PRIVACY FOR LOCATION DATA IN MOBILE NETWORKS

A. Escudero-Pascual
<aep@kth.se>
IMIT
IT University - KTH
Stockholm. Sweden

T. Holleboom
<thijs@cs. kau.se>
Computer Science Dept.
Karlstad University
Karlstad. Sweden

S.Fischer-Huebner
<simone@cs.kau.se>
Computer Science Dept.
Karlstad Universit y
Karlstad. Sweden

Abstract - The new EU Directive 2002/58/EC has introduced with its Art. 9 special protection for location data other than traffic data. In this paper, we argue that also location data within traffic data can contain sensitive information about the ”relative positioning” and ”co-located displacements” of mobile nodes and thus also requires special protection.

After a brief introduction to how mobility is supported in IP networks, to the level of privacy protection for location data introduced in the new European Union data protection directive, and to means of protecting privacy by technology, we introduce the concept of *co-located displacements in MobileIP* and show how the home agent will be able to determine whether or not a set of mobile nodes move in a co-located fashion.

Finally, we present how privacy-enhancing technologies can be used to provide the level of privacy protection as required by Art. 9 of the EU Directive 2002/58/EC for location data other than traffic data, also for location information within traffic data.

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 inform a group of friends when or where a friend is close in the neighborhood.

Traditionally security in computer networks include different aspects of message integrity, authentication, and confidentiality. However, in wireless networks, where users move between different networks and media types, another issue becomes equally important: location privacy.

This paper focuses on the situation where the absolute or relative position is computed in the infrastructure (i.e., home agent) in MobileIP-based networks.

The actual task of a home agent on a mobile node’s home network is to tunnel datagrams for delivery to the mobile node when it is away from home (see section I.A). In the future, however, it might become more and more common that mobile nodes are also offering value-added services, such as LBS.

In these scenarios the user is not in full control of the location information associated with the mobile device. The problem arises when location information is required in order to obtain a service and at the same time the user does not want to reveal more personal identifiable information than is strictly necessary for the provision of a concrete service. 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 1 gives an introductory overview to mobility in IP networks, the European Union data protection directive concerning the processing of location data and to privacy-enhancing technologies useful for protecting location data, such as the Platform for Privacy Preferences Protocol (P3P) and *mix nets*.

Section 2 describes co-located displacements in MobileIP and proposes a formal method that allows a home agent to determine whether or not two mobile nodes move in a co-located fashion.

Section 3 explains how mix nets can be used to anonymise location information and how to use P3P to technically support the legal requirement of informed consent for the processing of location data within traffic data for value-added services.

I. BACKGROUND

A. Mobility support in IP networks

The protocol operation defined for mobility in IP networks is known as MobileIP[1]. MobileIP allows a mobile node to move from one link to another in the Internet without changing the mobile node's home IP address. With MobileIP the mobile node can seamlessly roam among IP networks and media types without restarting any of the ongoing connections or associated applications. A mobile node is always addressable by its home address (HoA), an IP address assigned to the mobile node within its home subnet, i.e., with the network prefix of its home link.

MobileIP allows users to move between different networks, while maintaining an addressable static identifier (home address). This is done by associating a dynamic identifier (care-of-address, CoA) with the mobile node when it is away from home at a foreign link. All traffic to the mobile node is intercepted in the home network by a home agent (HA) that tunnels the data to the care-of-address that is in use in that moment. Packets may be routed to the mobile node using their home address regardless of the mobile node's current point of attachment to the Internet (CoA), and the mobile node may continue to communicate with other nodes after moving to a new link. With MobileIP the movement of a mobile node away from its home link is thus transparent to transport and higher-layer protocols and applications.

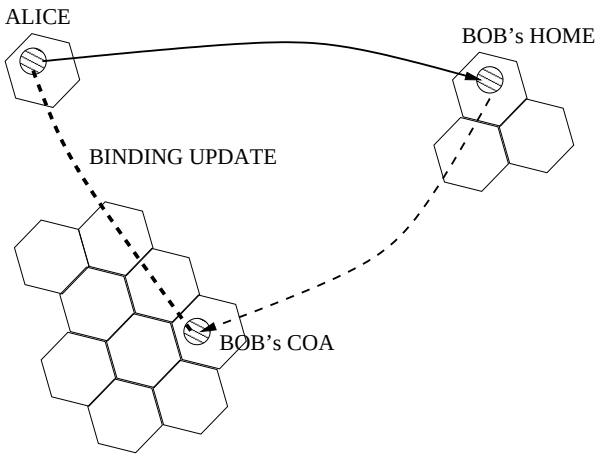

Fig. 1. Route Optimization in MobileIPv6.

MobileIPv6 shares many features with MobileIPv4, but the protocol is now fully integrated into IPv6. As in MobileIPv4 the mobile mode is responsible for discovering its current location. When the mobile mode is attached to its home link it directly receives packets and when roaming in a foreign network, it must acquire a co-located care of address and notify its home agent of this address.

MobileIPv6 on the other hand also includes the mechanisms that allows the mobile node to inform selected IPv6 correspondent nodes (CN) of its care-of-address, so packets from these correspondent hosts can be redirected straight to the mobile node instead of using the home agent as an intermediary (route optimization) [Fig .1].

B. European Union Directive on privacy in electronic communication

On July 12, 2002 the EU Directive 2002/58/EC concerning 'processing of personal data and protection of privacy in the electronic communication sector' [2] was officially adopted. The new Directive is part of a package of initiatives which will form the future regulatory framework for electronic communications networks and services. It aims to adapt and update the existing Data Protection Telecommunications Directive (97/66/EC) [3] to take account of technological developments.

The new EU Directive 2002/58/EC establishes a common framework for data protection in telecommunication services and networks regardless of the technology in use in electronic communication services and networks.

Whereas in the Directive 97/66/EC traffic data only refers to "calls" in so-called circuit switched connections (traditional voice telephony or plain old telephone system aka. POTS), the new EU Directive 2002/58/EC covers all traffic data in a technology neutral way including Internet traffic data.

Traditionally content data has had a high level of privacy protection, and it has been acknowledged that strict privacy requirements for location data other than for traffic data are needed, as they enable exact positioning and hence a permanent surveillance of users.

While it is questionable if the traditional classification of the data in traffic, content and location can be applied to the Internet [4], in contrast to the Directive 97/66/EC, in the EU Directive 2002/58/EC in Art.5 *(Confidentiality of the communication)*, traffic data has been added. Hence, at least according to the new

Directive, traffic data is supposed to have the same level of privacy protection as content data. Thus EU Directive 2002/58/EC is thereby acknowledging that traffic data needs the same level as protection as content data.

The EU Directive 2002/58/EC differentiates between location data other than traffic data, allowing the exact positioning of a mobile user's device, and location data within traffic data, giving geographic information that is often less precise. If used for value-added services, location data other than traffic data has a higher protection. Whereas for traffic data informed consent is required (Art. 6 par. 3,4), for location data other than traffic data either anonymisation or informed consent is required (Art. 9 par.1) with the possibility for users that have given their consent to temporarily refuse the processing for each connection or transmission of a communication (Art.9 par.2).

In this paper, we argue that also traffic data can contain sensitive information about the *relative positioning* and *co-located displacements* of two mobile nodes, and thus also needs a high level of privacy protection.

According to the principle of data minimization and avoidance derived from the principle of necessity of data collection and processing, location data, no matter whether within traffic data or other than traffic data, should be anonymised if the effort involved is reasonable in relation to the desired level of protection. Also for location data within traffic data, users that have given their consent should have the possibility to ”revoke” their consent for each connection or transmission.

C. Privacy-Enhancing Technologies

There are basically two major ways of enhancing privacy in the mobile Internet by technology.

Privacy can be protected most effectively by the first group of privacy technologies that avoid or at least minimize personal data that are exposed on the communication lines and at network sites, and are thus providing anonymity, pseudonymity, unlinkability or unobservability. Mix nets are examples for effective privacy technologies for anonymising communication.

The second way to protect privacy is by using technologies that can control that personal data are only used according to legal provisions. P3P [5] for example, is a technology which can provide technical support for implementing that personal data is only forwarded to web sites with the user's informed consent. According to data protection legislation, informed user consent is often required for the legitimacy of data processing.

1) Mix networks: David Chaum described in [6] 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 generally, 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.

2) Platform for Privacy Preference (P3P) Protocol: The Platform for Privacy Preferences (P3P) Protocol, which has become an official W3C recommendation in April 2002, enables web sites to express their privacy policies in a machine-readable XML format that can be retrieved automatically, interpreted easily and compared with the user's privacy preferences by user agents. Thus, it enables users/ user agents to come to a semi-automated agreement with web sites about the privacy practices for personal data processing by that sites.

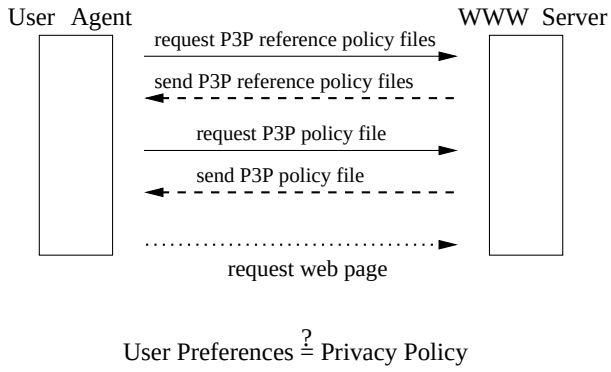

Fig. 2. P3P for informed consent

How a P3P agreement is done is described in [5] and depicted in [Fig. 2]. The P3P user-agent will typically, when an HTTP request is made, fetch a reference file, which is a site map, matching policy files with pages, parts of the site or the whole site, and is typically stored at a well-known location at a website, *”/w3c/p3p.xml”*.

According to this reference file, the appropriate policy file will be retrieved, and matched against the user's preferences. If there is a match, the page will be requested, and if not, the user-agent will take some kind of action to warn the user.

II. Co-located displacements

As explained in [Sect. 1] the home agent of a mobile node keeps track of the binding between the home address (HoA) and the mobile node's care-of-address (CoA) and is fully aware of the network prefix of the link to which a mobile node is attached to. This prefix carries information about the geographical position of the mobile node. Even though a prefix cannot generally be converted into an exact geographical position it will usually confine the possible values of the geographical position to an area that is small in comparison to the area of the surface of the earth.

It also is conceivable that knowledge of the prefix confines the possible positions to a limited area without being able to exactly locate that given area. In that case, however, it will still be possible to determine for two mobile nodes whether or not they are located in the *same* limited area. In other words, for two mobile nodes that use the same home agent, that home agent is aware of possible proximity, and hence the relative positioning, of two mobile nodes.

What is more, however, is that since the care-of address is a function of time, the home agent is able to record at which instance of time a mobile node moves its point of attachment from one foreign link to a new, different, foreign link. That also means that the home agent is able to determine whether or not two mobile nodes move in a co-located fashion. We consider that two mobile nodes that have the same home agent *move in a co-located fashion* if they change to a new care-of-address in the same foreign links a number of times *simultaneously.* An example of such movement is two people traveling in the same car or train. A sketch of how the prefixes of the care-of addresses of two such nodes change as a function of time is given in [Fig. 3]. Note that two nodes generally not change prefix at *exactly* the same time due to the nature of the events that trigger the mobility handovers (signal/noise ratio, network latency etc).

The care-of address as such only determines the geographical position of a mobile node up to the area covered by the foreign link associated with that specific

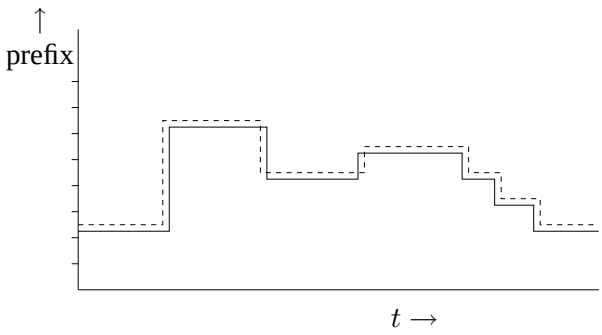

Fig. 3. *Sketch of prefixes of care-of addresses as a function of time. Values, i.e., prefixes, that fall in the same slot on the vertical axis are identical. line:* $CoA^{(i)}(t)$*, dashed line:* $CoA^{(j)}(t)$

care-of address. Movement of a mobile node while connected to the same foreign link will be undetected by the home agent. The care-of addresses of two mobile nodes will allow the home agent to determine the distance between two mobile nodes with an accuracy of approximately the size of the area covered by the foreign link. However, by studying the dynamics of the care-of addresses, it is possible to obtain a more accurate picture of the actual movements of these two mobile nodes. If two mobile nodes change their care-of addresses at almost the same time it is likely that their actual geographical distance was small at the time of change. If this happens a few times in a row it is likely that these nodes were also close at intermediate times. Hence, by studying the *dynamics* of the care-of addresses of two mobile nodes it is possible to extract information about the geographical distance of these two mobile nodes.

A. Analysis of co-located displacements

The care-of address, as a function of time, of a mobile node i will be denoted as $CoA^{(i)}(t)$. For two mobile nodes, i and j, consider the function

$$\Gamma(CoA^{(i)}(t), CoA^{(j)}(t)) = \begin{cases} 1 & \text{prefi x } CoA^{(i)}(t) = \text{prefi x } CoA^{(j)}(t) \\ 0 & \text{otherwise} \end{cases}$$

Then the integral

$$T = \int_{t_1}^{t_2} dt \Gamma(CoA^{(i)}(t), CoA^{(j)}(t)) \qquad (1)$$

gives the time, within the interval $[t_1, t_2]$, that the nodes i and j were co-located. This could equivalently

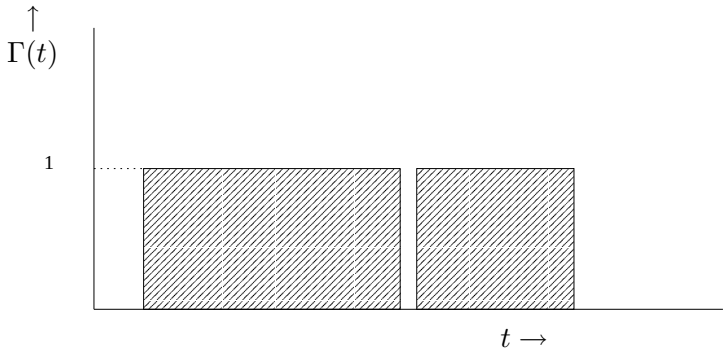

Fig. 4. *The area under $\Gamma(t)$ as a measure of co-location*

be expressed as a percentage $p = T * 100/(t_2 - t_1)$. The measure T does provide information about the *duration* of co-location, irrespective of the *movements* of the nodes i and j. As a consequence two nodes that are connected to the same foreign link during the whole interval $[t_1, t_2]$ will produce $p = 100$, like two nodes that are not static but *move* in a co-located fashion, i.e., simultaneously change to the same new foreign link any number of times. As mentioned above, two roaming nodes will in reality never change prefix at exactly the same instance of time. Such nodes will therefore always produce a number p slightly less than 100 %, even if they move in a fully co-located fashion.

The function $\Gamma(CoA^{(i)}(t), CoA^{(j)}(t))$ implicitly depends on time through the care-of addresses and can also be denoted $\Gamma(t)$. In figure 4 this function is sketched. The shaded area gives the duration of co-location. Small periods of non-co-location that arise when two nodes change prefix only marginally affect the total area, being equivalent to the integral in equation 1.

In order to be able to distinguish co-located roaming from static co-location, i.e. non moving nodes connected to the same link, one can simply count the number of hops where two mobile nodes simultaneously change their care-of address prefixes to the same new value, again within a certain time interval $[t_1, t_2]$. This number, H, is then a functional of the care-of addresses $CoA^{(i)}(t)$, and $CoA^{(j)}(t)$, which in turn are functions of time, and has the following functional form

$$H = h\left[CoA^{(i)}(t), CoA^{(j)}(t), t_1, t_2\right] \qquad (2)$$

The two explicit time arguments t_1 and t_2, indicate the boundaries of the time interval under consideration. H can easily be calculated by analyzing the functions $CoA^{(i)}(t)$ and $CoA^{(j)}(t)$, which in turn can be done by analyzing logged data at, for example, the home agent. Since, as pointed out above, two roaming nodes never change prefix at exactly the same time, it is necessary to use an interval Δt. Two nodes that change prefix of care-of-address at times t and t', where $|t - t'| < \Delta t$ are considered to have changed simultaneously. The interval Δt should be small, at least in comparison to the duration of the entire measurement $t_2 - t_1$.

In summary, the number of simultaneous hops H, of two nodes i and j, can be extracted from logged data by finding all instances where i and j change prefix at times t and t' separated by less than some predetermined amount Δt. Only hops where both the 'old', and the 'new' prefixes are the same should be counted, since otherwise there is no co-location. More formally H can be calculated as follows. If the care-of address $CoA^{(i)}(t)$ changes at times $t_k, k = 1 \cdots n$ then define

$$h_k = \begin{cases} 1 & CoA^{(j)}(t) \text{ shows identical} \\ & \text{change at } t = t', |t' - t_k| < \Delta t \\ 0 & \text{otherwise} \end{cases} \qquad (3)$$

Now the quantity H defined in equation 2 can be expressed as the sum

$$H = \sum_{k=1}^{n} h_k \qquad (4)$$

III. Privacy-enhancing technologies for protecting location data

In this section, we will discuss how privacy-enhancing technologies can be applied to technically support and enforce legal privacy requirements of Art. 9 of the EU Directive 2002/58/EC for location data, no matter whether location data other than traffic data or within traffic data.

A. Mix nets for anonymisation of location data

The mix network concept was implemented as part of the Freedom System [7,8]. Freedom is a pseudonymous IP network that provides privacy protection by hiding the user's real IP addresses, email addresses, and other personal identifying information from communication partners and eavesdroppers.

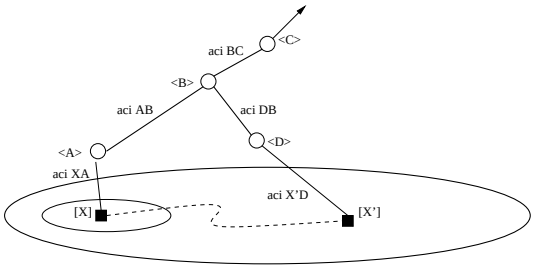

Fig. 5. Mobility extensions for the Freedom System. The virtual circuit is partially recreated during a vertical handover $[X] \rightarrow [X^{'}]$. The exit node $< C >$ is not aware of any mobility.

The Freedom System could be seen as an overlay network composed of globally distributed servers that runs on top of the Internet. Freedom routers or Anonymous Internet Proxies (AIP) are the core network privacy daemons and they are in charge of passing encapsulated packets between themselves until they reach an exit node or AIP wormhole. When a certain AIP runs as an exit node, it works as a traditional network address translator.

Symmetric link encryption is applied between AIP pairs and the freedom-client and the selected AIP entry point to hide the nature and characteristics of the traffic between them. Once the route is created from the freedom client to the wormhole, the data packets travel toward the wormhole over the virtual circuit, being link decrypted, telescope unwrapped and finally link encrypted at each point. The data is routed to the next hop by use of an Anonymous Circuit Identifier mapping table. The ACIs indicate, along with a packet's implicit source address and port, the next hop in a particular route.

When a freedom client communicates with a correspondent node via a previously built virtual circuit in the Freedom System, the correspondent node sees that the traffic as coming from the wormhole IP address instead of the client's real IP address.

In [9] we introduced a set of protocol extensions to the Freedom System architecture to permit a mobile node to seamlessly roam among IP subnetworks and media types while remaining untraceable and pseudonymous. The extensions make it possible to support transparency above the IP layer, including the maintenance of active connections in the same way that MobileIP does but with the addition that the home and foreign network are unlinkable [Fig. 5].

The concept of a mix network for location based services was also introduced in [10] where a Privacy Enhanced-Location Based Services (PE-LBS) proxy can be configured to act as a "mix" by buffering and changing the sequence of the service requests. The mobile device can use a chain of PE-LBS proxies configured as a "mixing network" to forward a location based service request. The architecture allows a mobile node to request location based services via a mix-network hiding the network location of the mobile device while providing service accountability.

B. P3P and processing of location data in MobileIP

The Platform for Privacy Preferences (P3P) Protocol can be used as a technical means for technically supporting the privacy principle of informed consent, and also for allowing users to later revoke their consent. Although P3P is a standard for controlling the personal data processing by web servers, we will discuss how it could also be used for obtaining informed consent for the processing of location data within traffic data by home agents for value-added services, such as location based services.

In the future, more effective solutions for automated privacy agreements between mobile nodes and home agents could be based on compact privacy policy or preference information included in newly to be defined extension headers for Mobile IPv6. Such a solution, however, will first require new protocol extensions, whereas a solution based on P3P can easily be implemented already today with available technologies.

Often there is a close administrative relationship between the owner of a mobile node and the owner of that mobile node's home agent. For example, a company that provides mobile nodes for its employees is also operating home agents for those mobile nodes, or a home agent could even be operated by the mobile user. If there is a trust relation between the mobile user and the owner of the home agent, an agreement about data processing practices do not have to be automated but can as well be done off-line. However, home agents could also be owned by a service provider or other organizations to which no close trust relation exists. Besides, if we demand the same level of privacy protection for location data within traffic data as for location data other than traffic data, mobile users should still have the possibility to revoke their consent for the

processing of location information within traffic data for each connection or transmission of a communication (as required by Art. 9 par. 2 for location data other than traffic data). Also for the enforcement of this requirement, an online solution as provided by P3P is required.

For enabling P3P agreements a home agent needs to have a web server interface and has to have a P3P privacy policy containing a statement describing data practices that are applied to location data.

```
<STATEMENT>
 <PURPOSE>
     <current/>
     <other-purposes required = "opt-in">
     Location-based-Services
     </other-purpose>
 </PURPOSE>
  <RECIPIENT>
              <ours/>
         </RECIPIENT>
         <RETENTION>
    <no-retention/>
       </RETENTION>
         <DATAGROUP>
             <DATA> ref="#dynamic.miscdata">
                    <CATEGORIES>
                          <location/>
                     </CATEGORIES>
                </DATA>
        </DATAGROUP>
</STATEMENT>
```

Fig. 6. P3P policy statement for a EU Directive 2002/58/EC compliant processing of location data.

In order to be compliant with the EU Directive 2002/58/EC, location data within traffic data should only be processed for the transmission of a communication (Art. 6 par. 1) or for marketing its own electronic communication services or for the provision of value-added services, such as location-based services (Art. 6 par.3). [Fig. 6] shows an example P3P policy statement for location data, allowing its processing for the current purpose of transmitting a communication and for location-based services. The opt-in requirement should be used to state that location data can only be processed for location-based services if the user explicitly requests that service and thus gives his/her consent for the use of location data for location-based services. At a policy's "opturi" link, instructions are provided for users how to decline from their request. Hence, the home agent could set up a web site that allows mobile users to fill-in forms for granting or revoking their consent for the processing of location data for the specified value-added services. This guarantees that also Art.9 par.2 can be technically supported.

Within the P3P policy statement, the RECIPIENT element should be set to <ours/>, meaning that the location data is only handled by the Home Agent or possibly entities processing the data on its behalf for the completion of the value-added service, as required by Art. 6 par.4 and Art. 9 par.3.

The RETENTION element that indicates the kind of retention policy that applies to the data should be set to <no-retention/> or <stated-purpose/> to state that the data are only processed for the duration necessary for the value-added service as required by Art. 6 par.3 and Art.9 par.1.

The mobile node has to have a P3P-compliant user agent including P3P privacy preferences defined by its user for the processing of location data. By accessing the Home Agent's web site, the mobile user can check the Home agent's privacy policy for processing of location data and can fill-in a form for requesting a value-added service, and for thereby giving his/her informed consent for the processing of traffic data for that service. A mobile user should evaluate the home agent's privacy policy at the time that she/he chooses a mobile node, and should reevaluate it before the expiry period of the policy file has passed, or in case that the mobile user has changed his/her preferences or wants to revoke his/her consent.

A problem, however, is that location information is included in all messages sent by a mobile node to its home agent. Thus, when the P3P user agent of a mobile node is fetching the P3P reference file and the policy file, it is already transferring location information with those requests, even though there has not been a successful P3P agreement with that agent yet. The home agent's web site should hence follow the so-called safe-zone practices for communications which take place as part of fetching a P3P policy or policy reference file, and thus should not collect location information that is available within the safe zone. If a user does not want to rely on the safe-zone practices, she/he should preferably initiate P3P negotiations at times that her/his node is located in its home network. If a mobile user does not succeed to select a home agent that fulfills her/his privacy preferences, she/he should

have the option to use anonymous communication.

P3P has been criticized by the Art.29 Data Protection Working Party [11,12] and others, as it cannot in itself secure privacy on the Web. Hence it needs to be applied according to a regulatory framework, such as given by EU Directive 2002/58/EC. Besides, P3P cannot ensure that web sites really follow privacy policies as they claim to do. Third party monitoring can enhance control over the compliance with the privacy policies published at web sites.

IV. Conclusions

In this paper, we have shown that traffic data in MobileIP-based networks can also contain sensitive information about the relative positioning and co-located displacements of two mobile nodes, and thus also needs high level of privacy protection. By studying the dynamics of the care-of addresses of two mobile nodes it is possible to extract information about the geographical distance of these two mobile nodes. The co-located displacements in MobileIP allow to the home agent to determine whether or not a set of mobile nodes move in co-located fashion.

Privacy-enhancing technologies should be applied to technically enforce legal privacy requirements of Art. 9 of the EU Directive 2002/58/EC for location data, no matter whether location data other than traffic data or within traffic data.

According to the privacy principle of data minimization and data avoidance, location data should be anonymized if the effect involved is reasonable in relation to the desired effect. Mix-nets based architectures (as presented in section III-A) provide an effective means for anonymising location data, and should preferably be provided to mobile users in order to fulfill the requirements of Art. 9 par. 1. We have also shown how the Platform for Privacy Preferences (P3P) Protocol can be used as an Online mechanism for obtaining informed consent of mobile users for the use of location data for value-added services, and also for allowing users to later revoke their consent, as required by Art. 9 par.1 and par.2. Hence, we have shown how existing technologies can be used to provide different levels of location privacy, even though we strongly propose that the future developments in the next generation Internet Protocol should also directly include features for location privacy.

References

[1] C. Perkins, IP Mobility Support, RFC 2002, October 1996.

[2] Directive 2002/58/EC of the European Parliament and of the Council concerning the processing of personal data and the protection of privacy in the electronic communications sector, Brussels, 12 July 2002, http://www.etsi.org/public-interest/Documents/Directives/Standardization/Data_Privacy_Directive.pdf

[3] European Union, Directive 97/66/EC of the European Parliament and of the Council Concerning the Processing of Personal Data and the Protection of Privacy in the Telecommunications Sector of 15 December 1997. http://europa.eu.int/ISPO/infosoc/telecompolicy/en/9766en.pdf

[4] A. Escudero, Location Privacy in mobile Internet in the context of the European Union Data Protection Policy. Proceedings of INET2002. Washington DC. June 2002.

[5] The Platform for Privacy Preferences 1.0 (P3P1.0) Specifi cation, W3C Recommendation, 16 April 2002, http://www.w3.org/TR/P3P/

[6] D. Chaum, Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms. Communications of the ACM (24)2, 1981.

[7] I. Goldberg, and A. Shostack, Freedom Network 1.0 Architecture and Protocols. 1999.

[8] A. Escudero, M. Hedenfalk, and P. Heselius, Flying Freedom: Location Privacy in Mobile Internetworking. INET2001. Stockholm. June 2001.

[9] A. Escudero, Anonymous and Untraceable Communications: Location Privacy in Mobile Internetworking. Licentiate Thesis ISSN 1403-5288. May 2001.

[10] A. Escudero, and G. Q. Maguire Jr, Role(s) of proxy in Location Based Services. Proceedings of 13th IEEE International Symposium IEEE on Personal, Indoors and Mobile Radio Communications, Vol.3 pp 1252-1257, Lisbon. September 2002.

[11] Working Party on the Protection of Individuals with regard to processing of Personal Data, Opinion 1/98, Platform for Privacy Preferences (P3P) and the Open Profi ling Standard (OPS), adopted on 16 June 1998, http://europa.eu.int/comm/internal_market/en/dataprot/wpdocs/wp11en.htm

[12] Article 29 - Data Protection Working Party, "Privacy on the Internet - An integrated EU approach to Online Data Protection", adopted on 21st November 2000, http://europa.eu.int/comm/internal_market/en/dataprot/wpdocs/wp37en.pdf