위치 정보 기반 어플리케이션을 위한 사용자 위치 정보 관리 메커니즘

장요철*, 최창열, 김성수
아주대학교 정보통신전문대학원
e-mail : {ggdoll, clchoi, sskim}@ajou.ac.kr

A Privacy Management Mechanism for Location Based Application

Yo-cheol Jang*, Changyeol Choi, Sungsoo Kim
Graduate School of Information and Communication, Ajou University

요 약

사용자 위치 정보를 보호하기 위해서는 암호화 작업이 필수적이며, 최근 위치 정보 기반 어플리케이션에 적용하기 위한 방안이 커다란 논점으로 자리잡고 있다. 그러나 데이터 암호화 작업은 일정한 시간을 소요하는 작업이므로, 이에 따른 시스템 운용에 있어서 속도와 보안 사이의 균형 문제가 야기 된다. 따라서 본 논문에서는 성능 측면에서 대립되는 속도와 보안 관련 문제를 통제할 수 있는 사용자 위치 정보 관리 메커니즘을 설계하였다. 이를 위해, 그 동안 연구되었던 각종 암호화 알고리즘에 대한 성능 분석과 함께 위치 정보에 대한 분류 작업을 수행하였으며, 해당 연구 결과를 토대로 하여 사용자 위치 정보 관리 메커니즘을 설계하였다. 따라서 본 메커니즘은 다변화하는 주변 환경에 적응적으로 대처하여 시스템의 성능을 항상 최적화할 수 있도록 한다.

1. 서론

최근 사용자들은 다양한 모바일 장치를 사용하고 이러한 장치를 이용한 많은 어플리케이션이 개발되면서, 특히 위치 정보 기반 어플리케이션 영역이 두드러지게 발전하였다 [1,2]. 위치 정보 기반 어플리케이션이란 사용자의 위치에 따라 서비스의 양상이 달라지는 어플리케이션을 의미하며, 예를 들어 자동차 네비게이션 (Navigation) 서비스, 안내 (Guide) 서비스, 사용자가 도서관에 들어갔을 때 자동적으로 핸드폰을 매너모드로 바꾸어주는 서비스 등이 있다.

위치 정보를 얻기 위해서 GPS (Global Positioning System), Wi-Fi (Wireless Fidelity), USN (Ubiquitous Sensor Network), 그리고 RFID (Radio Frequency Identification) 와 같은 다양한 기술을 이용할 수 있다 [3]. 그러나 이러한 기술의 발달은 외부의 악의적인 공격자에게 사용자의 위치 정보가 유출될 가능성을 높이는 결과를 초래한다. 따라서 부정한 방법으로 유출된 사용자의 위치 정보는 악의적인 목적으로 이용될 수 있으므로, 위치 정보의 보안 문제는 위치 정보 기반 어플리케이션에 있어서 큰 문제가 되고 있다.

이러한 문제를 해결하기 위해서 데이터 암호화 기술이 쓰여지고 있지만, 암호화 과정은 많은 시간을 필요로 하는 작업인데 반해, 위치 정보 기반 어플리케이션의 운용 환경이 대부분 일반 PC 보다 낮은 사양의 성능을 갖기 때문에 시스템 운용 시간의 상당량이 데이터 암호화 과정에 소모되어 결국 사용자의 시스템 성능을 현저히 떨어뜨리는 결과를 낳게 된다.

본 논문에서는 이러한 문제를 해결하기 위해 두 개의 대치되는 요소인 속도와 보안, 이 두 가지를 통제할 수 있는 사용자 위치 정보 관리 메커니즘을 설계하였다. 본 메커니즘은 동적 보안 기술을 이용해 사용자의 위치 정보 유출을 막으면서 암호화 작업 시간을 최소화한다.

본 연구는 정보통신부 21 세기프론티어연구개발사업의 일환으로 추진되고 있는 유비쿼터스컴퓨팅네트워크원천기술개발사업의 지원에 의한 것임.
이 논문은 2005 년도 두뇌한국 21 사업에 의하여 지원되었음.

2. 위치 정보

기술적인 진보는 개인의 사생활 노출 문제를 야기시켰고 이러한 문제를 해결하고자 데이터 암호화 기술이 사용되었지만, 과거의 정적인 보안 정책에는 한가지 문제점이 있다 [3,4]. 즉, 데이터의 중요도에 관계 없이 한가지 암호화 기술을 모든 데이터에 적용한다는 점이다. 그 결과, 암호화 시간은 데이터 처리 과정에서 매우 큰 비중을 차지하게 되었다.

암호화 시간은 각기 다른 플랫폼에서 각기 다른 양상을 보이는데, 이 특성은 표 1 에서의 Palm M130 과 Sony Ericsson P800 장치에서의 다양한 암호화 알고리즘의 성능 분석 결과에서 알 수 있다 [5].

표 1. 알고리즘 성능 분석의 예

장치	프로세서	암호화 속도
Palm M130	Motorola Dragonball VZ 33 Mhz	Rijndael < 3-DES < Serpent < Skipjack < RC2 < AES Light < DES < IDEA < CAST6 < RC6 < AES < CAST5 < Twofish < AES Fast < RC5 32-bits < Blowfish < RC5 64-bits < RC4
Sony Ericsson P800	32-bit RISC ARM9 156 Mhz	Rijndael < 3-DES < Serpent < CAST6 < AES < AES Light < Skipjack < RC2 < IDEA < CAST5 < RC6 < DES < Twofish < RC5 32-bits < Blowfish < AES Fast < RC5 64-bits < RC4

표 1 에서 보여지듯이, 각 장치에서의 암호화 속도는 큰 차이점을 보이며, 동일한 알고리즘이라도 그 성능이 장치 별로 달라진다. 예를 들어 Palm M130 모델에서는 RC6 가 DES 보다 빠르나, Sony Ericsson P800 모델에서는 그렇지 않다. 따라서 우리는 대상 데이터를 암호화 하기 위해 각 장치에 최적의 알고리즘을 적용해야만 한다. 위치 정보 기반 어플리케이션에서의 대상 데이터는 위치 정보이다. 표 2 는 "Where is Jane?" 이라는 위치 정보 질의에 대한 결과물이다.

표 2. 위치 정보 질의 결과 "Where is Jane?"

	레벨 1	레벨 2	레벨 3	레벨 4
상대적	방안에 있다	401호에 있다	팔달관 401호에 있다	아주대학교 팔달관 401호에 있다
절대적	위도 37, 경도 127	위도 37-16, 경도 127-03	위도 37-16-31, 경도 127-03-15	위도 37-16-31.8529, 경도 127-03-15.2638
	낮은 상세도			높은 상세도

위치 정보는 정보 제공자에 따라 크게 2 가지로 구분 된다. 상대적 위치 정보는 RFID, USN, 스케쥴러에 의해서 얻어진 것들이며, 반면에 절대적 위치 정보는 GPS, Wi-Fi, 휴대폰 등을 통해서 얻어진 것들이다. 더 나아가 위치 정보는 정보의 상세도에 따라서 레벨 별로 구분되며 상세도는 정보의 사적인 정도를 나타내는 척도가 된다. 사용자는 낮은 레벨의 정보에 대해 많은 암호화 시간을 허비하지 않기를 원하기 때문에 과거와 같은 정적인 보안 정책을 채택해서는 안 된다. 따라서 다음 장에서는 동적인 보안 기술을 채택한 사용자 위치 정보 관리 메커니즘에 관해 설명한다. 즉, 본 메커니즘은 위치 정보의 레벨에 따라 각기 다른 암호화 알고리즘을 적용하여 위치 정보 기반 어플리케이션 시스템의 성능을 높이고자 한다.

3. 시스템 설계

3.1 사용자 위치 정보 관리 메커니즘

위치 정보 기반의 어플리케이션이 정상적인 동작을 하기 위해서는 적절한 레벨의 사용자 위치 정보가 요구된다. 만약 요구되는 정보 레벨이 충분히 낮은 경우 정보를 암호화할 필요가 없게 된다. 이와 같이, 암호화 작업의 오버헤드가 제거되므로 위치 정보 기반 어플리케이션은 정보 제공자로부터 훨씬 빠르게 사용자의 위치 정보를 얻을 수 있게 된다. 이 경우 사용자의 사생활 보호까지 보장되게 되는데, 이것이 사용자 위치 정보 관리 메커니즘의 핵심 아이디어이다. 다시 말해, 본 논문에서 제안하는 메커니즘은 시스템의 총 암호화 시간을 최소화하는 것을 목표로 한다. 본 위치 정보 관리 메커니즘은 그림 1 에서 살펴볼 수 있다.

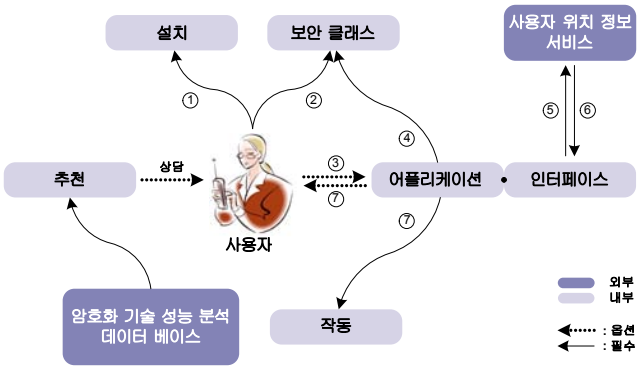

그림 1. 사용자 위치 정보 관리 메커니즘

• 새로운 어플리케이션 설치 (1, 2 단계)

사용자가 새로운 어플리케이션을 장치에 설치한다. 어플리케이션은 사용자에게 표 3 과 같이 요구되는 최소 정보를 알려준다. 사용자는 해당정보가 자신에게 얼마나 중요한가를 판단하여 어플리케이션에 적합한 보안 기술을 채택한다. 어플리케이션은 사용자에게 다음과 같은 보안 정책에 대한 추천을 하도록 한다.

- 표 1 과 같은 사용자 장치에서의 암호화 알고리즘의 성능 평가 자료를 제공한다.
- 어플리케이션 제작사가 추천하는 보안 기술

표 3. 위치 정보 기반 어플리케이션의 최소 정보 요구

어플리케이션	최소 정보 요구
자동차 네비게이션	도-분-초 형태의 위도, 경도 위치 정보
핸드폰 자동 매너 모드 서비스	도서관에 들어갔는가?

사용자는 표 4 와 같이 자신이 선택한 기술을 보안 클래스에 기록하며, 사용자의 장치에 설치되어 있는 위치 정보 기반 어플리케이션에 설정된 보안 정책 또한 보안 클래스에 기술되어 있다.

표 4. 보안 클래스의 예

어플리케이션	보안 기술	추천 보안 기술
자동차 네비게이션	3-DES	DES
핸드폰 자동 매너 모드 서비스	No encryption	RC4

사용자는 2 개의 자동차 네비게이션과 핸드폰 자동 매너 모드 서비스를 등록하였고, 이중 자동차 네비게이션 서비스는 보안 기술로서 DES 알고리즘을 추천하였다. 하지만 사용자는 DES 보다 암호화 시간이 긴 3-DES 알고리즘을 선택하였다. 이는 사용자가 자동차 네비게이션 서비스에 이용되는 자신의 위치 정보가 사적으로 매우 중요하다고 생각하기 때문이다.

• 어플리케이션의 보안 정책 추천

어플리케이션은 사용자에게 적절한 보안 정책을 추천하는데, 이는 사용자로 하여금 적합한 보안 정책을 수립하도록 돕기 위함이다. 이 때, 어플리케이션은 표 1 과 같은 알고리즘 성능 분석 자료를 이용한다. 장치별로 각 암호화 알고리즘의 성능이 다르므로, 이러한 정보는 사용자의 장치에 최적화된 보안 정책을 수립하는데 있어 필수적이다.

• 어플리케이션 동작을 위한 준비 (3, 4 단계)

세 번째 단계는 사용자의 명령을 받는 일을 수행한다. 예를 들어, 자동차 네비게이션의 경우 사용자가 “목적지까지의 최단 경로를 찾아라” 라는 것과 같다. 네 번째 단계는 어플리케이션이 보안 클래스를 통해 사용자 위치 정보를 전달하는데 적용할 보안 기술을 알아오는 작업이다. 어플리케이션과 사용자 위치 정보 서비스간에 정보를 주고 받을 시에는 반드시 해당하는 암호화 기술을 통해 전달이 이루어 진다.

• 어플리케이션과 사용자 위치 정보 서비스 간의 데이터 교환 (5, 6 단계)

어플리케이션은 사용자 위치 정보 서비스 인터페이스를 통해 현재 사용자의 위치 정보를 얻어온다.

• 어플리케이션 작동 (7 단계)

5, 6 단계에서 수집된 사용자 위치 정보를 토대로 어플리케이션의 작동이 이루어지는 단계이다. 예를 들어, 자동차 네비게이션 서비스가 현재 사용자의 위치를 지도상에 표시해주는 것과 같다.

3.2 사용자 위치 정보 서비스

1 장에 언급하였듯이, 위치 정보 기반 어플리 케이션은 다양한 정보 제공자로부터 사용자의 위치 정보를 얻을 수 있다. 모든 제공자가 동일한 인터페이스를 제공하는 것이 아니므로, 각 제공자에게 접속 가능한 인터페이스를 구현해야 한다. 그러나 이러한 특성은 새로운 인터페이스를 설치할 때마다 사용자의 장치를 무겁고 느리게 만들 가능성이 존재한다. 본 논문에서는 이러한 문제를 해결하기 위해 사용자 위치 정보 서비스를 설계하였다. 이 서비스는 개인 위치 정보를 모아서 허가된 클라이언트들에게 제공하는 역할을 한다. 그림 2 에서 볼 수 있듯이, 사용자 위치 정보 서비스는 여러 하위의 정보 제공자를 합쳐 놓은 하나의 가상 정보 제공자이다 [4]. 결국, 클라이언트 장치는 단지 사용자 위치 정보 서비스 인터페이스 만으로 위치 정보를 획득할 수 있게 된다.

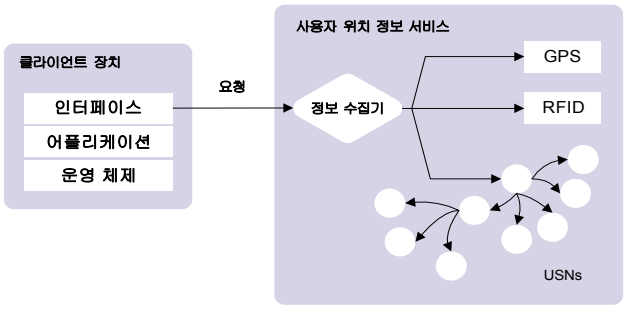

그림 2. 사용자 위치 정보 서비스 구조

3.3 동적 보안 클래스

사용자의 기호는 상황에 따라 변하는데, 보안 클래스 역시 사용자가 시스템의 우선순위를 속도에 두느냐, 보안에 두느냐에 따라 바뀌기 마련이다. 그러므로 사용자 위치 정보 관리 메커니즘은 보안클래스를 수정할 수 있는 기능을 갖추도록 하였다. 이때 중요한 것은 위치 정보 전송 프로세스 (5, 6 단계) 도중에는 보안 클래스의 수정이 발생해서는 안 된다는 점이다. 이러한 기능은 임계 구역을 이용한 다음 그림 3 의 알고리즘을 통해 작동한다.

- 위치 정보 서비스와 어플리케이션 간의 통신 알고리즘

```
while (enter critical section(LBA)) ;
location information request();
receiving message from PLIS();
exit critical section (LBA);
```

- 보안 클래스 수정 알고리즘

```
if (new measure == old measure)
    return ;
else
    while  (enter critical section(LBA)) ;
    old measure  = new measure;
    exit critical section (LBA);
```

그림 3. 동적 보안 클래스를 위한 알고리즘

4. 성능 분석

4.1 성능 분석 모델

제안한 메커니즘은 위치 정보 보호와 사용자 시스템의 성능 향상 즉, Serviceability 향상을 위한 것으로, 성능 분석 모델을 다음과 같이 정의하며, 이는 사용자 시스템의 Serviceability 를 측정하기 위한 것이다.

$$serviceability = \frac{T-t}{T} \times \frac{(T-t)\times a + t\times(a-b)}{T\times a},$$
$$= \frac{(T-t)\times(aT-l)}{T^2\times a},$$
$$t = \frac{l}{b} \qquad (b \neq 0)$$

T 는 전체 시스템 운용 시간 (초) 을 의미하고, t 는 암호화 작업에 사용된 시간 (초) 을 뜻한다. 그리고 a 는 최대 이용 가능한 네트워크 대역폭 (비트/초), b 는 암호화 알고리즘의 초당 암호화 가능한 데이터 양 (비트) 을 말하며, l 은 암호화 대상 텍스트의 길이 (비트) 를 뜻한다.

4.2 Serviceability 분석

본 논문에서 "Serviceability = 1" 은 모든 리소스가 공급 가능하다는 뜻을 갖는다. 반대로 0 에 가까워 질수록 사용자의 장치에는 남아있는 유휴 프로세스나 네트워크 대역폭이 없다는 의미를 갖는다. 그림 4 는 정보의 양이 많거나 낮은 속도의 알고리즘이 채택되었을 때, Serviceability 가 떨어지는 모습을 보여준다.

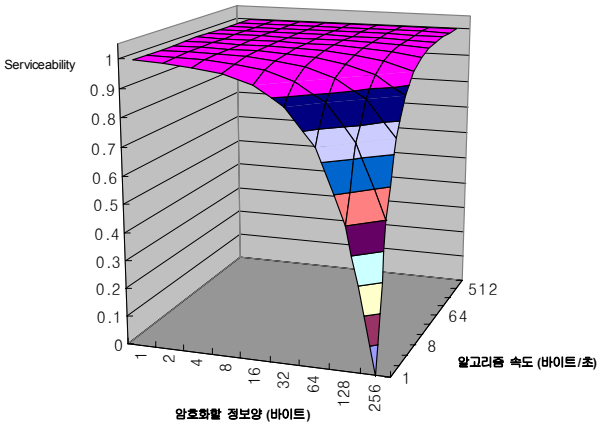

그림 4. Serviceability 측정 (T = 250 초, a = 1 메가 비트/초)

제안한 위치 정보 관리 메커니즘은 사용자로 하여금 최상-최하의 Serviceability 를 얻을 수 있도록 해준다. 이것은 곧 사용자의 기호에 따라 달라진다. 사생활 보호에 있어서 사용자의 허가는 최우선 사항이므로 이러한 특성은 필수적이라고 할 수 있다. 만약 사용자가 서비스의 속도만을 최우선시 한다면, 속도가 빠른 알고리즘을 선택하거나 보안 정책을 수립하지 않을 수 있다. 그림 5 는 Palm M130 장치에서의 가장 빠른 알고리즘과 가장 느린 알고리즘상에서의 Serviceability 를 비교한 것이다. 그래프에서 알 수 있듯이 정보양이 늘어나면서 급격한 Serviceability 감소가 일어난다. 물론 사용자가 어떤 선택을 할지는 모르지만, 본 위치 정보 관리 메커니즘을 통해 최상의 시스템 성능을 유지할 수 있다.

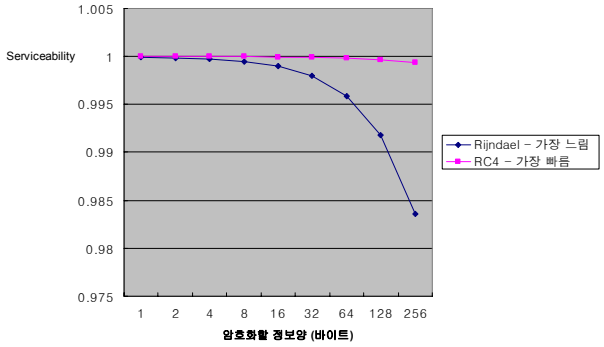

그림 5. Palm M130 에서의 Serviceability 측정

5. 결론

본 논문에서는 사용자 위치 정보를 다루는데 있어 2 개의 충돌하는 요소인 속도와 성능을 제어할 수 있는 메커니즘을 제안하였다. 또한 각종 암호화 알고리즘에 대한 성능 분석 및 위치 정보에 대한 분류 작업을 통해 동적 보안 정책 기능을 부여하였다. 그 결과 사용자 시스템의 성능을 최적화할 수 있었으며, 동적 보안 클래스의 개념을 통해 다변화하는 유비쿼터스 환경에도 사용 가능하게 되었다. 향후에는 사용자 위치 정보 관리 메커니즘의 핵심 요소인 사용자 위치 정보 서비스에 대한 연구를 수행할 예정이다.

참고문헌

[1] G. Myles, A. Friday, and N. Davies, "Preserving Privacy in Environments with Location-Based Applications," *IEEE Pervasive Computing, Vol.* 2, *No.* 1, pp. 56-64, Jan. 2003.

[2] M. Gruteser and X. Liu, "Protecting Privacy in Continuous Location-Tracking Applications," *IEEE Security and Privacy, Vol.* 2, *No.* 2, pp.28-34, Mar. 2004.

[3] U. Hengartner and P. Steenkiste, "Implementing Access Control to People Location Information," *Proceedings of Ninth ACM Symposium on Access Control Models and Technologies,* pp. 11-20, June 2004.

[4] G. Judd and P. Steenkiste, "Providing Contextual Information to Pervasive Computing Applications," *Proceedings of First IEEE International Conference on Pervasive Computing and Communications,* pp. 133-142, Mar. 2003.

[5] B. Filho, et al., "PEARL: a PErformance evaluAtor of cRyptographic aLogarithms for Mobile Devices," *Proceedings of First Mobility Aware Technologies and Applications,* pp. 275-284, Oct. 2004.