Ensuring Anonymity for LBSs in Smartphone Environment

Mohammed Alzaabi*, Chan Yeob Yeun* and Thomas Anthony Martin*

Abstract—With the rapid growth of GPS-enable Smartphones, the interest on using Location Based Services (LBSs) has increased significantly. The evolution in the functionalities provided by those smartphones has enabled them to accurately pinpoint the location of a user. Because location information is what all LBSs depend on to process user's request, it should be properly protected from attackers or malicious service providers (SP). Additionally, maintaining user's privacy and confidentiality are imperative challenges to be overcome. A possible solution for these challenges is to provide user anonymity, which means to ensure that a user initiating a request to the SP should be indistinguishable from a group of people by any adversary who had access to the request. Most of the proposals that maintain user's anonymity are based on location obfuscation. It mainly focuses on adjusting the resolution of the user's location information. In this paper, we present a new protocol that is focused on using cryptographic techniques to provide anonymity for LBSs users in the smartphone environment. This protocol makes use of a trusted third party called the Anonymity Server (AS) that ensures anonymous communication between the user and the service provider.

Keywords—Location Based Services, Anonymity, Location Information

1. INTRODUCTION

The massive evolution in wireless communications and the dramatic increase in the usage of smartphones have facilitated a greater ability to access mobile networks and their services. Because smartphones are easy to carry and available while the users are moving around, accessing network services has become easier and ubiquitous.

At the same time, Location Information (LI) introduced a new and highly personalized class of applications and services. The availability of such functionality along with the ability to uniquely identify smartphones, enabled service providers to provide services based on their location removing the time and location constrains that are associated with providing services to customers.

Information services that make use of the location of users by either utilizing satellites or mobile network cells, with the intention of providing services that are customized to their precise geographical area are called Location Based Services (LBSs). LBSs are usually accessible by mobile devices such as Smartphones, Personal Digital Assistants (PDAs) and mobile phones. There are varieties of LBS applications that include emergency services, point of interest search,

※ This research was supported by Ministry of Land, Transport and Maritime Affairs of Korean gorernment (Grant 36-2007-CAirport)
Manuscript received August 6, 2010; accepted August 31, 2010.
Corresponding Author: Mohammed Alzaabi
* Information Security Group, Khalifa University, Sharjah Campus, Sharjah, United Arab Emirates ({mohammed.zaabi, cyeun, Thomas.martin}@kustar.ac.ae)

tracking, car and personal navigation, etc. For instance, emergency services can locate the position of the caller's smartphone once he/she calls the emergency call number or sends an SOS message to the service.

Moreover, users visiting a location for their first time can use their smartphones to find places of interest or to find the nearest restaurant. Although different LBSs address different needs for users, they all depend on where the users are currently located to provide best suited services or information for them.

Consequently, the LI must be obtained precisely to ensure a high quality service for the users. There are two main positioning techniques, namely Global Positioning System (GPS) and Network-Based Positioning techniques. The former uses satellites to determine the localization of the user. This technique is the most commonly used since most of today's smartphones are GPS-enabled. The latter uses the time difference in transmission between the user and the associated base station.

This paper is divided into six main sections. In the first section, a general introduction about the project is stated. Some security challenges and threats that might occur in LBSs are addressed in section two. Section three discusses some previous works in the field of the security in LBSs. Also, David Chaum's protocol is explained and illustrated in detailed steps. The discussion of our new protocol starts in section four where an overview of the proposed protocol is explained that is based on enhanced modifications of Chaum's protocol for providing anonymity for LBS in the smartphone environment. A detailed description of the protocol is also provided. A security analysis is conducted to verify how effective our novel proposal is against some security features and attacks in section five. The last section concludes the paper with the summary of the work done.

2. SECURITY THREATS AND CHALLENGES

This section discusses the security threats associated with LBSs. It also focuses on explaining what privacy in a LBS context is and related issues. Moreover, some challenges that the LBS faces are addressed.

2.1 Security Threats

The existence of a variety of LBSs greatly facilitates our lives and fulfills our demands. However, LBSs raise serious privacy concerns that should be addressed before the deployment of those LBSs. For instance, a malicious service provider can misuse the LI of the user to reveal information about their interests and activities. It is possible to reduce the accuracy of the LI such as by adjusting the position of the user to be included in a wider range. Some services, however, like tracking services, need precise LI details in order to satisfy user's demand [1].

Furthermore, a user might be placed in a physical danger if the LI is revealed and used by a stalker to continuously track user's location. Also, there are some advertisement services that send unwanted messages to users based on their locations. This is called location based spam [2].

In this context, privacy can be defined as a controlled disclosure of LI. Some services may require the location of the user only, whereas others may require the location as well as the identity of the user. For example, services like personal or car navigation do require the location of the requesters to provide the service (such as search for POI places) but not their exact identity.

Consequently, the privacy issue is not essential in such services. On the other hand, services like social networking and people tracking require knowledge of the users' locations and their identity.

Privacy varies from one user to another. Sometimes, it is fine for some users to disclose their location information to their supervisors while they are on vacation. Nevertheless, others may not be willing to do so. Consequently, in order to handle location privacy properly, it is important to know what location information to disclose and under what circumstances [1].

Controlling the disclosure in such services is crucial. In order for these services to succeed in the mass market, privacy concerns must be addressed carefully to gain the trust of the users. The LI of a user must only be accessed with the right authorization [2].

2.2 Security Challenges

There are many challenges associated with the security and privacy in LBSs. These challenges are becoming the main areas of interest for most researchers in this field, such as in [1, 3, 4, 6]. Addressing these challenges is vital in order to gain success in the mass market.

The nature of LBSs is a major challenge since it mostly relies on wireless communication. At the same time, wireless communication is vulnerable to many security challenges and attacks. Therefore, it is crucial to provide communication security. To provide communication security, all links between different nodes in LBSs must be protected. In order to provide robust security frameworks, those frameworks should maintain some security services. Some of these security services are confidentiality, integrity, and availability.

Providing privacy is another great challenge in LBSs. The challenge is raised because of the location information provided with each request sent from the user to the service provider. This location information is necessary to provide the service to the user. In some situations, location information is considered as source for identifying individuals and violating their privacy. For example, a user requests LBS from his/her home can cause a violation of his/her privacy. The reason behind this is the location information that directly pinpoints a user's home. Since this home identifies the owner and people who live there, the user who requested the service can be identified easily. As a result of that, the nature of LBSs contrasts the aim of providing privacy for LBSs users.

Since LBSs rely on using mobile devices as the user end-point, this environment raises another challenge in designing a robust security protocol. Previously, mobile devices such as Smartphones and PDAs faced major limitations in terms of their computation power and storage capacity. However, because of the development that we encounter nowadays in mobile devices environment, those limitations are reducing. We now have Smartphones with 1GHz processing speed and 32 GB internal storage (e.g. iPhone 4). Comparing these features with the small sizes and functionalities of Smartphones, we can say it is considerably high. On the other hand, the major challenge that exists to date is the limitation on the power source. This is crucial especially if a security framework is to be deployed in a mobile device. Most security frameworks implement some intensive security algorithms that utilize a large portion of the processing time, therefore they consume more power. Hence, it is highly recommended that power consumption is considered before any security framework is implemented.

Additionally, it is essential for any security framework to provide a protocol that is able to defend against attacks or malicious activities. LBSs are vulnerable to many attacks such as Man-in-the-Middle, Replay attack, and Traffic Analysis. Considering the service provider to be mali-

cious should also be taken into account due to its ability to reveal the private information of users. All this makes designing the security protocol much more challenging and difficult. In section 5, the proposed protocol is analyzed against some common and effective attacks which are Man-in-the-Middle and Replay attack.

3. RELATED WORK

In [3], the authors proposed a constrained-based solution for location based services. In their proposal, a set of constraints are used in order to allow a subject to have control over the distribution of location information. Location information constraints are simply a set of rules that will restrict the way in which location information can be disclosed or used. In addition, to make their proposal more effective, cryptographic means were used to bind location information with the corresponding constraints. The proposed constraints were: storage time constraints, distribution constraints, usage constraints and accuracy constraints.

The protocol proposed in [4] focuses on using a Trusted Third Party (TTP) to carry out the necessary communications. It consists of three parties, namely Users, Trusted Mobile Operator (MO), and Service Provider (SP). A Secure Job Delegation concept is provided by this protocol where users delegate their jobs to the MO. The MO is responsible for selecting, identifying and authenticating SPs as well as to identify services offered at the location of the user. It also conceals the identifiable information of users so that SPs cannot reveal their identities and violate their privacy. All of these actions are supported using cryptographic techniques such as encryption and digital signature.

In [6], the authors investigated privacy issues related to location based services usage. They claim that even if the identity of the user is not explicitly disseminated to the service providers, some sensitive information about individuals can still be revealed from geo-localized history of user requests. Collecting information from multiple requests can act as quasi-identifiers. Moreover, a framework is proposed that evaluates the risk associated with exposing identifiable information via location information. It also proposes some ideas regarding how these issues can be avoided.

Another solution, which is a TTP-free protocol, is proposed in [7]. It aims to provide location privacy without the involvement of any TTP. The main proposal is to allow a set of users to collaborate and to exchange their location information among themselves. The exchanged information will then be used to compute a new value, a so-called centroid that will replace the users' real location information. Upon computing a centroid value, users will then use it as their own location. Hence, service providers will not be able to distinguish between users.

Moreover, two approaches were proposed that specify how a centroid is computed. The first approach is centralized where a single user collects location information from other users and calculates a centroid value. The second approach is non-centralized where location information is not collected by one user; nevertheless it travels across multiple users to create a chain of location information.

A considerable number of researches were performed to use anonymity as a privacy-preserving solution in LBSs. One of the most widespread approaches is discussed in [5]. The authors developed a privacy protection approach based on anonymity. They use the concept of k-anonymity which means that "a subject is k-anonymous with respect to location information,

if the location information of that subject cannot be distinguished from the location information of at least k-1 other subjects". Their approach is based on adjusting location information resolution using a middleware architecture as well as some adaptive algorithms. The adjustment of location information is done in spatial and temporal dimensions to satisfy anonymity requirements.

Another anonymity-based approach is proposed in [16]. The user sends his/her actual location to the server along with some dummy locations. Therefore, the server will not be able to recognize the correct location. The server will process the query with each reported location to provide the answer set. When the user receives the answer set, he/she can identify the exact answer. A similar approach is proposed in [17] where a location of a nearby landmark is reported to the server.

A distributed architecture is proposed in [18] that uses anonymity for privacy preservation. In this architecture, mobiles users communicate among each other using a fixed infrastructure such as a base station. A distributed data structure is maintained through these communications where the stored location information is used by the users to hide their exact location into k-anonymous cloaked locations.

More proposals in the anonymity-based approaches are in [19, 20].

3.1 Previous Anonymity Protocol

Privacy conservation is a challenging issue in LBSs. A probable solution for this issue is to provide user anonymity, which means ensuring that a user initiating a request to the SP should be indistinguishable from a group of people by any adversary who had access to the requests [8]. In this section, we are going to discuss one of the initial protocols in anonymous communications in detail. It is worth mentioning that our proposal is an extension from that protocol.

Anonymity in LBSs can encourage many solutions regarding cases where users' security and privacy are required. For instance, a user requesting a drug treatment center might be a cause of embarrassment for the requestor. Hence, providing anonymous communication is an appropriate solution in that case. Since LBSs are mainly depending on the location information provided by the requestor, ensuring users' anonymity will also depend on how and from whom location information is protected.

We cannot deny that there is other identifiable information that might be requested by SPs such as name, age, gender, and phone number. However, these details are not required by all SPs (i.e. not all SPs depend on them). In [9], the author proposed other information that affects the anonymity of a user.

David Chaum is one of the pioneers in the field of anonymous communications. He proposed in [10] a protocol that is based on Public Key Cryptography to ensure anonymity in mail systems. The protocol hides the identity of the sender and leaves no traceable objects of the transaction.

Moreover, it hides the content of the message from the unsecured communication media. The protocol does not require a universal TTP. Along with the feature of allowing the sender to remain anonymous to the recipient, the protocol provides an untraceable return address that allows the recipient to send the response back to the sender.

The idea of Chaum's protocol is that rather than sending the message directly to the recipient, a middle computer node called *Mix* is used to process each message before it is delivered. As-

suming Alice would like to send message M_1 to Bob at address A_{Bob}, she generates M_1 and encrypts it with the public key of Bob (K_{Bob}). In the context of email systems, Bob's address refers to his email address. The address of Bob (A_{Bob}) is appended to the previously encrypted part and the whole message is then encrypted by the public key of Mix (K_{Mix}). The overall message that is sent from sender to Mix node is shown below. R represents a random number.

$$K_{Mix}(R_1, K_{Bob}(R_0, M_1), A_{Bob}) \quad (1)$$

where:

K_x is the public key of X.

R is a random number.

M is the message.

This message is received by Mix and decrypted using its private key. R_1 will be thrown away, so the output of Mix is $K_{Bob}(R_0, M_1)$ which will be forwarded to address A_{Bob} (i.e. to Bob). Fig. 1 illustrates the protocol.

Mix's main purpose is to remove correspondence between its input and output. It is vital to make sure that there should be no items in the input are repeated in the output; otherwise a correspondence can be identified. In case there are more than one input, Mix permutes there order before outputting them. Doing this can make traffic analysis more difficult. Furthermore, padding can be used to ensure that all output messages have similar sizes.

In order to allow Bob to respond to Alice without revealing her identity, an untraceable return address is used, $K_{Mix}(R_1, A_{Alice}), K_{Alice}$ where A_{Alice} is the actual address of Alice, K_{Alice} is a temporary public key of Alice, and R_1 is a random number. The specific feature of the temporary public key is that it is only used once for each transaction. This part is appended to the message described previously in formula (1). When Bob receives M_1, it will create the response message M_2, encrypt it with Alice's temporary public key and send it to Mix.

The next step is to decrypt the untraceable address by the Mix node to know where this response message must be sent. Also, R_1 which is decrypted from $K_{Mix}(R_1, A_{Alice})$ is used as a key to encrypt $K_{Alice}(R_2, M_2)$ which has the response message. Chaum's protocol with return address is shown in Fig. 2.

This technique is very practical as long as the Mix node remains genuine. Chaum's protocol introduced another concept called cascading. It strengthens the anonymity by using a series of Mix nodes called a Mix net. Messages are navigated through the mix net until they reach their destinations. In order to maintain anonymity, only one Mix node is required to be genuine.

If we attempt to analyze the protocol, it is noticeable that it is heavily dependent on the number of packets in transit at any given time interval. In more detail, both time and the number of

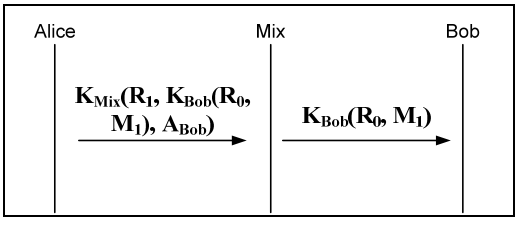

Fig. 1. Chaum's protocol

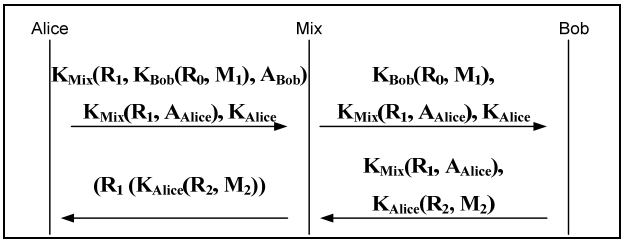

Fig. 2. Chaum's protocol with return address

packets can be combined to expose the pairing between the two communicating parties (user and server). For instance, a user and a server are both communicating at a certain time interval, and they are not functioning before or after that time interval, then it is most likely that they were interacting with each other.

Similarly, if the number of packets transmitted from a user to a server is different than other pairing parties, it can reveal a clue that they were communicating with each other. Hence, in order to maintain a high level of anonymity in Chaum's protocol, the following two assumptions must be preserved [11]:

1. In the Mix net, at least one Mix should be genuine.
2. Messages sent and received between users and servers must have the same number of packets and the same size.

4. New Anonymity Protocol for LBSs

Most of the proposed protocols [5,13,14,15] in the area of anonymity in LBSs are based on adjusting the resolution of location information to preserve the privacy of users. Our proposal is mainly focused on using cryptographic techniques to provide anonymity for LBS's users. Our protocol is based on Chaum's Mix protocol discussed in the previous section.

A number of changes were made to the original protocol so that it fits the LBSs context as well as fulfills all security and anonymity requirements. In some situations, generalization of location information is performed in order to ensure anonymity for the users. A case where this applies is when a user is requesting for LBS while he/she is at home. Since location information refers directly to his/her home, privacy and anonymity could be easily violated.

The main objective behind the protocol is to provide an appropriate level of anonymity for LBS users. Users should be able to request services while their privacy and anonymity are protected. Because location information is what all LBSs depend on, our protocol is mainly focused on how location information is protected and from whom. Location information in the LBSs can be obtained from calculating the geographical location of a user. This type of location information can accurately pinpoint the physical location of the user. A Global Positioning System (GPS) can be used to gather such location information. Another type of location information is implicated [12].

Attackers or malicious service providers should not gain any identifiable information of the users. Since service providers have legitimate access to location information of users (in order to provide the service), this piece of information should not allow them to accurately identify who

the requestor was. In some situations where the risk of location information being identifiable (i.e. can reveal the identity of the requestor), location generalization is applied which will be discussed in more details in the coming section.

Attackers should not be able to obtain location information. They can carry out eavesdropping, replay attacks and traffic analysis and the protocol should prevent these attacks (or in practice, reduce their effectiveness). Throughout our protocol we assume that the anonymity server is trusted. The anonymity server can be provided by the mobile operator in any country. Since mobile operators usually sign contracts with the governments, they can be trusted.

It is important to mention that our proposal is best suited for free services. Since paid services need some billing information to be provided to another party, such as a TTP or SP, this information will affect the anonymity of the user, particularly if it reaches malicious hands.

One of the practical applications for this protocol is to provide anonymity for VIPs to hide their whereabouts.

4.1 New Proposed Protocol

The detail of the protocol is described in Fig. 3. Throughout the explanation of the protocol we will use the following symbols:

where:

U is the user of a smartphone.
AS is the anonymity server.
SP is the service provider.
P_X is the public key of *X*.
Sym_X is a symmetric key of *X*.
$CLoc_X$ is the current location of user *X*.
A_X is the address of *X*.
TR_X is a transaction of id *X*.
R_X is a random number generated by *X*.
M is a message.

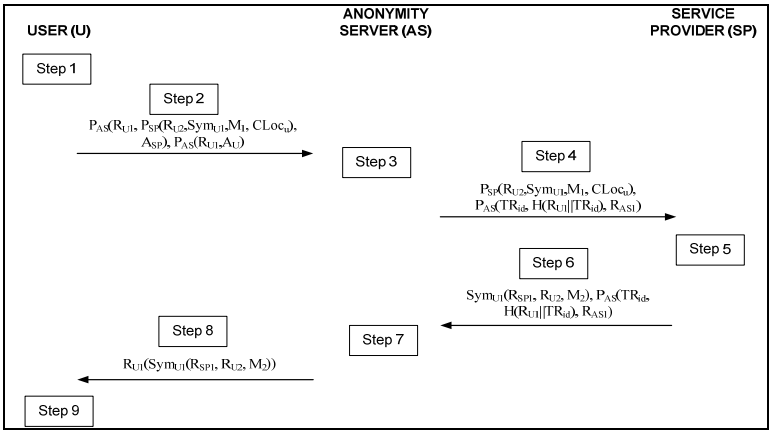

Fig. 3. New proposed protocol

Step 1. The protocol is initiated by the LBS application installed in the user smartphone. The first job for the user (*U*) is to create the whole message that will be navigated through the Anonymity Server (*AS*) in order to reach the Service Provider (*SP*). For instance, we will assume that the request message M_1 is to ask for the closest restaurant to the user. The created message looks like:

$$P_{AS}(R_{U1}, P_{SP}(R_{U2},Sym_{U1},M_1, CLoc_u), A_{SP}), P_{AS}(R_{U1},A_U) \quad (2)$$

where M_1= "Get me the closest restaurant."

We can divide this message into two main parts. The first part ($P_{AS}(R_{U1}, P_{SP}(R_{U2},Sym_{U1},M_1, CLoc_u), A_{SP})$) is responsible for delivering the request message (M_1) to the *SP*. M_1 as well as a random number (R_{U2}) all of which is encrypted by the public key of the *SP*. From the GPS enabled smartphone, the current location of the user ($CLoc_u$) is detected and added to the message. Sym_{U1} is a temporary symmetric key created by the user which will be used by the *SP* to encrypt the response message in step 5.

To define which *SP* is to be communicated with, the address of the *SP* (A_{SP}) is included in the message. It permits the *AS* to know which *SP* is intended to receive the request message (M_1). Usually, A_{SP} is the IP address of the server. Along with that, a random number (R_{U1}) is included to ensure message freshness.

The second part ($P_{AS}(R_{U1},A_U)$) is used to allow the response message that is created by the *SP* to be sent back to the user (*U*). The user creates a return address that contains the actual IP address of the user (A_U). This part is mainly used by the *AS* (in step 7) to know the address of the user.

Although the message's two parts are encrypted with the same public key, they are actually separated in the structure of the message. Since the return address is only needed in step 7, the *AS* can directly store it (in step 3) while it is encrypted without the need for decrypting it and encrypting it again for safe storage.

Step2. The message created in the first step will be sent to the *AS*.

Step3. Once the message has been received, the *AS* will decrypt the first part of the message to deduce the address of the *SP* (A_{SP}). The random number R_{U1} will also be decrypted which later on will be checked (by the *AS*) against the random number (R_{U1}) sent in step 8 to prevent any replay attack attempts. $P_{SP}(R_{U2},Sym_{U1},M_1, CLoc_u)$ will be kept as it is, since it is encrypted by the public key of the *SP* and hence the *AS* can't read the request message (M_1).

The second part of the message will be stored in the *AS*. As indicated earlier, it contains the actual physical address of the user (in this situation it is the IP address). At a later stage, when the response from the *SP* is to be sent to the user (step 7) the *AS* will decrypt this part to get the actual address of the user. The *AS* creates a transaction id (TR_{id}) for each request in order to refer to the corresponding stored return address. Since the part that includes the transaction id is encrypted by *AS*'s public key, an adversary that holds *AS*'s public key (which can be obtained easily, such as from previous genuine transactions) can substitute this part with another one. Hence, the transaction id should be protected from tampering.

In order to protect the integrity of the transaction id, R_{U1} and TR_{id} are hashed and included in the message. Also, a new random number (R_{AS1}) is generated in order to ensure freshness of the message. Those elements are encrypted by the public key of the *AS*.

One of the main characteristics of *AS* is to act as a mixer. All requests sent from different users will be received by the *AS* and permutated before forwarding them on. In more details, if there are three users (U_1, U_2, U_3) who sent three respective messages (M_1, M_2, M_3), the order of forwarding these messages will be randomly changed. Hence, assuming that the order of receiving these messages is (M_1, M_2, M_3), then, a possible forwarding order can be (M_3, M_1, M_2). Achieving this can significantly reduce the effectiveness of traffic analysis attack. An attacker who tries to perform traffic analysis will have difficulty in matching the messages coming into and out of the *AS*.

The message after processing the previous step is:

$$P_{SP}(R_{U2},Sym_{U1},M_1),\ P_{AS}(TR_{id},\ H(R_{U1}||TR_{id}),\ R_{AS1}) \tag{3}$$

Step 4. *AS* passes the message modified in step 3 to the *SP*.

Step 5. Once the *SP* receives the message, it uses its private key to decrypt the first part of the message. It reads the request message, processes it according to the user request and produces the result. In our case where the closest restaurant is required by the user, the result produced might be a list of restaurants. The *SP* will form the result in another message (M_2) and will encrypt it with the temporary symmetric key of the user (Sym_{U1}) which is included in the first part of the message. This symmetric key is only known by the user and the *SP*. It prevents the anonymity server from reading the response message created by the *SP*. In addition, a random number (R_{SP1}) is included to the message. The second part of the message will be forwarded back to the *AS*.

The message can be formed as:

$$Sym_{U1}(R_{SP1},\ R_{U2},\ M_2),\ P_{AS}(TR_{id},\ H(R_{U1}||TR_{id}),\ R_{AS1}) \tag{4}$$

where M_2= “Restaurant 1, Restaurant 2 and Restaurant 3.”

Step 6. The previous message is then sent to the *AS*.

Step 7. The next step is to deliver the result message (M_2) to the user. The *AS* needs firstly to retrieve the actual address of the user (A_U). It can be done by identifying the transaction id (TR_{id}) included in the second part of the message. The integrity and freshness of transaction id are verified using R_{AS1} and the stored R_{U1} (that is attached with the return address). The corresponding stored return address (A_U) and random number (R_{U1}) will be retrieved and decrypted. Accordingly, the *AS* will use A_U to deliver the response message to the user. Since it is essential to eliminate any correspondences between *AS*’s input and output messages, the entire message is encrypted again by a new symmetric key deduced from the random number R_{U1}. The final message that will be sent to the user will be:

$$R_{U1}(Sym_{U1}(R_{SP1},\ R_{U2},\ M_2)) \tag{5}$$

Step 8. The *AS* forwards formula (5) to the user.

Step 9. The user receives the message and will use its random number R_{U1} and the corresponding symmetric key to decrypt it and to get the response of the *SP*. Also the random number (R_{U1}) will be checked in order to ensure the freshness of that message.

4.2 Location Generalization

One of the situations where a practical level of anonymity is maintained while providing high quality location information is when a user who is asking for a LBS is walking in the middle of a crowded city. Since large number of people might be present in a physical location, a malicious SP will not be able to precisely identify the requestor.

However, in some situations, providing high quality location information may violate the privacy of a user. Assume that a user is asking for LBS while he/she is at home. In this case, the physical location of the user (which pinpoints his/her home) can effectively be used by a malicious SP to identify that user, hence violating his/her privacy. Although the location information is protected from eavesdroppers, malicious SP's who have authorized access to location information can misuse it.

For this reason, the desire for generalizing location information that is sent to the SP is essential. To generalize location information, the quality of the submitted location information from the smartphone can be reduced. Therefore, instead of providing an exact physical location of where the user currently is, we can make it more general to include a range of physical locations or to include a larger area. Achieving this will strengthen the anonymity of the user and will solve the problem discussed above.

Although location generalization is a practical solution for some situations where the privacy of a user might be violated, some LBSs require high quality location information in order to provide the best service to the user. For instance, if a user is asking for a personal navigation service to have directions from his/her current location to another one, the LBS needs an accurate location information in order to provide the best routing direction to the user.

Consequently, maintaining high quality location information is also an important aspect that must be addressed. In our protocol, we addressed this issue by two possible approaches. The main concept behind these approaches is not to apply location generalization to all requests initiated by the user. The user can specify if the current location might violate his/her privacy or affect his/her anonymity.

Approach 1. Whenever a user requests for a LBS, a message will appear asking the user to specify his/her location. A list of possible places is provided such as: home, work, hospital, a place I frequently visit and others. In case the user chooses a place where providing high quality location information might affect his/her anonymity, location generalization must be applied. For example, if the choice was "home", then location information is generalized to include a wider area of where the user is currently located. Nevertheless, in case the choice was "others", location generalization will not be performed since that location can be public and will not reveal any information about the requestor.

Approach 2. The idea is similar; however, we allow the user to pre-specify some locations (landmarks) like home, work, and places where he/she frequently visits. We can assume that providing accurate location information of these places can affect the user's anonymity. These places can be added to or updated to the smartphone at any time by capturing their physical locations while the user is there. A small database in the smartphone can preserve these landmarks. Whenever the user is closed to one of the stored landmarks, location generalization will take place.

5. ANALYSIS

This section consists of two sub-sections. One is security analysis and the other is design comparison. The first will analyze the proposed protocol against some mostly common and effective attacks as well as some anonymity properties. The second sub-section is a comparison between some protocols discussed in the related work and our proposal.

5.1 Security Analysis

5.1.1 Man-in-the-Middle Attack

One of the attacks that is considered as active eavesdropping is Man-in-the-Middle (MITM) attack. It is a critical issue especially if the communicating parties believe that they are directly communicating with each other while in fact they are not. The attacker places himself between the sender and the receiver and controls the communication between them which involves intercepting, modifying and deleting data. In most circumstances, the attacker intercepts messages between them and injects new ones.

This attack can be performed even if the communication is encrypted. In LBSs, this attack can cause some threats such as exploiting the location information of a user. A probable scenario where MITM attack can be effective is when the attacker detects the encrypted message between the user and the AS. Since the first part of the message that has the request message is encrypted by the AS's public key, the attacker can remove that part, create a new message and encrypt it with AS's public key (since it is publicly available).

The proposed protocol defeats this kind of attack. Although the previous procedure can be done perfectly by an attacker, the random number that was bonded with the original message sent by the user can detect that a modification of the original message has occurred. It is less likely that the attacker can generate the same random number used by the user, hence, when the response is received by the user, the random number is checked against all previously stored random numbers before accepting that response, which in most situations will not match. It can clearly be seen that the requirement for a robust random number generator and not reusing previous random numbers are essential.

5.1.2 Reply Attack

A replay attack can be considered as a subsidiary of the Man-in-the-Middle attack. In this type of attacks, the attacker intercepts the communication between two entities in order to gain an unauthorized copy of a data packet that contains some credentials like username and password. That packet will be delayed or resent again by the attacker in order to impersonate the sender and to gain unauthorized privileges.

Furthermore, even if the communication is encrypted, the attacker can still launch the attack without the need to know what the content of that packet is. In LBSs, a replay attack can violate the privacy and anonymity of a user by exploiting the location information of that user. For instance, if an attacker was able to intercept the communication between the user and the service provider and gain the requesting message for a service, the attacker can resend that message again to the service provider (even if it is encrypted). From the response, the attacker can recognize an approximate location of that user.

In order to prevent replay attacks, the protocol employs random numbers. Random numbers

ensure the freshness of messages and that the message is not a replay of a previous one. Each request or response from the user or the service provider is bonded to a random number that can uniquely identify the corresponding request or response. Each entity in the protocol maintains a list of all random numbers received or transmitted with previous messages. This behavior can lead to long lists of random numbers; hence, those lists can be reset from time to time.

Consequently, if an attacker tried to initiate a replay attack, the entity (which can be the user, anonymity server, and service provider) checks the encrypted random number in the replayed message with the stored random numbers. If there was a match, then the message will be discarded.

5.1.3 Forward Anonymity

The ability to provide anonymity to a user in future communications, even if the anonymity of the current communication is compromised, is known as forward anonymity. It is essential to provide such a property in order to make sure that the anonymity of an entity is maintained while the current communication is compromised.

In LBSs, an example of when forward anonymity can be applied is when a key is compromised by an attacker and location information was linked to the user. In this situation, in order to maintain forward anonymity, this information cannot be used to identify the next key or location information.

To provide forward anonymity in our protocol, temporary symmetric keys are used to allow the SP to communicate with the user. It prevents the SP from linking some identifiable information like public keys or digital certificates to identify the corresponding user.

Hence, if a temporary symmetric key for a transaction is compromised, it will only reveal the information involved in that transaction. Next time the user initiates a transaction or requests for a new service, another temporary symmetric key will be used to encrypt the new message.

5.1.4 Backward Anonymity

Since forward anonymity deals with preserving the anonymity for future communications, backward anonymity is just the opposite. It maintains anonymity for previous communications in case the current secret information is compromised. Once more, the temporary symmetric key can provide backward anonymity.

In case the current key is compromised, it does not link to previous used keys. It is noticeable that forward and backward anonymity necessitate the requirement to avoid reuse of the temporary symmetric keys.

5.2 Design Comparison

The features that our contribution provides are examined against other proposals discussed formerly in the related work. We have noticed that most of the proposals are focused on the confidentiality and integrity features; however, few were targeting the anonymity feature. Although M. Gruteser and D. Grunwald in [5] proposed a new protocol based on anonymity, their contribution was mainly focused on information obfuscation.

Our contribution has targeted the confidentiality and integrity features as well as anonymity. Not only is the provided anonymity based on information obfuscation (using the Location Generalization concept), but also added an extra layer of anonymity with the aid of some crypto-

Table 1. Design Comparison between Different Protocols

Proposal	Confidentiality	Integrity	Anonymity	
			Using Cryptographic Techniques	Using Information Obfuscation
Gajparia et al. [3]	✓	✓		
Konidala et al. [4]	✓	✓		
Gruteser and Grunwald [5]				✓
Our protocol	✓	✓	✓	✓

graphic techniques to provide a more robust anonymity protocol. The summary of the comparison is shown in Table 1.

6. CONCLUSION

In this paper, we have presented a new protocol that ensures anonymity for Location Based Services in the smartphone environment. Our protocol is an extension of Chaum's Mix protocol with a number of changes in order to fit the LBSs context as well as to fulfill all security and anonymity requirements.

Moreover, in situations where location information can be used efficiently to identify the requestor, location generalization is used to adjust the resolution of location information in order to ensure the best user's anonymity.

This protocol makes use of a trusted third party called the Anonymity Server (AS) that ensures anonymous communication between the user and the service provider.

REFERENCES

[1] N. Poolsappasit and I. Ray, "*Towards Achieving Personalized Privacy for Location-Based Services,*" *Proceedings of Transactions on Data Privacy 2*, Catalonia, Spain, 2009 April, pp.77-99.

[2] L.F. Cranor and B.A. LaMacchia, "Spam!," *Communications of the ACM*, Vol.41, No.8, 1998, pp.74-83.

[3] A.S. Gajparia, C.J. Mitchell and C.Y. Yeun, "*Supporting User Privacy in Location Based Services,*" *Proceedings of Mobile Multimedia Communications on IEICE Transactions on Communications*, 2005 July, pp.2837-2847.

[4] D.M. Konidala, C.Y. Yeun and K.J. Kim, "*A Secure and Privacy Enhanced Protocol for Location-based Services in Ubiquitous Society,*" *Proceedings of IEEE Global Telecommunications Conference 2004*, Dallas, Texas, USA, 2004 November, pp.2164-2168.

[5] M. Gruteser and D. Grunwald, "*Anonymous Usage of Location-Based Services through Spatial and Temporal Cloaking,*" *Proceedings of the 1st International Conference on Mobile Systems, Applications and Services (MobiSys '03)*, San Francisco, CA, USA, 2003 May, pp.31-42.

[6] C. Bettini, X.S. Wang, S. Jajodia, "*Protecting privacy against location-based personal identification,*" *Proceedings of the 2nd VLDB Workshop on Secure Data Management (SDM'05)*, Trondheim, Norway, 2005 September, pp.185-199.

[7] M. Gheorghita, A. Solanas and J. Forne, "*Location Privacy in Chain-Based protocols for Location-Based services,*" *Proceedings of Third International Conference on Digital Telecommunications*, Bucharest, Romania, 2008 June, pp.64-69.

[8] C. Bettini, S. Mascetti, X.S. Wang, and S. Jajodia, "*Anonymity in Location-Based Services: Towards a General Framework,*" *Proceedings of the International Conference on Mobile Data Management,*

Mannheim, Germany, 2007 May, pp.69-76.

[9] C. Bettini, L. Pareschi, S. Jajodia. "*Anonymity and diversity in LBS: a preliminary investigation,*" *Proceedings of Fifth IEEE International Conference on Pervasive Computing and Communications (PERCOM-07)*, DC, USA, 2007 April, pp.577-580.

[10] D. Chaum, "Untraceable Electronic, Mail Return Addresses, and Digital Pseudonyms", *Communication of the ACM*, Vol.24, No.2, 1981, pp.84-90.

[11] A.Y.Lindell, *Anonymous Authentication* [online database], http://www.aladdin.com/blog/pdf/AnonymousAuthentication.pdf.

[12] A.S. Gajparia, C.Y. Yeun and C. Mitchell, "*Using constraints to protect personal location information*", *Proceedings of the 58th IEEE Semi-annual VTC 2003-Fall*, Orlando, Florida, USA, 2003 October, pp.2112-2116.

[13] B. Gedik , L. Liu, "*Location Privacy in Mobile Systems: A Personalized Anonymization Model,*" *Proceedings of the 25th IEEE International Conference on Distributed Computing Systems*, Columbus, Ohio, USA, 2005 June,pp.620-629.

[14] P. Kalnis, G. Ghinita, K. Mouratidis and D. Papadias, "Preventing Location-Based Identity Inference in Anonymous Spatial Queries", *IEEE Transactions on Knowledge and Data Engineering (IEEE TKDE)*, Vol.19, No.12, 2007, pp.1719-1733.

[15] L. Sweeney, "k-anonymity: a model for protecting privacy", *International Journal on Uncertainty Fuzziness and Knowledge-based Systems*, Vol.10, No.5, 2002, pp.557-570.

[16] H. Kido, Y. Yanagisawa, and T. Satoh, "*An anonymous communication technique using dummies for location-based services*", *Proceedings of the International Conference on Pervasive Services (ICPS)*, Santorini, Greece, 2005 July, pp.88-97.

[17] J. I. Hong and J. A. Landay, "*An architecture for privacy-sensitive ubiquitous computing*", *Proceedings of the International Conference on Mobile Systems (MOBISYS)*, New York, NY, USA, 2004, pp.177-189.

[18] G. Ghinita, P. Kalnis, and S. Skiadopoulos, "*Priv´e: Anonymous location-based queries in distributed mobile systems*", *Proceedings of the International World Wide Web conference*, Banff, Canada, 2007 May, pages 476-485.

[19] G. Ghinita, P. Kalnis, A. Khoshgozaran, C. Shahabi, and K. L. Tan, "*Private queries in location based services: Anonymizers are not necessary*", *Proceedings of the International conference on Management of data (SIGMOD)*, Vancouver, BC, Canada, 2008 June, pp.121-132.

[20] G. Ghinita, P. Kalnis, and S. Skiadopoulos, "*Mobihide : A mobile peer-to-peer system for anonymous location-based queries*", *Proceedings of the Symposium on Spatial and Temporal Databases (SSTD)*, Boston, MA, 2007 July, pp.221-238.

Mohammed Alzaabi

He has graduated from Khalifa University with Bachelor degree in Computer Engineering. In Oct. 2009, he joined the Master's program in information security at the same university. He chose Digital Forensics as his main theme in the program. His master's research project dealt with security and privacy in Location Based Services (LBSs). He is currently working towards his PhD degree. His researches interests include Digital Forensics and security and privacy in LBSs.

Chan Yeob Yeun

After completing his PhD at University of London, Dr. Chan Yeob Yeun joined Toshiba TRL in Bristol. Then, he became a Vice President at LG Electronics, Mobile Handset R&D Center in 2005. He was responsible for developing the Mobile TV Technologies and its Mobile Security such as CAS and DRM. He left LG Electronics in 2007. I joined at KAIST-ICC, Korea until August 2008 and moved on to Khalifa University of Science, Technology and Research (KUSTAR) as an Assistant Professor. He currently enjoys lecturing MSc. Information Security Courses at KUSTAR. He has published various International Journals and Conferences all together 38 papers, 2 book Chapters as well as 9 International Patent Applications.

Thomas Anthony Martin

He received a Ph.D. in Information Security from Royal Holloway, University of London in 2004. Until 2009 he was a researcher at BT, where he developed several security related patents, as well as participated in such projects as the EU FP7 MASTER Project. He is currently lecturing in Khalifa University, UAE. His research interests include: Cryptography, Multi-party communications, Digital Rights Management, Identity Management, Penetration Testing, Risk Assessment and Computer Forensics.