신뢰 기관을 통한 위치 정보 기반 서비스의 프라이버시 보호 및 인증 기법

한규석*, 김광조*

*한국정보통신대학교 국제정보보호연구소

Enhancing Privacy and Authentication in Location Based Service using Trusted Authority

Kyusuk Han*, Kwangjo Kim*

*IRIS, Information and Communication University

요 약

위치 정보 기반 서비스는 휴대 무선 통신 기기 사용의 확대에 따라 서비스의 범위가 크게 확장될 것으로 예상되고 있다. 그러나 단순한 정보 제공이 아닌 원격 제어, 콘텐츠 서비스 등의 경우에서 위치 정보에 대한 위변조 문제와 사용자의 프라이버시 문제가 발생할 것으로 예상된다. 기존의 위치 정보 보호에 대한 연구는 프라이버시 보호 측면을 위주로 하고 있으며, 인증에 대한 연구는 특정 센싱 기술에 특화되어 있거나, 네트워크상의 DNS를 통한 논리적인 위치 인증에 치우치고 있다. 본 연구에서는 위치 정보 기반 서비스에서의 보안 요구 사항을 분석하여, 기존의 위치 정보 보호 모델을 기반으로 위치 정보를 관리하는 신뢰되는 기관의 필요성을 논하며, 이를 토대로 타임스탬프나 키 갱신을 이용하는 두 가지 프로토콜을 제안한다.

I. 서론

휴대 무선통신기기 사용의 발전에 따라 단순히 전화나 데이터 통신 서비스만이 아닌 위치 기반 서비스의 비중이 점점 늘고 있다.

현재의 위치 기반 서비스는 내비게이션 등의 단순한 정보 제공의 수준에 머무르고 있으나, 유비쿼터스 환경에서는 차츰 위치 정보의 이용 범위가 확대되어 위치 정보를 통한 접근 관리 및 디지털 콘텐츠의 저작권 관리도 예상할 수 있다. 실제로 미국의 방송사인 ABC에서는 미국 내의 시청자들을 위해 인터넷을 통한 무료 드라마 스트리밍 서비스를 제공하고 있으며, 미국 외의 지역에서는 시청을 할 수 없다.

그러나 이러한 기술적 제한을 회피하고자 하는 여러 시도가 있으며[1], 이러한 시도를 통해 위치 정보의 위조가 가능하며, 네트워크 상의 DNS를 통한 위치 정보 확인이 아닌, 실제 물리적인 위치 정보를 통한 확인이 요구 된다. 한편, 위치 기반 서비스에서의 프라이버시 침해 가능성은 지속적으로 제기되고 있는 문제이기도 하다.

현재 위치 기반 서비스에서의 프라이버시 보호와 인증에 대한 여러 연구가 진행되고 있으나, 양자 모두를 만족하는 연구는 미진하며, 또한 인증에 대한 연구는 특정 하드웨어에 특화되어 있는 경우가 대다수이다.

따라서 본 논문에서는 위치 정보 보호에 대한 보안 요구 사항을 정리하여, 이를 위한 보안 모델을 제시하며, 프라이버시 보호와 인증이 가능한 프로토콜을 제시한다.

본 논문의 구성은 다음과 같다. 2장에서 관련 연구를 기술하며, 3장에서 보안 요구 사항에 대해 정리한 후, 4장과 5장에서 제안 모델과 프로토콜 소개, 6장에서 프로토콜의 안전성 분석 후, 그리고 마지막으로 7장에서 결론을 내린다.

II. 관련 연구

2.1 위치 정보 센싱 기술

위치 정보 센싱 기술은 GPS, Active Badge, Active Bats, MotionStar, Smart Floor, Easy Living, E911, SpotON 등 다양하게 연구되고 있다. 이러한 위치 정보 기술은 특성에 따라 여러 가지로 구분되고 있으며[2], 본 논문에서는 사용자가 스스로 위치 정보를 계산할 수 있는 Localized Location Computation (LLC)기능의 유무에 의한 구분에 주목한다. LLC의 기능이 없는 경우, 주변의 위치 정보 서버로부터 위치 정보를 전달 받게 된다. 이러한 범주에는 Cricket [3] 등 대부분의 위치 정보 센싱 기술이 속한다.

2.2 위치 정보 프라이버시 보호 모델

Geopriv Working Group은 위치 정보의 프라이버시 보호를 위한 위치 기반 서비스 구조에 대해 정의하고 있다 [4]. 이의 정의에 의하면, 위치 정보 생성자 (Location Generator), 위치 정보 서버 (Location Server), 정책 관리자 (Privacy Manager), 그리고 위치 정보 수신자 (Location Receiptment)의 4가지 컴포넌트로 구성되어 있으며, 이들의 역할에 의해 사용자 통제 모델, 사용자 중개 모델, 써드 파티 모델, 그리고 혼합 모델로 분류된다. 이 중 사용자 통제 모델은 LLC의 역할이 포함되며, 사용자 중개 모델은 포함되지 않는다.

2.3 위치 정보 인증

GPS 기반의 위치 정보 및 사용자 인증에 대해 [5]에서 연구되어 있다. 그러나 DGPS를 사용하며, 위치 정보 서명 센서 (Location Signature Sensor)를 통한 '위치 정보 서명'을 사용한다는 점에서 특정한 하드웨어를 필요로 한다. 한편, 위치 정보 교환 프로토콜 [6]은 RFID를 사용하여 사용자의 익명성을 보호하며 위치 정보를 검증하도록 하고 있다. 그 외, 전파의 속도를 이용한 연구 [7], Wi-Fi, Bluetooth 등을 사용한 연구 [8] 등이 있다. 그러나, 이러한 연구는 사용자에 대한 프라이버시 보호에 대한 고려는 결여되어 있으며, [8]의 경우, 위치 정보의 전달을 통해 위치 정보 위변조가 가능하다.

III. 보안 요구 사항

본 연구에서는 위치 정보 기반 서비스를 위한 보안 요구 사항을 다음과 같이 정리한다.

- **인증** - 서비스 제공자는 사용자의 위치 정보에 대한 확인이 가능해야 한다.
- **위변조 방지** - 공격자는 사용자의 위치 정보를 위변조할 수 없어야 한다. 또한, 사용자 역시 자신의 위치 정보를 위변조할 수 없어야 한다.
- **프라이버시** - 공격자는 사용자의 위치 정보를 알 수 없어야 한다. 또한, 서비스 제공자는 사용자의 위치 정보를 단지 필요한 정도만 알 수 있어야 한다.
- **재사용 방지** - 사용자의 위치 정보가 인증되고 서비스를 제공받았다면, 이후 그 위치 정보는 다시 사용될 수 없어야 한다.

IV. 제안 모델

대부분의 ,위치 정보 센싱 기술은 단독으로 프라이버시 보호와 인증을 보장하지 못한다. LLC가 가능한 경우, 사용자에 의해 위치 정보가 계산되므로, 위치 정보는 메시지 형태로 전달될 수 있으며, 프라이버시 보호가 상대적으로 수월하다. 그러나, 이러한 경우 사용자에 의한 위치 정보 위조가 가능하다는 문제점이 있다. [5]에서는 LLC가 가능한 GPS를 기반으로 하고 있으며, LSS라는 특수한 하드웨어를 사용하여 사용자의 위조 문제를 해결하고 있다.

위치 정보 서버를 사용하는 경우는 사용자의 위치 정보에 대한 계산을 제 3자에 의존하며, 사용자 위치에 대한 위조는 어렵지만, 프라이버시 문제에 대한 위험성이 높다. 또한, 위치 정보 서비스 제공자와 위치 정보 서버가 다른 경우, 역시 중간에 있는 사용자에 의한 위치 정보의 위변조가 발생할 가능성이 있다.

따라서, 본 논문에서는 Geopriv Working Group의 위치 정보 프라이버시 보호 모델을 기반으로 다음의 모델을 제안한다.

사용자와 위치 정보를 관리하는 신뢰할 수 있는 관리 기관, 그리고 서비스 제공자가 있다고 가정한다. 신뢰할 수 있는 관리 기관는 PKI에서의 Trusted Authority (TA)의 역할과 유사하다. TA와의 차이점은, TA가 공개키 혹은 세션 키에 대한 생성 및 배포를 담당하고 있으나, 제안 모델에서의 관리 기관은 사용자와 위치 정보 센싱을 하여 사용자의 위치 정보를 관리하며, 서비스 제공자에게 사용자 위치 정보에 대한 서명을 전달한다는 점에 있다.

제안 모델에서 사용자는 서비스 제공자에게 위치 기반 서비스를 요청하게 된다. 서비스 제공자는 사용자에게 위치 정보를 요구하고, 사용

자는 위치 정보 관리 기관에게 위치 정보에 대한 증명을 요구하게 된다. 위치 정보 관리기관은 요구에 따른 증명을 사용자에게 제공하고, 사용자는 위치 정보와 위치 정보의 증명을 서비스 제공자에게 전달한다. 서비스 제공자는 위치 정보를 검증한 후, 서비스 제공 여부를 판단한다.

본 모델에서 서비스 제공자와 위치 정보 관리 기관은 독립적이며, 따라서 서비스 제공자가 별도의 위치 정보 센싱에 대한 부담을 얻을 필요가 없다.

V. 프로토콜 설명

본 장에서는 앞 장에서 제안한 위치 기반 서비스 보안 모델을 기반으로 하여 위치 정보 기반 서비스에서 인증과 프라이버시 보호를 보장하는 두 가지 프로토콜을 제시한다. LAP-T는 타임스탬프를 사용한 프로토콜이며, LAP-K는 키 갱신을 사용한 프로토콜이다.

사용자 C는 공개키 쌍 (PK_C, SK_C)와 신뢰되는 관리 기관 OP와 공유하는 비밀키 K_C를 갖고 있다. 또한, OP는 공개키 쌍 (PK_{OP}, SK_{OP})와 C와의 공유 키 K_C, 서비스 제공자 SP와의 공유 키 K_{SP}를 갖고 있다. SP는 공개키 쌍 (PK_{SP}, SK_{SP})와 공유키 K_{SP}를 갖고 있다.

위치 정보 기반 서비스를 위해 C는 그의 위치 정보 $LocInfo$를 필요로 한다. C는 $LocInfo$를 위치 정보 센싱을 통해 얻는다. 위치 정보 센싱은 OP와 C 사이에서 이루어지며, 이 경우 LLC의 기능이 없는 경우는 OP에서 생성하여 C에게 전달하게 되고, 반대의 경우는 OP와 C 모두가 위치 정보 센싱이 가능해야 한다. DGPS의 경우가 후자에 해당한다. 이러한 위치 정보 센싱 과정은 임의의 위치 정보 센싱 기술을 사용하는 것으로 간주한다. 따라서 본 논문에서는 센싱을 통한 위치 정보 생성 과정에 대한 상세한 내용은 생략한다.

위치 정보 생성 후, SP의 인증 과정에서 아래의 두 가지 프로토콜을 사용한다.

- ***LAP-T***의 과정은 다음과 같다.

1) C는 SP에게 서비스 요청을 한다.

2) SP는 C의 위치 정보와 타임스탬프 TS를 요구한다.

3) C는 서비스 제공자의 ID인 ID_{SP}와 TS를 OP에게 인증 메시지와 함께 요구한다.

4) OP는 ID_{SP}의 K_{SP}와 PK_{SP}를 찾고, 역시 C 의 ID_C를 통해 $LocInfo$와 TS를 찾는다.

5) OP는 $M_{SP} = MAC_{K_{sp}}(ID_C, LocInfo, TS)$와 $M_C = MAC_{K_c}(ID_C, LocInfo, TS, M_C)$를 계산한다.

6) OP는 M_C, M_{SP}, TS를 C의 공개키 PK_C로 암호화하여 $E_{PK_c}(M_C, M_{SP}, TS)$를 생성하고 C에게 전달한다.

7) C는 $E_{PK_c}(M_C, M_{SP}, TS)$를 복호화하고, $M_{SP} = MAC_{K_c}(ID_C, LocInfo, TS, M_C)$가 일치하는 지 확인한다. 만약 다르다면 C는 OP에게 위 과정을 재요청한다.

8) C는 M_C, TS, $LocInfo$, ID_C를 SP의 공개키 PK_{SP}로 암호화하여 $E_{PK_{sp}}(ID_C, M_C, LocInfo, TS)$를 생성하고 ID_C와 함께 SP에게 전달한다.

9) SP는 $E_{PK_{sp}}(ID_C, M_C, LocInfo, TS)$를 자신의 개인키 SK_{SP}로 복호화한다. 만약 TS가 기한 만료가 되었다면 SP는 C에게 서비스 제공을 거부하고, 재요청한다.

10) SP는 $M_C = MAC_{K_{sp}}(ID_C, LocInfo, TS)$를 검사한다. 일치한다면 SP는 C의 위치를 인증한다.

- ***LAP-K***의 과정은 다음과 같다.

1) C는 SP에게 서비스 요청을 한다.

2) SP는 C의 위치 정보를 요구한다.

3) C는 서비스 제공자의 ID인 ID_{SP}를 OP에게 인증 메시지와 함께 요구한다.

4) OP는 ID_{SP}의 K_{SP}와 PK_{SP}를 찾고, 역시 C 의 ID_C를 통해 $LocInfo$를 찾는다.

5) OP는 $M_{SP} = MAC_{K_{sp}}(ID_C, LocInfo)$와 $M_C = MAC_{K_c}(ID_C, LocInfo, M_C)$를 계산한다.

6) OP는 M_C, M_{SP}를 C의 공개키 PK_C로 암호화하여 $E_{PK_c}(M_C, M_{SP})$를 생성하고 C에게 전달한다.

7) C는 $E_{PK_c}(M_C, M_{SP})$를 복호화하고, $M_{SP} = MAC_{K_c}(ID_C, LocInfo, M_C)$가 일치하는 지 확인한다. 만약 다르다면 C는 OP에게 위

과정을 재요청한다.

8) C는 M_C, $LocInfo$, ID_C를 SP의 공개키 PK_{SP}로 암호화하여 $E_{PK_{SP}}(ID_C, M_C, LocInfo)$를 생성하고 ID_C와 함께 SP에게 전달한다.

9) SP는 $E_{PK_{SP}}(ID_C, M_C, LocInfo)$를 자신의 개인키 SK_{SP}로 복호화한다. SP는 $M_C = MAC_{K_{SP}}(ID_C, LocInfo)$를 확인하고, 일치하는 경우 C의 위치를 인증한다.

10) SP는 OP에게 키 갱신을 요청한다.

VI. 안전성 분석

6.1 인증

SP는 C의 위치 정보인 $LocInfo$를 해시 함수를 통한 $MAC_{K_{SP}}(ID_C, LocInfo)$를 통해 검증할 수 있다. C가 $LocInfo$를 다른 사용자 C'에게 전달하는 경우 SP는 이러한 위조를 알 수 있다. C와 C'는 K_{SP}에 대한 정보가 없기 때문이다. C'가 SP를 속이는 것에 성공하는 확률은 메시지 길이 n에 대해 $1/2^n$이며, 무시할 수 있다.

6.2 위변조 방지

C는 $LocInfo$를 메시지 형태로 암호화하여 전달한다. 이 경우 공격자의 변조 가능성은 사용되는 암호 기법의 안전성에 좌우된다. 또한, C가 $LocInfo$를 변조하여 $LocInfo'$를 생성하는 경우 역시 사용되는 해시 함수의 안전성에 좌우된다.

6.3 프라이버시

공격자는 암호화된 C의 $LocInfo$를 알 수 없으며, 성공확률은 역시 사용된 암호 기법의 안전성에 좌우된다. 또한, SP는 C의 $LocInfo$를 메시지 형태로 전달받으므로, 필요한 수준의 위치 정보만 얻을 수 있게 된다. Geopriv Working Group에 의해 위치 정보의 형식은 국가, 도시, 거리 등의 필드가 정의되어 있다. 필요한 필드만 전달하는 것이 가능하다.

6.4 재사용 방지

위치 정보 $LocInfo$를 재사용하거나 오랜 시간이 지난 후 사용하고자 하는 경우, OP는 C가 보관하고 있는 $MAC_{K_{SP}}(ID_C, LocInfo)$에 사용된 K_{SP}를 일정 시간이 지난 후 취소하거나, 한번 사용된 경우 갱신할 수 있다. 또한 $TLAP$의 경우, SP에 의해 TS를 확인할 수 있다.

VII. 결론

본 논문에서는 물리적인 위치 정보를 사용하는 위치 정보 기반 서비스에서의 프라이버시 보호 및 인증 모델과 이를 기반으로 하는 프로토콜을 제시하고 있다. 따라서 기존의 위치 정보 프라이버시 보호 모델을 보완할 수 있으며, 또한 특수한 하드웨어를 요구하지 않는 범용성을 추가적으로 얻을 수 있다.

본 연구를 통해 점차 응용 범위가 넓어지고 있는 위치 정보 기반 서비스에서 보안 서비스의 제공을 용이하게 할 수 있을 것으로 예상된다.

[참고문헌]

[1] Ultraresearch, http://www.ultrareach.com/company/

[2] G.Roussos, Location Sensing Technologies and Applications, JISC 2002

[3] N.B.Priyantha, A.Chakraborty, H.Balakrishnan, The Cricket Location-Support system, Proc. 6th ACM MOBICOM, Boston, MA, Aug, 2000

[4] http://www.ietf.org/html.charters/geopriv-charter.html

[5] D.E.Denning, P.F.Macdoran, Location-Based Authentication: Grounding Cyberspace for Better Security, Computer Fraud & Security, Feb, 1996

[6] K.Kakanishi,J.Nakazawa,LEXP:Preserving User Privacy and Certifying the Location Information,Security workshop of Ubicomp 2003

[7] N.Sastry,U.Shankar,D.Wagner,Secure Verification of Location Claims, WiSE'03, Sep 19, 2003

[8] T.Kindberg,K.Zhang,Context Authentication Using Constrained Channels, HPL-2001-84, HP, Apr. 2, 2001