      <SOAP-ENV:Envelope
         xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/"
         SOAP-ENV:encodingStyle="http://schemas.xmlsoap.org/soap/encoding/">

       <SOAP-ENV:Body>
       <m:GetTemperature xmlns:m="http://weather.org/query">
          <TIME>2001-01-01T12:00:01+02:00</TIME>
          <LAT>N59.40.54</LAT>
          <LONG>E017.94.36</LONG>
        </m:GetTemperature>
       </SOAP-ENV:Body>

      </SOAP-ENV:Envelope>
```

The previous example can be translated as: Ask www.lbs-proxyserver.com (a SOAP server) to provide the temperature (GetTemperature) at latitude: N59.40.54 and longitude: E017.94.36 at 2001-01-01T12:00:01+02:00 from http://weather.org/query
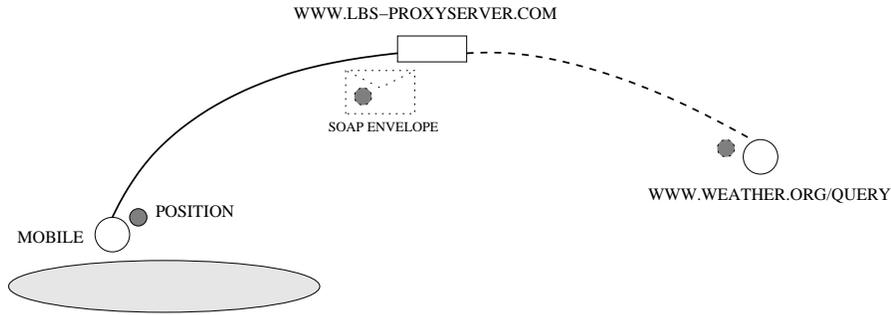
Figure 2: Position information in LBS request

2.4 Transport Service

This module implements the equivalent of OSI layer 4 by providing reliable transparent data transfer between end points, along with error recovery, and flow control. It is responsible for the transport of the remote procedure call to the location based service proxy server.

2.5 Location Based Service Proxy Server

The functionality of the LBS Proxy Server is to process SOAP (message envelope) requests and generate responses. When the SOAP request is recieved by a server, it gets bound to the class specified in the request. The proxy server works as a *SOAP Dispatcher*, by determining which class should handle a given request, and loading that class, if necessary. The SOAP server acts as an intermediary between a SOAP client and the requested service provider.

2.6 Service Modules

A service module acts as SOAP interface, a frontend that requests information or the execution of a procedure, parses and formats the response and returns it according to the request (if necessary). The procedure can run in the same server (e.g. return a prime number of n bits) or be the result of a call in a remote server (e.g. send an e-mail message to a certain address).

Let us consider again the example presented in section 2.3, where a mobile device with a unique identifier *mobileID* requests the temperature information for a certain position and time. In this case, the SOAP server (LBS-proxy) works as a proxy of the SOAP client (mobile device) and the temperature service provider. In fact, the proxy can conceal from the temperature server the mobile device's *mobileID* and protect its identity as this information is not required to obtain the requested service. But, must the proxy know about the location of the mobile device to proxy the temperature request service? No, we can hide the position information from the proxy and still get the temperature in that position. To do this we use a privacy enhanced proxy.

3 Privacy enhanced LBS architecture. *PE-LBS*

The architecture described below is composed of six modules: location acquisition hardware, XML data record parser, XML service request, transport module, LBS proxy and service modules. In this section we are going to describe some technologies that carefully integrated can enhance the privacy of our architecture by protection personal identifiable information.

3.1 XML encryption

XML Encryption [7] is a recently developed cryptographic format that describes the process for encrypting data and representing the result in an XML Encryption *EncryptedData* element which contains or identifies the cipher data. XML Encryption may be used on a whole XML document, an XML entity, an XML entity content, or on arbitrary binary data.

XML Encryption supports both symmetric cryptographic algorithms (AES and Triple DES) and asymmetric cryptographic algorithms (also referred to as key transport algorithms such as RSA).

After encryption the resulting cipher text is either included within the original XML document encoded as a base64 octet sequence or if the cipher text is located outside the document an URI reference reveals the location where the cipher text can be found. The <Encrypted-Data> entity replaces the original entity or entity content. The <EncryptedData> entity contains both the cipher text and related information, needed for decryption of the cipher text into plain text.

In summary, by combining XML Encryption with XML Signature we can provide both message digest and message authentication functionality.

Consider again the example presented in section 2.3, by using XML encryption we can conceal from the proxy server the values LAT, LONG, TIME of the GetTemperature request. The next example shows the use of *3des-cbc* symmetric encryption to encrypt the content of the GetTemperature request.

```
POST /Temperature HTTP/1.1
Host: www.lbs-proxyserver.com
Content-Type: text/xml
Content-Length: 357 SOAPAction: "http://weather.org/query#GetTemperature"
      <SOAP-ENV:Envelope
        xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/"
        SOAP-ENV:encodingStyle="http://schemas.xmlsoap.org/soap/encoding/">
       <SOAP-ENV:Body>
        <m:GetTemperature xmlns:m="http://weather.org/query">
         <EncryptedData xmlns='http://www.w3.org/2001/04/xmlenc#'
            Type='http://www.w3.org/2001/04/xmlenc#Content'>
          <EncryptionMethod Algorithm='http://www.w3.org/2001/04/xmlenc#3des-cbc'/>
          <ds:KeyInfo xmlns:ds='http://www.w3.org/2000/09/xmldsig#'>
          <ds:KeyName>KeyID
           </ds:KeyName>
           </ds:KeyInfo>
         <CipherData>
             <CipherValue>XkIHMHS4ka4CXFWA3yESBqQzIp21D1
                MHYgeREk3i5OBBDrPGPUCkL7bXoC8S9tQlIKbghA
                kHbZDgrzBI6yvP33</CipherValue>
         </CipherData>
        </m:GetTemperature>
       </SOAP-ENV:Body>
      </SOAP-ENV:Envelope>
```

(W) Transport Layer Security

SOAP ENVELOPE

SOAP HEADER

SOAP BODY

XML Content

Elements

XML encryption

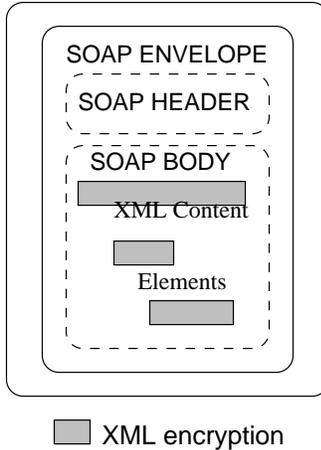Figure 3: Privacy Enhanced Location Based Service Request

3.2 Transport Security Protocols

A transport security protocol provides confidentiality; data integrity, and authentication for information exchanged between a client and a server from the session layer and above in the OSI model and in the WAP stack. The most frequent used protocol for securing plain text transmissions for wired usage is IETF's Transport Layer Security (TLS) based on Netscape's Secure Socket Layer (SSL) [9].

For wireless usage the WAP forum developed the optional Wireless Transport Layer Security (WTLS) protocol that operates below the WDP and WTP protocols [8].

A transport security protocol as (W)TLS can be used to provide confidentiality; data integrity, and authentication for SOAP messages exchanged between the LBS proxy server and the mobile device.

4 Private LBS with GPS-equipped mobile terminal

4.1 Introduction to GPS positioning

The Global Positioning System (GPS), originally a US military technology, was made available for civilian uses by its owner the US Department of Defense in the early 1990's. The GPS system is one of the most accurate navigation systems available today. The system consists of a network of 24 active satellites orbiting the Earth once every 12 hours and in six orbits orbits at inclinations of 55 degrees from the equator and at aproximately 20200 Km altitude.

The Global Positioning System (GPS) provides positioning services to both U.S. Department of Defense and civil user communities. Most of the civil GPS user community uses the Standard Positioning Service (SPS) broadcast at L1 (1575.42 MHz) frequency. Most of the military uses of GPS uses the SPS for signal acquisition and the Precision Positioning Service (PPS) broadcast at L2 (1227.6 MHz) frequency for tracking.

PPS provides 3D accuracy of about 16 meters 95% of the time. The scientific and geological surveying GPS user communities have been able to make use of both L1 and L2 on the ground, with a differential service, to achieve horizontal and vertical error of less than one meter.

The Federal Aviation Administration (FAA) and the Department of Transportation are developing the Wide Area Augmentation System (WAAS) program [10] for use in precision flight approaches. Currently, GPS alone does not meet the FAA's navigation requirements for accuracy, integrity, and availability. Systems like the FAA's WAAS makes use of both L1 and L2 to compute corrections for the ionosphere, ephemeris, and clock, which are then broadcast over L1. WAAS is being designed to achieve Category I precision approach requirements.

New advances in accuracy are expected in the next years, as part of the GPS modernization initiative two additional signals would be made available for civil use. One of these signals (second civil signal) at 1227.60 MHz (L2) frequency will be available on satellites to be launched beginning in 2003 for non-safety critical applications. The other signal (third civil signal) at 1176.45 MHz (L5) frequency will be available on GPS satellites to be launched beginning in 2005 and GPS augmentation satellites (Geostationary) to be launched in 2004/2005 for civil aviation safety-of-life services and other applications.

4.2 Position calculation in GPS

Each satellite is carrying atomic clocks for transmitting timing signals worldwide. Any observer who can receive signals from four of these satellites can determine his accurate position on earth. The satellites orbit the earth twice each day which allows a receiver to see from five to eight of them from any position on the Earth at anytime.

To calculate its position, the receiver needs to know at least the position of three satellites (four satellites are needed to include the time) and the distance from the GPS receiver to the satellites.

In order to know where the satellites are located the GPS receiver collects the almanac and ephemeris information from the radio signals. The "almanac" contains information about the satellite's orbit and provides the approximate location of the satellite, the second type of information, "ephemeris", is uploaded to the satellites from groundstations and provides for a period of four to six hours the neccesary corrections to adjust the planned orbit information to the actual orbit.

Each satellite transmits two signals: L1 (1575.42 MHz) and L2 (1227.60 MHz). The L1 signal is modulated with two pseudo-random noise signals - the protected (P) code, and the coarse/acquisition (C/A) code. The L2 signal only carries the P code. Each satellite transmits a unique code, allowing the receiver to identify the signals. When a feature called "Anti-Spoofing" is active, the P code is encrypted, and known as P(Y) or Y code.

Civilian navigation receivers only use the C/A code on the L1 frequency (although some high-end civilian surveying GPS receivers utilize the carrier frequency of the L2 band for more precise measurements).

The receiver measures the time required for the signal to travel from the satellite to the receiver, by knowing the time that the signal left the satellite, and observing the time it receives the signal, based on its internal clock.

If the receiver had a perfect clock, exactly in synchronization with those on the satellites, three measurements, from three satellites, would be sufficient to determine the receiver's position in 3 dimensions.

Each measurement ("pseudorange") gives a position on the surface of a sphere centred on the corresponding satellite. Due to receiver clock error, the four spheres will not intersect at a single point, but the receiver will adjust its clock until they do, providing very accurate

time, as well as position information. Since the receiver must adjust its clock to be precisely in synchronization with GPS time, a GPS receiver can be used as a precise time reference.

4.3   NMEA General Message Format

The National Marine Electronics Association (NMEA) issues standards for interfacing to marine electronics. NMEA 0183 is a standard protocol, use by GPS receivers to transmit data to attached devices. The data transmition accours at 4800 bps, with 8 data bits, no parity, and one stop bit (8N1). NMEA 0183 sentences are all ASCII (from 20 ... 127 decimal or from HEX 20 to HEX 7F). In the case of GPS data the messages starts with '$GP' followed by message id field. Message data fields are separated by commas (,) and the message ends after the checksum field and carriage return <CR> and line feed <LF> control characters. Delimiter '*' precedes the checksum field.

```
$GP<messageid>,<data field>,<data field>,...*<checksum><CR><LF>
```

For example the NMEA 0183 message:
```
$GPGLL,5924.3131,N,01756.5752,E,134703.77,A,A*61
```

is a Geographic Position Latitude/Longitude message (GLL) that provides: Latitude, Longitude, UTC time of fix and status and has the following general format:
```
$GPGLL,xxmm.dddd,<N|S>, yyymm.dddd,<E|W>,hhmmss.dd,S,M*hh<CR><LF>
```

`xxmm.dddd`   Latitude: xx = degrees, mm = minutes, dddd = decimal part of minutes

`<N|S>`   Either character N or character S, (N = North, S = South)

`yyymm.dddd` Longitude: yyy = degrees, mm = minutes, dddd = decimal part of minutes

`<E|W>`   Either character E or character W, (E = East, W = West)

`hhmmss.dd` UTC time: hh = hours, mm = minutes, ss = seconds, dd = decimal part of seconds

`S`   Status indicator: A = valid, V = invalid

`M`   Mode indicator: A=autonomous, N=data not valid

4.4   About iTrax02

Fastrax's GPS (Global Positioning System) receiver, shown in Fig. 4, is roughly the size of a postage stamp, 25x25x4 mm. The small foot print combined with ultra-low power consumption (130mW in full operational mode) and low cost make it feasible to utilize GPS positioning technology in mass-market applications, particularly those designed for small portable devices, in which low power consumption and small size are crucial parameters, such as in mobile phones, sports instruments, and handheld computers.

Fastrax receivers have very good sensitivity. Receiver sensitivity is one of the most important features of all GPS receivers as all other functions are dependent on receiver's ability to find satellites fast and receive the information from the satellites and convert these measurements into a 3D navigational vector. iTrax02 is able to produce and interpret standard NMEA as well as their own binary format *iTalk*.
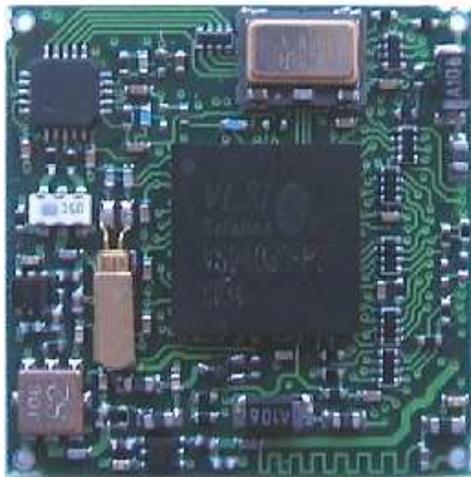
Figure 4: iTrax02: 25x25x4 mm GPS receiver

5 Scenarios

In this section we are going to describe some scenarios where location information is required to access/provide a service and how our privacy enhanced location based services architecture can be introduced in each of them.

5.1 Publishing location information in DNS LOC resource records

5.1.1 Introduction to DNS Resource Record LOC and TSIG

The DNS LOC is described in [11], DNS LOC is a new Domain Name Server Resource Record (DNS RR) type for experimental purposes and describes a mechanism to allow the DNS to carry location information about hosts, networks, and subnets. The records contains information about latitude, longitude, altitude, horizontal and vertical error, and size of the described entity.
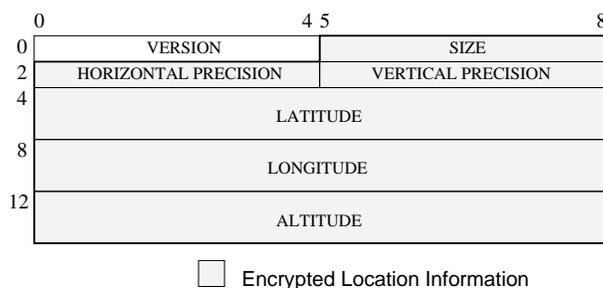

Figure 5: DNS LOC. RDATA

The Transaction signatures (TSIG) provide an authentication mechanism that uses shared secret keys to establish a trust relationship between two entities. TSIGs are described at [12] along with the way that DNS messages should be treated by a forwarding server. If the name on the TSIG is not of a secret that the server shares with the originator the server must

10

forward the message unchanged including the TSIG.

5.1.2 Description of the scenario

In this scenario a mobile node wants to make available its location only to a set of correspondent of nodes. The mobile node share a set of secrets with the DNS server and the correspondent nodes.

- **Location Acquisition Hardware:** At a certain time the iTrax02 GPS receiver sends a GPGLL NMEA 0183 message with the location information.

- **XML data record:** The location and time information is extracted from the NMEA message and converted to XML format.
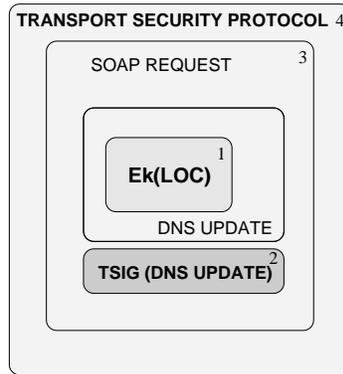

Figure 6: SOAP request (DNSSec LOC Update)

- **XML service request:** A SOAP request is created as follows:
  - Instead of including the original location data in the DNS LOC update, the LOC RDATA is encrypted with the secret shared with the correspondent nodes. A DNS Update message is created that contains the encrypted location information, shown in Fig. 6 as item 1.
  - Once the outgoing DNS update message has been constructed, the keyed message digest operation can be performed *(hmac-md5)* using the shared secret with the DNS server. The resulting message will then be stored in a TSIG which is appended to the additional data section, shown in Fig. 6 as item 2.
  - The DNSUpdate service request can be contructed as a SOAP request to the LBS proxy server. In the body a TSIG DNS Update message is included as an entity in the request <DNSSecUpdate>, shown in Fig. 6 as item 3.

- **Transport Security Protocol:** A Secure Socket Layer is established between the mobile node and the LBS proxy. The SOAP request is used as a method invocation mechanism encapsulated in a HTTP over the SSL tansport channel, shown in Fig. 6 as item 4.

- **LBS Proxy Server:** When the SOAP request is recieved by the LBS server, it gets bound to the DNSUpdate method specified in the request.

- **DNS Update Service Module:** The DNS Update module extracts the DNS Update message from the XML and sends a DNS Update message to the remote DNS server. Thus the DNS Update Service Module acts as a TSIG DNS forwarding server.

Note that (1) the DNS Server, accepts the DNS update based on the TSIG, (2) neither the proxy nor the DNS server knows the mobile node coordinates - since they can't read the encrypted LOC RDATA, and (3) the DNS server can't even know the mobile's current network attachment point. The mobile's location is now available to any node which knows the key to decrypt the results of a DNS LOC query.

5.2   Restaurant Info request

Let us consider another scenario when a mobile node wants to request the GPS coordinates of the spanish restaurants in the neighborhood open Saturday night, in this case the location information and the nature of the information requested (spanish restaurant, open Saturday night) is encrypted using a shared secret with the Information Server. The proxy server is only aware that an *Info request* has been done, but not the type of information requested (which includes location and time).

The architecture also allows a mobile node to hide its true *location of interest* by including more than one location based request in the same SOAP Body. Sending multiple requests obscures the *location of interest* from the Information Server. The Information Server can't tell if the mobile is actually at or near any of these locations.

Note in this restaurant example, the proxy will see the Information Server's reply/replies, hence the need to either (1) obscure via multiple query results or (2) the mobile must provide a symmetric key to be used by the Information Server to encrypt its reply so the proxy only has to pass on the opaque reply. However, this second case requires the server to implement an additional privacy enhancement.

6   MIXes and PE-LBS proxies

David Chaum described in [13] a technique based on public key cryptography that allows an electronic mail system to **hide** who a participant communicates with as well as the **content of the communication**.

More generaly, messages are exchanged through a chain of one or more intermediaries called "mixes". The purpose of a mix is to hide the correspondences between the items in its input and those in its output. The main function of a mix is to: receive and decrypt messages, buffer messages until a defined number of messages has been received, change the sequence of the received messages in a random manner and encrypt and forward the messages to the next mix or to the receiver.

Three of the benefits of our arquitecture are: the possibility of a PE-LBS proxy to act as a "mix" by buffering and changing the sequence of the service requests, a mobile device can use a chain of PE-LBS proxies configured as a "mixing network" to forward a location based service requests and that these functionalities can be done independently of the specific transport network.

7 Conclusions

By using a proxy server between the mobile node and the location based service we have shown that we can hide the network location of the mobile device and in some cases even provide misleading physical location(s) for the mobile device.

Combining XML Encryption with XML Signature in Simple Object Access Protocol service requests provide both message digest and message authentication functionality. Taking advantage of the extensibility and flexibility of XML it is easy to implement and extend the set of privacy enhanced location based services while still hiding the mobile node's network and physical location as desired.

References

[1] **A. Escudero,** *Privacy and Identity in the Information Society - Protection of personal identifiable information in mobile internet".* IPSC-IPTS (EU). Brussels. October 2001.
`http://www.it.kth.se/~aep/publications/privacy-iis-ws-escuderoa.ppt`

[2] **ETSI GSM 03.71**, *"Digital cellular telecommunications system (Phase 2+); Location Services (LCS). Version 8.0.0".* 2000

[3] **C. Perkins,** *"IP Mobility Support"*, RFC 2002, October 1996.

[4] **W3C** *"Simple Object Access Protocol (SOAP) 1.1",* Technical Report. May 2000.
`http://www.w3c.org/TR/SOAP`

[5] **M. Korkea-aho and H. Tang.** *"A Common Data Set and Framework for Representing Spatial Location Information in the Internet - Internet Draft"*, draft-korkea-aho-spatial-dataset-01.txt, May 2001.

[6] **F. Yergeau.** *"RFC 2279: UTF-8, a transformation format of ISO 10646",* 1998

[7] **W3C** *"XML Encryption Syntax and Processing",* Working Draft, 18 October 2001.
`http://www.w3.org/TR/xmlenc-core/`

[8] **Wireless Applications Protocol Forum.** *"WAP Wireless Transport Security Specification",* February 2000.
`http://www.wapforum.org`

[9] **T. Dierks and C. Allen**. *"RFC2246: The TLS Protocol Version 1.0".* January, 1999.

[10] **US FAA.** Wide Area Augmentation System for GPS
`http://gps.faa.gov/Programs/WAAS/waas.htm` (date accessed 10 Dec 2001)

[11] **C. Davis, et al.** *"RFC 1876: A Means for Expressing Location Information in the Domain Name System",* January 1996.

[12] **P. Vixie et al.** *"RFC 2845: Secret Key Transaction Authentication for DNS (TSIG)",* May 2000.

[13] **D. Chaum.** *"Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms".* Communications of the ACM (24)2, 1981 pp. 84-88