A Secure Web Services for Location Based Services in Wireless Networks*

Minsoo Lee[1], Jintaek Kim[1], Sehyun Park[1†], Jaeil Lee[2], and Seoklae Lee[2]

[1]School of Electrical and Electronics Engineering, Chung-Ang University,
221, HukSuk-Dong, DongJak-Gu, Seoul, Korea
lemins@wm.cau.ac.kr, groundiv@ms.cau.ac.kr, shpark@cau.ac.kr
http://bkmodem.cau.ac.kr/main.htm
[2] Korea Information Security Agency
78, Karak dong, Songpa-Gu, Seoul, Korea
{jilee, sllee}@kisa.or.kr
http://www.kisa.or.kr

Abstract. While Location Based Services (LBS) can make our lives more comfortable and productive, it may cause an invasion of privacy by disclosure and commercial use of location information. In this paper, we discuss privacy and security problems that may happen in the current LBS system and propose solutions. We propose a new secure Web services architecture for LBS in wireless network. Our architecture allows mobile users to create and enforce dynamic policy for safe and consistent LBS. We also describe some practical scenarios in which our architecture protects user's location privacy and security.

Keywords. Location Based Service, Privacy, Security, Interoperability

1 Introduction

With the development of mobile communication technologies, LBS are beginning to attract attention as a new research area of networking. LBS can offer much convenience to dynamic users in wireless network as well as provide significant revenue to mobile operators and content providers.

But the dark side of LBS, it also involves the threat of an invasion of privacy and security caused by indiscreet location tracking [1, 2, 21, 22, 23]. For example, if a company is using location tracking service to grasp where each employee is on duty hours, it must not observe their positions anymore off duty hours. If the tracking is continued, it will bring about a violation of privacy for the employees of the company. As another example, let's consider the case in which a LBS provider advertises to arbitrary users in a specific region. This may be also an incident of privacy violation if mobile users in the area do not want to receive these advertisements. Crimes

---

* This Research was supported by the Chung-Ang University Research Grants in 2003.

† The corresponding author

N. Mitrou et al. (Eds.): NETWORKING 2004, LNCS 3042, pp. 332–344, 2004.

that use illegal location tracking may also be possible. So, LBS related groups [16, 17] are considering privacy problems in various aspects.

The problem which we have to consider next is location security. Since LBS are based on message exchange in wireless network, there are always security risks as location information could be stolen, lost, or modified. Therefore, we must concern the security mechanism for location information. The security mechanism must eliminate or minimize the potential for attacks against LBS entities and must reduce exposure of the user's identity and location.

The last point that we should discuss is interoperability problem. One of the concerns about national and global LBS roaming is ensuring the interoperability of LBS platforms. Most of LBS platform have optional and proprietary features that can interfere with interoperability. There is no guarantee that user's location privacy policies and authorization rules are observed through various LBS platforms.

In order to ensure a robust, consistent LBS environment, we need a secure architecture that is capable of supporting dynamic enforcement of user privacy policies, security mechanisms and convergence of services.

Therefore, this paper identifies these LBS problems and outlines the requirements for securing the LBS. And we propose a secure Web services architecture to protect the location information. We design LBS Policy Authority to resolve privacy problems and LBS Broker to solve authentication and authorization problems. The proposed architecture can overcome differences in LBS platforms, location information, and positioning technologies and network architectures. The architecture enhances interoperability among various LBS providers building Global LBS service on various platforms in the ubiquitous environment. Our model also guarantees Single Sign-On (SSO) among multi-vendor topologies by exchanging authentication and authorization information using Security Assertion Markup Language (SAML) token.

The rest of this paper is organized as follow. Section 2 identifies the problems of current LBS and requirements to solve them. Section 3 suggests a new web service architecture enhancing privacy, security and interoperability of LBS. Section 4 shows some of LBS scenarios applying the proposed architecture. Section In section 5, we discuss the simulation environment and the results. Finally, we conclude in Section 6.

2 Motivations and Requirements

2.1 Privacy Problems

LBS are considered as one of the main revenue generators for next generation wireless services. However, LBS do raise new privacy issues [1, 2, 27, 28, 29] integral to LBS. The major problem arises when location information is required in order to obtain a service and at the same time the user does not want to reveal more personal identifiable information. Users wish to have complete control over the visibility of their location, but in the most part of LBS scenarios users are not in full control.

After all, location privacy will have to be carefully managed and we need systematic method as well as technological method [3, 4]. One of the ways to solve the location privacy problem is to provide fine-grained privacy policies in user control. Policies that require service provider to adhere to strong privacy practices are needed to counterbalance the invisible nature of location collection in the wireless world.

In this paper, we present classified user profiles and location policy to access location information to cope with the privacy problem. The user's policy is created with the agreement of user and is effectively used by dynamic condition for access to user's location information.

2.2 Security Problems

Beside location privacy problems, there are some risks about location information itself. Location information may be sniffed, modified or stolen by attacker from communication channel between LBS entities. Security requirements and mechanisms must be addressed to ensure the safety of location information exchange among various location server that support different positioning methods. The mechanism should provide confidentiality against eavesdroppers and integrity to assure that the location information was not modified accidentally or deliberately in transit. The mechanism should provide mutual authentication guarantees that access to LBS applications is restricted to only those who can provide the appropriate proof of identity.

These requirements can be satisfied by using digital signature and encryption of location data because they concern how to protect communicated data. Apart from these mechanisms, we also have to consider the protection of location information so that only appropriate entities are allowed to access location information. Authorization process is required to decide whether or not the entity can access the particular location information. These cryptographic operations could create so many burdens of user's mobile terminal in LBS environments where network resources and computing power are usually limited.

To effectively perform these tasks, Agent or Broker could be deployed. The agent may provide combination features such as better communication facilities, high speed cryptographic engine and memory mechanism. In order to ensure a robust, consistent LBS environment, our model uses two agents on behalf of mobile terminal for enhancing security operation like secure key management, authentication and authorization.

2.3 Interoperability Problems

Another issue of LBS community is that LBS are challenged by the disparate location technology implemented by wireless infrastructure providers, service providers and equipment vendors. Most of LBS community are faced with having to support multiple, disparate location-determining technologies (LDT), and content implementations, and multiple data transport protocols. This is simply cost prohibitive. Thus the LBS technologies used must vary with the service context i.e. time constraints, location positioning method, network connection status.

The key to interoperability will be the development and adoption of a ubiquitous set of interconnected wireless communications and Internet location service standards. Open and scalable LBS architectures and common data structures are necessary for various types of location information. These common structures could be defined by XML. Location Inter-Operability Forum (LIF) developed the XML based Mobile Location Protocol (MLP) [15] standard, which is concerned with the integration of position or location information. And Open GIS Consortium (OGC) issues Request for Technology for Web Services Initiative [18] to provide interoperable Spatial Web Services.

However, in some complicated services, such as LBS roaming which includes service continuity and hand-off issues, more consistent security features should be partnered with these efforts for interoperability. In the future of LBS environment, LBS roaming scenario is likely widespread where many LBS service providers are used to implement functionality "behind the scenes." If a user does not know whether or not the location information is broadly secure in various LBS platform, when roaming across boundaries within interconnected wireless networks, LBS roaming may create new security and privacy challenges. Therefore, we should figure out how to seamlessly provide secure location information utilizing heterogeneous wireless networks without reauthenticating each time. In this paper, we consider these interoperable and consistent security needs as addressed by Web service security mechanisms, and map each of the requirements onto the construct of future global LBS environments.

3 Secure Web Services Architecture for LBS

In this section, we propose a secure Web Services architecture which is designed to meet the requirements in previous sections. The objective of the proposed architecture is to ease the development of secure LBS by providing customized privacy and security profiles which can be assembled to create concrete LBS applications. The Figure 1 shows proposed LBS privacy and security Enhanced Web Services architecture.

3.1 Enhanced Interoperability with Web Services

The need to integrate disparate LBS applications that run across the Internet on heterogeneous wireless networks, and the realization that proprietary approaches would not solve the integration problem, gave rise to use of Web Services for LBS. Web services are going to play a big role in the evolution of mobile business. A Web Services supports direct interactions with other software applications using XML based messages via internet-based protocols such as HTTP, SMTP, and FTP, including Simple Object Access Protocol (SOAP). For easier configuration, Web Services interfaces could be defined and modified by Web Services Description Language (WSDL). The defined Web Services can be registered and discovered at Universal Description, Discovery, and Integration (UDDI) registry.

Consequently, these advantages of Web Services could bring maximum efficiency and interoperability to the LBS in next generation wireless networks where loosely coupled and highly dynamic environments are expected. Global LBS [5] also could be provided by cooperation of LBS providers in different country.

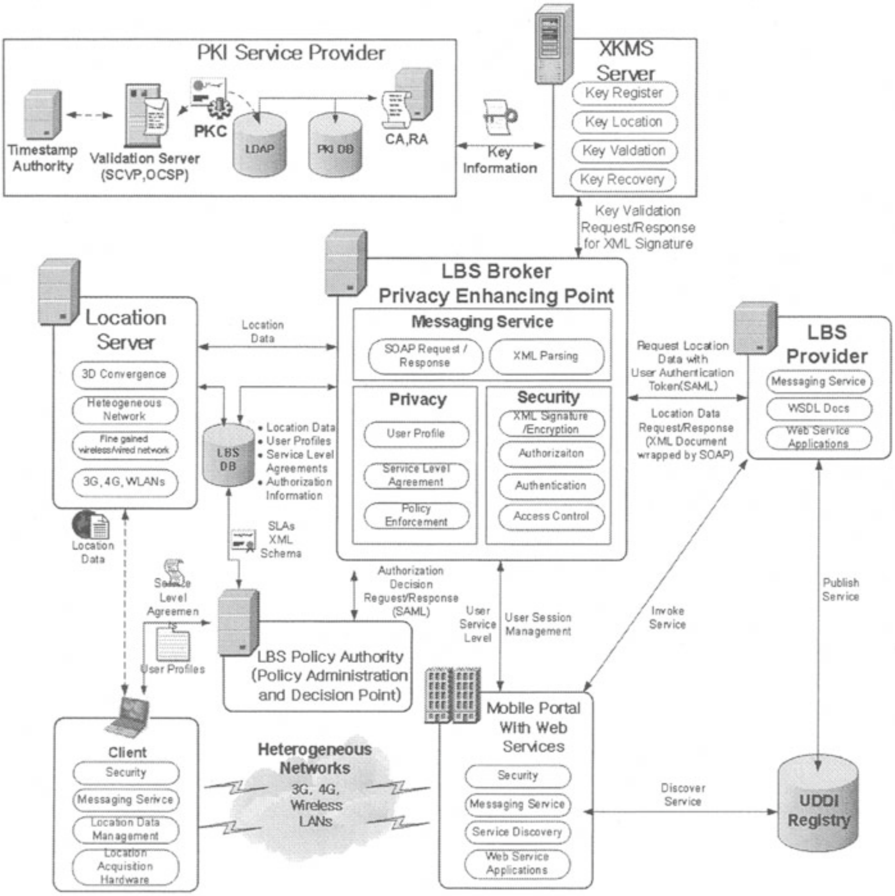


Fig. 1. LBS Privacy and Security Enhanced Web Service Architecture

3.2 Web Services Security for LBS

The Secure Socket Layer (SSL) is used to provide an encrypted means of data exchange between a web browser and a web server. Although SSL is widely treated as a standard, SSL is insufficient for Web Services Security in several ways. SSL only supports data in transit, not in storage. SSL does not support multi-party transactions and non-Repudiation. SSL is not granular enough because it encrypts everything.

To overcome the limited features of SSL, XML Signature [6] and XML Encryption [7] are used to forming a strong foundation for the development of secured web services by enabling partial signature and partial encryption respectively. These XML security specifications could provide authentication, encryption and non-repudiation in multiple participants from different location service domains. Additionally, distributed authorization and federated identity management like SSO are among the great challenges for LBS. Authorization policies for location information and other QoS parameters. To meet such security requirements, location information could be partnered with SAML [8] as addressed in [14]. SAML provide the basis for interoperable authentication, authorization and attributes among disparate systems including a SSO facility [9]. In our architecture, we took the advantage of incorporating location information with these Web Services security mechanisms to enhance the security and privacy of location based services.

3.3 LBS Broker

We design a LBS Broker to solve security problems of LBS. In some architecture, it may be useful to use a Broker to improve performance or security [19, 20]. LBS broker plays key role in protecting user's location information from unauthorized LBS service provider or malicious users.

The LBS broker act as a Policy Enforcement Point (PEP) that checks permission with the LBS policy authority, the Policy Decision Point (PDP) by exchanging SAML message before making decision and releasing the secured location information to the LBS service providers. LBS broker could provide users the greatest amount of control over their personal information, since the user is in control to choose whether their location is transmitted to the server for others to access. LBS broker supports XML signature and XML encryption to validating the signature of the SOAP messages. To validate the keys used in XML signature, it interacts with XML Key Management Specification (XKMS) [11] servers. XKMS helps to remove the complexity of working with PKI. SAML assertions are employed to for exchanging authentication and authorization token across different LBS entities like LBS brokers, LBS policy authorities, LBS service providers and mobile portals over Internet.

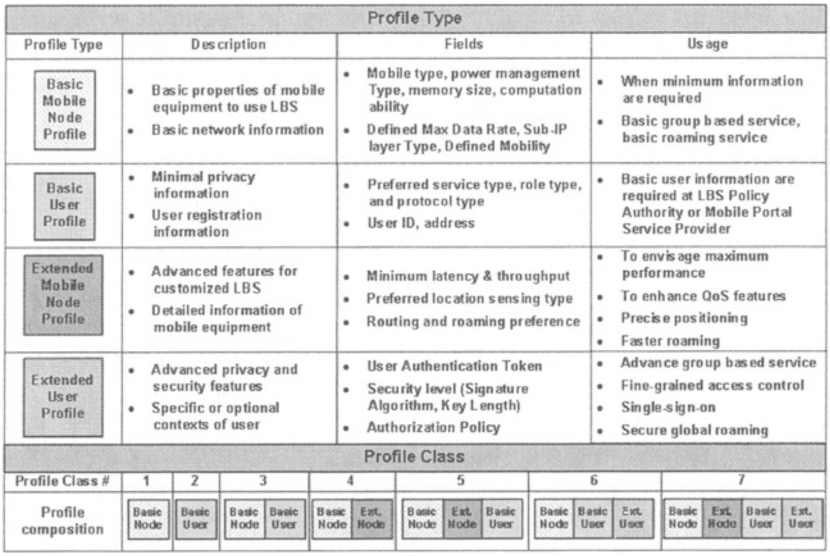
3.4 LBS Policy Authority for LBS Privacy

LBS Policy Authority acts as a Policy Administration Point (PAP) in LBS privacy agreement step and a PDP in LBS service step. As a PAP, it creates a LBS policy set to LBS Service Level Agreements (SLAs) with users using predefined XML Schema. The policy includes user profiles and other LBS service attributes.

3.4.1 Profiles for LBS Privacy

A simple set of location privacy rules is insufficient to enforce dynamic and consistent privacy when users roam. In Figure 2, we propose classified privacy and security profiles to accommodate more adaptive and optimal LBS environments. A key advantage that profiles offer is that LBS can be customized to fit user's specific needs.

Customization of LBS is performed through the classification of profiles. The classification of security needs to provide a wide scope for various LBS users. LBS Client adaptively modifies its profile for heterogeneous wireless networks. This mechanism could bring minimized leakage of privacy information that users wanted.



Profile Type

Profile Type	Description	Fields	Usage
Basic Mobile Node Profile	Basic properties of mobile equipment to use LBS Basic network information	Mobile type, power management Type, memory size, computation ability Defined Max Data Rate, Sub-IP layer Type, Defined Mobility	When minimum information are required Basic group based service, basic roaming service
Basic User Profile	Minimal privacy information User registration information	Preferred service type, role type, and protocol type User ID, address	Basic user information are required at LBS Policy Authority or Mobile Portal Service Provider
Extended Mobile Node Profile	Advanced features for customized LBS Detailed information of mobile equipment	Minimum latency & throughput Preferred location sensing type Routing and roaming preference	To envisage maximum performance To enhance QoS features Precise positioning Faster roaming
Extended User Profile	Advanced privacy and security features Specific or optional contexts of user	User Authentication Token Security level (Signature Algorithm, Key Length) Authorization Policy	Advance group based service Fine-grained access control Single-sign-on Secure global roaming

Profile Class

Profile Class #	1	2	3	4	5	6	7
Profile composition	Basic Node	Basic User	Basic Node Basic User	Basic Node Ext. Node	Basic Node Ext. Node Basic User	Basic Node Basic User Ext. User	Basic Node Ext. Node Basic User Ext. User

Fig. 2. Profile types and classes for LBS Privacy

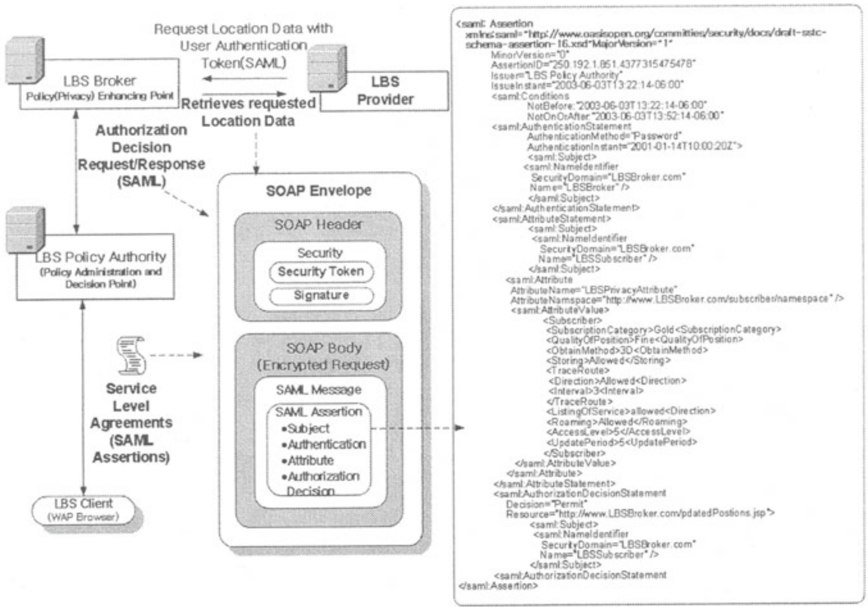
3.4.2 Policy Setting

The policy model proposed in this paper provides direct control function to a user through policy decision procedures with LBS Policy Authority which performs effective policy enforcement. Figure 3 shows LBS SLAs procedures and examples of SAML message about user privacy.

4 Scenarios

4.1 A Secure LBS Push Scenario

The push scenario happens when LBS service provider requests user's location information for providing location services to user. When LBS service provider requests user's location information to LBS broker, Figure 4 presents a scenario in which validation of user's privacy, authentication and authorization are enforced. In the scenario, XML based protocol is used for interoperability between all type of system. LBS Policy Authority could prevent improper usages of location service in specific area, time or users. The model with LBS Broker can improve efficiency and performance of authorization and authentication validation.


Request Location Data with User Authentication Token(SAML)
LBS Broker
Policy(Privacy) Enhancing Point
LBS Provider
Retrieves requested Location Data
Authorization Decision Request/Response (SAML)
LBS Policy Authority
(Policy Administration and Decision Point)
SOAP Envelope
SOAP Header
Security
Security Token
Signature
SOAP Body (Encrypted Request)
SAML Message
SAML Assertion
•Subject
•Authentication
•Attribute
•Authorization Decision
Service Level Agreements (SAML Assertions)
LBS Client
(WAP Browser)

```
<saml: Assertion
  xmlns:saml="http://www.oasisopen.org/committies/security/docs/draft-sstc-
  schema-assertion-16.xsd"MajorVersion="1"
        MinorVersion="0"
        AssertionID="250.192.1.851.4377315475478"
        Issuer="LBS Policy Authority"
        IssueInstant="2003-06-03T13:22:14-06:00"
        <saml:Conditions
                NotBefore:"2003-06-03T13:22:14-06:00"
                NotOnOrAfter:"2003-06-03T13:52:14-06:00"
        <saml:AuthenticationStatement
                AuthenticationMethod="Password"
                AuthenticationInstant="2001-01-14T10:00:20Z">
                <saml:Subject>
               <saml:NameIdentifier
                SecurityDomain="LBSBroker.com"
                Name="LBSBroker" />
                </saml:Subject>
        </saml:AuthenticationStatement>
        <saml:AttributeStatement>
                <saml:Subject>
                 <saml:NameIdentifier
                  SecurityDomain="LBSBroker.com"
                  Name="LBSSubscriber" />
                </saml:Subject>
          <saml:Attribute
           AttributeName="LBSPrivacyAttribute"
           AttributeNamspace="http://www.LBSBroker.com/subscriber/namespace" />
           <saml:AttributeValue>
                  <Subscriber>
                   <SubscriptionCategory>Gold<SubscriptionCategory>
                   <QualityOfPosition>Fine<QualityOfPosition>
                   <ObtainMethod>3D<ObtainMethod>
                   <Storing>Allowed</Storing>
                   <TraceRoute>
                    <Direction>Allowed<Direction>
                    <Interval>3<Interval>
                   </TraceRoute>
                   <ListingOfService>allowed<Direction>
                   <Roaming>Allowed</Roaming>
                   <AccessLevel>5</AccessLevel>
                   <UpdatePeriod>5<UpdatePeriod>
                  </Subscriber>
            </saml:AttributeValue>
          </saml:Attribute>
        </saml:AttributeStatement>
        <saml:AuthorizationDecisionStatement
          Decision="Permit"
          Resource="http://www.LBSBroker.com/pdatedPostions.jsp">
                <saml:Subject>
                 <saml:NameIdentifier
                  SecurityDomain="LBSBroker.com"
                  Name="LBSSubscriber" />
                </saml:Subject>
        <saml:AuthorizationDecisionStatement
</saml:Assertion>
```

Fig. 3. Secure Messaging for LBS policy setting

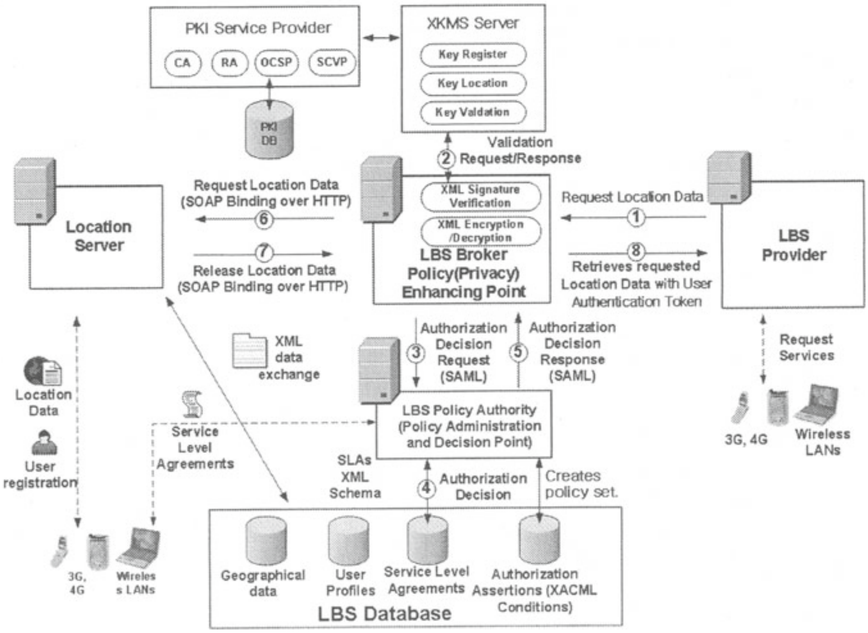

PKI Service Provider
CA
RA
OCSP
SCVP
PKI DB
XKMS Server
Key Register
Key Location
Key Validation
② Validation Request/Response
Location Server
Request Location Data (SOAP Binding over HTTP)
⑥
⑦
Release Location Data (SOAP Binding over HTTP)
XML Signature Verification
XML Encryption /Decryption
LBS Broker Policy(Privacy) Enhancing Point
Request Location Data
①
⑧
Retrieves requested Location Data with User Authentication Token
LBS Provider
Request Services
3G, 4G
Wireless LANs
③ Authorization Decision Request (SAML)
⑤ Authorization Decision Response (SAML)
XML data exchange
Location Data
User registration
Service Level Agreements
LBS Policy Authority (Policy Administration and Decision Point)
SLAs XML Schema
④ Authorization Decision
Creates policy set
3G, 4G
Wireless LANs
Geographical data
User Profiles
Service Level Agreements
Authorization Assertions (XACML Conditions)
LBS Database

Fig. 4. A Secure LBS Web Service Scenario

4.2 A Convergence Model

In this scenario, we propose a convergence model for more consistent LBS environments. For future global LBS roaming, location information of users, which exist in various LBS platform, should be managed on secure interoperable manner. Figure 5 depicts the integrated LBS architecture using LBS Brokers. Our model supports multiple, disparate LDT and supports SSO functionality with LBS Brokers.

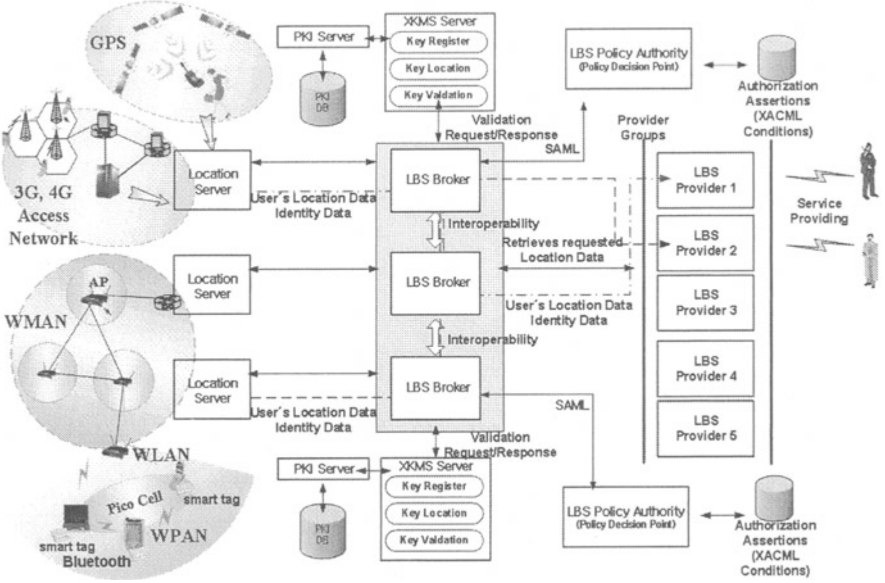


Fig. 5. The integrated LBS architecture using LBS Brokers

5 Simulations

We have modeled our architecture as a closed queuing system as in Figure 6, and we analyzed of approximate Mean Value Analysis (MVA) as described in [24, 25]. In the scenario of Figure 4, the secure LBS procedure has two job classes, initial secure location update step and secure LBS roaming step. $r_{im,jn}$ means the probability that a class *m* job moves to class *n* at node *j* after completing service at node *i*. And *ratio* represents a ratio of total users to secure LBS roaming users. Analyze steps of class switching closed queuing system are following.

Step1: Calculate the number of visits in original network by using (1)

$$e_{ir} = \sum_{j=1}^{K} \sum_{s=1}^{C} e_{js} r_{js,ir} \tag{1}$$

where K = total number of queues, C = total number of classes.

Step 2: Transform the queuing system to chain.

Step 3: Calculate the number of visits e_{iq}^{*} for each chain by using (2)

$$e_{iq}^{*} = \frac{\sum_{r \in \pi_q} e_{ir}}{\sum_{r \in \pi_q} e_{1r}} \tag{2}$$

where r = queue number in chain q, π_q = total queue number

Step 4: Calculate the scale factor α_{ir} and service times s_{iq} by using (3) with (1).

$$s_{iq} = \sum_{r \in \pi_q} s_{ir}\alpha_{ir}\ ,\ \alpha_{ir} = \frac{e_{ir}}{\sum_{s \in \pi_q} e_{is}} \tag{3}$$

Step 5: Calculate the performance parameters for each chain using MVA.

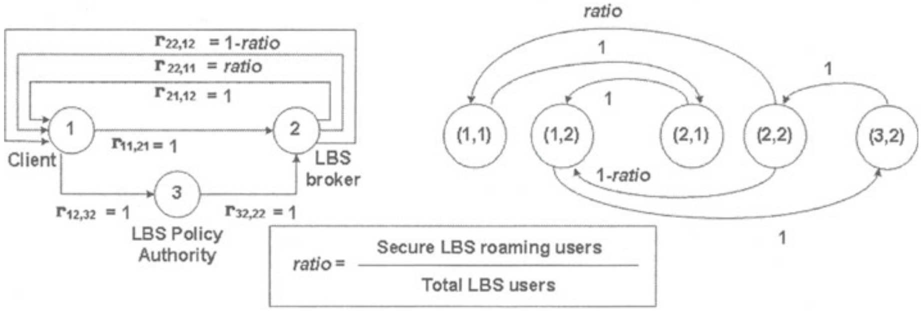
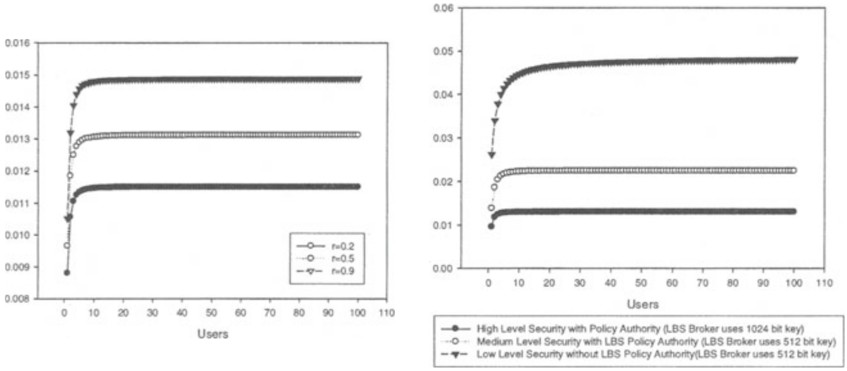


Fig. 6. Multiple class queuing system in the secure LBS push scenario

Table 1 summarizes the base parameter settings underlying the performance experiments. LBS Broker and LBS Policy Authority used Solaris 8 machine with Pentium III 933 MHz, 512 MB RAM. Mobile node used Pentium III 500 MHz, 128MB RAM, WindowsXP as operating system with Lucent Orinoco IEEE 802.11b wireless LAN card. The cryptographic library was Openssl 0.9.7a [12], and SAML Library was OpenSAML 0.9.1 [13]. Data size was 1KB in digital signature. Figure 7(a) shows average throughput at high security level when the roaming ratio *r* varies. As the initial secure location update needs more cryptographic operation, our secure Web service architecture show better performance in secure LBS roaming environments where users move fast. Figure 7(b) shows throughputs of secure location update with three security levels. Our secure Web service architecture could manage 12 users at high security level and up to 45 at one second. These simulation results could be useful to provide guidelines as to how the security level is set to meets the user needs. As we can see, the advantages of protecting privacy and security could far outweigh its overhead in specifying security assertions in XML.

Table 1. Base parameter settings of the queuing model

Entity	Operation in scenario	Description	Perform-ance
	Initial secure location update		
Mobile Node	Token Request with User's Private key	RSA with SHA-1 signature sign with a 512 bit key	5.5 ms
LBS Broker	Signature verification using User's Public key	RSA with SHA-1 signature verify with a 512 bit key	0.1 ms
LBS Broker	SCVP(OCSP) Request Message - signature of LBS Broker's Private Key	RSA with SHA-1 signature sign with a 1024 bit key	7.4 ms
XKMS with PKI	X.509 Certificate validation	Validate user certificate	30.3 ms
LBS Broker	OCSP Response Message validation	RSA with SHA-1 signature verify with a 1024 bit key	0.4 ms
LBS Broker	SAML Authorization Request	XML Parsing and RSA 1024 signature	27.4 ms
LBS Policy Authority	SAML Authorization Response	XML Parsing and RSA with SHA-1 1024 bit key signature verify	20.4 ms
LBS Policy Authority	SAML Authentication Token generation (and response to MN)	3DES Symmetric key encryption	7.702 MB/s
LBS Broker	Token Response with Location information	RSA encrypt on 512 bit keys	31.201 KB/s
LBS SP	Decrypt Token Response with Location Update Response	RSA decrypt on 512 bit keys	8.517 KB/s
	Secure LBS roaming		
Mobile Node	Location Request with Security Token	Average hand-off latency	30 ms
LBS Broker	Token verification	3DES Symmetric key decryption	1.090MB/sec
LBS Broker	Token Response with Location information	RSA encrypt on 512 bit keys	31.201 KB/s
LBS Provider	Decrypt Token Response with Location Update Response	RSA decrypt on 512 bit keys	8.517 KB/s



(a) Throughput of secure location update at high level security

(b) Throughputs of secure location update with various security levels

Fig. 7. Simulations results of the secure Web Services architecture

6 Conclusion

In this paper, we analyze privacy and security issues on location based service and give our view on the future prospects of LBS for the next generation wireless network. Users are increasingly concerned with the disclosure of location information to third parties and the potential consequences for their privacy. As the location privacy and security is emerging as one of the key issues that will have to manage before fulfilling the LBS revenue promise, we propose a secure Web Service architecture for location based service.

The architecture takes advantages of Web Services and is designed to maximize the efficiency and interoperability for the LBS in wireless networks where loosely coupled and highly dynamic environments are expected. We design a LBS Broker to effectively solve privacy, authentication and authorization problems. We introduce LBS Policy Authority with classified privacy and security profiles. Our model also guarantees SSO among LBS service providers by exchanging authentication and authorization information using SAML token. We also have shown some practical scenarios in which strong authentication and authorization are provided while preserving user's location privacy. And the simulation results could be useful to provide guidelines as to under which circumstances one security scheme may be used in preference to another.

References

1. Jorge Ceullar, John B. Morris, Deirdre Mulligan, Jon Peterson and James Polk, "Geopriv Requirements," draft-ietf-geopriv-reqs-0.3, 3, 2003-07-30
2. WLIA, "Adopted WLIA Privacy Policy (First Revision)," http://www.wliaonline.com/ indstandard/privacy.html
3. Dan Greening, "Location Privacy," location interoperability forum, 2002
4. Shereen Fink, "The Fine Line Between Location-Based Services & Privacy," http://www.sun.com/aboutsun/media/presskits/sp/
5. Ulf Leonhardt and Jeff Magee., "Security Considerations for a Distributed Location Service", Journal of Network and System Management, Vol 6(1):51-70, March 1998.
6. W3C Recommendation. D. Eastlake, J. Reagle, and D. Solo., "XML-Signature Syntax and Processing", February 2002.
7. W3C Recommendation T. Imamura, B. Dillaway, J. Schaad, E. Simon., "XML Encryption Syntax and Processing", December 2002.
8. OASIS Standard, Security Assertion Markup Language (SAML) 1.0, November 2002.
9. Ben Galbraith, et. al., *Professional Web Services Secuirty*, Wrox Press, 2002.
10. Alberto Escudero-Pascual, Gerald Q. Maguire Jr., "Role(s) of a proxy in location based services" 13th IEEE International Symposium on Personal, Indoor and Mobile Radio Communications. PIMRC2002. Lisbone. Portugal. September 2002.
11. W3C working draft, "XML Key Management Specification (XKMS) v 2.0", April 2003.
12. OpenSSL, http://www.openssl.org/
13. OpenSAML, http://www.opensaml.org/
14. Harsha Srivatsa, "Location, location, location-based services", IBM, November 2002.
15. Location Inter-operability Forum (LIF), Mobile Location Protocol (MLP), TS 101 Specification Version 3.0.0 6, June 2002.
16. Location Inter-operability Forum (LIF), "Privacy Guidelines", LIF TR 101 Report, 2002
17. 3GPP, Enhanced support for User Privacy in location services, TR 23.871,
18. Open GIS Consortium (OGC), "A Request for Technology In Support of an OGC Web Services Initiative," 2003

19. Michael Berger, et. al., “An Approach to Agent-Based Service Composition and Its Application to Mobile Business Processes”, IEEE Transactions on Mobile Computing, VOL. 2, NO. 3, July-September 2003.
20. Aura Ganz, Se Hyun Park, and Zvi Ganz, "Security Broker for multimedia wireless LANs", Computer Communications, Vol.23, issue 5-6, pp. 588-592, March 2000.
21. Alberto Escudero-Pascual, Thijs Holleboom, and Simone Fischer-Hiibner, “Privacy for Location Data in mobile networks”
22. Euro Beinat, “Privacy and Location-based Stating the Policies Clearly”, GEO Informatics, Volume 4, September 2001
23. Alastair R. Beresford and Frank Stajano, “Location Privacy in Pervasive Computing”, PERVASIVE computing, January-March 2003.
24. Boudewijn R. Haverkort John, “Performance of Computer Communication Systems : A Model-Based Approach” , Wiley & Sons, October 1999.
25. Gunter Bolch, Stefan Greiner, Kishor Trevedi, “A Generalized Analysis technique for queueing networks with mixed priority strategy and class switching”, Technical Report TR-I4-95-08, Oct. 1995.