A Secure and Private LBS Protocol on Mobile Communication Network

Yu-Yi Chen[1,*] Shin-Yi Hsiao[2]

[1] Department of Management Information System
National Chung Hsing University
Taichung 403, Taiwan, ROC
chenyuyi@nchu.edu.tw

[2] Institute of Computer Science and Engineering
National Chung Hsing University
Taichung 403, Taiwan, ROC
crazydogg1234@yahoo.com.tw

Received 8 October 2007; Revised 15 December2007; Accepted 12 January 2008

Abstract. We have proposed a mobile mechanism [1] that offers location-based service in unfamiliar environment. Through the Mobile Network Service Provider (MNSP), subscribers can look for service providers nearby their positions. In our previous proposal, all service providers are assumed to be local dealers. However, after our further consideration, we believe that service providers may be mobile dealers. Such kind of design, Zhu has proposed a protocol [2] in 2003. However, his approach cannot be applied to current mobile communication system. In this paper, we will propose how to integrate mobile dealers into the location-based service of mobile communication system.

Keywords: Location-Based Service, Mobile Service, Security, Privacy.

1 Introduction

With the development of the internet and electronic technologies, all kinds of mobile devices, such as cell phones and PDAs are beginning to have basic computation and wireless communication capabilities. We will be able to use these mobile devices to make some electronic transactions [3-6] anywhere and anytime. Location-based service [7-11] is expected to be a suitable application for mobile transaction. It can provide a list of services nearby the mobile device's position. For example, we can use this service to make choices about hotel and restaurant reservations as we are upon arrival to an unfamiliar place.

In 2004, Konidala proposed a "secure and privacy enhanced protocol for location-based services in ubiquitous society" [12]. However, Konidala's scheme has the following disadvantages:

- There only exist a symmetric session key between the MNSP and the subscriber. In the transaction, all messages are encrypted by the session key for security. However, the non-repudiation can not be guaranteed since there is not any signature in the transaction.
- The MNSP handles all of the transaction's details, the privacy of subscribers may be invaded.

In 2007, we have proposed a new design [1] to conquer the above problems. We introduced an "observer" character to assist subscribers to complete the transaction with non-repudiation signature and privacy protection. In our previous proposal, all service providers are assumed to be local dealers. However, after our further consideration, we believe that service providers may be mobile dealers. Such kind of design, Zhu has proposed a protocol [2] in 2003. Service providers may not be stationary, they can also be mobile users. For instance, an ill person suddenly has an accident in an unfamiliar place, he may use mobile device to search for local doctor or related medical services. Those coffee stands on wheels are another instance, mobile device may be used for people to conveniently search for their service at scenic spots.

In Zhu's scheme (Fig.1), there are four types of component: client user, service provider, directory server, and proxy server. It assumes that a passive sensing system is set up around the area of a building, which lets mobile clients and services read location information. The sensing system consists of two types of component: reader and tag. The mobile devices of clients and services are embedded with reader function. There are many tags in the building which emit information either periodically or after readers' requests. The service providers use the tags' information to determine that they have moved to new locations and notify the proxy server. The clients

[*] Correspondence author

use the location information to search for the relevant services from the directory server. The non-repudiation and privacy are regarded as the most important issues. Under these considerations, the setup of location-base service claims the needs of powerful mobile device and public key infrastructure. The privacy of transaction will be guaranteed with the assistant of proxy server. There also need to set up a directory server for the registration of mobile service providers. Moreover, its location sensing system is using tags to label locations around the service area such that mobile device can read location information. Then mobile users can make transaction with those mobile service providers in such environment.

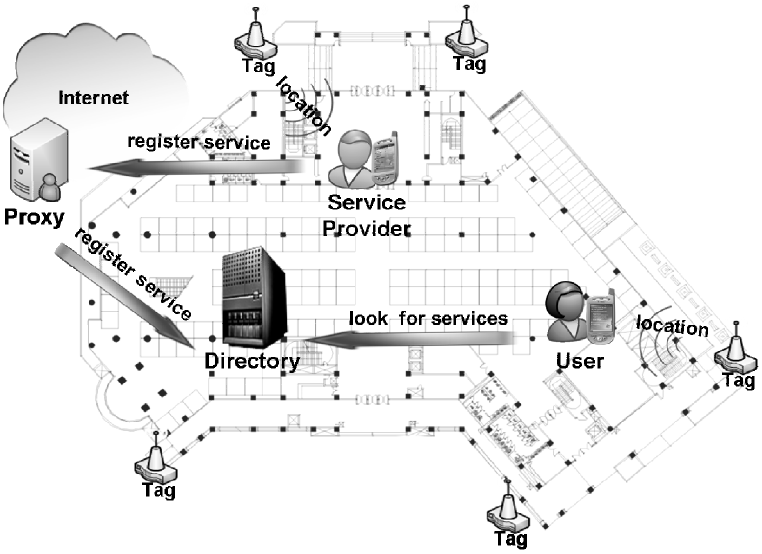

Fig. 1. Zhu's scheme

However, Zhu's scheme has the following disadvantages:

- The service area must have a directory server for the registration of mobile service providers. It should set up a passive sensing system, using tags to label locations around the service area. Then mobile devices can read location information. The cost will be very high if the scheme is considered to applied everywhere.
- The directory server is responsible for verifying the identities of both parties under the Public Key Infrastructure. It needs to assume that all mobile devices have powerful computing ability. However, most cell phones are not so powerful, the scheme is not practical to be integrated into current mobile communication systems.
- By the assistant of the proxy server, service providers can keep anonymous in the transaction. However, the users cannot keep anonymous since their certificates should be verified by the directory server. That will be unacceptable for people if their privacy cannot be guaranteed.

In this paper, we will propose how to integrate mobile dealers into location-based service of mobile communication system. In consideration of practicability, such kind of scheme should satisfy the following properties.

- Anonymity:
  During the transaction, people should keep anonymous.
- Privacy:
  The MNSP must not know the transaction's details even the order is transferred via the MNSP.
- Non-repudiation:
  Each transaction should not suffer from any false denial.
- Simplicity and Practicability:
  The design must be easily implemented in current cell phones and mobile communication system.

2 Our scheme

In this section, we will introduce how our protocol works. Our design is based on the Mobile Location Based Service (MLBS) is available in the mobile network service. The location of a cell phone can be detected by the cellular base stations. The cell phone can get its location information by the mobile network service provider.

There already exist this kind of mobile location technology such as Cell-ID, AOA, TOA, E-OTD, and A-GPS [13]. There are five parties be involved in our scheme as follows.

- User: People use cell phones or PDAs to request location-based service of mobile communication system.
- Service Provider (SP): Mobile dealers can announce their services on the location-based service system.
- Mobile Network Service Provider (MNSP): It provides secure and stable mobile communication system for people.
- User's observer (U-observer): A trusted web site that acts as user's agent.
- SP's observer (SP-observer): A trusted web site that acts as SP's agent.

We divide the location-based service protocol into three phases: Service Registration Phase (Fig.2), Service Query Phase (Fig.3), and Service Request Phase (Fig.4). In our scheme, we involve a key role of "observer" to coordinate the transaction. It also integrates some cryptology such as public key infrastructure, hash chain, and digital signature. The notations used in our scheme are listed in the Table 1:

Table 1. Notation table

Notations	Description
$\|\|$	concatenate operation
+	additive operation
-	subtractive operation
$\oplus$	exclusive-OR operation
$H()$	a one way hash function
H_M	the hash value of message M
SG_M	the signature of message M
PK_X	the X's public key
SK_X	the X's secret key
$S_X()$	the signature function using X's secret key to sign
$V_X()$	the verify function using X's public key to verify
ID_X	the X's identity
$Nick_{SP}$	the nickname of service provider
$SrvDscp_{SP}$	the service description of the service provider, it contains transaction time, location, and price,…,etc.
Loc_X	the X's current location
SN	the serial number assigned by the MNSP in a transaction
TS	timestamp
TK	the transaction token which contains (SN, TS, SG_{SN})
$R\,eq_U$	the user's request

Initially, the SP must pre-coordinate a set of hashing chain (b_0, b_1 , ..., b_m) with the chosen SP-observer, where b_0 is a random seed, $b_1 = H(b_0)$, $b_2 = H(b_1)$, ..., $b_i = H(b_{i-1})$.Similarity, the user also pre-coordinate a set of hashing chain (a_0, a_1 , ..., a_n) with the chosen U-observer, where a_0 is a random seed, $a_1 = H(a_0)$, $a_2 = H(a_1)$, ..., $a_j = H(a_{j-1})$. The pre-coordination process can be run via the Internet and then the hashing chain values are downloaded into the user's mobile device. Out of the MNSP's control, the hashing chain values will not be revealed to the MNSP. Moreover, the pre-coordination process must be protected by Secure Socket Layer (SSL) or any secure session communication. Afterward, the user and the chosen observer can use these hashing values to authenticate messages to each other during the transaction.

Phase 1. Service Registration Phase

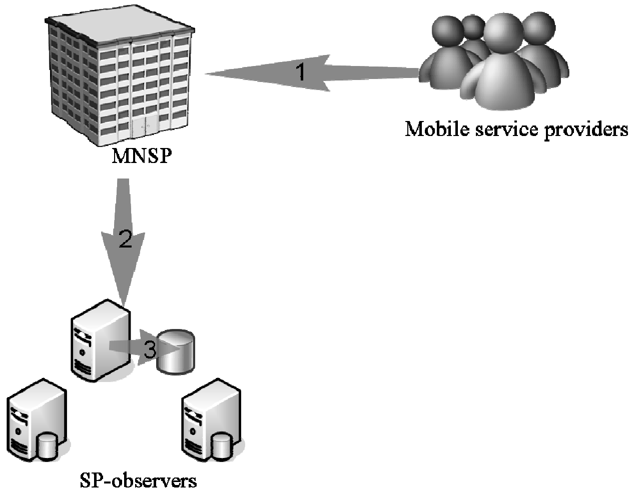

Fig. 2. Service Registration Phase

Step 1. Suppose a subscriber wants to register as a mobile SP, his nickname $Nick_{SP}$ and service description $SrvDscp_{SP}$ should be proposed to the chosen SP-observer as the following format:

$$R_1 = (Nick_{SP} \,||\, SrvDscp_{SP}) \oplus b_i + b_{i-1}$$
$$R_2 = (Nick_{SP} \,||\, SrvDscp_{SP}) \oplus b_{i-1} + b_{i-2}$$

The subscriber generates his register message M_1 containing the above values R_1 and R_2, the chosen SP-observer's identity ID_{SP-obs} and public key PK_{SP-obs} :

$$M_1 = (R_1, R_2, ID_{SP-obs}, PK_{SP-obs})$$

Then the above register message M_1 and its hashing value H_{M_1} are sent to the MNSP.

Step 2. Upon receiving the above message, the integrity of the message M_1 can be verified as follows:

$$H(M_1) \overset{?}{=} H_{M_1}$$

The subscriber's position Loc_{SP} can be located by the MNSP, and be combined into the following message M_2:

$$M_2 = (Loc_{SP}, R_1, R_2)$$

Then the MNSP uses its secret key to sign M_2 as follows:

$$SG_{M_2} = S_{SK_{MNSP}}(H(M_2))$$

The above message M_2 and its signature SG_{M_2} are encrypted by the chosen SP-observer's public key PK_{SP-obs} as follows:

$$C_2 = E_{PK_{SP-obs}}(M_2, SG_{M_2})$$

After, the ciphertext C_2 , the subscriber's identity ID_{SP}, and the MNSP's public key PK_{MNSP} are sent to the chosen SP-observer.

Step 3. Upon receiving the above message, the ciphertext C_2 can be decrypted by the SP-observer's secret key. Then the integrity of message M_2 can be verified as follows:

$$H(M_2) \overset{?}{=} V_{PK_{MNSP}}(SG_{M_2})$$

The SP-observer uses the pre-coordinated hashing values of b_i, b_{i-1}, and b_{i-2} to decrypt the values R_1 and R_2. Then the subscriber's nickname $Nick_{SP}$ and service description $SrvDscp_{SP}$ can be obtained and verified as follows:

$$(R_1 - b_{i-1}) \oplus b_i \overset{?}{=} (R_2 - b_{i-2}) \oplus b_{i-1}$$

Finally, the subscriber's identity ID_{SP}, the current location Loc_{SP}, the nickname $Nick_{SP}$, and the service description $SrvDscp_{SP}$ are recorded for the possible query.

Phase 2. Service Query Phase

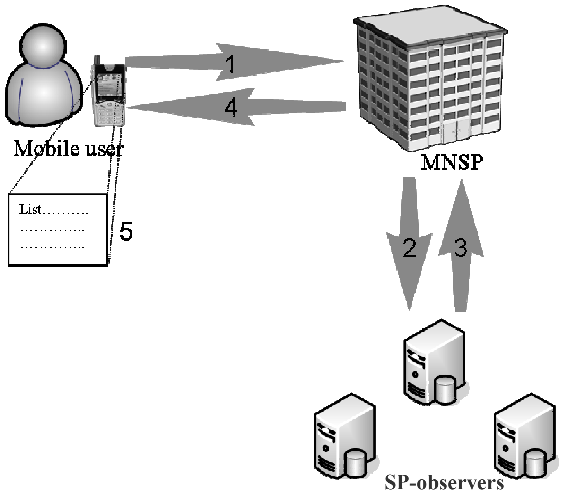

Fig. 3. Service Query Phase

Step 1. Suppose a mobile user makes a query Qry_U for looking some kinds of location-base service. He generates his query message M_3 as follows

$$M_3 = Qry_U$$

Then the above query message M_3 and its hashing value H_{M_3} are sent to the MNSP.

Step 2. Upon receiving the above message, the integrity of the message M_3 can be verified as follows:

$$H(M_3) \overset{?}{=} H_{M_3}$$

The user's position Loc_U can be located by the MNSP, and be combined into the following message M_4:

$$M_4 = (Qry_U, Loc_U)$$

Then the MNSP uses its secret key to sign M_4 as follows:

$$SG_{M_4} = S_{SK_{MNSP}}(H(M_4))$$

The message M_4 and its signature SG_{M_4} are broadcasted to all SP-observers.

Step 3. For each SP-observer, upon receiving the above message, the integrity of message M_4 can be verified as follows:

$$H(M_4) \overset{?}{=} V_{PK_{MNSP}}(SG_{M_4})$$

According to the user's query Qry_U and location Loc_U, all of the suitable SPs' recorders will be retrieved and collected as a list $\{Nick_{SP}, SrvDscp_{SP}\}$. Then this list is combined with the SP-observer's identity ID_{SP-obs} and public key PK_{SP-obs} into the following message M_5:

$$M_5 = (\{Nick_{SP}, SrvDscp_{SP}\}, ID_{SP-obs}, PK_{SP-obs})$$

Each SP-observer uses its secret key to sign M_5 as follows:

$$SG_{M_5} = S_{SK_{SP-obs}}(H(M_5))$$

After, the message M_5 and its signature SG_{M_5} are sent to the MNSP.

Step 4. Upon receiving the above messages from each SP-observer, the MNSP can verify the integrity as follows:

$$H(M_5) \overset{?}{=} V_{PK_{SP-obs}}(SG_{M_5})$$

Then all lists will be collected as the following response message M_6 with an assigned transaction token TK:

$$M_6 = (TK, \{\{Nick_{SP}, SrvDscp_{SP}\}, ID_{SP-obs}, PK_{SP-obs}\})$$

$$\textit{where } TK = (SN, TS, SG_{SN}),\ SN \textit{ is a serial number},\ TS \textit{ is a timestamp},\ SG_{SN} = S_{SK_{MNSP}}(SN, TS)$$

After, the response message M_6 and its hashing value H_{M_6} are sent to the user.

Step 5. Upon receiving the above messages, the integrity of the message M_6 can be verified as follows:

$$H(M_6)\overset{?}{=}H_{M_6}$$

Finally, the user gets the transaction token TK and all SPs' service list $\{\{Nick_{SP}, SrvDscp_{SP}\}, ID_{SP-obs}, PK_{SP-obs}\}$ of current location on his mobile device.

Phase 3. Service Request Phase

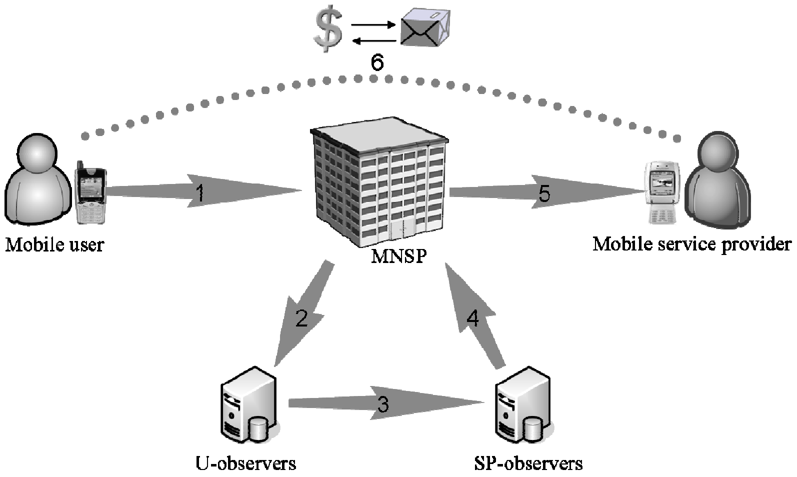

Fig. 4. Service Request Phase

Step 1. Suppose a SP is selected, the user request $R\,eq_U$ and the SP's nickname $Nick_{SP}$ should be proposed to the chosen U-observer as the following format:

$$N_1=(R\,eq_U\,\|\,Nick_{SP}\,\|\,TK)\oplus a_j+a_{j-1}$$

$$N_2=(R\,eq_U\,\|\,Nick_{SP}\,\|\,TK)\oplus a_{j-1}+a_{j-2}$$

The user generates his request message M_7 containing the above values N_1 and N_2, the SP-observer's identity ID_{SP-obs} and public key PK_{SP-obs}, and the chosen U-observer's identity ID_{U-obs} and public key PK_{U-obs}:

$$M_7=(N_1,N_2,ID_{SP-obs},PK_{SP-obs},ID_{U-obs},PK_{U-obs})$$

Then the above request message M_7 and its hashing value H_{M_7} are sent to the MNSP.

Step 2. Upon receiving the above messages, the integrity of the message M_7 can be verified as follows:

$$H(M_7)\overset{?}{=}H_{M_7}$$

A partial parameters of the message M_7 will be forwarded to the U-observer:

$$M_8=(N_1,N_2,ID_{SP-obs},PK_{SP-obs})$$

Then, the MNSP uses its secret key to sign M_8 as follows:

$$SG_{M_8}=S_{SK_{MNSPs}}(H(M_8))$$

The message M_8 and its signature SG_{M_8} are encrypted by the U-observer's public key PK_{U-obs} as follows:

$$C_8=E_{PK_{U-obs}}(M_8,SG_{M_8})$$

After, the ciphertext C_8, the user's identity ID_U, and the MNSP's public key PK_{MNSP} are sent to the U-observer.

Step 3. Upon receiving the above messages, the ciphertext C_8 can be decrypted by the U-observer's secret key. Then the integrity of the message M_8 can be verified as follows:

$$H(M_8)\overset{?}{=}V_{PK_{MNSP}}(SG_{M_8})$$

The U-observer uses the pre-coordinated hashing values of a_j, a_{j-1}, and a_{j-2} to decrypt the values N_1 and N_2. Then the user's request $R\,eq_U$, the SP's nickname $Nick_{SP}$, and this transaction token

TK can be obtained and verified as follows:

$$(N_1 - a_{j-1}) \oplus a_j \overset{?}{=} (N_2 - a_{j-2}) \oplus a_{j-1}$$

The U-observer should make the following "proxy-request" message M_9:

$$M_9 = (Nick_{SP}, R\,eq_U, TK)$$

Then the U-observer uses its secret key to sign M_9 as follows:

$$SG_{M_9} = S_{SK_{U-obs}}(M_9)$$

The message M_9 and its signature SG_{M_9} are encrypted by the SP-observer's public key PK_{SP-obs} as follows:

$$C_9 = E_{PK_{SP-obs}}(M_9, SG_{M_9})$$

After, the ciphertext C_9 and the U-observer public key PK_{U-obs} are sent to the SP-observer.

Step 4. Upon receiving the above messages, the ciphertext C_9 can be decrypted by the SP-observer's secret key. Then the integrity of the message M_9 can be verified as follows:

$$H(M_9) \overset{?}{=} V_{PK_{U-obs}}(SG_{M_9})$$

Moreover, the transaction token $TK = (SN, TS, SG_{SN})$ in the message M_9 should be verified as follows:

$$(SN, TS) \overset{?}{=} V_{PK_{MNSP}}(TK)$$

If the above equality is hold, it means the request is guaranteed by the MNSP for its validation.

According to the nickname $Nick_{SP}$ in the message M_9, the corresponding SP's identity can be retrieved. Then the above message M_9 and its signature SG_{M_9} should be proposed to the corresponding SP as the following format:

$$R_3 = (M_9 \,\|\, SG_{M_9}) \oplus b_{i-2} + b_{i-3}$$

$$R_4 = (M_9 \,\|\, SG_{M_9}) \oplus b_{i-3} + b_{i-4}$$

The SP-observer should make the following "request-confirmed" message M_{10}:

$$M_{10} = (R_3, R_4, ID_{SP})$$

Then, the SP-observer uses its secret key to sign M_{10} as follows:

$$SG_{M_{10}} = S_{SK_{SP-obs}}(H(M_{10}))$$

The message M_{10} and its signature $SG_{M_{10}}$ are encrypted by the MNSP's public key PK_{MNSP} as follows:

$$C_{10} = E_{PK_{MNSP}}(M_{10}, SG_{M_{10}})$$

After, the ciphertext C_{10} is sent to the MNSP.

Step 5. Upon receiving the above messages, the integrity of the message M_{10} can be verified as follows:

$$H(M_{10}) \overset{?}{=} E_{PK_{SP-obs}}(SG_{M_{10}})$$

Only parameters R_3 and R_4 will be forwarded to the corresponding SP:

$$M_{11} = (R_3, R_4)$$

Then the above message M_{11} and its hashing value $H_{M_{11}}$ are sent to the SP.

Step 6. After receiving the above messages, the integrity of the message M_{11} can be verified as follows:

$$H(M_{11}) \overset{?}{=} H_{M_{11}}$$

The SP uses the pre-coordinated hashing values of b_{i-2}, b_{i-3}, and b_{i-4} to decrypt the message R_3 and R_4. Then the message M_9 and its signature SG_{M_9} can be obtained and verified as follows:

$$(R_3 - b_{i-3}) \oplus b_{i-2} \overset{?}{=} (R_4 - b_{i-4}) \oplus b_{i-3}$$

According to the user's request $R\,eq_U$, which is contained in the message M_9, the SP will provide his service on the requested time and location.

3 Analysis

A. Anonymity Issue:

In our design, the user and SP will not know each other when they are transacting, because:

I . In step 5 of the service query phase, the user gets the list $\{\{Nick_{SP}, SrvDscp_{SP}\}, ID_{SP-obs}, PK_{SP-obs}\}$. Clearly, there is no any identity of the *SPs*. The user just needs to appoint the nickname in his service request, then the request will be forwarded to the corresponding SP finally.

II . In step 6 of the service request phase, the SP gets the user's request $R\,eq_U$. Of course, there is no any identity in the request message. It's just the time and location information for the SP needs to know.

B. Privacy Issue:

In our protocol, the transaction message will be transferred by the MNSP. However, the transaction's detail such like SP's service description $SrvDscp_{SP}$ and user's request $R\,eq_U$ should not be known by the MNSP for the reason of privacy:

I . In step 1 of the service registration phase, the registration message is performed as follows:

$$R_1 = (Nick_{SP} \,||\, SrvDscp_{SP}) \oplus b_i + b_{i-1}$$
$$R_2 = (Nick_{SP} \,||\, SrvDscp_{SP}) \oplus b_{i-1} + b_{i-2}$$

The above message then be forwarded to the chosen SP-observer via the MNSP. The MNSP will not be able to decrypt R_1 and R_2 without b_i, b_{i-1}, and b_{i-2}, thus preventing it from obtaining the SP's service description $SrvDscp_{SP}$.

II . In step 4 of the service query phase, the MNSP will collect all of the suitable SPs' recorders:

$$\{\{Nick_{SP}, SrvDscp_{SP}\}, ID_{SP-obs}, PK_{SP-obs}\}$$

There will only be known the nickname of the SPs, the MNSP will not know who the SPs are.

III . In step 1 of the service request phase, the request message is performed as follows:

$$N_1 = (R\,eq_U \,||\, Nick_{SP} \,||\, TK) \oplus a_j + a_{j-1}$$
$$N_2 = (R\,eq_U \,||\, Nick_{SP} \,||\, TK) \oplus a_{j-1} + a_{j-2}$$

The above message then be forwarded to the chosen U-observer via the MNSP. The MNSP will not be able to decrypt N_1 and N_2 without a_j, a_{j-1}, and a_{j-2}, thus preventing it from obtaining the user's request $R\,eq_U$.

Moreover, the user's request will be further forwarded to the SP-observer in step 3 of the service request phase. And the request message is then embedded in the following message M_9:

$$R_3 = (M_9 \,||\, SG_{M_9}) \oplus b_{i-2} + b_{i-3}$$
$$R_4 = (M_9 \,||\, SG_{M_9}) \oplus b_{i-3} + b_{i-4}$$

The above message then be forwarded to the corresponding SP via the MNSP. Clearly, the MNSP will not be able to decrypt R_3 and R_4 without b_{i-2}, b_{i-3}, and b_{i-4}, thus preventing it from obtaining the user's request $R\,eq_U$ contained in message M_9.

C. Non-repudiation Issue

In our protocol, the final signature SG_{M_9} reserved by the SP is a non-repudiation evidence for the transaction. In the message M_9, the user's request $R\,eq_U$ is confirmed by the U-observer in step 3 of the service request phase:

$$(N_1 - a_{j-1}) \oplus a_j \overset{?}{=} (N_2 - a_{j-2}) \oplus a_{j-1}$$
$$where \quad N_1 = (R\,eq_U \,||\, Nick_{SP} \,||\, TK) \oplus a_j + a_{j-1}$$
$$N_2 = (R\,eq_U \,||\, Nick_{SP} \,||\, TK) \oplus a_{j-1} + a_{j-2}$$

Only the original user in agreement with the U-observer on a set of hashing chain a_0, a_1, $\cdots, a_n$ can generate the correct N_1 and N_2. Based on the trusty between the user and the U-observer, the user should be responsible for the chosen U-observer's signature. That means the user's request cannot be denied if it has been received by the SP to provide his service.

Suppose the user denies his request, the SP will show the "proxy-request" message M_9 and its signature SG_{M_9} to the MNSP. Then it can be verified by the U-observer's public key PK_{U-obs} as follows:

$$H(M_9)\overset{?}{=}V_{PK_{U-obs}}(SG_{M_9})$$

Moreover, the transaction token $TK=(SN,TS,SG_{SN})$ in the message M_9 should be verified as follows:

$$(SN,TS)\overset{?}{=}V_{PK_{MNSP}}(TK)$$

If the above equality is hold, the user's identity will be retrieved according to the serial number SN which is assigned by the MNSP in step 4 of the service query phase. Therefore, the SP will not worry about the user's repudiation.

D. Simplicity and Practicability Issue:

In our protocol, we assume that all communication is secure between the MNSP and the mobile device. There is not necessary to design extra encryption for those communication. Only exclusive-OR, addition, and hash operations are used in mobile device. All of these operations are easy to implement into current cell phone hardware. Moreover, our protocol can be easily applied to current mobile communication system without need of extra infrastructures. The setup cost of our scheme will be more reasonable than Zhu's scheme.

4 Conclusion

We propose scenarios that include the registration, query, and request phase for providing location-based service on mobile communication system. Our proposal contributes a practical protocol that meets all important issues: anonymity, non-repudiation, and simplicity.

References

[1] Y.-Y. Chen and S.-Y. Hsiao, "The Study on Secure Location-Based Service," *Proceedings of the 17th Information Security Conference*, June 2007.

[2] F. Zhu, M. Mutka, and L. Ni, "A Secure, Private, and Location-aware Service Discovery Protocol Supporting Mobile Services," *Proceedings of the First IEEE International Conference on Pervasive Computing and Communications (PerCom 2003)*, pp.235-242, Mar. 2003.

[3] P. Ahonen and R. Savola, "Security Threats to Mobile Service Development in the Age of Digital Convergence," *Proceedings of the International Conference on Computer as a Tool (EUROCON 2005)*, Vol. 2, pp.1052-1055, 2005.

[4] G. Bartolomeo, N. BlefariMelazzi, G. Cortese, A. Friday, G. Prezerakos, R. Walker, and S. Salsano, "Simplifying Mobile Services - for Users and Service Providers," *Proceedings of the* International Conference on Internet and Web Applications and Services/Advanced International Conference on Telecommunications *(AICT-ICIW '06*), pp.209-213, Feb. 2006.

[5] S. Ryu, S. K. Park, D. Oh, G. Sihn, K. Han, and S. Hwang, "Research activities on next-generation mobile communications and services in Korea," *IEEE - Communications Magazine*, Sept. 2005, pp.122-131.

[6] J. Tacken, T. Janssen, S. Flake, and D. Fischer," A service creation environment for interactive, menu-driven mobile services," *Proceedings of the 20th International Conference on Advanced Information Networking and Applications (AINA 2006)*, Apr. 2006.

[7] C. Ardagna, M. Cremonini, E. Damiani, SDC di Vimercati, and P. Samarati, “Supporting location-based conditions in access control policies,” Conference on Computer and Communications Security, *Proceedings of the 2006 ACM Symposium on Information, computer and communications security*, Taipei Taiwan, pp. 212-222, March 2006.

[8] A. H. John Cardiff, P. Magee, and J. Doody, “An architecture and development methodology for location-based services,” *Electronic Commerce Research and Applications*, Vol. 5, No. 3, pp.201-208, 2006.

[9] J. C. Kim, T. W. Heo, J. W. Kim, and J. H. Park, **“**Ubiquitous location based service,**”** *2005 IEEE Proceedings - Intelligent Transportation Systems*, pp.841-845, Sep. 2005.

[10] M. F. Mokbel and C. Y. Chow, “Challenges in Preserving Location Privacy in Peer-to-Peer Environments,” *Proceedings of the Seventh International Conference on Web-Age Information Management Workshops (WAIM 06)*, pp.1-8, June 2006.

[11] S. Y. Wu and K. T. Wu, “Effective location based services with dynamic data management in mobile environments,” *Wireless Networks*, Vol. 12, No. 3, pp.369-38, 2006.

[12] D. M. Konidala, Y. Y. Chan, and K. Kwangjo, “A secure and privacy enhanced protocol for location-based services in ubiquitous society,” *Proceedings of the IEEE GLOBECOM '04 - Global Telecommunications Conference*, pp.2164-2168, Nov. 2004.

[13] W. Tsui, C. Y. Yin, and C. N. Chen, “A Survey on Current Mobile Location Technology,” *ICL Technical Journal,* Vol.115, pp.54-60, Mar. 2006.