Available online at www.sciencedirect.com
SCIENCE DIRECT®
Telematics and Informatics 23 (2006) 211–225
TELEMATICS AND INFORMATICS
www.elsevier.com/locate/tele

Applying privacy on the dissemination of location information

G.F. Marias *, L. Kazatzopoulos, C. Delakouridis, P. Georgiadis

Department of Informatics and Telecommunications, University of Athens, Athens TK15784, Greece

Received 27 July 2005; accepted 27 July 2005

Abstract

Recent achievements in the positioning technology enable the provision of location-based services that require high accuracy. On the other hand, location privacy is important, since position information is considered as personal information. Thus, anonymity and location privacy in mobile and pervasive environments has been receiving increasing attention during the last few years, and several mechanisms and architectures have been proposed to prevent "big brother" phenomena. In this paper, we discuss an architecture to shield the location of a mobile user and preserve the anonymity on the service delivery. This architecture relies on un-trusted entities to distribute segments of anonymous location information, and authorizes other entities to combine these portions and derive the actual location of a user. The paper describes how the proposed architecture takes into account the location privacy requirements, and how it is used by the end users' devices, e.g., mobile phones, for the dissemination of location information to Service Providers. Furthermore, it discusses performance study experiments, based on real location data, and summarizes the threats analysis results.

Keywords: Mobile computing; Location privacy; Threshold cryptography

1. Introduction

Phevos, a sports fan from a European county, had plans to visit Athens as a spectator of the 2004 Olympic Games. He thought that this would be an excellent chance to test his

* Corresponding author.
E-mail addresses: marias@mm.di.uoa.gr (G.F. Marias), kazatz@di.uoa.gr (L. Kazatzopoulos), delak@di.uoa.gr (C. Delakouridis), georgiad@di.uoa.gr (P. Georgiadis).

0736-5853/$ - see front matter
doi:10.1016/j.tele.2005.07.006

new mobile device which is equipped with an embedded GPS receiver. Back in Greece, the national cellular operator announced the provision of a new location-based service, called ''Olympic Navigator'', to the mobile users. This service covers the urban areas of Athens and each sport complex, providing navigation services into Olympic facilities and rich multimedia content that is related to the event the spectator is attending. Phevos was enthused over this news. He was registered to the ''Olympic Navigator'' from its home PC, using the Internet and Web forms (in that case a pre-pay method has to be introduced for the service provision). He decided to register his mobile phone number to the ''Olympic Navigator'' service, but just before to enter his credit card number a thought came up to his mind: ''how can I be sure that my location will not be unauthorized used or revealed?''. This paper introduces an innovative architecture, called ''share the secret—STS'', to address several aspects of the Phevos location privacy concerns. Firstly, it elaborates on the control of privacy that Phevos should have over his location. Phevos is able to define different levels or rules of privacy (i.e., secrecy) over different portion of location information, depending on the operation environment (e.g., hostile) and the service that indents or asks to use location data. Additionally, it provides Phevos with the capability to explicitly identify services or pervasive applications that might collect, store, and use his location information. Finally, it provides anonymity on the distribution of Phevos' location information. The proposed architecture is designed to operate over un-trusted environment. Portions of Phevos' location data can be distributed to public available nodes, which act as intermediate and temporal Location Servers. In that sense, Phevos authorizes the ''Olympic Navigator'' service to access and combine the distributed location information. This is accomplished implicitly, through the disclosure of the mapping between a pseudonym and Phevos' location data. The architecture is applicable to environments that consist of devices with several idiosyncrasies, such as luck of energy autonomy, memory and processing power. To provide secrecy it avoids complex computational tasks, such as producing key pairs, hashing and message authentication codes. Instead, it deals with the division of location data into pieces and the distribution of these pieces to serving entities. Thus, it is applicable to smart spaces featuring ubiquitous services through the involvement of small gadgets, RF-tags, and sensors that activated to infer the location of a target.

The remainder of this paper is structured as follows. First we briefly discuss some alternative approaches that address the location privacy issue. In Section 3 we provide the assumptions that STS considers for its operation, we introduce the STS architecture, the entities that it consists of and the secret share mechanism that enables the anonymity and privacy of location information. Subsequently, in Section 4 we discuss the procedures followed by the entities of the architecture. In Section 5, we provide some results concerning the performance and the robustness of the STS architecture against attacks. In Section 6, we illustrate the applicability of the STS to the Phevos real case scenario. Finally, we provide some concluding remarks.

2. Location and privacy

Location information is considered as an essential component for the development and delivery of context-aware services to mobile and nomadic users (Satyanarayanan, 2001; Saha and Mukherjee, 2003; Harter et al., 1999) and several approaches have been proposed to gather the location of a user, or asset. They differ in several semantics, such as scale (e.g., worldwide, indoor, outdoor), accuracy, location measurement units involved,

time-to-first-fix and costs (e.g., computational, or investment). These approaches include the worldwide GPS, cellular-based methods, and indoor positioning mechanisms based on wireless local area network (WLANs). Recently, positioning systems incorporated RF-tags and specialized sensors that provide higher accuracy, enabling location aware applications that require the calculation of the exact position. Positioning technologies provide the means for easily location gathering, monitoring, and management, operations that considered essential for the elaboration of pervasive computing and the exploitation of location-based services (LBS). On the other hand, the wireless networking technologies (e.g., GSM/GPRS) offer the infrastructure for advertisement of the location information, and, thus, potential eavesdropping and unauthorized use (or misuse) of it. An adversary can potentially derive location information at different layers of the network stack, from the physical to the network layer (Gruteser and Grunwald, 2003a). Furthermore, data collection and mining techniques might produce historical location data and movement patterns (Gruteser and Grunwald, 2003a), which they are subject to unauthorized use, as well. Since location is considered as personal information its privacy should be protected. According to Beresford and Stajano location privacy is defined as ''the ability to prevent other parties from learning one's current or past location'' (Beresford and Stajano, 2003). Minch presents and discusses several risks that are associated with the unauthorized disclosure, collection, retention, and usage, of location information (Minch, 2004). The EU Commission under the directive of Privacy and Electronic Communications (Directive 2002/58/EC,) regulates the use of the location data, since article 9 of this directive demands that these data can be processed anonymously or with the consent of the user. Additionally, the Location Privacy Protection Act, announced on 2001 in the United States, addresses the necessity and identifies several risks related to the privacy of the location information (US Location Privacy Protection Act, 2001). Location privacy is considered of high importance, since individuals should be able and free to explicitly identify what location information will be disclosed, when this can happen, how this information will be communicated and to whom this information will be revealed. Even through anonymization, as defined in Pfitzmann and Koehntopp (2000), personal and location data collection is combined with privacy, the disclosure of the personal identity might be useful for the delivery of personalized services, especially when accounting and charging is a requirement.

2.1. Positioning

As previously mentioned, position technologies differ in terms of scale, accuracy, time-to-first-fix, installation and operation costs. Additionally, the position of an object can be either physical (e.g., at 38014′49″N by 23031′94″W) or symbolic (e.g., in the office, in Athens). Another classification uses the absolute or relative position definitions. Absolute position is depicted on a common coordinates system, and the position for an object is the same and unique for all the observers. Unlike, the relative position represents the position of a located object in reference to the observer. LocInfo is defined to incorporate any of the four aforementioned position semantics. In terms of scale, GPS is a technology that focuses on outdoor, wide range, location identification, providing high accurate results (less than 30 feet) using a trilateration positioning method in the three-dimensional space (Bajaj et al., 2002). Location determination can also be achieved through terrestrial, infrastructure-based, positioning methods. These positioning methods rely on cellular networks

equipment to infer an estimation of a mobile users' position. In Marias et al. (2004) a general brokerage architecture that gathers the location information independently of the positioning technology is proposed. Location retrieval can rely on the infrastructure of the WLAN communication network, such as the IEEE 802.11, to provide higher accuracy in indoor environments. Positioning systems like RADAR (Bahl and Padmanabhan, 2000) and Nibble (Castro et al., 2001) operate using the IEEE 802.11 data network to gather the location of a user or object. For context-aware services that require higher accuracy, specialized positioning infrastructure needs to be established (e.g., sensors or RF-tags). Among the positioning systems that have ben proposed to provide finer granularity to the pervasive applications is the Active Badge, (Want et al., 1992), Active Bat (Harter et al., 1999), Cricket (Priyantha et al., 2000), SpotON (Hightower et al., 2000), Pseudolites (Kee, 2000), and MotionStar. According to Hightower and Borriello (2001), there are several other types of tags and sensors that provide user's location with high accuracy, such as the Easy Living, the Smart Floor and the Pin Point 3D-iD.

2.2. Location privacy

Several approaches that enable location privacy have been proposed in the literature. Some of them focus on the secrecy of medium access control (MAC) identifiers or IP-layer address. On the MAC layer, Gruteser and Grunwald discuss the problem of interface identifiers (Gruteser and Grunwald, 2003b) that uniquely identify each client, allowing the tracking of the location over time. They introduce privacy through the frequent disposal of a client's interface identifier. In the IP-layer, Mobile IP (Fasbender et al., 1996a) address location privacy by associating two different IPs to the same subject; the static one, related to the user's home network, and the dynamic, related to the current network. As the user roams through different networks, his/her mobile device registers the current location to a home agent located at the user's home network. The Non-Disclosure Method (Fasbender et al., 1996b) considers the existence of independent, security, agents that are distributed on the IP network. Each security agent holds a pair of keys and forwards the packets in an encrypted format. The sender routes a message to a receiver through a path that consists of security agents. Mist System (Al-Muhtadi et al., 2002a,b) handles the problem of routing a message though a network while keeping the sender's location private from intermediate routers, the receiver and potential eavesdroppers. The system consists of a number of routers, called Mist routers, ordered in a hierarchical structure. According to Mist, special routers, called "Portals", are aware of the user's location, without knowing the corresponding identity, whilst "Lighthouse" routers are aware of the user's identity without knowing his/her exact location. The aforementioned methods deal with location privacy in the MAC and IP-layer, and propose solutions that apply to MAC authentication, IP mobility and IP routing methods. On the other hand, the STS scheme addresses location secrecy on the application layer. Thus, some of these methods (e.g., the Mist) can be considered as complementary, or underlying, secure infrastructures for the deployment of STS.

Beyond the solutions that apply to the lower layers of the OSI stack, two main approaches have been proposed to address the location issue on the application layer. The first is the policy-based approach, which incorporates a Service Provider as the basic element for privacy building. The Service Provider introduces privacy policies that identify rules concerning data collection (type of data that can be collected, purpose of collection)

and data dissemination. The subjects (i.e., target of location) communicate with the Service Provider in order to evaluate and select a privacy policy. The second is the anonymity-based approach that aims to unlink the location information from the subject, before the collection of the location information. In the context of location privacy in the application layer, several architectures introduce the idea of using of pseudonyms instead of users' identities. Leonhardt and Magee (1998) propose the replacement of the identity with a sequence of chained idempotent filters governed by a rich formal policy language. Kesdogan et al. (1998), propose the use of temporary pseudonymous identities to protect the identity of users in the GSM system. Furthermore, the IETF Geopriv Workgroup[1] addresses the location privacy issue by introducing the usage of a Location Server (LS) which registers the position of the subject (i.e., a target of location). The LS discloses this information using specific rules. These rules are generated by a Rule Maker (e.g., the subject itself) and managed by a service called Rule Holder which enables the subjects to explicitly specify the desired level of privacy.

The majority of the aforementioned schemes are based on the existence of a trusted third party (TTP, e.g., the Geopriv's LS). The LS entity maintains access to the data related to both user's identity and location. As a result it could jeopardize the user's location privacy by revealing this information to unauthorized users. Furthermore, due to the fact that LS is the central storage of the location information, the privacy architecture becomes sensitive to eavesdropping and attacks. The former might reveal location information through traffic analysis, whilst the latter might produce availability risks (e.g., denial of service attacks and flooding), or derogation of the privacy service (e.g., though impersonation and spoofing). On the other hand, non-TTPs based systems, such as the Mist, enable location privacy using rerouting and hard encryption, and, therefore introduce heavy processing tasks, which influence their applicability in real scenarios. Finally, in several mobile and wireless networks, such as ad hoc networks, TTPs servers are ephemerally present, due to the mobility of the nodes. Thus, centralized location privacy architectures that rely on a trust server might be inapplicable.

3. STS architecture

The proposed STS architecture enables location privacy without relying on the existence of trusted parties (e.g., TTPs, LS). The main idea is to divide the location information into pieces and distribute it to multiple servers, called STS servers. These are no-trustworthy, intermediate, entities, assigned to store, erase and provide segments of location information that anonymous users register or update. Third party services, such as LBS or pervasive applications, access multiple STS servers to determine user's location data through the combination of the distributed pieces. This is achieved after a well-defined authentication process motivated by the corresponding user. Furthermore, due to the decentralized STS architecture, a possible collusion between STS servers, each of one maintaining only partial knowledge of the user location, is fruitless. The secret i.e., (location of a user) is not distributed to specific STS servers, and, furthermore, each user dynamically chooses different servers to distribute the location information segments, according to the requested service (e.g., location-based friend-find service) and to policy

[1] http://www.ietf.org/html.charters/geopriv-charter.html.

rules. Additionally, even if multiple STS servers collude successfully, the actual location information is not revealed, since the segments are stored through pseudonyms. The main characteristics of the STS are:

- Location privacy is offered as a service to users who desire to hide their location information.
- Different privacy levels can be defined, through various users' profiles, policies or end-applications that the users are registered to (e.g., segmentation of location information into different segments).
- The user maintains full control over the location data. The position is calculated on the user's device, the user defines which STS Servers will have partial knowledge of it, and which third-party services are authorized to access and combine it.
- The location privacy is achieved within rational or distrusted environments; it does not employ trustworthy or reliable entities for data storage.

3.1. Assumptions

As Location information (LocInfo) we use a variation of the definition introduced in Friday et al. (2002), i.e., we use the triple of the following form: {*Position*, *Time*, *ID*}. Thus, LocInfo is defined as a combination of the "Position" that the entity with identifier "ID" maintained at time "Time", within a given coordinate system. This triple is adopted in order to emphasize that, within the STS architecture, time is considered as a critical parameter in terms of location identification, as well. Friday et al. (2002), provide further details on the semantics of this definition. The STS scheme incorporates multiple user profiles to provide different precision of LocInfo i.e., a drive-navigation service needs high precision location data to provide exact instructions, whilst a point-of-interest service requires data of lower precision. A user could use different pseudonyms per service and choose a discrete profile to denote the required level of the precision on the LocInfo. We assume that each STS server keeps a table called "Location Information Table" (LIT). Each record of the LIT table keeps a pair of values (ID, σ(LocInfo)), where σ(LocInfo) is a random segment of the LocInfo of the corresponding user, produced from the SSA algorithm, as will be discussed later.

The positioning technologies, previously discussed, are divided into two main categories: centralized and distributed. Technologies of the former category rely on a centralized, dedicated, server, responsible for calculating the position of the registered users. Methods of the latter category are based on specialized software of hardware, installed on the subject's device, which performs advanced calculations to estimate user's current position. The STS architecture takes advantage of the distributed approach; the entity ID determines the *Position*, either autonomously or using contributed measurements, based on calculations performed at a given *Time*.

3.2. Architecture

The STS architecture does not rely on the existence of a single and trusted third party. Multiple STS servers are geographically distributed. A subset of them is assigned to store portions of the location information of a target. The segments of the location information

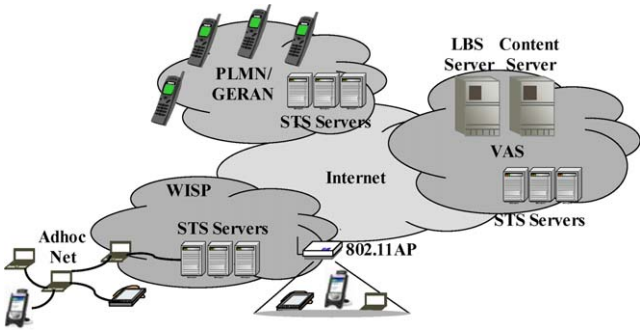

Fig. 1. Entities of the STS architecture.

are constructed through the "Secret Share Algorithm" (SSA), a novel threshold scheme that is proposed here to cope with location privacy. In Fig. 1 the entities of the proposed STS architecture are depicted. STS servers might offered by a Wireless Internet Service Provider (WISP), an Internet feed provider, a VAS and content provider, or offered by a mobile operator. In the ad hoc networking scenario, in the presence of STS servers the targets might use these as location information storage areas. If the STS servers are unreachable, ad hoc nodes, RF-tags and sensors might be used as local caches to store the LocInfo segments.

The value added service (VAS) provider offers location based and pervasive services to subscribers (registered users) or to ephemeral users (pay per view model). VAS might offer a wide range of services, such as indoor/outdoor navigation, proximity services (e.g., find-friend), positioning and point-of-interest, tracking person's location (e.g., children, elderly), localized advertisement and content delivery (e.g., city sightseeing), and emergency (e.g., E911). Hereafter we use the term *Service* to denote value added or pervasive applications that require the location information of a user, asset or device to operate and provide a location service. Each *Service* requires the location information, maintained in intermediate STS servers, to provide the required level of service to an individual.

3.3. Secret share algorithm

Several variations of the SSA have been proposed (Hoffman, 2004). The basic algorithm is the "Trivial Secret Sharing". According to this basic form, the secret is divided into n pieces and all the pieces are required to restore it. An improved SSA, called "Perfect Scheme", assumes that the secret is shared among the n out of m available entities ($n < m$) and any set of at most $n-1$ entities cannot rebuild the secret. The SSA we have adopted for the STS architecture is the perfect sharing scheme of Shamir, referenced to as *threshold scheme* (Shamir, 1979). Let assume that the secret is some data L, which is (or can be easily made) a number. According to Shamir's (n,m) threshold scheme, to divide L into pieces L_i one can pick a random, $n-1$ degree, polynomial

$$f(x) = S_0 + S_1x^1 + S_2x^2 + \cdots + S_{n-1}x^{n-1}$$

in which $f(0) = S_0 = L$ and evaluate $L_1 = f(1), \ldots, L_i = f(i), \ldots, L_m = f(m)$. Given any subset of n of these L_i values, we can determine the coefficients of $f(x)$, and rebuild L, since

$L = f(0)$. On the other hand, knowledge of at most $n - 1$ of these values is not sufficient to determine L. In the STS architecture, L is the LocInfo triple.

4. STS procedures

Using real life identifiers, such as user names, in each LIT entry enables STS servers to collude by combining entries with identical identifiers, and, eventually, reconstitute the location information of a user, based on Phevos username. To prevent collusions and the disclosure of LocInfo, we replace the username of the LIT entries with a pseudonym. This approach does not prevent hackers from obtaining the location of an unknown entity, by combining entries with identical pseudonyms. Instead, it discourages them from obtaining the location of a specific user. Only the entities that have a prior knowledge about the mapping between a pseudonym and a real identity can combine segments to produce useful conclusions. To increase the security level, the pseudonym is divided into parts, as well. Each segment of the LocInfo is sent to the STS server along with a discrete part of the related pseudonym. As a result, a potential eavesdropper should map multiple pseudonym's segment (say p_i) in order to obtain the correct record $(p_i, \sigma_i(\text{LocInfo}))$ from all the STS servers for the monitored user. If a perfect SSA is used, the pseudonym is divided into m parts where m corresponds to the "n out of m" perfect scheme. Regulating the value of m, one can increase the complexity, and the privacy level. Note that for each *ID* only one LIT record is stored on a STS server. We assume that a software random integer generator is running on user's device and performs the generation of the pseudonym. If there are m STS servers and at least n ($m > n$) can rebuild the LocInfo, the random integer generator generates a random m^*k-bits number (i.e., the pseudonym). This number is then divided into m segments ($1,\ldots,k$-bits represent the first segment, $k+1,\ldots,2k$ represents the second segment, etc.) where each segment acts as user's pseudonym. The robustness of the aforementioned scheme could be enhanced if the secret is not shared to m STS servers but to x, randomly selected, servers, where $x \leqslant m$. In this approach the secret can be recovered from y segments, $y < x$ (i.e., a "y out of x" perfect scheme). This variation increases the complexity required by an eavesdropper to identify which STS servers keep the location of a specific user. To provide a paradigm let assume that a farm of 15 STS servers are available and the secret is being shared among x, randomly selected, servers, where $8 \leqslant x \leqslant 12$. An attacker should first determine the value of x and then calculate all the possible, C_1, combinations of the STS servers in order to combine the pseudonym

$$C_1 = \sum_{i=m-A}^{m} \binom{15}{i}$$

Assume m STS servers, where x of them have the secret, and y ($y < x$) is the minimum number of servers required to obtain the LocInfo. Furthermore, let each pseudonym constitutes of k^*x-bits. The random pseudonym generator splits the pseudonym into x segments (p_x), each of k-bit length. The variable x takes values from $(m - A, m)$ where A ($A \geqslant 0$) is an integer that affects the desired security level of the STS architecture. More specifically, if A is small, an attacker has to gain access to a greater number of STS servers. However, small A reduces the number of different combinations of STS servers keeping the secret's segments, and, thus, the security level of the system is diminished. On the other hand, for a large A, the number of different combinations of STS servers sharing the secret

is increased. For large A the number of servers that an attacker has to gain access to reveal the secret is reduced. Regarding the maximum value of variable y, this is set to $x - t$, where t ($t > 0$) is an integer that depends on the desired robustness of the STS architecture. If t is set close to zero and B out of x STS servers go down at the same time, where $B > t$, the system eventually runs out of service. The variables A and t may vary per *Service*, based on e.g., charging policy or the user profile. Furthermore the value of t is a function of x, ($t = f(x)$), where as x increases t increases, as well. Thus, the variables A, and t establish different privacy profiles that an end-user might choose. The steps followed by the target during the creation of its pseudonym, the calculation of the updated LIT *entries* and the dissemination of these to the STS servers (location update procedure) are as follows:

Step 1. Find a random x, such that $m - A < x < m$	
Step 2. Generate a random x^*k-bit length number	Pseudonym and STS registration procedure
Step 3. Split that number into x segments of k-bit length each	
Step 4. Register to the x STS servers	
Step 5. Apply the SSA at the LocInfo to derive the σi pieces	LocInfo segmentation and update procedure
Step 6. Produce the pairs $(p_x, \sigma_x(\text{LocInfo}))$	
Step 7. Send to each one of the x STS servers the LIT pair $(p_x, \sigma_x(\text{LocInfo}))$	
Step 8. LocInfo is changed go to step 5	

Steps 1–4 are followed once, per user and per *Service* that requires the LocInfo. Each time the location information is altered, the target performs the steps 5–7 to inform STS servers and update the LIT entries.

To exploit the advantages of the STS architecture, Phevos, that has already registered to use an LBS service (e.g., the "Olympic Navigator", see Section 6), should also register to the STS service that is provided e.g., from the cellular operator. This will allow Phevos to select a privacy profile when disseminating his location info, including his pseudonym and the number of STS servers that are required to share his location secret. When this happen, he will also have to inform the LBS provider for these options, and this is materialized though a single, encrypted and signed message. The following procedures required to be followed by Phevos (in order to use the STS service) and the operator (in order to track Phevos) when location privacy is a requirement.

4.1. Registration to the STS service

This step requires for the end-user device to transparently perform the steps 1–3 of the STS procedure, according to the selected privacy profile. The random generators that reside in different user's device might produce identical pseudonyms. In such a case, one STS server might receive two location segments that belong to the LocInfo of two discrete users, but associated with the same pseudonym. As a result, the STS server might forward an inaccurate segment to the *Service* that requested the user's LocInfo. To avoid such a conflict, the STS scheme requires from each user to perform a registration procedure (step

4), and to enter Phevos pseudonym's segments to the x STS servers. This procedure requires a handshake between the user and each STS server, which is further discussed in Marias et al. (2005).

4.2. Notification of the LBS Provider

Beyond the registration procedure to the STS service, Phevos has to provide to the LBS provider the details of how to obtain his location information. Therefore, Phevos provides the following information to the *Service* Provider:

- The x STS servers that store his location information (e.g., IP address or URL).
- His pseudonym's segments, created by the user for the specific *Service*.
- The mapping between pseudonym's segments and STS servers (i.e., to which STS server each segment corresponds).

The aforementioned information is communicated to the *Service*, though a public key scheme, ensuring authentication, confidentiality and integrity.

4.3. Location retrieval procedure

When the *Service* requires user's location, it sends a request to each one of the x STS servers. When the x segments are received, the *Service* rebuilds user's location. This is achieved through the usage of the Shamir's recover scheme (Shamir, 1979), and the known mapping between the user's name and its pseudonyms' segments. During the location retrieval some LIT entries might not be synchronized among the STS servers. To avoid this, each LIT entry is tagged with a sequential number (SEQ).

4.4. LIT update procedures

When an STS server receives an update request (step 7) it searches the existing LIT records to determine whether the p_x already exists. If so, it updates the corresponding LIT entry.

4.5. LIT entries remove policy

Normally, Phevos authorizes a *Service* to access his location information for a given period of time, (e.g., a month), through a selection of a predefined policy. Consequently, LIT records of each STS server should be deleted after that period. This can be performed explicitly or implicitly. In the former case Phevos sends a specialized message requiring the deletion of the LIT entry from a specific STS server. This message can be sent when the user desires to prohibit a previously authorized *Service* from accessing his location information. A multicast message can inform the entire set of the x STS servers to perform a deletion, as it is described in Marias et al. (2005).

4.6. Location information validity period

In ubiquitous environments users are characterized by high mobility. Thus, the location information that is stored on the STS servers must be associated with a validity period

(VP). VP is an additional field on the $(p_i, \sigma_i(\text{LocInfo}), \text{TTL}_i)$ record. The VP period depends on several parameters, such as:

- The nature of the *Service* provided: A navigation *Service* might require higher location-update rates to provide exact instructions, whilst a tourist guide *Service* needs periodical updates.
- User's velocity. For a driver the location is continuously altered, while for a walker the location changes at a slower rate. The former requires lower VP, whilst a higher VP is sufficient for the latter.

5. Experiments and threats analysis against STS

To evaluate the performance of the STS architecture we have implemented a real experiment scenario of a nomadic user, using a real WLAN network that consists of twelve IEEE 802.11b access points, installed in the University of Athens. The nomadic user, e.g., Phevos, registers on an existing location service. This no profit service provides the nearest point-of-interest (e.g., a printer) and navigation services (e.g., where is the meeting room) to the user through a specialized location gateway, introduced in Papazafeiropoulos et al. (2003). On the end user's laptop the Nibble positioning module (Castro et al., 2001) captures and logs the location data, a Shamir's secret sharing component[2] splits the LocInfo into segments and the IEEE 802.11 acts as bearer to transmit the LocInfo segments to the STS servers over the wireless links. We managed to load each access point with an average of 1 Mbps real traffic (constant bit rate connections). The STS component, that uses the Nibble, was set to refresh the location of the user every 1.5 min and the Shamir's secret sharing component to split and send the LocInfo segments to the STS servers at the same rate. The end-user discovers the STS server through the Jini service discovery mechanism. The time period of the experiment was set to 3 h (validity period). Regarding the underlining protocol used to transmit the LocInfo segments we alternatively use TCP and UDP connections. During the experiments the overhead of the STS method was measured, and compared with an alternative scheme that encrypts the entire LocInfo without segmentation. For the purpose of the alternative scenario the "Bouncy Castle"[3] cryptographic provider was used and the entire LocInfo were enciphered through a RSA 1024 asymmetric keys. This key size was selected for communication confidentiality. As mentioned in Shamir and Tromer (2003) and Lenstra and Verheul (2001) using a hypothetical device (and ignoring the initial R&D costs), it appears possible to break a 1024-bit RSA key in one year using a device whose cost is about $10 million. Fig. 2 illustrates the results for six different experiments in terms of end user's performance.

As it is depicted, TCP protocol introduces higher communication costs than UDP due to the reliable data transmission that it offers (e.g., acknowledgements). Taking into account that the STS system is fault tolerant, since the location segments are stored in redundant STS servers (i.e., $x - y$ Servers), the reliability of TCP is not essential, and, thus, UDP protocol would be a suitable solution for low cost data transmission. An interesting conclusion

[2] http://www.cs.cornell.edu/boom/2003sp/ProjectArch/SecretSharing/.
[3] http://www.bouncycastle.org/.

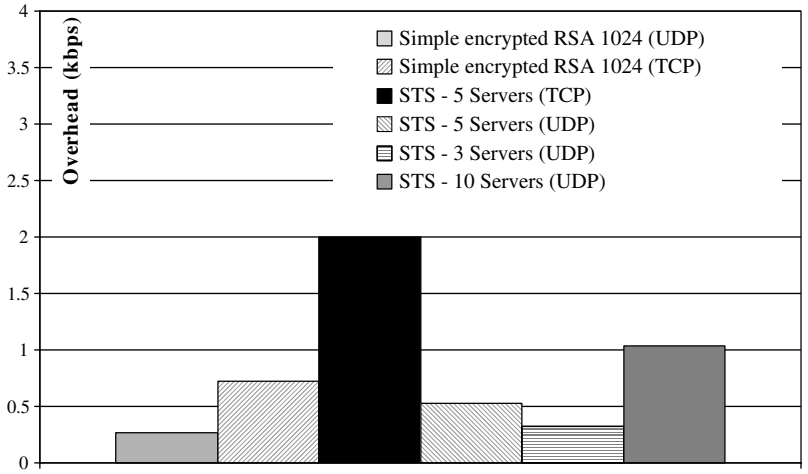

Fig. 2. Experiment results—overhead of the STS scheme in the wireless link.

is that the network load produced when using 3 STS servers is almost equivalent to the scenario where the entire LocInfo is encrypted but not segmented. Another interesting observation deals with the limited overhead introduced by the STS scheme (1 Kbps on the wireless link for 10 STS servers). Due to this low communication cost, the STS scheme can be applied on environments that facilitate limited amount of bandwidth, such as GSM/GPRS.

In Marias et al. (2005) we have further elaborated on the proposed architecture, evaluating the potential threats and its robustness against brute-force and sophisticated attacks, and we have proved that the STS architecture is stealth against such attacks. If $y = 7$ is minimum number of STS servers needed to rebuild the location information, $z = 10$ is the STS servers under attack and $m = 20$ is the total number of STS servers, the attacker must try an average of 5×10^{29} combinations in order to find out if the location segments obtained from the z servers are sufficient to rebuild the location information of any (and not specific) user. Even if the attacker is able to try 10^{12} (THz) combinations per second he/she will need an average of 10^{10} years in order to determine if the compromised set of z STS servers can rebuild the location of a random user, and this can happen with probability $P = 0.00156$.

6. Phevos in Athens revised

The Service Provider offers an enhanced "Olympic Navigator" service that takes advantage of the recently deployed STS servers. Before entering its credit card number, Phevos visited the Web pages that contain the privacy statements of the LBS service. These pages include explanations about the "Olympic Navigator" service and provide further details on the offered profiles that Phevos might select, as well as the corresponding charges. Phevos is convinced about the privacy countermeasures the provider will take over its location information, registers for five days (validity period) and finally enters its credit card number. Phevos arrives by plane and intents to stay in Athens for five days. During the registration procedure, the service informs Phevos that he will be traced every T seconds, unless

Phevos explicitly asks for a complementary navigation service, which is charged on a per-use policy. Phevos uses the "Olympic Navigator" and, at the same time, keeps his position private from any other unauthorized entity. In order to do so, a software module is downloaded at Phevos' device, to run the location-update procedure, to produce the pseudonym of Phevos and to communicate segments of Phevos' LocInfo, as gathered by the GPS, to STS servers. The latter is performed every T seconds, and this is achieved transparently to the end-user. Additionally, the module creates the pseudonym of Phevos, and sends this information to the provider of the "Olympic Navigator" service. This communication is performed exactly once, and it might be associated with public key cryptography to provide strong authentication, confidentiality and integrity. This step enforces the LBS provider to rapidly resolve the LocInfo of Phevos, combining the pieces from the LIT entries. For five days the "Olympic Navigation" service is authorized to obtain the location information of Phevos. During the registration procedure Phevos chooses the "spectator" profile. This profile corresponds to a specific location privacy policy, and defines specific values of several parameters that correspond to the number of the STS server that will be exploited on behalf of Phevos (i.e., A, t and m), as well as the parameters TTL and VP. Different registration profiles might be offered to athletes, members of Olympic Committees, sponsors, or journalists. After five days of "unforgettable and dream games",[4] Phevos departs; his is automatically unregistered from the "Olympic Navigator", and his location information is permanently deleted from the STS system.

7. Conclusions

This paper introduces an architecture to provide privacy during the dissemination of location information over an insecure, wireless and pervasive environments. It relies on threshold algorithms to divide the location information into small segments and distribute those in a numerous, public available, STS servers. The scheme is enriched with pseudonyms, and, thus, guarantees that only the authorized entities, such as location-based services and pervasive applications, have the knowledge to rebuild the secrets based on the distributed segments. Since the STS architecture does not utilize hard computational and processing tasks, such as cryptosystems, it is applicable to ad hoc as well as spontaneous networks and systems. The STS scheme introduces low communication cost over the wireless links, and thus it is applicable to mobile systems with limited bandwidth, such as the GSM/GPRS systems. Furthermore, the STS servers might be maintained by the actors of the LBS value chains. According to Schiller and Voisard (2004), those include LBS providers, cellular operators, content aggregators, wireless Internet Service Providers, accounting and charging third parties, etc. When Phevos registers on an LBS service using encrypted and authenticable means, the provider downloads software to his mobile. According to the profile that Phevos selects, and the bilateral agreements between the LBS provider and other actors of the value chain, the downloaded module performs the STS and sends the location information segments to the appropriate STS servers. The STS architecture addresses location privacy in the application layer. Existing solutions in the lower layers of OSI model that provide secrecy and authentication (i.e., tunneling, IPSec, SSL, see Staling (2000)), can be used as underlying assets to enhance privacy and

[4] Dr. J. Rogge, IOC president, Athens Olympics 2004 Closing Ceremony, August 29, 2004, Athens.

prevent attacks, such as traffic analysis. Such heavyweight schemes can be applied to the information exchange between the STS servers and the Service Provider, since this part of communication involves stationary and powerful processing units, fixed networks and high capacity lines (e.g., broadband links).

References

Al-Muhtadi, J., Campbell, R., Kapadia, A., Mickunas, D., Yi, S., 2002a. Routing through the Mist: Privacy preserving communication in ubiquitous computing environments. In: Proceedings of the International Conference of Distributed Computing Systems, July 2002.

Al-Muhtadi, J., Campbell, R., Kapadia, A., Mickunas, D., Yi, S., 2002b. Routing Through the Mist: Design and Implementation, Technical Report UIUCDCS-R-2002-2267, March 2002. Available from: <http:ciae.cs.uiuc.edu/mist>.

Bahl, P., Padmanabhan, V.N., 2000. RADAR: An in-building RF-based user location and tracking system. In: Proceedings of IEEE INFOCOM2000, March 2000.

Bajaj, R., Ranaweera, S.L., Agrawal, D.P., 2002. GPS: location- tracking technology. IEEE Computer, 92–94.

Beresford, A.R., Stajano, F., 2003. Location privacy in pervasive computing. IEEE Pervasive Computing 2 (1), 46–55.

Castro, P., Chiu, P., Ted, K., Muntz, R., 2001. A probabilistic room location service for wireless networked environments. In: Proceedings of Ubicom2001, September 2001.

Directive 2002/58/EC of the European Parliament and of the Council on privacy and electronic communications, July 2002, Official Journal of the European Communities, L 201/37.

Fasbender, A., Kesdogan, D., Kubitz, O., 1996a. Variable and scalable security: Protecting of location information in mobile IP. In: Proceedings of the 46th IEEE VTC, March 1996.

Fasbender, A., Kesdogan, D., Kubitz, O., 1996b. Analysis of security and privacy in mobile IP. In: Proceedings of the Fourth International Conference on Telecommunication Systems, Modelling and Analysis, March 1996.

Friday, A., Muller, H., Rodden, T., Dix, A., 2002. A lightweight approach to managing privacy in location-based services. In: Proceedings of Equator Annual Conference, October 2002.

Gruteser, M., Grunwald, D., 2003a. A methodological assessment of location privacy risks in wireless hotspot networks. In: Proceedings of Security in Pervasive Computing, March 2003.

Gruteser, M., Grunwald, D., 2003b. Enhancing location privacy in wireless LAN through disposable interface identifiers: A quantitative analysis. In: Proceedings of WMASH'03, September 2003.

Harter, A., Hopper, A., Steggles, P., Ward, A., Webster, P., 1999. The anatomy of a context-aware application. In: Proceedings of the Fifth ACM/IEEE International Conference on Mobile Computing and Networking, August 1999.

Hightower, J., Borriello, G., 2001. Location systems for ubiquitous computing. IEEE Computer 34 (8), 57–66.

Hightower, J., Borriello, G., Roy Want, 2000. SpotON: An Indoor 3D Location Sensing Technology based on RF Signal Strength, University of Washington, Technical Report #2000-02-02, February 2000.

Hoffman, B.C. et al., 2004. Secret Sharing Schemes, Project Specification. COSC 645, Spring 2004.

Kee, C., et.al, 2000. Development of indoor navigation system using asynchronous pseudolites. In: Proceedings of ION GPS-2000, September 2000.

Kesdogan, D., Reichl, P., Junghärtchen, K., 1998. Distributed temporary pseudonyms: A new approach for protecting location information in mobile communication networks. In: Proceedings of the Fifth European Symposium on Research in Computer Security, September 1998.

Lenstra, A.K., Verheul, E.R., 2001. Selecting cryptographic key sizes. Journal of Cryptology 14 (4), 255–293.

Leonhardt, U., Magee, J., 1998. Security considerations for a distributed location service. Journal of Network and Systems Management 6 (1).

Marias, G.F., Prigouris, N., Papazafeiropoulos, G., Hadjiefthymiades, S., Merakos, L., 2004. Brokering positioning data from heterogeneous infrastructures. Wireless Personal Communications 30 (2–4), 233–245.

Marias, G.F., Delakouridis, C., Kazatzopoulos, L., Georgiadis, P., 2005. Location privacy through secret sharing techniques. In: Proceedings of IEEE Workshop, Trust, Security and Privacy for Ubiquitous Computing, TSPUC 2005, Taormina, Italy, June 2005.

Minch, R.P., 2004. Privacy issues in location-aware mobile devices. In: Proceedings of the 37th Hawaii International Conference on System Sciences, January 2004.

Papazafeiropoulos, G., Priggouris, N., Marias, G.F., Hadjiefthymiades, S., Merakos, L., 2003. Retrieving position from indoor WLANs through GWLC. IST Mobile and Wireless Communications Summit, Portugal, June 2003.

Pfitzmann, A., Koehntopp, M., 2000. Anonymity, unobservability, and pseudonymity—a proposal for terminology. In: Proceedings of Workshop on Design Issues in Anonymity and Unobservability, July 2000.

Priyantha, N.B., Chakraborty, A., Balakrishnan, H., 2000. The cricket location-support system. In: Proceedings of the Sixth ACM MOBICOM, August 2000.

Saha, D., Mukherjee, A., 2003. Pervasive computing: a paradigm for the 21st century. IEEE Computer Magazine, 25–31.

Satyanarayanan, M., 2001. Pervasive computing: vision and challenges. IEEE Personal Communication, 10–17.

Schiller, J., Voisard, A., 2004. Location-Based Services. Morgan Kaufmann/Elsevier.

Shamir, A., 1979. How to share a secret. Communications of the ACM 22, 612–613.

Shamir, A., Tromer, E., 2003. On the cost of factoring RSA-1024. RSA CryptoBytes 6 (2), 10–19.

Staling, W., 2000. Network Security Essentials. Prentice Hall, ISBN 0-13-016093-8.

US Location Privacy Protection Act of 2001, Bill Number S.1164, Introduced July 11, 2001, US Congress. Available from: <http://www.techlawjournal.com/cong107/privacy/location/s1164is.asp>.

Want, R., Hopper, A., Falcao, V., Gibbons, J., 1992. The active badge location system. ACM Transactions on Information Systems 10 (1), 91–102.