W-PKI기반의 인증 및 키 교환 프로토콜을 이용한 LBS 보안 구조 연구

박상덕, 이동훈
고려대학교 정보보호대학원

A Study on LBS Security Structure using W-PKI based Authentication and key Agreement protocol

Sang-Duk Park, Dong-Hoon Lee
Graduate School of Information Security, Korea University

요 약

위치기반서비스(Location Based Service)는 이동중인 사용자의 위치 정보를 타 정보와 결합해 사용자가 요청, 혹은 필요로 하는 부가적인 응용 서비스를 제공하기 위한 기술을 말한다. 현재의 개인 위주의 서비스에서 국가 전반적인 인프라 차원으로 급속히 확대 발전함에 따라 사용자의 프라이버시(Privacy) 문제나 접근제어와 같은 인증 문제가 중요한 이슈로 대두되고 있다. 본 논문에서는 LBS 기업체 동향 및 전반적인 사항을 분석하여 문제점을 도출하고 LBS 프라이버시(Privacy) 보호를 위한 접근제어 문제, 인증 문제 및 키 신규성 확인 기능을 제공하는 타원곡선 기반의 인증 및 키 교환 프로토콜 기술을 제시한다.

1. 서론

미래 정보화 산업에 발맞추어 LBS는 현재의 개인 위주의 서비스에서 위치측위 기술의 발달, 서비스 고도화에 따라 전자 상거래, 교통, 환경, 의료등 국가 전반적인 인프라 차원으로 확대 발전 추세에 있다. 위치기반서비스는 현재의 보조기능에서 2007년경에는 모든 모바일 단말에 필수적으로 내장 될 것이고 다양한 value-chain이 존재하여 전후방 효과등 연관 산업 파급 효과가 매우 크게 작용할 것이 분명하다 [1].

위치기반서비스가 중요한 이슈로 급격하게 부상하고 있는 이유는 무선 인터넷 시장의 성장과 이에 따른 무선 인터넷 가입자 수의 증가에 기인한다. 이동성을 강조하는 무선 인터넷상에서는 위치기반정보가 사용자가 요구하는 컨텐츠이며 실제로 무선 기술의 발달과 무선 인터넷 가입자 수가 증가함에 따라 위치기반서비스는 무선 인프라를 구성하는 핵심적인 정보로 작용하고 있다 [2]. 위치기반서비스의 활성화를 위해서는 위치기반 기술인 무선 측위기술, LBS 플랫폼 기술 그리고 LBS 응용기술과 같은 순기능의 개발과 홍보도 중요하지만 사용자의 위치정보, 즉 개인의 프라이버시와 같은 역기능의 조기 해소에도 노력을 기울일 필요가 있다. 현재 위치기반 서비스 기술이 제공하는 편리성에 도취되어서 정보보호 문제의 심각성이 제대로 인식되지 못하고 있는 것이 사실이다. 이용자 개인의 위치가 실시간으로 노출되고 이러한 정보를 악용할 경우 개인의 사생활 침해는 물론 범죄에도 악용될 소지가 다분하다. 또한 안전성에 관련된 기술적, 이론적 연구도 부족한 상황이다. 그러므로 사용자가 위치정보 서비스를 요구할 때 이에 따르는 접근 제어 기술 및 위치 정보 관리 기술 등이 포함된 효율적이고 안전한 전자 서명 기반의 통합 인증 프로토콜 연구가 필요하다.

유·무선 통신 서비스를 제공하는 시스템에서는 비밀성, 무결성 및 인증 그리고 부인봉쇄가 중요한 정보보호 이슈였다면, 위치기반서비스를 제공하는 시스템에서는 시스템을 구성하고 있는 개체들의 상이한 연산 능력 및 환경에 적합한 정보보호 서비스가 요구되어져야 한다. 이와 더불어 개체들이 상호 작용함으로써 제기되는 새로운 보안문제들이 발생할 수 있다.

본 논문에서는 위치기반 서비스의 전반적인 사항 및 위치기반 기술을 분석하고 그에 따른 문제점을 도출하여 위치기반 서비스에서 개인정보를 보호할 수 있는 방안을 제시한다. 즉, 타원곡선을 기반[3]으로 한 인증 기술 도입은 위치기반정보가 각 개체들에게 상

호 전달 될 때 필요한 접근권한 문제, 인증 문제 그리고 키 신규성 확인을 제공한다.

이러한 측면에서 본 논문에서 제시하는 제한된 모바일에 적합한 타원곡선 기반의 인증 기술은 위치기반 시스템의 개인위치정보 및 프라이버시를 보호할 수 있는 대안을 제시하며 차세대 위치기반 서비스 환경에서의 보안 기술에 중요한 토대가 될 것이다.

2. 위치기반서비스의 개요

LBS는 이동 통신 기지국과 위성 확인 시스템을 통해 개인이나 차량의 위치 정보를 파악하여 각종 첨단 서비스를 제공한다 [4]. 앞에서 살펴본 바와 같이 LBS가 큰 기대를 모으는 것은 위치 정보가 이동 통신망과 연결함으로서 대중적이고 일반적인 서비스로 거듭날 수 있기 때문이다.

3GPP, OGC, FCC 는 LBS 를 다소 달리 정의 한다 [5]. 세계 각국에서는 LBS의 도입 및 검토를 위한 배경이 다르기 때문에 그 목적도 달리하고 있다.

미국에서의 LBS는 주로 범죄방지나 인명구조 등 보안에 중점을 두고 있으며, 유럽의 경우는 유통관리 시스템의 일환으로서 업무용 매체에 중점을 두고 있는데 GPS기반의 서비스보다 기지국 중심의 cell 방식을 취하고 있다. 일본에서는 주로 상업적인 목적을 위해 서비스 사업자가 중심이 되어 LBS를 도입하고 있다 [6].

국내의 LBS는 주로 3개 이동통신 사업자 중심의 서비스가 근간을 이루고 있다 [7][8]. LBS에 관련된 업체들은 통신 사업자의 공급 전략에 따라 LBS 기술 개발에 참여하고 있으며 컨텐츠 및 서비스 제공자들은 통신망을 통한 서비스를 제공하고 있다 [9].

위치기반 서비스 시스템은 무선 단말기 사용자, 위치기반 서비스 제공자, 위치 정보 관리 시스템 및 위치 획득 장비로 구성된다. 사용자는 하나의 위치기반 서비스 제공자를 지니게 되고, 이러한 다수의 위치기반 서비스 제공자가 위치정보 관리 시스템에게 사용자의 요구를 대신해서 특정 사용자의 위치정보를 요청하게 된다. 요청을 받은 위치 정보 관리 시스템은 위치 획득 장비에게 위치정보를 요청하게 되고 위치정보 획득 장비는 무선망에서 위치를 측정하여 좌표 값으로 위치 정보 관리 시스템에게 전달하게 된다 [10].

최종적으로 위치 정보 관리 시스템은 위치기반 서비스 제공자에게 위치정보를 전달하게 되고 위치기반 서비스 제공자는 사용자의 요구에 따라 서비스를 제공한다.

3. LBS 보안 구조 제안

위치기반서비스는 국외뿐 아니라 국내에서도 이동통신 사업자 주도로 다양한 관련 응용 서비스가 개발되면서 LBS는 이용자들에게 높은 관심을 보이고 있다. 여러 이동통신 응용서비스에 LBS 기술이 도입되면서 무선 인터넷 산업의 새로운 정보의 주체가 되고 있다. 그러나 이러한 긍정적인 LBS 산업 전망에도 불구하고 시장 성장에 부정적인 영향을 미칠 요소도 존재한다. 그 부정적인 요인 중의 하나가 개인 프라이버시 침해 및 개인위치정보 노출로 인한 각종 범죄에 악용될 수 있는 소지들 이다. 이러한 부정적인 문제점을 해결하기 위해 본 논문에서는 LBS시스템의 발전 방향에 필요한 MT와 LBS-SP아래 AP간의 위치 정보 송수신과 부인 방지를 위한 신뢰관계를 보장하고 특히 로밍시 개인 위치 정보를 보장받을 수 있는 방안을 제시한다.

다음은 프로토콜에 필요한 타원곡선군위에서 고려한 매개변수와 각각의 역할을 설명한다.

표1. 매개변수와 그 역할

매 개 변 수	역 할
P	타원곡선 군의 생성자
x	MT(사용자) 개인키
V	MT(사용자)의 공개된 등록정보 . V = xP
Y	AP_{new}의 공개키 (Y=x'P)이고 x'는 AP_{new}의 개인키
a . b	개체의 임시 개인키. 매 세션마다 랜덤하게 생성되어 공개되지 않음.
A . B	a . b 에 해당하는 임시 공개키
k	세션키
H . H_1	강한 일방향 해쉬 함수
Pwd_M	MT의 고유값 (Password)

프로토콜 진행 전에 V=xP(P:basepoint)는 이미 생성되어 신뢰기관(CA)으로부터 발급받은 $cert_M$과 함께 AP_{old}에 안전하게 저장되고 AP_{old}는 AP_{new}와 미리 상호 인증되어 세션키 k'를 공유하고 있다고 가정 한다 [11]. 또한, 유선 구간인 AP-위치장비시스템은 안전한 채널이라고 가정하고 본 논문에서의 제안된 프로토콜은 다음과 같다.

①AP_{old}에서 AP_{new}로 로밍시 MT는 AP_{old}과의 SNR(signal to noise ratio)값[12]이 기준치 이하로 떨어지면 이동하고자 하는 영역의 가장 큰 SNR을 갖는 AP_{new}로의 인증 및 키 설정을 위한 MT의 등록 정보 V와 인증서 $cert_M$를 AP_{new}에게 전송한다 [13].

② MT는 난수 a (random number in E(GF(Z)))를 택하여

AP_{old}로부터 안전하게 세션키 k'를 받아 $A=E_{k'}(a)$를 계산하고 A를 AP_{new}에게 전송한다.

③ AP_{new}는 난수 b (random number in $E(GF(Z_p))$)를 택하여 B=bP을 계산하고 자신의 개인키 x'로 공개키 Y=x'P을 생성하여 B,Y, $cert_{AP}$를 MT에게 전송한다. 그리고 MT로부터 메시지를 기다리는 동안 $E_{k'}(a)$로부터 a를 복호화 하여 $k = H(abP \| x'V)$를 계산한다.

④ MT는 개인키 $x=H(Pwd_M)$를 이용하여 $k = H(abP \| xY)$를 계산한다. 다음으로 MT는 $V_M = MAC_k(A,B) = H_1(k \| A \| B)$를 계산하여 AP_{new}에게 전송한다.

⑤ AP_{new}는 전송받는 V_M을 확인하고 맞다면 AP_{new}는 MT를 검증했다고 확신한다. 다음으로 AP_{new}는 $V_A = MAC_k(A,B,V_M) = H_1(k \| A \| B \| V_M)$을 계산하여 MT에게 전송한다.

⑥ MT는 $MAC_k(A,B,V_M) = H_1(k \| A \| B \| V_M)$을 계산하여 AP_{new}로부터 전송받은 V_A와 같은지 확인한다. 두 값이 같다면 MT는 AP_{new}를 검증했다고 확신하고 이전의 AP_{old}와 세션을 종료하고 설정된 세션키 k를 이용하여 곧바로 AP_{new}와 협상이 완료된다.

⑦ MT는 자신의 위치 정보를 LBS-SP에게 전달하고 LBS-SP는 LBS-System 및 위치획득장비를 이용하여 MT에게 적합한 위치기반 응용 서비스를 제공한다.

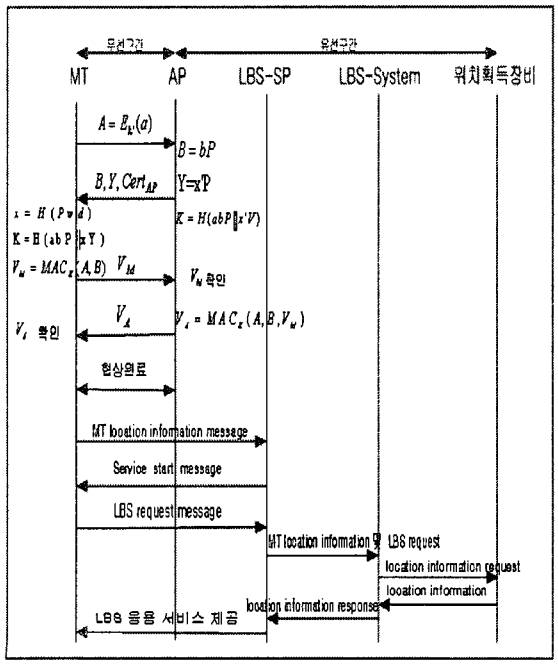

그림 1. AKE-ECC

4. 안전성 및 성능 분석

MT가 주체가 되어 AP_{new}가 MT를 인증하기 위해 사용하는 정보는 MT의 등록정보 V(=xP) 이다. 이 등록정보는 일반적인 공개키 시스템에서 공개키에 해당하지만 제안된 프로토콜은 사용자가 로밍시 해당 AP_{old}에게 request message를 보내면 이동 하고자 하는 지역의 다른 AP_{new}로 안전한 채널을 이용하여 PMK(V=xP)를 전송한다.

제안된 프로토콜의 안전성은 다항식 시간에 풀기 어렵다고 알려져 있는 ECDLP와 H의 강한 일방향 해쉬 함수에 근거하며 중간 침입자 공격(Man-in-the-Middle attack)에 안전하다. 임의의 수동적인 공격자가 도청을 통하여 A, B, Y, V_M, V_A 을 얻을 수 있다고 하더라도 이 정보들로부터 Pwd, 세션키 k를 계산할 수 있는 방법은 없다. 또한, 능동적인 공격자가 반송 공격(replay attack)을 통하여 부정확한 세션키의 생성을 유도할 수 있다. 즉, MT가 보낸 A, V_M을 공격자가 MT에게 되돌려 보냄으로써 공격을 수행한다고 하더라도 MT와 AP_{new}간에 매 세션마다 항상 임의의 랜덤값 a, b가 사용되기 때문에 이전 키 생성은 불가능하다.

AP_{new}를 가장한 공격자가 패스워드 기반 프로토콜의 취약점을 이용하여 B=b'P를 만들어 MT에게 보내더라도 랜덤값 a가 공개되지 않으므로 세션키 생성은 불가능하게 된다.

제안된 프로토콜은 완전한 전방향 보안성(Perfect Forward Secrecy)을 제공한다. 공격자가 Pwd 노출로 인하여 개인키 x를 알아냈다고 하더라도 이전 세션키를 유추할 수 없다. 이것은 ECDH가 안전하다는데 기인한다.

또 다른 특징을 살펴보면 MT와 AP_{new} 는 각각 자신의 랜덤값 a, b를 생성하여 세션키를 만들기 때문에 어느 한쪽에서 세션키를 컨트롤 할 수 없게 된다. 또한, MT의 등록 정보(V)와 인증서($cert_M$)가 AP_{new}에게 전송되고 AP_{new}의 공개키 Y와 인증서($cert_{AP}$)가 MT에게 전송됨으로서 상호 교환을 통해 세션키(k)가 공유되고 MAC값을 통해 상호 키 인증을 제공받게 된다.

성능 면에서 살펴보면 타원곡선 이산대수를 기반으로 설계했다는 점에서 계산 능력, 전력 소모량, 메모리 크기가 제한된 이동통신 시스템에 적합한 프로토콜이라 여겨지며 메시지 패스의 수를 4회로 최소화함으로서 프로토콜 진행의 효율성을 이루도록 하였다.

MT는 자신의 개인키가 프로토콜 진행 도중 생성되기 때문에 별도로 암기하거나 저장할 필요가 없다. 또한, 로밍시 AP간 상호인증을 통하여 CRL 검색 과정을 생략함으로서 MT와 AP_{new}간의 인증시 오버헤드를 줄일 수 있다.

5. 결론

차세대 LBS 산업은 모든 통신 산업의 핵심 축으로 자리 매김 할 것이다. A-GPS, 측위 정확도 향상 기술, 이동 개체 DB 기술 등이 급속도로 발전함에 따라 LBS 제도 개선으로 인해 다양한 응용서비스가 제공 될 것이다.

실제적으로 본 논문 첫 장에서 국내외 기업체 LBS 산업 동향을 살펴본 바와 같이 LBS 기반기술의 조기 확보, 무선 인터넷 활성화를 통한 세계 이동통신 분야의 선도 국가로 부상이 기대되며 119, 112등 긴급 서비스에 적용될 경우 국가, 사회적인 위기관리 능력 제고가 기대된다. 그러나 LBS 제공의 부정적인 영향으로 개인의 위치 정보를 특정인 및 특정 집단에 제공하여 개인 정보보호 차원에서 문제가 발생할 수 있다. 특히 스팸 메일이 사회적 문제가 되고 있는 상황에서 개인정보의 제공으로 LBS를 통해 무분별한 모바일 마케팅이 실시되거나, 특정 개인에 대한 감시와 통제의 목적으로 사용되는 등의 부작용이 있을 수 있다.

본 논문은 이러한 문제점들을 정보보호기술 측면에서 살펴보았다. ECDLP 기반의 프로토콜을 LBS 보안 메카니즘에 적용시킴으로서 기존에 노출되었던 취약점들에 대하여 안전하도록 설계되었으며 타원곡선 알고리즘을 적용함과 동시에 효율적인 군 연산을 이용하여 모바일 환경에 적합하도록 설계 되었다. 또한 스마트카드와 같은 부가적인 장비 없이 프로토콜 진행 중에 상호 인증, 세션키 생성 및 확인이 이루어질 뿐만 아니라 MT의 비밀정보(x)의 노출 없는 프로토콜이 진행되어 LBS 환경에서 개인 프라이버시가 보장되는 유용한 시스템으로 적용되리라 기대된다.

그러나 향후 유비쿼터스 환경에서 LBS가 보급되기 위해서는 앞에서 살펴본 바와 같이 LBS의 기술적인 문제 해결뿐만 아니라 법적, 제도적 문제도 선결되어야 할 것이다.

우선, 기술적인 문제는 국내 이동통신서비스 업체들이 상호 운용성 보장으로 표준화된 방법이 필요하다. 즉, 서로 다른 LBS-SP 장치들 간의 위치 정보의 획득 및 제공을 통한 LBS 확산 및 보안 기술을 고려해야 한다. 또한, 본 논문에서 제시한 PMK (V)가 AP간에 전달될 때 안전한 채널이 보장될 수 있도록 해야 할 것이며 개인의 위치정보 제공에 따른 사생활 침해 소지의 논란이 일어나지 않도록 가능성에 대한 원천적인 차단을 위한 법적-제도적 장치가 필요하다.

[참고문헌]

[1] 안병익, "국내외 LBS 산업 동향 및 대응 방안", 포인트아이(주) 2003년 1월

[2] "LBS 산업현황과 LGT사업전개 방향", LG텔레콤 서비스 개발실 Data 사업팀.

[3] 이용기, 이정규 "타원곡선을 이용한 안전한 패스워드 프로토콜",*정보보호학회논문집,*제9권 제1호 pp 85-102 , 1999년 3월

[4] "LBS서비스 현황 및 사업전략", SK 텔레콤 , 2003년 1월

[5] 이성휘, "세계 LBS 시장 환경 분석", 정보조사분석팀, *주간기술동향*, 2003년 9월

[6] 이진우, 황지은, 김관연, 박세현 "W-PKI를 이용한 LBS 응용서비스의 보안 모델 연구", *한국정보보호학회 하계정보보호학술대회 논문집,* Vo.13, NO.1 pp 245-248 , 2003년 7월

[7] "KTF LBS 사업계획 및 협력 방안", 인터넷 사업담당 매직엔메세징팀, 2003년 1월

[8] "이동체 시큐리티 사례발표", (주) 에스원 , 2003년 1월

[9] 정보통신부 "LBS산업 육성 정책 방향", 소프트웨어진흥과 , 2003년 1월

[10] "LBS측위 기술 개발", 삼성 전자 통신연구소, 2003년 1월 (LBS산업협의회 세미나)

[11] IEEE 802.11i, "Wireless Medium Access Control (MAC) and physical (PHY) specifications: Specification for Robust Security", February 2003.

[12] 정종민, 이주남, 이구연 "공개키 기반구조에서 빠른 핸드오프를 위한 무선랜 인증 기법 설계", *정보보호학회 논문집,* 제13권 제5호 pp 49 , 2003년 6월

[13] Kuo-Feng Hwang, Chin-chen Chang "A Self-Encryption Mechanism for Authentication of Roaming and Teleconference Services", vol.2, no.2, MARCH 2003