LETTER Special Section on Emerging Technologies of Ubiquitous Computing Systems

Enhancing Credibility of Location Based Service Using Multiple Sensing Technologies

Kyusuk HAN†a), *Nonmember*, Kwangjo KIM†b), *and* Taeshik SHON††c), *Members*

SUMMARY Recent Location Based Services (LBS) extend not only information services such as car navigation services, but supporting various applications such as augmented reality and emergency services in ubiquitous computing environments. However location based services in the ubiquitous computing environment bring several security issues such as location privacy and forgery. While the privacy of the location based service is considered as the important security issue, security against location forgery is less considered. In this paper, we propose improved Han et al.'s protocol [1] that provides more lightweight computation. Our proposed model also improves the credibility of LBS by deploying multiple location sensing technologies.

key words: *ubiquitous computing, context-awareness, Location Based Service, privacy, authentication, credibility*

1. Introduction

Location based service (LBS) is a service using a user's location information that is sensed by location sensing technologies, and widely deployed in the ubiquitous computing environment. Wider deployment of LBS invoke the concern of security problems such as privacy and location forgery.

While many studies such as [2]–[5] focused on the privacy problem in LBS, less interests are given to preventing location forgery. Han et al. [1] proposed authentication protocols that provides both credibility and privacy to LBS, and only few studies such as [6] are done since then.

However, the concerning of credibility of the location information is becoming more important in wider applications of LBS, it is important to provide the credible solution for preventing location forgery.

Therefore, our motivation is to provide more reliable solution that provides privacy and credibility of location based service. Although Han et al. [1] showed basic location authentication protocol, that was difficult to be implemented for ubiquitous environments due to deployed PKI that needs quite heavy computation. In this paper, we improve Han et al.'s protocol [1] by substituting the public key based computation to symmetric key based computation. Our improved protocol deploys two different types of location sensing technologies.

The paper is organized as follows: We categorize LBS model using two different sensing technologies and location sensing architecture in Sect. 2. We propose our improved protocols in Sect. 3, and analyze our protocols in Sect. 4. We conclude our paper in Sect. 5.

2. Location Sensing Technologies

2.1 Location Sensing Methods

We focus ourselves on the capability of localized location computation (*LLC*). By the characteristic of *LLC*, various location-sensing technologies can be divided into two categories; *LLC* and non-*LLC* that depending on recognition without the capability of *LLC*. Using *LLC*, the object being located actually computes its own position. GPS and Cricket [7] 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 such as SpotON [8] have recognition capability. Location service via mobile network is also considered as non-*LLC*. Figure 1 shows the location sensing using *LLC* and non-*LLC*.

In the case of *LLC*, users privacy is easily guaranteed since user computes own location for himself. However, a risk exist that a malicious user can forge the information. On the contrast, non-*LLC* has potential threat that the privacy may not be guaranteed since the infrastructure knows the

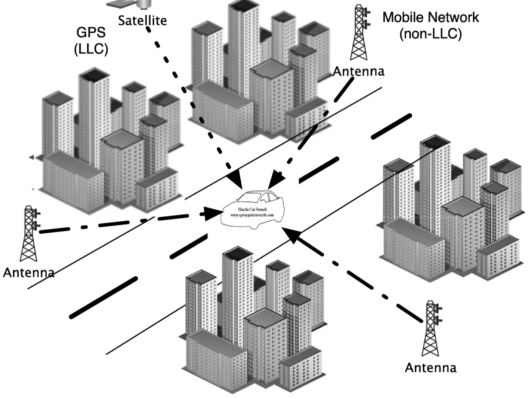

Fig. 1 Example scenario: Car navigation service using GPS (*LLC*) and mobile network (non-*LLC*).

Manuscript received November 11, 2010.
Manuscript revised March 4, 2011.

†The authors are with Korea Advanced Institute of Science and Technology, Daejeon, Korea.
††The author is with Division of Information and Computer Engineering, College of Information Technology, Ajou University, Suwon 443–749, Korea (corresponding author).
a) E-mail: hankyusuk@kaist.ac.kr
b) E-mail: kkj@kaist.ac.kr
c) E-mail: tsshon@ajou.ac.kr

DOI: 10.1587/transinf.E94.D.1181

location with recognition.

2.2 Location Service Architecture

A location service architecture for protecting location privacy is defined by The Geopriv Working Group [9], [10]. The architecture consists of four main components; a location generator, a location server, a rule holder and a location recipient. 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.

2.3 Security Requirements

We use security requirements for the location information defined in [1] as follows:

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

Prevention from over-collection 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 over-collection 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.

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 [11].

3. Improved Location Authentication and Privacy Protocol

In this section, we show our improved scheme for authentication and privacy of location information. We adopt the service architecture defined in [1]. Our model comprises three entities, a user U, a service provider SP, and a trusted operator OP. U wants to prove his current location to SP, while SP needs to verify U's location information $\mathcal{L}_U$. OP has an important role similar to a *trusted authority* of PKI. The similar model is introduced in [12] that multiple OPs only share the secret and U directly communicates with SP. Our protocol deploys two different types of location sensing technologies, while we do not define specific location sensing methods. We show the improved location authentication and privacy protocol in following section.

3.1 Protocol Description

We assume that U knows ID_{OP} and ID_{SP}. The protocol mainly has four parts as below.

P.1 U request authentication of his location $\mathcal{L}_U$ to OP in order to get a service from SP.

P.2 OP generates credit of $\mathcal{L}_U$ for U.

P.3 U request service to SP by proving $\mathcal{L}_U$.

P.4 SP verifies U's location, $\mathcal{L}_U$.

Table 1 shows notations used in the paper. Detailed protocols are as followings.

P.1 **a)** U self-generates $\mathcal{L}_U$ using LLC based device such as GPS, and SEN_U^0, where $SEN_U^0 = e_{K_U}(REQ \| ID_{SP} \| \mathcal{L}_U)$. U also generates M_U^0, where $M_U^0 = MAC_{K_U}\ (ID_U \| ID_{OP} \| SEN_U^0)$.
b) After that U sends SEN_U^0 and M_U^0 to OP.

$$U \to OP : SEN_U^0 \| M_U^0$$

P.2 **a)** After verifying M_U^0 and decrypting SEN_U^0, OP finds a key K_{SP} shared with SP, and also verifies $\mathcal{L}_U$ using non-LLC. The number '1' in RTN or SEN denotes that the parameter is decrypted or verified by U. The number '2' is for SP, and '0' is for OP.
b) OP randomly selects R_{OP} and generates CRT_{SP} and CRT_U, where $CRT_{SP} = MAC_{K_{SP}}(ID_U \| \mathcal{L}_U \| R_{OP})$, and $CRT_U = MAC_{K_U}\ (ID_U \| \mathcal{L}_U\ \| CRT_{SP})$ respectively.
c) OP then generates RTN_U^1, RTN_{SP}^2, M_{OP}^2 and M_{OP}^1 sends them to U, where
$RTN_U^1 = e_{K_U}(CRT_{SP} \| CRT_U \| R_{OP} \| H_U \| TS_{OP})$,

Table 1 Notations.

Notation	Description
A‖B	sequence of A and B
A→B : M	A sends M to B
K_U	Symmetric key shared between U and OP
K_{SP}	Symmetric key shared between OP and SP
$e_K(M)$	Encrypt M using a key K
$MAC_K(M)$	Message authentication code of M using K
$\mathcal{L}_U$	A user U's location information
REQ	authentication request message
ID_U	Identity of a user U
ID_{OP}	Identity of an operator OP
ID_{SP}	Identity of a service provider SP
TS_{OP}	Timestamp generated by OP
R_{OP}	Random nonce generated by OP
CRT	Credit of user's location
SEN	Encrypted message for sending
RTN	Encrypted message fore receiving

$RTN^2_{SP} = e_{K_{SP}}(R_{OP}||H_{SP}||TS_{OP})$,
$M^2_{OP} = MAC_{K_{SP}}(ID_U||RTN^2_{SP})$, and
$M^1_{OP} = MAC_{K_U}(RTN^1_U||SEN^1_U\ ||RTN^2_{SP}||M^2_{SP})$.

$$OP \rightarrow U : RTN^1_U||RTN^2_{SP}||M^2_{OP}||M^1_{OP}$$

$H_U = h(K_{SP}||R_{OP}||TS_{OP})$, and $H_{SP} = h(K_U||R_{OP}||TS_{OP})$, where $h(m)$ denotes hash of m.

P.3 **a)** After verifying M^1_{OP} and decrypting RTN^1_U, U finds CRT_{SP}, CRT_U, R_{OP}, H_U and TS_{OP}.
b) U then verifies CRT_U, and then generates TK_U, where $TK_U = h(H_U||H_{SP})$.
c) After that, U generates SEN^2_U and M^2_U, and sends them to SP, where $SEN^2_U = e_{TK_U}(CRT_{SP}||\mathcal{L}_U)$ and $M^2_U = MAC_{TK_U}(ID_U||ID_{SP}||SEN^2_U)$.

$$U \rightarrow SP : RTN^2_{SP}||SEN^2_U||M^2_U||M^2_{OP}$$

Remaining part (P.4) is operated by SP.

P.4 **a)** After verifying M^2_{OP}, SP decrypts RTN^2_U and retrieves R_{OP} and TS_{OP}.
b) SP also generates TK_U, decrypts SEN^2_U, and then retrieves CRT_{SP} and $\mathcal{L}_U$.
c) After verifying CRT_{SP}, SP authenticates $\mathcal{L}_U$.

4. Design Analysis

We analyze that our protocol holds security requirements as follows:

Privacy Adversary $\mathcal{A}$ cannot know U's location $\mathcal{L}_U$ without K_U or K_{SP}. Also, U cannot know K_{SP} from TK_U and vise versa. The success probability of $\mathcal{A}$ relies on the strength of encryption schemes.

Prevention of Over-Collecting SP only receive $\mathcal{L}_U$ from U, and verification information from OP. OP identifies location of U, and generates CRT_{SP} for SP that needs location. Since each SP may need proper level of location information and the accuracy of each location sensing technologies is different, we can use civic addresses for location information.

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 civil addresses are defined as national subdivision, county, city, city division, neighborhood, group of streets below the neighborhood level in [5].

Figure 2 shows the example of services. In case of delivery services, very accurate information is required. By contrast, only country information is sufficient to verify users for online stores that sell digital contents. Thus, when U has very accurate information from GPS, U convert it to civic address and sends only proper level of information to SP. OP also generates CRT_{SP} with such level.

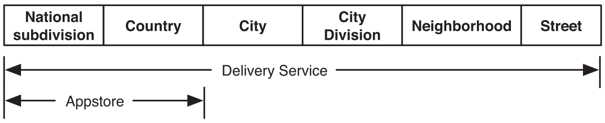

Fig. 2 Example of location information: Delivery service requires accurate information including street information, while Appstore only requests national subdivision and country information.

Authentication SP verifies U's $\mathcal{L}_U$ from CRT_{SP}. Although a malicious U sends $\mathcal{L}_U$ to other user $U^{\mathcal{A}}$, SP can check $\mathcal{L}_U$ from $U^{\mathcal{A}}$ is invalid. Since CRT_{SP} is infeasible by $U^{\mathcal{A}}$ without K_{SP}. Computational infeasibility of hash function is well known property.

Unforgeability Adversary $\mathcal{A}$ fails to forge $\mathcal{L}_U$ without key. The success probability of $U^{\mathcal{A}}$ cheating SP is $1/2n$ for the message length n.

Replay-attack by User The protocol prevents U's malicious trial of reusing $\mathcal{L}_U$ by timestamp TS_{OP}. SP verifies $\mathcal{L}_U$ by CRT_{SP}. Since R_{OP} is updated in each session, malicious trail by U fails.

5. Conclusion

The credibility of location information is one of critical issues in ubiquitous computing environments. We believe that the proposed model is an applicable solution for the issue. In this paper, we presented improved location authentication and privacy protocol proposed in [1]. The distinguished points are the location information is generated by multiple sensors: LLC and non-LLC, and the protocol is fully based on symmetric key based cryptosystem for supporting massive interaction. In future work, we will concentrate on the research to improve the accuracy of a location sensing service by combining multiple sensors.

References

[1] K. Han and K. Kim, "Enhancing privacy and authentication for location based service using trusted authority," 2nd Joint Workshop on Information Security, 2007.

[2] S. Gajparia, C.J. Mitchell, and C.Y. Yeun, "The location information preference authority: Supporting user privacy in location based services," 8th IFIP TC-6 TC-11 Conference on Communications and Multimedia Security, pp.15–18, Cumbria, UK, 2004.

[3] J. Al-muhtadi, A. Ranganathan, R. Campbell, and M.D. Mickunas, "A flexible, privacy-preserving authentication framework for ubiquitous computing environments," Proc. IWSAEC 2002, pp.771–776, 2002.

[4] A. Novobilski, "Pervasive/invasive computing; Two sides of the location-enabled coin," PDPTA '02: Proc. International Conference on Parallel and Distributed Processing Techniques and Applications, pp.1063–1067, CSREA Press, 2002.

[5] Dynamic host configuration protocol (DHCPv4 and DHCPv6) option for civic addresses configuration information, RFC 4776.

[6] W. Luo and U. Hengartner, "Proving your location without giving up your privacy," HotMobile 2010, Annapolis, Maryland, USA, 2010.

[7] N.B. Priyantha, A. Chakraborty, and H. Balakrishnan, "The Cricket

location-support system," Proc. 6th Annual International Conference on Mobile Computing and Networking, MobiCom '00, pp.32–43, ACM, New York, NY, USA, 2000.

[8] J. Hightower, C. Vakili, G. Borriello, and R. Want, "Design and calibration of the spoton ad-hoc location sensing system," Technical Paper, University of Washington, Seattle, WA, Aug. 2001.

[9] A.R. Beresford, "Location privacy in ubiquitous computing," Technical Report no 612, UCAM-CL-TR-612, ISSN 1476-2986, University of Cambridge, 2005.

[10] J.R. Cuellar, J.B. Morris, D.K. Mulligan, J. Peterson, and J. Polk, "Geopriv requirements," RFC3693, 2004.

[11] A. Corradi, R. Montanari, and D. Tibaldi, "Context-based access control for ubiquitous service provisioning," Proc. 28th Annual International Computer Software and Applications Conference (COMPSAC '04), 2004.

[12] C. Delakouridis, L. Kazatzopoulos, G.F. Marias, and P. Georgiadis, "Share the secret: Enabling location privacy in ubiquitous environments," Location and Context-Awareness, Lec. Notes Comput. Sci., vol.3479, pp.289–305, 2005.