Enhancing Privacy and Authentication for Location Based Service using Trusted Authority

Kyusuk Han, and Kwangjo Kim

Information and Communications University (ICU)
119,Munjiro,Yuseonggu,Daejeon, 305-714, Korea
{hankyusuk,kkj}@icu.ac.kr

Abstract. Not only the privacy but also the authentication is an important issue using the location based serviced in the critical areas, from forging the location information. There are many studies on the privacy, while less number of studies on the authentication of message, which relies on the various location sensing technologies. However, they rely on the specific sensing technologies, who cannot be used in common environments. In this paper, we argue the authentication problem and the privacy threat from the location accuracy. And then we show the security requirements for location based services, and design the lightweight security model that is independent from specific hardware and cryptographic algorithms. We also introduce two protocols based on proposed the basic model which guarantees the authentication and privacy from location accuracy. We believe our model and protocol can be widely used in wireless sensor network with the simple customization.

Keywords: Ubiquitous, context-awareness, location based service, privacy, authentication

1 Introduction

The ubiquitous computing is the method of enhancing computer use by making many computers available throughout the physical environment, but making them effectively invisible to the user. In the ubiquitous computing environment, various sensing technologies are used to provide 'context-awareness' services to users. The 'context' comprises human's health information, date and time, location, temperatures, and so on. Currently the location based service (LBS) is most widely used in the various areas; car navigation services, emergency medical services, and so on. We expect the usage of LBS will not limited to the informing the location, but expanded to the proving the location.

From the expansion of LBS, not only the threat to the privacy, but also the threat to the integrity of the location are raised. There are many studies on the privacy problem [1–5]. These studies focused on hiding a user's identity anonymously, while the proper location based service is provided to the user. However, there is lack of consideration of the privacy problem from 'the level of location accuracy'. We define the location accuracy from the location information expression as civic addresses. There are two common ways to identify the location of an object, either through geospatial coordinates or civic addresses. Geospatial coordinates indicate longitude, latitude, and altitude, while civic addresses indicate a street address. 6 divisions of civi addresses are defined as national subdivision, county, city, city division, neighborhood, group of streets below the neighborhood level in [6]. We argue that the divisions should be considered in privacy concept.

Also, several location authentication methods were studied. Those studies focus on the authentication of user for service provider, who based on GPS [8], Time difference of the velocity of signals [9], RFID [10], or *etc.* However, these studies are lack of the privacy consideration, and depend on specific characters of location sensing technologies, which limit the application of the method.

In this paper, we show the risk analysis of the location based service model and define security requirement. And then, we introduce the improved model of location based service which enables the authentication of location information. Based on the model, we show the protocols satisfying the security requirements, also can be adopted in practice. After that we analyze that the proposed protocols hold requirements.

2 Location Based Service Model

2.1 Location Based Service Scenarios

Several examples of location based service are described in [16]. Followings are the some of examples.

Location based billing Through location based billing, the user can establish personal zones such as a home zone or work zone. Through arrangements with the serving wireless carrier, the user could perhaps enjoy flat-rate calling while in the home area and special rates while in other defined zones. This type of application can be especially useful when use in conjunction with other mobile applications such as prepaid wireless.

Tracking Fleet applications typically entail tracking vehicles for purposes of the owning company knowing the whereabouts of the vehicle and/or operator. Tracking is also an enable of mobile commerce services. A mobile user could be tracking and provided information that he has predetermined he desires, such as notification of a sale on men's suits at a store close to the user's current proximity.

Access Control Researches on the context-aware access control consider 'contexts' as the the parameters for defining the security policies; locations, temperatures, health information, the date and time, and so on [17–19]. When the classified information is only accessible in the authorized areas, a user accessing that information should prove his current location is in that area.

Digital Right Management The legal distribution of digital contents, like music and movies are limited to the border of nations. However, for the various reasons, the same content can have a difference value in different countries. Therefore, proving the location is requested to dealing digital contents.

For the location based service which need the proof of location, adversaries may try to forge the location. As above billing scenario, an adversary may want the discount with forging the location that he is in the campus, even not there actually, or with reusing the authenticated location information. Adversary may try to access from unauthorized area in the access control scenario, while many people try to find the cost-saving way in DRM scenario.

2.2 Location Service Architectures

There are many studies on location sensing technologies. In this paper, we focus ourselves on the capability of localized location computation (LLC). By the characteristic of LLC, location sensing technology can be divided into two categories; using LLC and depending on recognition, which has no capability of LLC. With LLC, the object being located actually computes its own position. It keeps privacy by mandating that no other entity may know where the located object is unless the object specifically takes action to publish that information. GPS,VHF-omni directional ranging, online map, and Cricket [12] are typical examples. In contrast, the methods that do not use LLC require the located object to periodically broadcast, respond with, or otherwise emit telemetry to allow the external infrastructure to locate it. Currently, most systems like Active Badge, Active Bats, MotionStar, MSR Radar, Pin-Point 3D ID, Easy Living, Smart Floor, Automatic ID system, Wireless Andrew, E911, and SpotON [13] have recognition capability.

In the case of LLC, user's privacy is easily guaranteed since user computes own location for himself. However, it requires relatively higher resource than the other. Recognition based system can be employed with less resource supply. However, it doesn't guarantee the privacy since the infrastructure knows the location with recognition.

Moreover, non-LLC based systems have the potential risk that any adversary forges user's location while sensing. LLC based systems also the risk of forgery by the user, since user can compute the location.

With this, The Geopriv Working Group defines a location services architecture designed to protect location privacy [14]. The architecture is well described by Beresfold [15].They defined four main components in the architecture; a location generator, a location server, a rule holder and a location recipient. The manner in which each of these components are owned and trusted can affect the level of location privacy offered by the architecture to the users of the system. By user ownership, four possible architectures are defined as *User-controlled model*, *user-mediated model*, *third-party model*, and *hybrid model*. *User-controlled model* has the capability of LLC. And, in the *User-mediated model*, the user does not control the location generators, which can therefore be inside-out or outside-in location systems, but instead the user owns and controls only the rule holder and location server. Also, in the *third-party model* user cannot control the location generators, the rule holder and location server. Hybrid model combines *user controlled model* and *third-party model*.

Based on the architectures described in [14], we define the security requirements for the authentication and privacy preserving location based service.

2.3 Security Requirements

We define security requirements for the location information as following. The whole security considerations from the communication in the location based service are not our consideration; Authentication of entities, confidentiality of common messages, temper resistance of a location generator and a location server, and so on [7].

Privacy An attacker cannot know a client's location during communications of LBS.

Prevention from overcollection A service provider should know only sufficient location information of the client.

Authentication The service provider can verify whether a client's location it correct.

Unforgeability An attacker cannot forge a client's location. Also, The client cannot forge own location.

Resistance to Replay-attack When a client's location is authenticated and used for the service, the location cannot be used again.

Preventing overcollection of location information is an important requirement for location privacy. For example, in the DRM scenario, the distributer only need to know whether the request of the purchase is from the inside of the national boundary. It shall not be allowed that the distributer requires more specific information like city and street. If there is no means of protection from overcollecting, an malicious distributer can collect all unnecessary information unlawfully. Note that current Korean location based service act, which was originally enacted in 2005, doesn't define the location information minutely.

3 Proposed framework

In this section, we show our proposed scheme for authentication and privacy of location information. We adopt the service architecture defined in [14]. Our model comprises three entities, a client C, a service Provider SP, and a trusted operator OP. C wants to prove his location to SP, while SP wants to verify C's location information. The trusted operator OP has an important role similar to the Trusted Authority of PKI. The similar model is introduced in [30] that multiple OPs only share the secret and C directly communicates with SP.

In our model, we do not consider location sensing method. We define the location sensing procedure as the pre-process of location authentication as following.

Location Sensing The client C and the trusted operator OP share the location information. In case of LLC, the location information *LocInfo* of C can be generated by both C and OP. In case of non-LLC, *LocInfo* of C is generated by OP. In this stage, OP should be able to check the validity of *LocInfo* of C.

Now, we show the sketch of the location privacy and authentication protocol.

$\mathcal{BLAP}$: Basic Location Authentication and Privacy Protocol Assume C and OP share key K_C, and OP and SP share key K_{SP}.

1. C requests a location-based service to the service provider SP.
2. SP requests $LocInfo$ of C.
3. C requests the proof of $LocInfo$ to OP.
4. OP sends $Enc(MAC_{K_{SP}}(ID_C,\ LocInfo),\ MAC_{K_C}\ (LocInfo,\ MAC_{K_{SP}}\ (ID_C, LocInfo)))$ to C.
5. C checks $MAC_{K_C}(LocInfo, MAC_{K_{SP}}(ID_C,\ LocInfo))$ with $MAC_{K_{SP}}\ (ID_C,\ LocInfo)$, ID_C and $LocInfo$. If C assure that $MAC_{K_C}(LocInfo,\ MAC_{K_{SP}}\ (ID_C,\ LocInfo))$ is not forged, C continues operation.
6. C sends $ID_C, Enc(LocInfo,\ MAC_{K_{SP}}(ID_C,\ LocInfo))$ to SP.
7. SP decrypt the received message and check the validity of $MAC_{K_{SP}}\ (ID_C,\ LocInfo)$ with ID_C, $LocInfo$ and K_{SP}.

In the protocol, C can check that $MAC_{K_SP}(ID_C, LocInfo)$ from OP is not forged, since C can verify $MAC_{K_C}(LocInfo, MAC_{K_SP}(ID_C, Loc\text{-}Info)$ with $MAC_{K_SP}(ID_C, LocInfo)$, ID_C, $LocInfo$ and K_C. Also, SP can verify $MAC_{K_SP}(ID_C, LocInfo)$ with K_SP, ID_C, and $LocInfo$ from C. Therefore the requirement of *unforgeability* from attacker holds. Also the fact that C doesn't know K_SP, C cannot forge $LocInfo$. $Enc(a)$ denotes the encryption of a. We assume that between OP and C and between C and SP has the secure association. We will argue the details later. Figure 1 shows operations of $\mathcal{BLAP}$. The number denotes the step in the protocol.

In the figure 1, we see *Location sensing* and *Key update* steps. *Location sensing* is already explained before. We will argue *Key update* step later.

We assume that the secure association between C and OP, also between OP and SP. Shared keys K_{SP} and K_C are pre-distributed. We do not justify the specific key distribution method here. We think the concept of *'resurrecting duckling'* [31] can be acceptable key distribution method for this case. In the concept, mother device gives the key to child device as face-to-face. When the mother device dies (expires), the key is revoked. Until then, child device fully trust the mother device. Client's device can be considered as child device, and operator as mother device.

For the encryption function $Enc(.)$, we can use both the symmetric key encryption and the public key encryption. We only show the generic encryption process in the $BLAP$, since each protocol using one of them is slightly different. If we use the symmetric key encryption for our protocol, each entity has to have the shared key for each communication. The larger number of entities requires

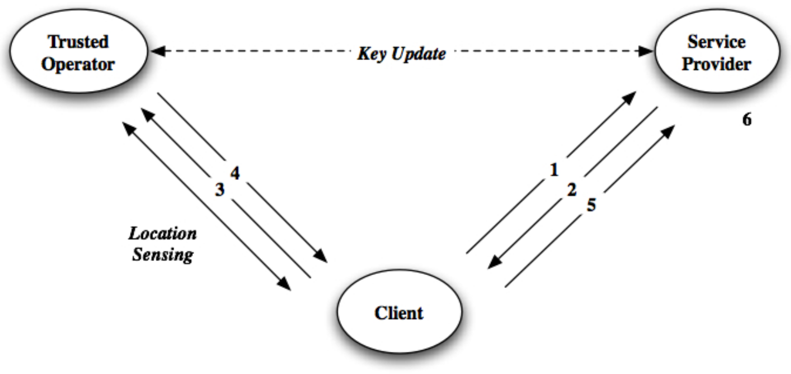

Fig. 1. Proposed Protocol: $\mathcal{BLAP}$

more keys. In contrast, using public key requires only small number of keys, or just public/private key pairs, it requires larger computation costs.

Finally, we show the last step of the protocol, $KeyUpdate$. After the authentication is successfully done, We need to consider the attack that $LocInfo$ is reused by an attacker or C himself. To protect from reuse of the $LocInfo$, two kinds of methods are good solution: Key Replacement and Timestamp.

Key Replacement OP and SP share K_SP for generating $MAC_{K_{SP}}(ID_C$, $LocInfo)$. When C sends $LocInfo$ and $MAC_{K_{SP}}(ID_C, LocInfo)$ to SP, OP and SP replace K_{SP} to new key, $K^{'}_{SP}$. Next time, $K^{'}_{SP}$ is used to generate $MAC_{K^{'}_{SP}}$ $(ID_C, LocInfo^{'})$. $LocInfo^{'}$ is new location information of C. In this case, OP has to check the validity of $LocInfo$, since $LocInfo$ should not be used after the lifetime. An example of replacing share key K_{SP} between OP and SP is using PKI. When SP request OP to change K_{SP}, OP generates the new key $K^{'}_{SP}$ and encrypts the key with SP's public key PK_{SP}. OP sends $E_{SK_{SP}}(K^{'}_{SP})$ to SP, and SP decrypts it with SP's private key SK_{SP}. Or, key exchange protocols like Diffie-Hellman can be used too.

Timestamp When C sends C's location information $LocInfo$ to SP, SP request Timestamp TS about $LocInfo$. SP checks TS for verification of validity of $LocInfo$. In the protocol, TS is included in MAC as $MAC_{K_{SP}}(ID_C, LocInfo, TS)$

If we use the timestamp, we can skip the final step *Key Update*. We define the process *Key Update* as follows.

Key Update If the timestamp TS is found in the received message, SP skip the process. If TS is not found, SP request OP for the replacement of K_{SP}. After the process K_{SP} is replaced to the new key $K^{'}_{SP}$.

We will show the full process of our protocol in the next section.

4 Our Protocol

We proposed the sketch of our protocol, $BLAP$ with generic encryption process. In this section, we shows the full process of our protocol using symmetric key encryption and public key encryption.

We assume a client C has a public/private key pair (PK_C, SK_C), and a shared key K_C with a trusted operator OP. Also, we assume that OP has a public/private key pair (PK_{OP}, SK_{OP}), a shared key K_C with C and a shared key K_{SP} with a service provider SP. SP has a public/private key pair (PK_{SP}, SK_{SP}), and a shared key K_{SP}.

For the location-based service, C needs to have his location information $LocInfo$. C acquire his $LocInfo$ with *Location Sensing*. We already defined the *Location Sensing* process before, but we need some modification.

Location Sensing C and OP share the location information sensing method. In case of *LLC*, $LocInfo$ of C can be generated by both C and OP. Or,$LocInfo$ of C is generated by OP. OP should be able to check the validity of $LocInfo$ of C. When $LocInfo$ is generated, OP also generates TS for that $LocInfo$.

After finishing the process, both C and OP have C location information. For the next step, C request SP who provides the proper location-based service. When C finds SP, C sends the service request to SP. We show two protocols using timestamp or key replacement: TLAP and KLAP.

$\mathcal{TLAP}$: Location Authentication and Privacy Protocol with timestamp

1. C sends the service request to SP.
2. SP requests the location information of C and a timestamp TS.
3. C requests the authentication message with service provider's ID ID_{SP} and a request of TS to OP.
4. OP finds the K_{SP} and PK_{SP} with ID_{SP} in the database. Also, OP finds $LocInfo$ and TS of C with C's ID ID_C.
5. OP generates $M_{SP} = MAC_{K_{SP}}(ID_C, LocInfo, TS)$.
6. OP generates $M_C = MAC_{K_C}(ID_C, LocInfo, TS, M_C)$.
7. OP encrypts M_C, M_{SP}, and TS using C's public key PK_C and sends it to C.
8. C decrypts $E_{PK_C}(M_C, M_{SP}, TS)$ and checks if $M_{SP} = MAC_{K_C}(ID_C,$ Loc $Info, TS, M_C)$. If both are different, C request OP again.
9. C encrypts M_C, TS, $LocInfo$, ID_C with SP's public key PK_{SP} and sends ID_C, $E_{PK_{SP}}(ID_C,$ $M_C, LocInfo, TS)$ to SP.
10. SP decrypts $E_{PK_{SP}}(ID_C, M_C, LocInfo, TS)$ with SP's private key SK_{SP}. If TS is expired, SP rejects C's location.
11. SP checks if $M_C = MAC_{K_{SP}}(ID_C, LocInfo, TS)$. If it is correct, SP authenticates C's location.

$\mathcal{KLAP}$: Location Authentication and Privacy Protocol with key replacement

1. C sends the service request to SP.
2. SP request the location information of C.
3. C requests the authentication message with service provider's ID ID_{SP} to OP.
4. OP finds ID_{SP} and PK_{SP} with ID_{SP} in the database. Also, OP finds $LocInfo$ of C with ID_C.
5. OP generates $M_{SP} = MAC_{K_{SP}}(ID_C, LocInfo)$.
6. OP generates $M_C = MAC_{K_C}(ID_C, LocInfo, M_C)$.
7. OP encrypts M_C and M_{SP} using PK_C and sends it to C.
8. C decrypts $E_{PK_C}(M_C,\ M_{SP})$ and checks if $M_{SP} = MAC_{K_C}$ $(ID_C,$ Loc $Info, M_C)$. If both are different, C request OP again.
9. C encrypts M_C, $LocInfo$, ID_C with PK_{SP} and sends ID_C, $E_{PK_{SP}}$ $(ID_C,$ $M_C, LocInfo)$ to SP.
10. SP decrypts $E_{PK_{SP}}(ID_C, M_C, LocInfo)$ with SK_{SP}. SP checks if $M_C = MAC_{K_{SP}}(ID_C, LocInfo)$. If it is correct, SP authenticates C's location.
11. SP request key replacement to OP.
12. SP and OP runs *Key Update* process.

Key Update SP and OP replace the shared key K_{SP} to new key $K^{'}_{SP}$. They use an pre-decided method like Diffie-Hellman key exchange protocol. Since key exchanging is out of focus, and we omit the detailed process.

The main difference between $TLAP$ and $KLAP$ is the use of a timestamp. Using the timestamp, $TLAP$ can reduce the additional *Key Update* process and the OP's lifetime validation of $LocInfo$. In contrast, $KLAP$ can reduce the message size in the communication. Therefore, two protocols can be selectively used with the load of communication. Also, the communication between OP and C can be run by symmetric key encryption. We can assume that each C already has an association with C, only a single key is additionally required between OP and C. We can measure between the key storage cost or the computational cost.

5 Protocol Analysis

5.1 Security Analysis

Privacy Attacker cannot know C's location $LocInfo$ without the key. The success probability of attacker relies on the strength of encryption schemes.

Overcollection SP has no information of C's location $LocInfo$ until C send location information $LocInfo$ to service provider SP, . In practical application, Location information has several fields;for example, nation, state, city, street, building number, *etc* [6]. When SP require the information of city, C sends only information of city to SP. In that case C doesn't have to inform the last information like street and building number.

Authentication SP can authenticate C's $LocInfo$ by $MAC_{K_{SP}}$ $(ID_C, LocInfo)$. If C sends $LocInfo$ to other user C', SP can check $LocInfo$ from C' is invalid. Since $MAC_{K_{SP}}(ID_C, LocInfo)$ is infeasible by C without key K_{SP}. Computational infeasibility of hash function is well known property. The success probability of C' cheating SP is $1/2^n$ for the message length n.

Unforgeability When the client C sends the encrypted message, attacker has no key. Also, with the property of hash function, Success probability of forgery by attacker is $1/2^n$ for the total message length n. For the client, even though client C generate $C^{'}$s fake location $LocInfo^{'}$, C cannot forge $MAC_{K_{SP}}(LocInfo^{'})$ without key K_{SP}. Success probability of forgery by C is $1/2^{n'}$ for the MAC of location, length n'.

Replay-attack by User Client C keeps $LocInfo$ and $MAC_{K_{SP}}$ $(ID_C, LocInfo)$ for a long time, and try to use later. But, when C keeps $LocInfo$ and $MAC_{K_{SP}}$ $(ID_C, LocInfo)$, OP can revoke K_{SP} after a lifetime. Or SP can check the timestamp TS. ($Timestamp$)

In addition to these security requirements, our protocol has following two properties.

Independency As we discussed in chapter 3, OP and C share $LocInfo$ using GPS, Triangulation, or Beacon. When SP authenticate C, C sends $LocInfo$ as a message. So, we can generalize as transmitting a message with encryption.

Covered Range Unlike previous works, C directly sends SP $LocInfo$. and the distance between C and SP has not important. So, there is no limits of range that SP can authenticate C in our design.

6 Related Work

Several researches focused on the location authentication. Main idea of GPS based Authentication is the generation of 'Location Signature' using *Location Signature Sensor* (LSS) from GPS [8]. They adopted differential GPS (DGPS) technique [20] for sharing the same location information between supplicant and verifier. Since both supplicant and verifier share supplicant's location information, forgery by supplicant or any attacker is impossible. But, for adopting this method, high cost in system design is the most problem. Also, it is difficult to use in indoor environment. Time-bound based authentication [21] focused the speed of sound and light. Physical distance can be measured by elapsed time of signal. When the elapsed time from supplicant to verifier is within the maximum allowed time, supplicant is authenticated. They proposed 'ECHO' protocol for this concept in [26]. It is lightweight protocol and available in both indoor and outdoor authentication. But physical state severally affect on the success of operation. The initial idea of Authentication via Constrained Channel [11] was from devices has their constrained channel like Transport Layer Security (TLS) [25]. Using Bluetooth, Wi-Fi, if the authenticator has direct access to a physically constrained (e.g. range-bounded) channel, it is trivial to implement location authentication. For example, Bluetooth transceiver located at a location, within the range of transceiver, the principal can employ a challenge-response protocol. If the authenticator does not have direct access to a physically constrained communication channel, the authenticator uses a trusted-channel proxy to be connected with the constrained channel.

Location Information Exchange Protocol [10] was designed to protect user's anonymity and verify location information. Four principals are in the model, a detector, a client, a service provider, and a resolver. The detector is a detection entity, connected to an RFID-reader. The resolver is the entity that manages a mapping table between clients' RFID and IP address. Clients send their address to the resolver every time the address has changed. (Address notification). When detectors detect an RFID inside their sensing area, they request the resolver to resolve the client's address that corresponds to the RFID (Address resolution), and send a notification to the address that a ticket is available. Then the client can obtain the ticket, which is presence evidence at the detector's sensing area. (Ticket publication) When clients are requested a ticket by a service provider, they decide whether they consume the ticket based on user's intention or a formulated policy. After service providers obtain a ticket, they request the detector, which published the ticket, to verify it. (Ticket verification)

In summary, the model of Time-bound based authentication method [21, 22] and Authentication method via constrained channel [11] is that only a supplicant has his location information initially, and a verifier verifies supplicant using specific method like time. For that, they have to be synchronized physically, and when the communication is disconnected, it fails. Since they rely on the time variance, their methods are only being able to be used in short distance where the a little distance changing makes big difference. And, in practice, they require large number of host (verifiers) to cover wide range for general use. While the model of LEXP [10] and GPS based authentication [8] is that supplicant and verifier share supplicant's location information. LEXP adopted RFID that is actively studied currently. Actually the service provider who wants to verify user's location doesn't have the exact location information of user, but the range of RFID is too small, it can be considered that service provider knows user's location. GPS based method used differential GPS which there two kinds of GPS receiver, one is static receiver and the other is roving receiver. When satellite transmit signal of supplicant's position, both supplicant and verifier receive the same information. From this, verifier can check if supplicant is valid. But those methods are device specific methods that LEXP relies on RFID and GPS based method relies on Location Signature Sensor (LSS) which is built for that specific purpose. In contrast, A. S. Ga jparia and C. Yeun [28, 29] showed the privacy protecting method for location based service. They assess the possible use of constraints to control the dissemination and use of location information within location based service architecture. And they considered various types of constraint that may be required.

Comparison We compared our design to other protocols. O denotes that the protocol holds the requirement in the row, X doesn't. Table 1 shows the comparison with protocols. Compared protocols partially guarantee the privacy in the location based service. They guarantee the privacy from the attacker but not from the service provider. Main difference between compared studies and ours is that we separated the *SP* and *OP* in the model. With our model, *SP* doesn't need the cost for location sensing. It is important in real environment that *SP* can save more resources. Time-bounded location authentication method [9] requires connectionless synchronization, and fails with disturbance of communication. Sound is disturbed by temperature, air pressure, and so on. Location signature sensor method [8] requires specific devices for authentication. Compare to our protocol, for sensing location information, generating location signature make additional overhead and devices. LEXP [10] doesn't need synchronization with verifier, but their availability is limited to RFID. Constrained channel method is just general model.

	Time-based [9]	LEXP [10]	GPS-based [8]	Constrained Channels [11]	Our Protocols
Authentication	O	O	O	O	O
Unforgeability	O	O	O	O	O
Privacy	X	O	O	O	O
Overcollection	X	X	X	X	O
Replay-attack	O	O	O	O	O
Universality	X	X	O	X	O
Covered range	Near	A few meters	Devices Specific	3,000km	No limit

Table 1. Comparison of protocols

7 Conclusion

In this paper, we showed important security requirements of the location-based service and showed the privacy and authentication schemes of location based service, which is adopting the IETF Geopriv Working Group's privacy model. And then, we proposed the privacy and authentication protocols who can be used in different cases. We showed our basic framework and introduced several protocols based on that framework. We also compared our schemes with several studies focus on location authentication and privacy, which have lack of consideration of privacy from collecting location information.

At first, we argued that a prover (client)'s privacy about location against a verifier (service provider) is also important. Previous studies on authentication of location depended on the specific location sensing technology and they did not guarantee privacy of prover's location. To achieve both the authentication of location and the privacy of a prover, we introduced a trusted entity, *Trusted Operator* which has the similar role as the *Trusted Authority* in general PKI. In our design, we divided the location sensing process from location based service providers, which enables the location information to be formed as generic message format during location based service. Since the location information signed by the trusted operator makes the information more stable.

Finally, we proved that our design meets all security requirements we defined. The significant difference from previous studies is that we do not require location sensing capability of the service provider. Between the client and the service provider, the location information is transferred as typical message. Therefore, our design does not rely on any specific devices like *LSS* [8], signaling [9] and RFID [10]. We believe that authentication of context information is critical issue in ubiquitous computing environments and our model is the most applicable solution for this issue.

References

1. J. Al-Muhtadi, A. Ranganathan, R. Campbell, M. D. Mickunas, "A Flexible, Privacy-Preserving Authentication Framework for Ubiquitous Computing Environments", Proc. of the 22nd ICDCSW'02, 2002
2. J. Al-Muhtadi, R. Campbell, A. Kapadia, M.D. Mickunas, and S. Yi, "Routing through the Mist: Privacy Preserving Communication in Ubiquitous Computing Environments,", Proc. of ICDCS'02
3. J. Al-Muhtadi, R. Campbell, A. Kapadia, M. D. Mickunas, and S. Yi, "Routing through The Mist: Design and Implementation, ", UIUC Technical Report UIUCDCS-R-2002-2267
4. P. G. McLean, "A secure pervasive environment", Australasian Information Security Workshop 2003
5. A. Novobilski, "Pervasive/Invasive Computing; Two sides of the location-enabled coin", March 11, 2002
6. "Dynamic Host Configuration Protocol (DHCPv4 and DHCPv6) Option for Civic Addresses Configuration Information", rfc 4776
7. "Geopriv Requirements", rfc 3693
8. D. E. Denning and P. F. Macdoran, "Location-Based Authentication: Grounding Cyberspace for Better Security", Computer Fraud & Security, Feb, 1996
9. N. Sastry, U. Shankar, and D. Wagner, "Secure Verification of Location Claims", WiSE'03, Sep 19, 2003, San Diego, California, USA, ACM 1-58113-769-9/03/0009
10. K. Nakanishi, and J. Nakazawa, "LEXP: Preserving User Privacy and Certifying the Location Information", H. Tokuda, Security workshop of Ubicomp 2003
11. T. Kindberg and K. Zhang, "Context Authentication Using Constrained Channels", HPL-2001-84, Hewlett-Packard, Apr 2, 2001

12. N. B. Priyantha, A. Chakraborty, and H. Balakrishnan, "The Cricket Location-Support system", Proc. of 6th ACM MOBICOM, Boston, MA, Aug 2000
13. J. Hightower, and *et al.*, "Design and Calibration of the SpotON Ad-Hoc Location Sensing System," UW CSE 01-08-?? University of Washington, Seattle, WA, August 2001
14. http://www.ietf.org/html.charters/geopriv-charter.html
15. A. Beresford, "Location Privacy in Ubiquitous Computing", Technical Report No 612, UCAM-CL-TR-612, ISSN 1476-2986, University of Cambridge, Jan. 2005
16. "Location-based Services (LBS)", MobileIN.com
17. A. Corradi, et al., "Context-based Access Control for Ubiquitous Service Provisioning", COMPSAC04
18. Y. Kim, et al., "Context-Aware Access Control Mechanism for Ubiquitous Applications", AWIC 2005, LNAI 3528, pp. 236?242, 2005.
19. S. Yokoyama, et al., "An Anonymous Context Aware Access Control Architecture For Ubiquitous Services", MDM'06, p. 74
20. "Differential GPS", GPS Tutor, http://www.mercat.com/QUEST/DGPS. htm
21. "Time-of-arrival location technique", LOS ALAMOS SCIENCE, Summer 1982
22. L. Stilp and B. Cynwyd, "TDOA technology for locating narrowband cellular signals: Cellphone location involves several practical and technical considerations. Time difference of arrival (TDOA) technology provides accuracy for locating analog cellphones in urban environments.", Mobile Radio Technology,Apr 1, 1997
23. H. Balakrishnan, and *et al.*, "Lessons from Developing and DEploying the Cricket Indoor Location System", Nov 2003, Preprint
24. N. Priyantha, A. Miu, H. Balakrishnan, and S. Teller, "The Cricket Compass for Context-Aware Mobile Applications", Proc. of 7th ACM MOBICOM, Rome, Italy, Jul 2001
25. T. Dierks and C. Allen, "Transport Layer Security", RFC2246, www.ietf.org, 1999
26. B. Frasco, "Enhanced Observed Time Difference (E-OTD)", Aerial Communications
27. J. LaMance, J. DeSalas, and J. Jarvinen, "Assisted GPS: A Low-Infrastructure Approach",GPS World, March 1, 2002
28. A. Gajparia, C.Y. Yeun, and C. Mitchell. "Using constraints to protect personal location information. In Proceedings of the 58th IEEE Semi-annual VTC 2003-Fall, Orlando, Florida, USA, 6-9 October 2003.
29. A. Gajparia, C.J. Mitchell and, C.Y. Yeun, "The location information preference authority: supporting user privacy in location based services, to appear at the Eighth IFIP TC-6 TC-11 Conference on Communications and Multimedia Security, Cumbria, UK, 15-18 September 2004.
30. C. Delakouridis, and *et al.*, "Share the Secret: Enabling Location Privacy in Ubiquitous Environment", LoCA 2005, LNCS 3479, pp. 289-305, 2005
31. F. Stajano and R. Anderson, "The resurrecting duckling: Security issues for ad-hoc wireless networks", Security Protocols, 7th International Workshop Proceedings, LNCS, 1999
32. E. Gilbert, and *et al.*, "Codes which detect deception", Bell Systems Technical Journal, 53 (1974), 405-424