Location-Based Services and Techniques

K. Demestichas, E. Adamopoulou, M. Masikos, C. Patrikakis

National Technical University of Athens, School of Electrical and Computer Engineering
9 Iroon Polytechniou St., Zographou 157 73, Athens, Greece,
Tel. +30 210 7721493
e-mail: cdemest@cn.ntua.gr, eadam@cn.ntua.gr, mmasik@telecom.ntua.gr, bpatr@telecom.ntua.gr

Abstract— In today's wireless access landscape, the evolution of positioning and tracking technologies has rendered feasible the provision of location dependent personalized services. This contribution deals with the following two interrelated topics: (a) Location-Based Services (LBS); and (b) Positioning and Tracking Technologies. The term Location-Based Services refers to services provided to the subscriber based on his current geographic location. Section I of this contribution deals with LBS. A thorough overview of currently deployed applications, along with future trends, is provided. Fundamental issues related to system architectures, security considerations and billing procedures are discussed. Focus is given on the various parameters that need to be taken into account, in order to develop a security framework and eliminate privacy threats imposed by malevolent parties. On the other hand, the development and deployment of this type of services presupposes the existence of effective and accurate positioning and tracking technologies. Several methods have been proposed up to now and considerable research efforts have been invested in this area. Section II is related to this topic. Firstly, the typical characteristics of positioning systems are summarized. Furthermore, a detailed classification of currently existing positioning methods, either commercial products or research prototypes, is carried out, revealing the special characteristics and capabilities of each one. The basic concepts of each technique are described and some representative examples are listed in the state-of-the-art subsection. Finally, a subsection describing current trends has been included.

Index Terms— Business Model, Location-Based Services, Positioning Techniques, Privacy and Security

I. Location Dependent Personalized Applications

A. Introduction

The knowledge of a mobile terminal's location can serve as the basis for the provision of advanced and innovative services to its user. Applications that utilize a mobile user's geographic location are called Location-Based Services (LBS) or, simply, Location Services (LCS) [1]-[3].

In general, the terminal's location can be the offered service by itself, but it can also be used to provide certain value-added services, for which the terminal's location is an important input parameter. A subscriber can, for example, request a list of nearby restaurants, after arriving in a foreign town.

Most often, the term "location detection" implies the use of a radiolocation function built into the cell network or the mobile terminal itself, e.g. the use of triangulation between the known geographic coordinates of the base stations through which the communication takes place.

A serious implication is that the information about a user's coordinates is controlled by the network operator, and not by the end user himself. This poses severe security and privacy concerns and may become a source of mistrust from the user's part towards the network operator. This is why specific security and privacy requirements have to be fulfilled when dealing with the provision of LBS.

Another important aspect of location detection is the degree of accuracy. Location information can be inferred by using various positioning techniques. However, the process of location estimation is not a trivial matter and estimation errors are commonplace. Therefore, the need for standardization arises, i.e. common criteria on the basis of which a location estimation procedure can be classified as acceptable or not. The conformance with such standards is especially useful when dialling an emergency telephone number, such as the enhanced 9-1-1 in North America, so that the operator can dispatch emergency police or fire-fighting services to the correct location. Nonetheless, these standards clearly affect the implementation of LBS as well.

In the U.S., the Federal Communications Commission (FCC) has issued the E911 specifications, which have been associated with the commercial implementation of LBS. E911 stands for electronic 911 and refers to the requirement by cellular network carriers to provide location information for emergency calls from cellular telephones. The FCC in the U.S. and similar bodies in other countries, in conjunction with associated public safety agencies, have mandated that cellular carriers provide approximate location of distress calls from cellular phones. Original date for completing this implementation in USA was October 1, 2001 but very few carriers were able to meet this date. Therefore, this date had to be relaxed somewhat.

Concerning the accuracy of the various location identification technologies, the FCC has set the following compliance expectations (Phase one – 1998, and Phase two

– October 2001): 100 metres for 67% of calls, and 300 metres for 95% of calls.

LBS can be classified into two broad categories: triggered and user-requested. In a user-requested scenario, the user is retrieving the position once and uses it on subsequent requests for location-dependent information. This type of service usually involves either personal location (i.e., finding where you are) or services location (i.e., where is the nearest place of interest). Examples of this type of LBS are navigation (usually involving a map) and direction (routing information). A triggered LBS, by contrast, relies on a condition set up in advance, which, once fulfilled, leads to the retrieval of the position of a given device. An example is when the user passes across the boundaries of the cells in a mobile network. Another example is in emergency services, where the call to the emergency centre triggers an automatic location request from the mobile network.

Another serious implication arises when dealing with triggered LBS. As an indicative example of this, imagine the ability of a restaurant to send an invitation (e.g., by SMS) to by-passers. This action can be regarded as unsolicited commercial e-mail or spamming. With the passing of the "Can Spam Act" in 2005, it became illegal in the U.S. to send any message to the end user without the end user specifically opting-in. This put an additional challenge on LBS applications as far as "carrier-centric" services were concerned. As a result, the focus has now shifted towards "user-centric" LBS and applications, which give the user control of the experience, typically by opting in first via a website or text message.

An especially interesting aspect of LBS is location-aware computing [4]-[5]. Today, thanks to technical progress on many fronts, digital location information is available to software applications running on many different mobile computing platforms. This new type of location-aware or location-based computing has rendered feasible the development of applications with the capability to sense their location and modify their settings, user interface and functions, accordingly.

The remainder of this section is structured as follows: Section I.B presents some typical examples of LBS and applications that have already been deployed or could potentially be deployed in the near future. Sections I.C and I.D study the charging and business models for LBS, respectively. Section I.E illustrates a typical network architecture for the provision of LBS. Section I.F deals in detail with the privacy and security concerns.

B. Applications

Since traditional mobile telephony cannot sustain their revenues, service providers are in search of additional sources of income. In this context, location-based services comprise a very promising area. The knowledge of a user's location can be utilized in many ways, with a view to the delivery of advanced and personalized services. In this subsection, some typical LBS and applications are identified and described. Some of the applications presented below have already been deployed, while the others might be developed in the future.

Routing is an area where LBS are by nature applicable. Satellite navigation is almost commonplace nowadays. Personal Digital Assistants (PDAs) equipped with a Global Positioning System (GPS) receiver can navigate a user to his destination, by providing both visual and vocal information. Moreover, if the user does not have such equipment, some operators provide a routing service to their customers, by exploiting location information retrieved from the network. However, such services are not provided by third-party application providers, as they still do not have access in users' positioning information.

Another trend is the growing demand for informative services, such as "guide me to the nearest pharmacy". So far, this type of services is delivered only if the user provides his location manually, e.g. "I want a pharmacy in the area X". The evolution of current positioning systems is expected to fully allow the detection of a user's position by the network itself. Furthermore, regarding the navigation systems, they will probably be further enriched with features such as the navigation of users through the less congested route.

Safety and security comprise another major area which can be enhanced via the implementation of LBS. New services have already developed for car theft and protection. For instance, some operators promise to find a customer's stolen car, by exploiting their network capabilities. Moreover, systems that monitor the condition and location of workers in a high-risk environment are also under development.

LBS can also be deployed successfully in the area of entertainment. The enhancement of positioning techniques will definitely give a boost to the formation of local communities of users. For example, people inside a club could vote, in order to form the play list, or they could respond to questions from people outside, in order to inform them about the club's quality and type of music. Local voting and competitions can be conducted based on the knowledge of users' positions. Sightseeing can even become more effective and enjoyable thanks to location awareness. Indeed, no guides are needed, and visitors can get customized information regarding a place or a monument.

LBS also include fleet management applications. Truck manufacturers have already implemented such systems, like the MAN Telematics system [37], offering their customers the ability to manage their fleet. Apart from this, current systems allow users to monitor their vehicles' critical functions, such as the engine temperature, the oil pressure, the engine's RPM etc. As a result, not only can they manage the routes of their vehicles, but they can also monitor driving behaviours and diagnose possible malfunctions. Similar systems are also used by ship-owners and help them monitor their ships at all times. These tools are truly invaluable for transport companies.

Another interesting case is the provision of localized mobile Yellow Pages. Yellow pages refer to the case of a user asking, e.g., for super markets in a certain area or for

plumbers in a certain area. Finally, localized advertising will probably grow to an even larger extent. For instance, a pedestrian passing near a supermarket might get messages regarding current offers in products. In this case however, we should not forget the implications of such a service related to spam and the ability of the user to opt-out (or opt-in).

C. Charging Models

Technological advances are not adequate by themselves to ensure a service's sustainability. Ways to produce revenues for the service providers are also necessary. In order for this to be achieved, the existence of a robust and easily operable LBS charging (billing) model is a prerequisite.

LBS are usually treated as value added services [2]. In general, the charging model should:

- Allow the service provider to retrieve a subscriber's location information along with any service characteristics.
- Allow the service provider to define the relationship between services and the parameters required for charging. These definitions should be dynamically configurable without interrupting the service.
- Provide the charging scheme in case of zone (i.e., geographic area) change.
- Validate the user's status (active/inactive) before charging to ensure the correctness of charging.

What follows is an overview of billing mechanisms for LBS applications [1]. The network operators own, in fact, the users' location information, and hence they can sell it to LBS providers. This also allows them to provide the payment service and carry out the final billing. Such a model is similar to the one adopted by NTT DoCoMo, where the network operator charges 9% of the transaction sum. This helps the service providers in at least two ways:

- users are not required to register with each service provider, which would be highly inconvenient, considering the low value of each transaction and the multitude of service providers,
- a credit card solution might not work.

The logging of chargeable events is not a difficult task. The problem lies in feeding that information to the main billing system, where the bill is created and sent to the user. As operators are often tied into their old and vast monolithic billing systems, it requires considerable effort to integrate new features to them.

Transactions are captured by customer data records (CDRs) and recorded into a database. This can either reside in the billing database or separately. The process can take place in real time (as for the prepaid mobile accounts) or in a batch mode (once a month, for the post-paid mobile accounts). The logic of how much to charge for each CDR could reside either in the billing system or the application server. In the latter case, the important point is that the interfaces are secure. How the interface works is dependent on the architecture, but in principle, the application server should be able to create a record in the billing CDR database.

A connection to the provisioning system also exists, controlling the access to the available services. This for example, prevents users from getting access to a service that requires prior subscription.

Network operators (especially in Europe) have recently realized the value of becoming micro-payment service providers, by offering a payment interface to service providers (through the use of reverse charged SMS). Although it is not a generic micro-payment engine (i.e., only certain predefined charge bands are offered), reversed charge SMS is proving to be a popular third-party interface into the network operator's billing systems. The next subsection relates to viable business models in greater detail.

D. Business models

Business models comprise a topic of utmost importance, especially for the network operators which paid significant amounts of money to acquire a third generation licence [1]. Since the network operator is the owner of the user's position, a simple solution would be to charge users for access to the positioning information. However, this does not build trust. Therefore, such a business model should be applied with caution. There are a number of ways in which the users can get charged for an LBS:

- per request,
- by subscription,
- or a combination of the two.

Network operators can also turn to revenue-sharing deals, where the users are charged for an LBS (not just for positioning information) and the network operator gets a fraction of the generated revenues. In this way, the network operators can also become payment aggregators/providers by using the mobile telephone bill to charge the users for all mobile services.

A supplementary source of income is location-based advertising. Because the mobile telephone is very personal, the solution might be to create even more personalized (i.e., adapted to the user's profile and/or current location) advertisements. The marketing advantage of location-based advertisements is significant and consists in its easily measurable success rate. Extra value-added features, such as coupons, can be included to attract users. Advertisers could be charged by the response rate or using the Web's similar notion of "click-through", i.e. by counting the number of times that information about the advertisers has been sought.

If a service provider has a sufficiently influential brand and market share, and its services are generating a lot of traffic volume, it might consider asking the network operator to pay for the traffic increase. This idea, however, is mostly undesirable for network operators, especially if they charge users a subscription fee for access to services rather than per-volume of traffic. Nonetheless, the

emergence of "virtual operators", in conjunction with the downturn in the economic climate might push operators to reconsider their business models.

E. Network Architecture

1) Logical Reference Model

Figure 1 illustrates the logical reference model for LCS provisioning. The Requestor is the entity from which a location request originates. It may consist in either of the following entities: a User Equipment (UE), a network provider or a service provider. The location request asks for the position of a Target UE. An LCS Client receives the location request and issues it to an LCS Server. In the most general case, the LCS Client and the Requestor are separate entities; however, in practice, they can be confined to a single entity. The LCS Server consists of a number of location service components and bearers needed to serve the LCS Clients [6]. An LCS Server consists of the functions that are needed for the Radio Access Network to support Location Services. It employs a positioning function to obtain the location information and furnish the information to the LCS Client

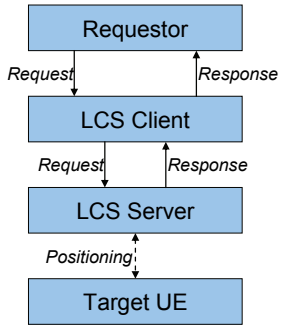

Figure 1: LCS Logical Reference Model

2) Cellular Network Architecture

Due to their large deployment, the use of cellular networks has become considerably widespread. Therefore, it is of high value to study the provision of location services within the framework of cellular networks. Figure 2 depicts a simplified, yet typical cellular network architecture for the provision of location services. This architecture is applicable to both Global System for Mobile Communications (GSM) and Universal Mobile Telecommunications System (UMTS).

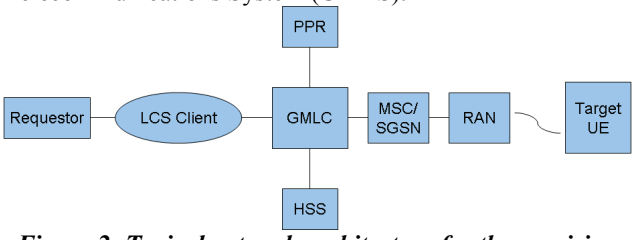

Figure 2: Typical network architecture for the provision of location services in cellular networks

The target UE corresponds to the subscriber whose location is requested to be disclosed. The Requestor is the originating entity, which has requested the location of the target UE from the LCS client. The LCS client requests location information for a target UE from the Gateway Mobile Location Center (GMLC). The GMLC contains functionality required to support LCS. In a Public Land Mobile Network (PLMN), there may be more than one GMLC. The GMLC is the first node an external LCS client accesses in a GSM or UMTS network. The GMLC may request routing information from the Home Location register (HLR) or the Home Subscriber Server (HSS). Privacy checks are carried out through cooperation with the Privacy Profile Register (PPR). The role of the PPR is to hold the users' privacy settings regarding location services, and to encompass functionality in order to perform the related privacy checks. After the authorization of the location request has been performed, the GMLC sends positioning requests to either the Visited Mobile Switching Center (VMSC), Serving GPRS Support Node (SGSN) or Mobile Switching Center (MSC) Server and receives final location estimates from the corresponding entity.

The architecture illustrated in Figure 2 is an adapted version of the LCS architecture described in the specifications provided by 3GPP in [7]. This architecture is targeted to support the enhanced privacy LCS requirements described in [7]-[8] and outlined in the following subsection. As may be observed, the PPR is attached to the GMLC. One similar architecture alternative is to attach the PPR to the MSC/SGSN. Another one is to associate the PPR only with the HSS.

A different architecture alternative is to let the subscribers' LCS privacy information to be available in a particular GMLC, i.e. the Home GMLC of the subscriber. In this case, the Home GMLC is responsible for holding the privacy settings and performing the relative privacy checks, so the use of a PPR is no longer necessary.

F. Privacy and Security

1) Introduction

The extensive deployment of location-based technologies endangers users' location privacy and exhibits significant potential for abuse [9]-[12]. Common privacy principles demand, among others, user consent, purpose binding, and adequate data protection for the collection and usage of personal information [13]. Complying with these principles generally requires notifying users (data subjects) both about the data collection and the collection's purpose through privacy policies.

2) Privacy

This subsection intends to describe the privacy requirements and mechanisms for the provision of enhanced LCS [7]-[8].

a) Variety of Privacy Requirements

LCS provisioning has to comply with a variety of privacy requirements. In more detail, a user's privacy requirements may differ according to the type of the location service, the identity of the LCS client, the identity of the requestor, as well as the user's context (e.g., day of week, time of day, place, etc.).

This implies that the user should be able to specify different privacy settings for different situations. Some LCS clients may be trusted more than others. In addition to this, the multitude of different services supported even by a single LCS client creates the necessity for further differentiation between privacy requirements. In others, it is clear that the target user will have different privacy demands for different services, even when only one LCS client offers the services.

Taking the latter requirement one step further, users should be given the ability to define the same setting for all services of the same type, regardless of the actual LCS client. For example, the user could allow all dating type services to get location information.

This also involves the use of an enhanced location request method, according to which a location request addressed by an LCS client to the GMLC should include not only the identities of the LCS client and the target UE, but also a service identity. The service identity will allow the GMLC to interpret the service type.

Service type checking can be performed either by the target UE or by the network. Service type checking by the target UE would is a "looser" way of defining services, and allowing users and client more freedom in defining services, while service type checking by the network requires some standardization, but allows the network to control "spamming" towards the target.

Although the above described way to handle the privacy related settings in the network is sufficient in order to support the increasing number of LCS clients and the varying privacy requirements for location services, some more advanced schemes can also be adopted, by exploiting the user's context. Hence, it would be convenient if a user's location-related privacy parameters could automatically change, according to his or her context (e.g., home environment, office environment, time, etc.).

b) Requestor Authorization

In general, the LCS client itself may be the originating requestor, or it may act on behalf of other requestors. The requestor may be either of the following entities: a UE, the network provider, or a service provider. It is useful for the target UE to be able to approve not only the LCS client but also the originating entity.

Thus, the target UE user should be able to allow the activation of a certain LCS service with a known LCS client, but still be capable of restricting who are allowed to get positioning information. A simple example of this type of service is a "Friends Finder" application. In such an application, the target UE user may trust the LCS client, but also wish to differentiate which of the subscribers are entitled to acquire his or her location information. This suggests that not only the identity of the LCS client, but of the originator as well, should be included to the LCS client's location request.

What is more, in the most general case, the requestor is connected to the LCS client as a separate entity, with its own identity. Because of this, the requestor should also be authenticated by the LCS client.

c) Types of User Control

The target user must have full control regarding who can retrieve his location information. This means that he should be able to easily change his private settings according to will, at any time. The main settings that the target UE user should be able to define and edit are included in the following:

The user must be able to define a privacy exception list, containing at least:

- the list of allowed LCS clients (or groups of allowed LCS clients),
- the target UE user notification settings (with/without notification),
- the default treatment that is applicable in the absence of a response from the target UE for each LCS client.

The user should optionally be able to define a privacy exception list, containing in addition:

- service-specific settings,
- context-specific settings,
- requestor-specific settings,
- codewords

d) Codeword Mechanism

The codeword is an optional function for location services, which may be adopted to protect UEs against third party monitoring their location.

In case the codeword mechanism is active, the location request from the LCS client and the Requestor includes the codeword for the target subscriber. The PLMN compares the codeword sent from the LCS client/Requestor with the codeword which is registered to the PLMN in advance. If the comparison of the codeword is successful, then the location request is not rejected. If the comparison fails, the PLMN judges that the location request must be rejected.

After the codeword is checked and if there is a match, the privacy setting in the current specification is checked. Thus, the privacy setting in the user's current privacy exception list is not overridden, even if the codeword check is successful.

The codeword is registered in the PLMN by the subscriber. The subscriber of the UE is responsible for distributing his codeword to his trusted requestors. Once the codeword has been set and properly distributed, the

subscriber is protected against the location request from a third party that is unaware of his codeword.

Multiple codewords can also be registered in the PLMN by a single user. In this case, the location request is not rejected if the received codeword is included in the codeword list of the subscriber.

e) Anonymity

For enhanced privacy, the subscriber's true identity (Mobile Station International ISDN Number - MSISDN) can be hidden and replaced with an alias that is used as a permanent or temporary reference of the subscriber, both when being a target and when being a requestor. The alias can be passed on from the terminal to the LCS client application when the subscriber invokes a request, e.g. to a specific service type. As another solution, a secured network proxy may allocate the anonymous ID (alias) to replace MSISDN. The LCS client will use alias as identifiers for the target subscriber, instead of using the true MSISDN identity. GMLC will use the same alias, when sending the response to the LCS client. Both permanent and temporary alias can be used.

f) Practical Anonymity – Spatial and Temporal Cloaking

Another notion within the LCS context is *practical anonymity*. In this approach, location-based services collect and use only de-personalized data, i.e. practically anonymous data [12], [14]. This approach promises benefits for all parties. For the service provider, practically anonymous data cause less overhead. They can be collected, processed and distributed to third parties without user consent. For users (data subjects), the need to evaluate potentially complex service provider privacy policies is eliminated.

Practical anonymity requires that the subject cannot be re-identified (with reasonable efforts) from the location data. Consider a message (request) to a road-map service comprising a network address, a user ID, and coordinates of the user's current location. Identifiers such as the user ID and the network address are obvious candidates for re-identification attempts, and thus they should remain hidden. In this example, the user ID can be omitted, and the network address can be hidden by a mechanism providing sender anonymity (e.g., a secured network proxy).

Nevertheless, the remaining location information can still be exploited, in conjunction with public knowledge, in order to track a person and its habits. Taking into account this aspect, some algorithms aim at decreasing the spatial and/or temporal resolution of location information, in order to meet specific anonymity constraints [12]. In this way, the positioning information and/or its timestamp lose precision, while still remaining useful for the location-based service for which they are gathered.

3) Related Work

Up-to-now work on privacy aspects of telematics and location-based applications has mostly focused on policy-based approaches [20]-[21], but anonymity-based approaches exist as well. According to the former, data subjects need to evaluate and choose from a list of privacy policies offered by the service provider. These policies serve as a contractual agreement about: (i) which data can be collected, (ii) for what purpose they can be used, and (iii) how they can be distributed. Typically, the data subject trusts that the service provider adequately protects the private data. In contrast, the anonymity-based approach de-personalizes data before collection, thus detailed privacy-policies and safeguards for data are not critical.

Specifically, the primary task of the IETF Geopriv working group [20] is to assess the authorization, integrity and privacy requirements that must be met, in order to transfer geographic location information, or authorize the release or representation of such information through an agent. Furthermore, the working group will select an already standardized format to recommend for use in representing location information. An additional goal is to enhance this format and present protocol approaches using the enhanced format, as well as to ensure that the security and privacy methods are available to diverse location-aware applications. Approaches under consideration include, among others, data formats incorporating fields that direct the privacy handling of the location information and possible methods of specifying variable precision of location.

Moreover, the following subjects are being investigated: authorization of requestors and responders; authorization of proxies (for instance, the ability to authorize a carrier to reveal what time-zone one is in, but not what city); taxonomy of requestors, as well as the resolution or precision of information corresponding to each type of requestor. The combination of the abovementioned elements is expected to provide a service capable of transferring geographic location information in a private and secure fashion (including the option of denying transfer). For reasons of both future interoperability and assurance of the security and privacy goals, the objective of this working group is to deliver a specification with broad applicability whose implementation will become mandatory for IETF protocols that are location-aware.

The Mist routing project for mobile users [22] combines location privacy with communication aspects. It addresses the problem of routing messages to a subject's location, while keeping the location private from the routers and the sender. To this end, the system comprises a set of "Mist" routers organized in a hierarchical structure. The leaf nodes have knowledge of user locations but not their identities. They refer to them through handles (or pseudonyms). Each user selects a higher-level node in the tree, which acts as a semi-trusted proxy. It knows the identity of the user but not his exact location. The project also describes a cryptographic protocol that is used to establish connections between users and their semi-trusted

proxies, as well as mechanisms to connect to communication partners through their proxies.

Location privacy has also been studied in sensor position systems. The Cricket system [23] places location sensors on the mobile device, as opposed to the building infrastructure. Thus, location information is not disclosed during the position determination process, and the data subject can choose the parties to which the information should be transmitted. Cricket is the result of several design goals, including user privacy, decentralized administration, network heterogeneity, and low cost. Rather than explicitly tracking user location, Cricket helps devices learn where they are and lets them decide whom to advertise this information to. It does not rely on any centralized management or control and there is no explicit coordination between beacons. It also provides information to devices regardless of the type of their network connectivity. Smailagic and Kogan describe a similar approach for a wireless LAN based location system [24].

Anonymous communication in packet-switching networks and web browsing has received a fair amount of attention. The fundamental concept of a "mix" has been proposed by Chaum [25] for email communications that can be rendered untraceable even for eavesdroppers and intermediary routers. A mix is a message router that forwards messages with the objective that an adversary cannot match incoming messages to outgoing messages. In particular, such Chaum-mixes have the following properties: messages are padded to equal size, incoming and outgoing messages are encrypted with different keys, messages are batched and reordered, and replay of incoming messages is prevented. Pfitzmann and colleagues [26] extend this mechanism to communication channels with continuous, delay-sensitive voice traffic.

Onion Routing [27] is a technique for pseudonymous (or anonymous) communication over a computer network, developed by David Goldschlag, Michael Reed, and Paul Syverson, is applicable to both connection-based and connectionless protocols. It is based on David Chaum's Mix networks, described above, though it includes a number of advances and modifications. Among these modifications is the concept of "routing onions", which encode routing information in a set of encrypted layers. Messages travel from source to destination via a sequence of proxies ("Onion Routers"), which re-route messages in an unpredictable path. To prevent an adversary from eavesdropping on message content, messages are encrypted between routers. The advantage of Onion Routing is that it is not necessary to trust each cooperating Router; if one or more routers are compromised, anonymous communication can still be achieved. This is due to the fact that each Router in an Onion Routing network accepts messages, re-encrypts them, and transmits them to another Onion Router. An attacker with the ability to monitor every Onion Router in a network might be able to trace the path of a message through the network, but an attacker with more limited capabilities will have difficulty even if he or she controls one or more Onion Routers on the message's path.

Crowds [28] adapts a rerouting system for anonymous web browsing. Crowds, named for the notion of "blending into a crowd", operates by grouping users into a large and geographically diverse group (crowd) that collectively issues requests on behalf of its members. Web servers are unable to learn the true source of a request, because it is equally likely to have originated from any member of the crowd, and even collaborating crowd members cannot distinguish the originator of a request from a member who is merely forwarding the request on behalf of another. The system does not require any encryption techniques.

Anonymizer [29] and SafeWeb [30] (on October 15, 2003, Symantec Corporation acquired the technology and interests of SafeWeb) are two similar user anonymity solutions provided to World Wide Web users. Anonymizer is a centralized approach to hide the web users' real identities from the web servers they access. Users can enjoy anonymity by rerouting their HTTP packets through the Anonymizer, which replaces the information in the packet headers so that the websites cannot infer the users' identities. This approach has the problem of having to entrust a centralized third-party entity. In others, the Anonymizer site can still track all the anonymous user activities and is also a single point of failure. Finally, the "Hordes" protocol by Shields and Levine [31] reduced the performance overhead inherent in such rerouting systems by exploiting multicast communications, and Guan et al. [32] contributed an analysis of anonymity properties of these systems using the probabilistic method.

In the database community, a significant amount of literature refers to security control in statistical databases, which is covered by Adam and Wortmann's survey [33]. This research addresses the problem wherein a database should grant access to compute statistical functions (sum, count, average, etc.) on the data records only under the condition that the results do not reveal any specific data record. Approaches fall into the categories: (i) conceptual, (ii) input data perturbation, (iii) query restriction, and (iv) output perturbation.

Instead of statistical point estimates, Agrawal and Srikant [34] describe how to obtain estimates of the distribution of values in confidential fields, which are suitable for data-mining algorithms. Confidential values are perturbed by adding a uniformly distributed random variable. The distribution of the original values can then be estimated through a Bayesian reconstruction procedure. An improved reconstruction procedure is described in [35]. Finally, Samarati and Sweeney [36] have developed generalization and suppression techniques, for values of database tables, which safeguard the anonymity of individuals.

4) Security

The provision of LCS services only needs to exploit the current security framework, as specified by 3GPP in [17]-[19].

Error! Reference source not found. gives an overview of the complete 3G security architecture, which is sufficient for LCS applications.

In this architecture, five security feature groups are defined. Each of these feature groups meets certain threats and accomplishes certain security objectives:

- Network access security (I)
- Network domain security (II)
- User domain security (III)
- Application domain security (IV)
- Visibility and configurability of security (V)

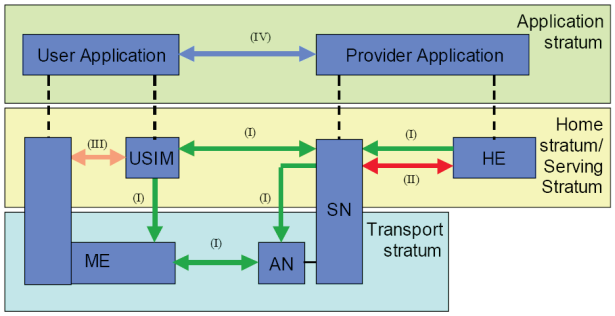

Figure 3: Overview of the 3G security architecture

a) Network Access Security

This is the set of security features that provide users with secure access to 3G services, and protect them in particular against attacks on the (radio) access link. This set of features contributes to several security domains, including user identity confidentiality, entity authentication, data confidentiality and data integrity.

The following security features related to user identity confidentiality are provided:

- **User identity confidentiality:** the property that the permanent user identity (IMSI) of a user to whom a services is delivered cannot be eavesdropped on the radio access link;
- **User location confidentiality:** the property that the presence or the arrival of a user in a certain area cannot be determined by eavesdropping on the radio access link;
- **User untraceability:** the property that an intruder cannot deduce whether different services are delivered to the same user by eavesdropping on the radio access link.

The following security features related to entity authentication are provided:

- **User authentication:** the property that the serving network corroborates the user identity of the user;
- **Network authentication:** the property that the user corroborates that he is connected to a serving network that is authorised by the user's HE to provide him services; this includes the guarantee that this authorisation is recent.

The following security features are provided with respect to confidentiality of data on the network access link:

- **Cipher algorithm agreement:** the property that the MS and the SN can securely negotiate the algorithm that they shall use subsequently;
- **Cipher key agreement:** the property that the MS and the SN agree on a cipher key that they may use subsequently;
- **Confidentiality of user data:** the property that user data cannot be overheard on the radio access interface;
- **Confidentiality of signalling data:** the property that signalling data cannot be overheard on the radio access interface;

The following security features are provided with respect to integrity of data on the network access link:

- **Integrity algorithm agreement:** the property that the MS and the SN can securely negotiate the integrity algorithm that they shall use subsequently;
- **Integrity key agreement:** the property that the MS and the SN agree on an integrity key that they may use subsequently;
- **Data integrity and origin authentication of signalling data:** the property that the receiving entity (MS or SN) is able to verify that signalling data has not been modified in an unauthorised way since it was sent by the sending entity (SN or MS) and that the data origin of the signalling data received is indeed the one claimed;

b) Network Domain Security

This is the set of security features that enable nodes in the provider domain to securely exchange signalling data, and protect against attacks on the wireline network.

c) User Domain Security

This is the set of security features that secure access to mobile stations. It comprises two basic features, user-to-USIM authentication and USIM-terminal link security.

User-to-USIM Authentication: This feature provides the property that access to the USIM is restricted until the USIM has authenticated the user. Thereby, it is ensured that access to the USIM can be restricted to an authorised user or to a number of authorised users. To accomplish this feature, user and USIM must share a secret (e.g. a PIN) that is stored securely in the USIM. The user gets access to the USIM only if he/she proves knowledge of the secret.

USIM-Terminal Link: This feature ensures that access to a terminal or other user equipment can be restricted to an authorised USIM. To this end, the USIM and the terminal must share a secret that is stored securely in the USIM and the terminal. If a USIM fails to prove its knowledge of the secret, it will be denied access to the terminal.

d) Application Domain Security

This is the set of security features that enable applications in the user and in the provider domain to securely exchange messages.

e) Visibility and Configurability of Security

This is the set of features that enable the user to be informed whether a security feature is in operation or not and whether the use and provision of services should depend on the security feature.

Visibility of Security: Although in general the security features should be transparent to the user, for certain events and according to the user's concern, greater user visibility of the operation of security features should be provided. This yields to a number of features that inform the user of security-related events, such as:

- Indication of access network encryption: the property that the user is informed whether the confidentiality of user data is protected on the radio access link, in particular when non-ciphered calls are set-up;
- Indication of the level of security: the property that the user is informed on the level of security that is provided by the visited network, in particular when a user is handed over or roams into a network with lower security level (3G → 2G).

Configurability of Security: Configurability is the property according to which the user can configure whether the use or the provision of a service should depend on whether a security feature is in operation. A service can only be used if all security features, which are relevant to that service and which are required by the configurations of the user, are in operation. The following configurability features are suggested:

- Enabling/disabling user-USIM authentication: the user should be able to control the operation of user-USIM authentication, e.g., for some events, services or use.
- Accepting/rejecting incoming non-ciphered calls: the user should be able to control whether the user accepts or rejects incoming non-ciphered calls;
- Setting up or not setting-up non-ciphered calls: the user should be able to control whether the user sets up connections when ciphering is not enabled by the network;
- Accepting/rejecting the use of certain ciphering algorithms: the user should be able to control which ciphering algorithms are acceptable for use.

II. POSITIONING AND TRACKING TECHNOLOGIES

A. Introduction

In order all the above location based services to be implemented the location of the user must be known. For this purpose many different positioning and tracking technologies have been developed until now. Below we try to present the parameters that characterize these techniques and to classify them according to their special characteristics. Afterwards, we present some representative techniques that are currently used as they are presented or slightly modified and we conclude with the presentation of current trends and future work in the positioning technologies domain.

B. Characteristics of Positioning Technologies

The classification of location systems is not very simple. Classifiers have to take into account several parameters that characterize these systems. The selection of a system for a specific application should be done after evaluating all these parameters in order to choose the most appropriate system. Below we are trying to present these parameters and explain their characteristics and their importance in a system selection process.

The most important parameters are accuracy and precision. We present them together because they are highly related. Accuracy corresponds to the deviation between the true position and the estimated one. Precision, on the other hand, indicates how often we expect to get at least the given accuracy. So, accuracy is usually expressed in meters or centimetres or a length unit, while precision is expressed in % percentage. Not to mention, a specific positioning system can, for example, achieve 2 meters accuracy 95% of the time or 1 meter accuracy 90% of the time. As both couples describe the same system, we realise how these metrics are connected. Namely, in a specific system accuracy can be traded for precision and the opposite. These two elements are presented in detail with the use of distributions, like the Gaussian distribution. Such a graph gives every detail to a user regarding system's performance. Also, in case of sensor systems that are used for indoor localisation, a dynamic adjustment according to the performance curve is possible in order to achieve energy saving.

Another important characteristic of positioning technologies is their scalability. For example, someone might design a positioning technique for outdoor environment, but then an arising problem is whether this technique can be also effective in an indoor environment. Also, an indoor positioning system based on sensor network might locate only a specific number of users simultaneously. In this case and generally in systems based on radio-frequency technology the bandwidth restrictions impose only a maximum number of communication sessions before the channel becomes congested. On the other hand, GPS can serve an unlimited number of receivers worldwide using 24 satellites plus three redundant backups. Having all these in mind assessment of the scalability of a system should include the coverage area per unit of infrastructure and the number of objects that can be traced per unit of infrastructure. Of course this number can be increased by sacrificing simultaneously either the latency

factor or the accuracy factor. In case there are more users than the system can trace then it is reasonable to have a higher positioning respond time. Moreover, the system tracks a user less frequently, resulting in worse positioning accuracy. Scalability issues include also the problems arising in case of expanding a positioning system. These problems consist of the cost part regarding the new equipment needed and the complexity part regarding the management, the self-organisation capability and the functionality of the expanded system. Consequently, scalability is a very important factor in the process of choosing a positioning system.

In the previous paragraph cost was reported as a very important parameter of the scalability factor. However, cost includes many other parameters too. Firstly, capital costs consist of infrastructure elements acquisition cost, installation cost, deployment cost and mobile elements acquisition cost. Secondly, operating costs consist of maintenance cost and support personnel salaries. In operating costs power consumption is also included. For example in case a large sensors network is used for localisation continuous battery recharging is not feasible. So the used sensors should be energy efficient. Furthermore, time cost is a very important parameter and is related to installation duration and to system expansion duration. Space cost, on the other hand, is also related to installation and expansion as the needed space for equipment may impose a different approach for positioning. Having in mind all the above, we conclude that cost is very important factor in positioning. For example, it is not a simple thing to build the necessary infrastructure for GPS positioning. Supporting personnel is needed 24h per day and a satellite system is also necessary. However, anyone can get a GPS receiver in a low cost in order to use the US GPS system for positioning. On the other hand, in case of an indoor positioning system extra equipment is needed not only for the extra users that are to be traced but also for the extra rooms where positioning is to be deployed.

Localization systems can also be sorted regarding their measurement results to absolute systems and relative systems. In absolute systems there is a common reference location for positioning of all objects. In GPS positioning, for example, the position of an object has the same coordinates regardless of the GPS satellites that are used for positioning. In relative systems, on the other hand, an object's position is given in relation to a special reference point. For example, in case of an indoor positioning system the relative position might indicate the object's position relative to the room's base system. It is obvious that the transformation from relative to absolute system is possible, if the absolute coordinates of the reference points are known.

Analogous to the previous sorting is the distinction of the localization systems in those that provide physical information and the rest that provide symbolic information. By physical information we refer to systems like GPS where the position of an object is defined via its three coordinates (longitude, latitude, elevation). On the contrary, symbolic information corresponds to positioning by using symbolic location names. This type of information is usual in Location Based Services, e.g. in case of sms spots regarding a nearby restaurant or pizza. In such cases, the symbolic information is derived from a database after the necessary processing of the physical information of object's location.

Another major parameter of localization systems is privacy. There are systems in which the user position is computed in the network side and other in which the user position is computed in the user side. A network side example is a system in which objects carry a RF tag and a user side one is the GPS positioning system. Of course, systems of the second category are more secure regarding the disclosure of user's position. However, even systems in the first category can provide position privacy in case they are designed carefully. And this is very important as user position is valuable information for marketing and other reasons.

Last but not least we report as an important parameter of localization systems their responsiveness. By responsiveness we mean the time it takes to the system to respond to a positioning request. The importance of this parameter is high and it has to do with the mobility of the tracked objects. Namely, in order to track effectively a fast moving object, the system must have high responsiveness (short respond time).

C. Classification

Up to now several positioning techniques have been developed. These techniques are either implemented in user or network side or they are based on different technology or they use different measurements or they use different methodologies or they are designate for positioning in different areas. According to these differences we try to make taxonomy of positioning techniques. This is very useful not only for helping users choose the more appropriate technique but it also helps new researchers to generate new ideas.

1) Mobile- or network-based techniques

Localization techniques can, firstly, be classified according to where the position is calculated. The user location can be measured or calculated either in the terminal side or in the network side or in both sides. For example, in GPS positioning location is calculated in the terminal side, in cell id method location is defined in the network side while in A-GPS both terminal and network contribute in positioning. As it is already mentioned, terminal-side techniques present increased security and privacy as the valuable location information is not accessible by third parties.

2) Based on the signaling technology

Localization techniques are based on the several signal technologies that are nowadays applicable. The use of a specific signal technology is defined according to the range,

propagation speed, cost, precision, bandwidth, etc. that the application requires. The applicable signal technologies are Radio Frequency, Infrared and Ultrasonic.

Radio Frequency systems are categorised in different categories according to the radio frequency they use. More precisely, they are categorised in Radio Frequency Identification (RFiDs), WLAN, Bluetooth, cellular and UWB. RFiDs systems are characterised by a unique identification number, which they transmit via electromagnetic waves. Depending on their power usage and the used frequency they can have a range up to 10 meters. Finally, RFiD tags are categorized as active or passive. Active ones are usually powered by an internal battery and they are heavier and more expensive. Passive ones obtain operating power generated from the reader, are lighter and less expensive.

WLAN stands for wireless local-area network. It is about a wireless network that uses radio waves as its carrier. Network areas may range from a single room to an entire campus. The backbone network usually uses cables, with one or more wireless access points connecting the wireless users to the wired network. The frequency that a particular device transmits on or receives from is designated in two ways: standard and channel. In 1990, the Institute of Electrical and Electronic Engineers (IEEE) formed a group to develop a standard for wireless equipment. On June 26, 1997, a standard was finally developed called 802.11. Since then a number of standards have been developed that are presented in Table I.

Table I: WLAN Standards

Standard	Data Rate
IEEE 802.11	Up to 2Mbps in the 2.4GHz band
IEEE 802.11a (Wi-Fi)	Up to 54Mbps in the 5GHz band
IEEE 802.11b (Wi-Fi)	Up to 11Mbps in the 2.4GHz band
IEEE 802.11g (Wi-Fi)	Up to 54Mbps in the 2.4GHz band
IEEE 802.16 (WiMAX)	Specifies WiMAX in the 10 to 66 GHz range
IEEE 802.16a (WiMAX)	Added support for the 2 to 11 GHz range.
HomeRF	Up to 10Mbps in the 2.4GHZ band
HiperLAN/1 (Europe)	Up to 20Mbps in the 5GHz band
HiperLAN/2 (Europe)	Up to 54Mbps in the 5GHz band
OpenAir	Pre-802.11 protocol, using Frequency Hopping and 0.8 and 1.6 Mb/s bit rate

Bluetooth is a radio standard primarily designed for low power consumption, with a short range (power class dependent: 1 meter, 10 meters, 100 meters) and with a low-cost transceiver microchip in each device. Bluetooth lets devices communicate with each other when they come in range, even if they are not in the same room, as long as they are within up to 100 meters of each other, dependent on the power class of the product. Power transmission rates vary in many Bluetooth products depending upon the power saving features available in a particular unit, bandwidth requirements, transmission distance, etc. Products are available in one of three power classes:

Class	Maximum Permitted Power (mW)	Maximum Permitted Power (dBm)	Range (approxi-mate)
Class 1	100 mW	20 dBm	~100 meters
Class 2	2.5 mW	4 dBm	~10 meters
Class 3	1 mW	0 dBm	~1 meter

A cellular network is a radio network made up of a number of radio cells (or just cells) each served by a fixed transmitter, known as a cell site or base station. These cells are used to cover different areas in order to provide radio coverage over a wider area than the area of one cell. Cellular networks are inherently asymmetric with a set of fixed main transceivers each serving a cell and they offer a number of advantages over alternative solutions like increased capacity, reduced power usage and better coverage. Until now several cellular networks have been developed like Global System for Mobile Communications (GSM) in 900 and 1800 MHz (2G), Enhanced Data rates for GSM Evolution (EDGE - 2.5G) and Universal Mobile Telecommunications System (UMTS - 3G).

Ultra Wide Band (UWB) is the last radio frequency technology that we report. UWB systems transmit signals across a much wider frequency than conventional systems and are usually very difficult to detect. The amount of spectrum occupied by a UWB signal, i.e. the bandwidth of the UWB signal is at least 25% of the center frequency. Thus, a UWB signal centered at 2 GHz would have a

minimum bandwidth of 500 MHz and the minimum bandwidth of a UWB signal centered at 4 GHz would be 1 GHz. The most common technique for generating a UWB signal is to transmit pulses with durations less than 1 nanosecond. The use of UWB technology in positioning gives more accurate and precise location estimations. Also, UWB is less affected by multipath than the traditional RF systems, but it is more expensive to apply and it demands a denser receiver's network.

Another signal technology used in positioning is InfraRed transmissions (IR). Signals are sent over distance by using light in frequencies above the range of visible light in the red end of the light spectrum. These IR signals are transmitted in order to be received by many listening devices or listening systems. IR's advantages are that it is not affected by radio or electromagnetic signals, it has low power consumption, low infrastructure cost and it is more secure. However, it is a short range technology (ti cannot go through walls), it is light and weather sensitive and as a result it is not applicable for outdoor applications.

Ultrasonic is also used for positioning reasons. It is about acoustic waves in frequencies above the audible frequencies to the human ear, which hears in the region 16Hz-20KHz. Piezoelectric receivers or optic means are used in order to detect and measure ultrasonic waves. The advantage of ultrasonic systems is that they propagate in the speed of sound, namely slower than electromagnetic waves. Because of this they provide more accurate measurements at low clock rates and they demand simpler and inexpensive systems. However, they are susceptible to environmental factors.

3) Based on the measured dimension

The first step in localization procedure is the measurement of a distance. The variety of techniques that exist for this purpose constitutes a classification criterion. The distance measurement can be done via range based distance measurement or via range free distance measurement. There are several techniques that belong to the first category like Time-of-arrival (ToA), Time difference of Arrival (TDoA), Angle-of-arrival (AoA), and Received Signal Strength Indication (RSSI). ToA and TDoA calculate the range of distance by using signal propagation time. AoA calculates the range of distance by estimating the relative angles between nodes. Of course, it is about a more expensive method as special antenna arrays are needed. RSSI is a simpler approach that makes calculations based on theoretical or empirical models in order to convert the received signal strength measurements to distance estimates. The second category consists of techniques that use an algorithm and calculate the distance in terms of hop count to anchor nodes [38]. Such algorithms are Centroid algorithm, DV-Hop, Amorphous, Point-In-Test (PIT) and Approximate Point-In-Test (APIT) [38].

4) Based on the location estimation technique

The second step in localization procedure is location estimation. As again several methods have been developed for this purpose localization techniques can be classified according to these methods.

The most common method is triangulation. Triangulation exploits the geometric properties of triangles in order to calculate an object's position. Depending on whether distance or angle measurements are used triangulation is characterized as lateration or as angulation respectively.

Lateration computes the position of an object by measuring its distance from multiple reference points. These distances can be calculated according to three different methods. The first one refers to the direct measurement of the distance, while the other two are indirect. An indirect approach is the measurement of the time-of-flight. By time-of-flight we mean the time between the transmission of the signal and its reception from a receiver. Usually we know the traveling velocity of the signal (like 344 meters per second for sound waves in 21^{o} C and $3*10^{8}$ m/sec for light pulses) and as a result we calculate the distance by using the formula velocity=distance/time. However, this approach presents certain difficulties. To be more precise, a serious problem is time synchronization. In case we measure the round-trip time of a signal transmitted and received by the same transceiver, synchronization is unnecessary. However, if the signal is transmitted and received by different transceivers, then time synchronization is needed between them. Furthermore, a second indirect approach is the attenuation measurement. By attenuation we mean the decrease of the intensity of the emitted signal in relation to the distance. Knowing the intensity of the emitted signal, the intensity of the received signal and the formula giving their relation to the distance, we can easily calculate the distance between transmitter and receiver. The formulas giving the relation of the distance to the attenuation usually give approximately results. This is due to the environment and effects like reflection, refraction and multipath. For example, in free space transmitted signal attenuates proportionally to the factor $1/r^{2}$ (where r is the distance), but in an environment with many obstacles the attenuation factor might become greater. So using these methods provide the distances from multiple reference points.

Afterwards, these distances are used in order to determine an object's position. For example in order to calculate an object's position in two dimensions we need the distance measurements from three non-collinear points. In the same way in order to calculate an object's position in three dimensions we need the distance measurements from four non-coplanar points. This is the normality. However, there are some methods that exploit some special characteristics of the object's domain in order to minimize the number of needed distance measurements. For instance, the Active Bat Location System measures the distance of indoor mobile tags, called Bats, to a grid of ceiling mounted ultrasound sensors [39]. In this case the Bat's 3-dimensional position can be determined using only 3 distance measurements as the sensors in the ceiling are always above the receiver. Consequently, such characteristics minimize the calculations' complexity.

Angulation as already reported, calculates the position of an object by taking into account angles from multiple reference points. So, in order to compute an object's position in two dimensions two angle measurements and one length measurement (such as the distance between the reference points) are required. In three dimensions, one length measurement, one azimuth measurement, and two angle measurements are needed to determine an object's position.

Except from triangulation, scene analysis and proximity are also used for location estimation. The scene analysis technique determines an object's location by exploiting features of the environment scene. Scene analysis is further divided into static scene analysis and differential scene analysis. In static scene analysis the features of the environment scene are already coded and stored in a database. So observed features are then searched in the database in order to determine the object's location. Differential scene analysis, on the other hand, is based on the differences observed between successive scenes that a moving object faces. As features of the environment are known to be at specific positions, the position of the moving object can be computed relative to their position. The information coded in the database can be either frames captures by a camera or any other measurement that characterizes the position and the orientation of an object. A very famous case is the storage of the received signal strength indications that correspond to each position of the considered scene. This scene analysis technique is widely known as fingerprinting.

Scene analysis presents some advantages and disadvantages in relation to triangulation. To be more specific, one advantage is that scene analysis is a passive technique. It does not demand the emission of signals, which requires power consumption and compromises user's privacy. It is just based on the observation of the environment. But this is simultaneously its disadvantage. Scene analysis presupposes that there is a database that contains the features of the environment. Moreover, this database must always be updated in case of changes in the scene. Consequently, scene analysis is not a very robust technique.

Finally, the third location estimation technique is proximity. According to this technique, objects are traced when they are near a known location. Proximity is calculated via three general approaches. The first one is based on the physical contact between the object and the reference point. A variety of sensors, like touch and pressure sensors can be used in order to detect physical contact. The second one is very famous and is the monitoring of wireless access points. This approach is implemented in many research projects and in the widely used 802.11 WLANs and in cellular networks. Finally, the last approach is based on the detection of ID tags. This approach is also widely used in systems such as e-Toll systems, product codes, injectable livestock identification capsules etc. Consequently, proximity is an effective location estimation technique except from the case of the physical contact approach, where the use of an extra system is needed for the exchange of identification information.

5) Based on Indoor vs. outdoor usage

Finally, positioning techniques can be classified according to the type of area where they can be implemented effectively. The main classification is in indoor and outdoor techniques, while outdoor ones can be further classified in urban, sub-urban and rural areas techniques. These different areas present different characteristics and up to now no method can provide satisfactory estimations in all types of environments. More precisely, indoor environments are usually more complicated and they demand higher accuracy as the whole area is usually smaller. In such environments Line-of sight paths is more difficult to be detected. Moreover, some techniques that are based on radio wave propagation from outdoor transmitters (like GPS) are very difficult and some times impossible to be implemented indoors. Generally, localization outdoors is usually easier. But as already said the area topology is very important as in urban areas line-of-sight paths are rarer and attenuation is more intense than in rural areas.

D. State-Of-The-Art

In this paragraph we are going to present some research and commercial positioning techniques and products that are representative of current positioning technology.

1) GPS

The widely used Global Positioning System (GPS) is officially named NAVSTAR GPS (Navigation Signal Timing and Ranging Global Positioning System) [40]. It was initially designed for military use by the US government but it quickly started to be used for civilian purposes too. It is managed by the Interagency GPS Executive Board (IGEB) and it is maintain by the US army. It is about a network of satellites that continuously transmit coded information. This information is then processed by a GPS receiver that uses triangulation techniques and position, velocity and time of the tracked object are computed. GPS constellation constitutes of 24 satellites that are orbiting the earth in a height of about 12,000 miles. They are travelling at speeds of 7,000 miles per hour in 2 different orbits. They are powered by solar energy and backup batteries in case of solar eclipse.

This widely used outdoor positioning system makes estimations with errors varying from a couple of meters to several tens of meters depending on propagation environment, sensitivity of the receiver and refractions of the GPS signal in ionosphere and troposphere. However, GPS errors can be lowered by the use of Differential GPS (DGPS). In DGPS location accuracy is improved by subtracting the positioning error of the GPS system in a known location from the solution in an unknown location. Errors in known location are usually broadcasted by using

FM radio transmissions. So DGPS lowers the positioning error in 1 to 3 meters.

2) A-GPS

A-GPS stands for Assisted GPS [41]. As we have seen above, GPS positioning is based on satellites' signals. Consequently, this system cannot operate indoors. For this reason, A-GPS was developed. In case of A-GPS the cellular network is used to assist the GPS receiver to perform its various functions. For instance, if the signals received from the GPS satellites are too weak for the receiver to extract the navigation messages, the necessary data can be sent to the receiver via cellular network. So, the cellular network provide GPS receivers with several other information, like satellite health data, atmospheric error coefficients, satellite clock error coefficients, timing information etc.

3) Pseudolites

Pseudolites are also a positioning system that tries to provide GPS positioning in areas where GPS signals are heavily attenuated [42]. It is about ground-based transmitters that generate and transmit GPS-like ranging signals. As they replace the GPS constellation no hardware modifications in GPS receivers are needed. So no extra receivers are needed from users. However, the L1 signal transmitted by pseudolites can jam GPS signals, causing interference to GPS receivers that detect signal from GPS satellites.

4) Active Badge

The first indoor localization system was developed at Olivetti Research Laboratory, now AT&T Cambridge, and it was called Active Badge [43]. It is about a proximity sensing technique that uses infrared technology. Objects to be located wear a small infrared badge that emits a globally unique identifier every 10 seconds or on demand. These identifying signals are collected by fixed infrared sensors that are spread all over the room.

5) Active Bat

The Active Bat location system was developed by AT&T researchers [39]. It is also a proximity sensing technique, but it is based on the use of ultrasound waves. More precisely, position is calculated by applying the time-of-flight lateration method. In this case objects to be located carry an Active Bat tag. When the Active Bat controller sends via short-range radio a request, the Active Bat tag emits an ultrasonic pulse to a grid of ceiling-mounted receivers. Also the controller at the same time with the request sends also a synchronized reset signal to the ceiling sensors using a wired serial network. So each ceiling sensor measures the time interval from reset to ultrasonic pulse arrival and computes its distance from the Bat via lateration techniques. Moreover, statistical analysis is applied on the computed results in order to eliminate erroneous measurements caused by reflected ultrasound pulses. According to the developer, this system achieves an accuracy of 9cm within 95% of the cases. Furthermore, the knowledge of the position of the tag on the object allows the computation of the orientation of the object.

6) Cricket

Similar to the Active Bat system, the Cricket Location Support System uses ultrasonic time-of-flight data and a radio frequency control signal in order to calculate an object's position [44]. However, in Cricket's case the objects to be located perform all their own the triangulation computations. Moreover, except from synchronization of the time measurement the radio frequency signal is also used for determining the time interval during which the receiver should consider the ultrasounds it receives. All the sounds received outside this interval will be ignored as wasteful reflections. A randomized algorithm allows multiple uncoordinated beacons to coexist in the same space. Finally, Cricket combines both a lateration and a proximity technique. Indeed, in case multiple beacons are received, receivers make a triangulation calculation. However, when only one beacon is received, it is combined with the semantic string of the radio signal providing useful proximity information.

7) RADAR

RADAR is an indoor tracking system and it was developed by a Microsoft Research group [45]. It is based on the IEEE 802.11 WLAN technology and it is a network based technique. Base stations, namely IEEE 802.11 access points, measure the signal strength and signal-to-noise ratio of signals that wireless devices send and then they use these data to compute the 2D position of an object within a building. RADAR implementation consists of two approaches, one using lateration and one using scene analysis. The first one, however, is less accurate than the second one. Generally, the RADAR system offers the advantage of no extra base stations, as it uses the already installed for networking reasons access points, but localization in three dimensions, like in case of multi-floor buildings, presents major difficulties.

8) Smart Floor

Smart Floor implements a proximity technique in order to locate objects [46]. Pressure sensors are embodied in the floor and the system uses the data derived from these sensors in order to locate objects. So objects do not have to carry or wear any kind of tag. However, as it is obvious it is about a very costly system with very poor scalability characteristics.

E. Current trends in positioning technology

It is a fact that the FCC E911 requirement has given a great boost to positioning techniques development. We have already seen that several techniques have been developed utilizing many different technologies, from acoustic to electromagnetic waves. However, these techniques present certain disadvantages. Firstly, usually each technique is specialized to perform better in certain environments, e.g. indoors or in urban areas etc. So they cannot provide universal results for positioning. Secondly, accuracy and precision of current techniques need still improvement. Moreover, required infrastructure is usually expensive, complex and inflexible in case of expansion. Consequently, all these matters are currently under consideration. The combining of different positioning techniques and the creation of hybrid ones is a major research activity. This is also triggered by the fact that future networks, like UMTS, is a mixture of several types of networks (GSM, WLAN, UMTS, satellites). As a result isolated techniques used in each network separately can now be combined. Furthermore, advanced algorithms and statistical processing techniques (like Kalman filters, Markov modelling and Bayesian analysis) are currently being used on the positioning results in order to improve accuracy and precision of estimations. The great development in the area of wireless sensor networks helped also the positioning techniques development. More precisely, researchers are trying to develop techniques that can be implemented in ad hoc networks. In such networks, objects can determine their position in reference to their mates by exploiting their positioning information altogether. Of course, arising positions are relative and not absolute, but the knowledge of one's object absolute position can immediately convert all relative positions to absolute ones. Finally, a lot should also be done regarding positioning systems quantitative evaluations that will allow users to evaluate them according their accuracy, precision and any relevant dependencies, such as the density of infrastructural elements.

REFERENCES

[1] T. D'Roza and G. Bilchev, "An overview of location-based services", *BT Technology Journal*, Kluwer Academic Publishers, Vol. 21, No. 1, pp. 20-27, Jan. 2003.

[2] D. Mohapatra and S. B. Suma, "Survey of location based wireless services", *in IEEE International Conference on Personal Wireless Communications (ICPWC 2005)*, pp. 358-362, Jan. 2005.

[3] Juha Corhonen, "Introduction to 3G Mobile Communications", Second Edition, *Artec House Inc.*, Mobile Communication Series, Boston, London, ISBN: 1-58053-507-0, 2003.

[4] I. Augustin, A. Yamin, J. L. V. Barbosa, and C. F. R. Geyer, "Towards Taxonomy for Mobile Applications with Adaptive Behavior", *International Symposium on Parallel and Distributed Computing and Networks (PDCN 2002)*, Innsbruck, Austria, Feb. 2002.

[5] R. Want and B. Schilit, "Expanding the horizons of location-aware computing", *IEEE Computer*, Vol. 34, No. 8, pp. 31-34, Aug. 2001.

[6] Mayank Tayal, "Location Services in the GSM and UMTS Networks", *IEEE ICPWC 2005*, pp. 373-378, 2005.

[7] 3GPP TS 23.271 V7.3.0 (2005-12): 3rd Generation Partnership Project, Technical Specification Group Services and System Aspects, "Functional stage 2 description of Location Services (LCS)", Release 7, December 2005.

[8] 3GPP TR 23.871 V5.0.0 (2002-07): 3rd Generation Partnership Project, Technical Specification Group Services and System Aspects System Aspects, Technical Report, "Enhanced support for User Privacy in location services", Release 5, July 2002.

[9] P. A. Karger and Y. Frankel, "Security and privacy threats to ITS", *in Proceedings of the Second World Congress on Intelligent Transport Systems*, Volume 5, Yokohama, Japan, Nov. 1995.

[10] Roy Want, Andy Hopper, Veronica Falco, and Jonathan Gibbons, "The active badge location system", *ACM Transactions on Information Systems (TOIS)*, 10(1):91–102, 1992.

[11] Philip E. Agre, "Transport informatics and the new landscape of privacy issues", *Computer Professionals for Social Responsibility (CPSR) Newsletter*, 13(3), 1995.

[12] Marco Gruteser and Dirk Grunwald, "Anonymous Usage of Location-Based Services Through Spatial and Temporal Cloaking", *in Proceedings of the MobiSys 2003*, pp. 31-42, 2003.

[13] Marc Langheinrich, "Privacy by design - principles of privacy-aware ubiquitous systems", *in* G.D. Abowd, B. Brumitt, and S. Shafer, editors, *Ubicomp 2001 Proceedings*, Volume 2201 of Lecture Notes in Computer Science, pp. 273-291, Springer, 2001.

[14] Andreas Pfitzmann and Marit Koehntopp, "Anonymity, unobservability, and pseudonymity - a proposal for terminology", *in* Hannes Federrath, editor, *Designing Privacy Enhancing Technologies - Proceedings of the International Workshop on Design Issues in Anonymity and Unobservability*, Volume 2009 of LNCS, Springer, 2000.

[15] 3GPP TS 23.271 V7.3.0 (2005-12): 3rd Generation Partnership Project, Technical Specification Group Services and System Aspects, "Functional stage 2 description of Location Services (LCS)", Release 7, December 2005.

[16] 3GPP TR 23.871 V5.0.0 (2002-07): 3rd Generation Partnership Project, Technical Specification Group Services and System Aspects System Aspects, Technical Report, "Enhanced support for User Privacy in location services", Release 5, July 2002.

[17] ETSI TS 133 102 V7.0.0 (2005-12): Universal Mobile Telecommunications System (UMTS), 3G Security, "Security architecture", 3GPP TS 33.102, version 7.0.0, Release 7, December 2005.

[18] ETSI TS 133 103 V4.2.0 (2001-09): Universal Mobile Telecommunications System (UMTS), 3G Security, "Integration Guidelines", 3GPP TS 33.103, version 4.2.0, Release 4, September 2001.

[19] ETSI TS 133 120 V4.0.0 (2001-03): Universal Mobile Telecommunications System (UMTS), 3G Security, "Security Principles and Objectives", 3GPP TS 33.120, version 4.0.0, Release 4, March 2001.

[20] J. Cuellar, J. Morris, and D. Mulligan, Internet engineering task force - geopriv requirements, http://www.ietf.org/html.charters/geopriv-charter.html, Oct 2002.

[21] Sastry Duri, Marco Gruteser, Xuan Liu, Paul Moskowitz, Ronald Perez, Moninder Singh, and Jung-Mu Tang, "Framework for security and privacy in automotive telematics", *in Proceedings of the Second International Workshop on Mobile Commerce*, pp. 25-32. ACM Press, 2002.

[22] Jalal Al-Muhtadi, Roy Campbell, Apu Kapadia, M. Dennis Mickunas, and Seung Yi, "Routing through the mist: Privacy preserving communication in ubiquitous computing environments", *in Proceedings of the IEEE International Conference of Distributed Computing Systems (ICDCS)*, pp. 65-74, Vienna, Austria, July 2002.

[23] Nissanka B. Priyantha, Anit Chakraborty, and Hari Balakrishnan, "The cricket location-support system", *in Proceedings of the 6th Annual International Conference on Mobile Computing and Networking*, pp. 32-43, ACM Press, 2000.

[24] Asim Smailagic and David Kogan, "Location sensing and privacy in a context-aware computing environment", *IEEE Wireless Communications*, 9(5):10-17, Oct. 2002.

[25] David L. Chaum, "Untraceable electronic mail, return addresses, and digital pseudonyms", *Communications of the ACM*, 24(2):84-90, 1981.

[26] A. Pfitzmann, B. Pfitzmann, and M. Waidner, "Isdnmixes: Untraceable communication with very small bandwidth overhead", *in* Wolfgang Effelsberg, Hans Werner Meuer, and Günter Müller, editors, Proceedings *of Kommunikation in Verteilten Systemen,*

Grundlagen, Anwendungen, Betrieb, GI/ITG-Fachtagung, Volume 267 of Informatik-Fachberichte, Mannheim, Germany, Springer, Feb. 1991.

[27] David Goldschlag, Michael Reed, and Paul Syverson, "Onion routing", *Communications of the ACM*, 42(2):39-41, 1999.

[28] Michael K. Reiter and Aviel D. Rubin, "Crowds: anonymity for Web transactions", *ACM Transactions on Information and System Security*, 1(1):66-92, 1998.

[29] Anonymizer, Anonymizer website, 5694 Mission Center Road #426, San Diego, CA 92108-4380, http://www.anonymizer.com, 2000.

[30] SafeWeb website, http://www.safeweb.com.

[31] Clay Shields and Brian Neil Levine, "A protocol for anonymous communication over the internet", *in Proceedings of the 7th ACM Conference on Computer and Communications Security*, pp. 33-42, ACM Press, 2000.

[32] Yong Guan, Xinwen Fu, Riccardo Bettati, and Wei Zhao, "A Quantitative Analysis of Anonymous Communications", *IEEE Transactions on Reliability*, Volume 53, No. 1, March 2004.

[33] Nabil R. Adam and John C. Worthmann, "Security-control methods for statistical databases: a comparative study", *ACM Computing Surveys (CSUR)*, 21(4):515-556, 1989.

[34] Rakesh Agrawal and Ramakrishnan Srikant, "Privacy-preserving data mining", *in Proceedings of the ACM SIGMOD Conference on Management of Data*, pp. 439-450, ACM Press, May 2000.

[35] Dakshi Agrawal and Charu C. Aggarwal, "On the design and quantification of privacy preserving data mining algorithms", *in Proceedings of the 20th ACM SIGMOD-SIGACT-SIGART Symposium on Principles of Database Systems*, pp. 247-255, ACM Press, May 2001.

[36] P. Samarati and L. Sweeney, "Protecting privacy when disclosing information: k-anonymity and its enforcement through generalization and suppression", Technical Report SRI-CSL-98-04, Computer Science Laboratory, SRI International, 1998.

[37] MAN Nutzfahrzeugehttp Group, Web site, http://www.man-mn.com/en/en.jsp.

[38] T. He, C. Huang, B. M. Blum, J. A. Stankovic, and T. Abdelzaher, "Range-free localization schemes for large scale sensor networks", *in Proceedings of the 9th Annual International Conference on Mobile Computing and Networking (MobiCom'03)*, pp. 81-95, ACM Press, 2003.

[39] Andy Harter, Andy Hopper, Pete Steggles, Any Ward, and Paul Webster, "The anatomy of a context-aware application", *in Proceedings of the 5th Annual ACM/IEEE International Conference on Mobile Computing and Networking (Mobicom '99)*, Seattle, WA, pp. 59-68, ACM Press, August 1999.

[40] E. Kaplan, Understanding GPS Principles and Applications, Artech House, 1996.

[41] R. Bryant, "Assisted GPS - Using Cellular Telephone Networks for GPS Anywhere," in Journal of GPS World, May 2005, pp. 40-46.

[42] Petrovski I., Surouvtcev I., Petrovskaia T., Okano K., Ishii M., Torimoto H., Suzuki K., Toda M., Akita J., "Precise navigation indoor", SICE Annual Conference in Sapporo, 2004.

[43] Roy Want, Andy Hopper, Veronica Falcao, and Jon Gibbons, "The active badge location system", ACM Transactions on Information Systems, 10(1):91-102, January 1992.

[44] Nissanka B. Priyantha, Anit Chakraborty, and Hari Balakrishnan. The cricket location-support system. In Proceedings of MOBICOM 2000, pages 32{43, Boston, MA, August 2000. ACM, ACM Press.

[45] Paramvir Bahl and Venkata Padmanabhan, "RADAR: An in-building RF based user location and tracking system", In Proceedings of IEEE INFOCOM, volume 2, pages 775-784, March 2000.

[46] Robert J. Orr and Gregory D. Abowd, "The smart floor: A mechanism for natural user identification and tracking", In Proceedings of the 2000 Conference on Human Factors in Computing Systems (CHI 2000), The Hague, Netherlands, April 2000, ACM.