위치정보 기반 어플리케이션을 위한 동적 암호화 메커니즘

장요철°, 최창열, 김성수
아주대학교 정보통신전문대학원
{ggdoll°, clchoi, sskim}@ajou.ac.kr

Dynamic Encryption Mechanism for Location Information Based Application

Yocheol Jang°, Changyeol Choi, Sungsoo Kim
Graduate School of Information and Communication, Ajou University

요 약

위치정보는 최근 모바일 장치 및 그 어플리케이션의 발달에 따라 커다란 논점이 되고 있다. 위치정보는 매우 개인적인 특성을 갖는 점에서 암호화 과정이 필수적이다. 하지만 이러한 암호화 작업은 일정한 시간을 소요하는 작업이다. 이는 현재 무선 데이터 전송 속도 및 모바일 장치의 프로세스 능력을 감안할 때 시스템에 있어 무시할 수 없는 성능 저하를 가져오게 된다. 따라서 본 논문에서는 이러한 모바일 장치의 성능 저하를 최소화 할 수 있는 동적 암호화 메커니즘을 설계하였다. 이를 통해 시스템의 성능과 보안 수준간의 적절한 균형을 유지하여 시스템 최적화에 기여한다.

1. 서 론

유비쿼터스 시대를 주창하는 현재, 다양한 모바일 장치들이 사용되면서 이러한 장치를 위한 수 많은 어플리케이션이 개발되고 있으며, 특히 위치정보 기반 어플리케이션 영역이 두드러지게 발전하고 있다[1, 2]. 위치정보 기반 어플리케이션이라 함은 사용자의 위치에 따라 서비스 양상이 달라지거나 위치정보를 주처리 데이터로 삼는 어플리케이션을 의미한다. 예를 들어 자동차 네비게이션(Navigation) 서비스, 안내(Guide) 서비스, 그리고 센서 네트워크 등이 있다.

위치정보는 다양한 소스를 통해 쉽게 얻을 수 있다. 위치정보를 얻기 위한 수단으로는 GPS(Global Positioning System), Wi-Fi(Wireless Fidelity), USN(Ubiquitous Sensor Network), 그리고 RFID (Radio Frequency Identification) 등이 있다[3]. 하지만 이러한 무선 네트워크 환경의 등장에 따라 새로운 유형의 보안 문제가 생겨나고 있다. 실제 무선 랜 환경의 예를 보면, 노트북과 무선 네트워크 카드만 있다면 누구나 무선 네트워크 상에 떠다니는 패킷을 가로챌 수 있다. 이와같은 무선 네트워크의 개방성(Openness)은 악의적인 스니핑(Sniffing), 인터셉션(Interception)이나 엿듣기(Eavesdropping) 등의 무선 네트워크 공격 기술을 가능하게 한다. 이와 같은 이유로 128비트 암호화 기술인 WEP(Wired Equivalent Privacy) 등의 알고리즘을 이용하여 무선 네트워크 보안에 힘쓰고 있다.

그러나 이러한 암호화 과정은 많은 시간과 프로세싱 파워를 소모하는 작업이다. 이에 반해 위치정보 기반 어플리케이션의 운용 환경이 대부분 일반 PC 보다 낮은 사양의 성능을 갖기 때문에 결과적으로 시스템 성능에 많은 부담을 안겨주게 된다. 특히 USN 환경에 접어들면서 전력 소모에 대한 문제가 급부상하고 있는 실정이므로 이러한 문제는 쉽게 간과할 수 없다.

본 논문에서는 이러한 문제를 해결하기 위해 두 개의 대치되는 요소인 시스템의 성능 유지와 보안을 조절할 수 있는 동적 암호화 메커니즘을 설계하였다. 본 메커니즘은 동적인 암호화를 통해 위치정보에 대한 보안을 유지하면서 암호화 작업 시간을 최소화 한다. 그리고 사례 연구로서 현재 센서 네트워크에서 가장 널리 사용되고 있는 Atmel 사의 AVR 시리즈를 통해 본 메커니즘의 효과를 검증한다[4].

2. 위치정보 관리 시스템

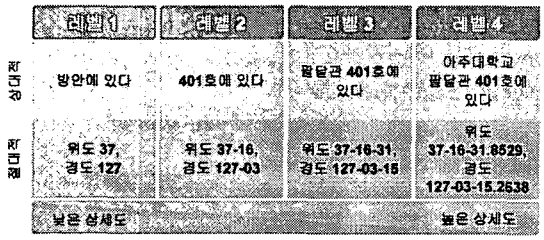
2.1 위치정보

위치정보는 정보 제공자에 따라 크게 상대적 정보와 절대적 정보, 2가지로 구분할 수 있는데, 상대적 위치정보는 RFID, 스케쥴러 등에 의해서 얻어진 것들이며, 반면에 절대적 위치정보는 GPS, Wi-Fi, USN 등을 통해서 얻어진 것들이다. 더 나아가 위치정보는 정보의 상세도에 따라서 레벨별로 구분되며 상세도는 정보의 개인적인

본 연구는 21세기프론티어연구개발사업의 일환으로 추진되고 있는 정보통신부의 유비쿼터스컴퓨팅네트워크원천기술개발사업의 지원에 의한 것임.

정도나 사적인 정도를 표현하는 척도가 된다. 표 1은 위치정보 질의 "Where is Jane?" 에 대한 결과물이다.

표 1. 위치정보 질의 결과 "Where is Jane?"



사용자는 낮은 레벨의 정보에 대해 많은 암호화 시간을 허비하지 않기를 원하기 때문에 그에 따른 암호화 정책에 변화가 필요하다. 본 동적 암호화 메커니즘은 위치정보의 레벨에 따라 각기 다른 암호화 알고리즘을 적용하여 시스템 성능을 높이고자 한다.

2.2 동적 암호화 메커니즘

그림 1은 동적 암호화 메커니즘과 사용자 위치정보 관리 메커니즘간 관계를 보여준다[5]. 동적 암호화 메커니즘은 사용자 위치정보 관리 메커니즘 내에 구현되어 있으며, 사용자 및 사용자의 보안 클래스 그리고 위치정보 기반 어플리케이션 간의 상호 관계로 표현된다.

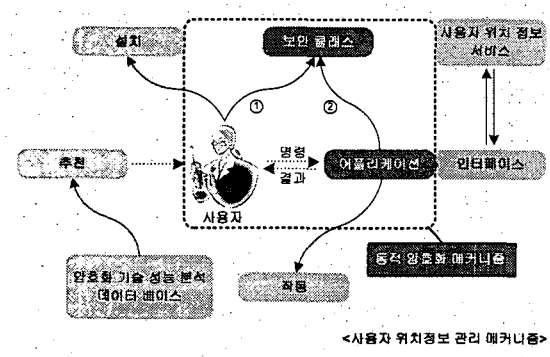


그림 1. 동적 암호화 메커니즘의 구성도

● 보안 클래스 등록 (①단계)

사용자는 표 2와 같이 어플리케이션에 알맞다고 판단한 암호화 기술을 보안 클래스에 등록하게 된다. 이러한 보안 클래스는 사용자의 기호에 따라 언제든지 수정이 가능하다. 표 2의 사용자는 자동차 네비게이션과 가이드 서비스를 사용하며, 각각 3-DES와 RC4를 선택하였다. 사용자 또는 시스템 관리자는 다음의 표 3과 같은 암호화 알고리즘 분석 자료를 이용하여 보안 클래스에 자신이 원하는 보안 수준 및 시스템 성능을 고려해 암호화 기술을 등록하게 된다[6]. 이를 통해 대상 시스템은 사용자의 기호에 따라 최적화되게 된다.

표 2. 보안 클래스의 예

어플리케이션	보안 기술	추천 보안 기술
자동차 네비게이션	3-DES	DES
가이드 서비스	RC4	RC4

표 3. 암호화 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

● 암호화 기술에 대한 선택 (②단계)

어플리케이션이 보안 클래스를 통해 사용자 위치정보를 암호화 하는데 적용될 보안 기술이 무엇인지를 확인 및 선택하는 과정이다. 사용자 위치정보 서비스와 데이터 교환 시에는 반드시 선택된 암호화 기술을 통해 이뤄진다. 표 2의 예를 보면 가이드 서비스 어플리케이션의 경우 RC4 알고리즘을 선택하여 작동하게 된다.

3. 성능 분석

3.1 성능 분석 모델

본 논문에서 제안한 메커니즘은 위치정보 보호와 사용자 시스템의 성능 향상, 결과적으로 Serviceability 향상을 위한 것으로, 성능 분석 모델을 다음과 같이 정의하며, Serviceability 값은 0 과 1 사이의 임의 값을 갖게 된다. Serviceability 값이 1 에 가까울수록 모든 리소스가 공급 가능하다는 뜻을 가지며 반대로 0 에 가까워 질수록 사용자의 장치에는 남아있는 유휴 프로세스나 네트워크 대역폭이 없다는 의미를 갖는다.

$$serviceability = \frac{T-t}{T} \times \frac{(T-t)\times a + t\times(a-b)}{T\times a},$$

$$= \frac{(T-t)\times(aT-l)}{T^2\times a},$$

$$t = \frac{l}{b} \qquad (b \neq 0)$$

'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 텍스트 (일반 텍스트, Plain Text) 의 길이 (비트) 를 뜻한다.

3.2 사례 연구: RC5

사례 연구로서 센서 네트워크에서 널리 사용되고 있는 Atmel 사의 ATmega128: AVR 8-bit RISC 마이크로 컨트롤러를 이용하였다[4]. ATmega128은 4Kbytes의 내부 SRAM을 가지며 18.432MHz의 외부 클럭을 입력해주었다[7]. 암호화 알고리즘으로는 RSA의 RC5를 선택하였다. 그 이유로는 모든 종류의 암호화 알고리즘을 구현하는 것은 한계가 있고, RC5의 가변 라운드 특성을 이용함으로써 그 한계를 어느 정도 해소할 수 있기 때문이다. RC5 알고리즘에서는 라운드 횟수를 조절하는 것만으로 암호화 속도와 암호화 강도를 조절할 수 있다. 실제 실험에서는 각기 다른 크기의 입력 데이터와 라운드 수를 통해 10,000 회 테스트를 수행하였다. 다음은 실험 환경의 기본 설정 값이다.

- 입력 데이터 크기: 8, 16, 32, 64, 128, 256 Bytes
- RC5 라운드: 1~255 라운드
- RC5 암호화 키 크기: 16 Bytes
- 컴파일러: avr-gcc 버전 3.4.1 (최적화 레벨 1에서 컴파일)

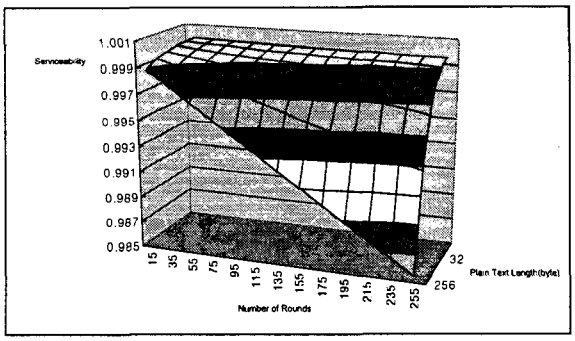


그림 2. RC5 의 Serviceability 측정
(T = 250초, a = 1Mbit/초)

그림 2는 RC5의 Serviceability의 측정 결과를 나타내고 있다. RC5는 실험에 사용된 테스트베드에서 최대 25Kbit/초 (1 라운드), 최저 2.2Kbit/초 (255 라운드) 의 처리량을 보이는 매우 속도가 빠른 알고리즘이다.

그림 3은 RC5의 일반 텍스트(Plain Text)의 길이에 따른 Serviceability 측정 결과를 보여준다. 그림 3의 오른쪽에는 각 그래프의 라운드 수를 나타낸다. 라운드 수를 암호화 알고리즘의 처리량으로 해석해보면, 가장 빠른 알고리즘은 15 라운드가 되며 가장 느린 알고리즘은 255 라운드가 된다. 그림 3 에서 볼 수 있듯이 일반 텍스트의 길이가 커질수록 가장 빠른 알고리즘과 느린 알고리즘 사이에 Serviceability의 차이가 벌어지는 것을 볼 수 있다. 이는 그만큼 동적 암호화 알고리즘을 이용하였을 때 최대 그 차이만큼의 시스템 성능을 보완할 수 있다는 것을 의미한다.

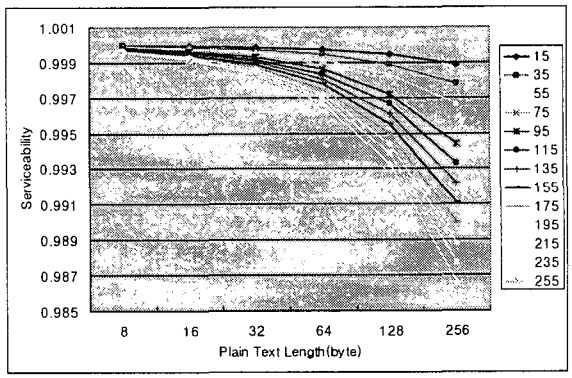


그림 3. 일반 텍스트 길이에 따른 RC5 의
Serviceability 측정 (T = 250초, a = 1Mbit/초)

4. 결론

본 논문에서는 위치정보 암호화 과정에서 발생할 수 있는 시스템 성능 저하 문제를 보완하기 위한 동적 암호화 메커니즘을 제안하였다. 각종 암호화 알고리즘에 대한 성능 분석을 기반으로 작성된 보안 클래스를 기반하여 선택적인 암호화 정책을 통해 동적 암호화 메커니즘을 수립하였다. 그 결과 사용자 시스템의 성능을 최적화할 수 있었으며 더 나아가 다변화하는 유비쿼터스 환경에 적합한 어플리케이션 작성에 도움을 줄 것으로 기대된다.

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] 박승민, "센서 네트워크 노드 플랫폼 및 운영체제 기술 동향," 전자통신동향분석, 제21권, 제1호, pp. 14-24, Feb. 2006.

[5] Y. Jang, C. Choi, and S. Kim, "Privacy Management Mechanism for Location Based Application with High Performance," Proceedings of the IASTED International Conference on Communication Systems and Applications, pp. 96-101, July 2005.

[6] 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.

[7] Atmel Corporation: ATmega128 (L) Complete Datasheet, http://atmel.com/dyn/resources/prod_documents/doc2467.pdf