RFID/USN 환경에서 Hash Lock과 PKI 방법을 이용한 인증 프로토콜의 설계

최용식° 신승호
인천대학교 컴퓨터공학과
{mars°, shin0354}@incheon.ac.kr

A Design on the authentication using the Hash Lock and PKI in RFID/USN

YongSik Choi° SeoungHo Shin
Dept. of Computer Engineering, University of Incheon

요 약

일방향 해시 함수의 역함수 계산 어려움에 기반한 Hash Lock에 PKI방법을 적용하여 MetaID를 비밀키로 써 사용한다. Reader는 미리 등록된 공개키(meta ID를 이용하여 생성된)로 Tag를 인증하고 meta ID로 각 Tag의 유일한 키(k)를 생성하며 이에 해당하는 meta ID = H(k)를 가지고 있다. 이 때 H()는 해쉬함수이다. Tag는 자신의 비밀키를 이용하여 생성된 meta ID를 Reader에 보내고 Reader는 해당되는 키(k)를 만들어내고 Tag에 보낸다. 이때 Tag는 Reader로부터 보내어진 키(k)를 해쉬값과 자신의 meta ID를 비교하여, 그 값이 동일하면 자신의 ID를 전송한다. 이는 해쉬함수와 PKI만을 사용하므로 효율적이고 저비용으로 구현 가능하다.

1. 서 론

언제 어디서나 네트워크에 접근하여 경제적이고 편리하게 정보를 교환할 수 있는 유비쿼터스 환경이 제대로 갖추어지기 위해서는 보안 기술이 필수적인 요소이다.[1]. 유비쿼터스 컴퓨팅 환경에서는 각 디바이스들이 생활의 곳곳에 널리 퍼져 있고 이러한 디바이스들을 통해서 어느 곳에서나 정보의 이동의 용이하다. 유비쿼터스 환경을 위한 핵심기술인 RFID(Radio Frenquency IDentification)를 통하여 사물의 인식정보 및 주변의 환경 정보까지 센싱하고 이를 연결하여 정보를 관리한다.[2]. 유비쿼터스 관련 서비스는 환경 정보 센싱, 자동차 분야, 환경 관리 분야, 물류 유통 분야에 사용 가능하다.[3] RFID/USN의 도입에 따라 개인 프라이버시 위협을 비롯한 다양한 보안 문제점들이 제기되고 있다. 특히 Tag 정보의 위변조, 위장 Reader, DoS 공격, 네트워크에서 개인 추적 정보 유출 등의 보안 위협에 노출될 우려가 있다. 즉 공격 대상은 기존의 컴퓨터에 저장된 정보 또는 통신 정보만이 아닌 개인이 소유한 모든 것으로 침해 범위가 확대되는 것이다. 그러므로 RFID/USN 서비스에 심각한 장애 요인이 되며 RFID/USN의 보안 문제가 해결 되여야 활성화 될 수 있다.[4].

일방향 해시 함수의 역함수 계산 어려움에 기반한 Hash Lock에 PKI방법을 적용하여 MetaID를 비밀키로써 사용한다. Reader는 미리 등록된 공개키(meta ID를 이용하여 생성된)로 Tag를 인증하고 meta ID로 각 Tag의 유일한 키(k)를 생성하며 이에 해당하는 meta ID = H(k)를 가지고 있다. 이 때 H( )는 해쉬함수이다. Tag는 자신의 비밀키를 이용하여 생성된 meta ID를 Reader에 보내고 Reader는 해당되는 키(k)를 만들어내고 Tag에 보낸다. 이때 Tag는 Reader로부터 보내어진 키(k)를 해쉬값과 자신의 meta ID를 비교하여, 그 값이 동일하면 자신의 ID를 전송한다. 이 방법은 고정된 meta ID를 이용하여 공격할 수 있는 방법에 대하여 안전하고 인가 받지 않은 사용자를 접근을 방지하고 합법적인 Reader기에 의해서는 식별 가능하다. 공개키에 의해 암호화된 암호문의 주어진 Tag의 연결성을 감소시키기 위하여 주기적으로 재암호화를 수행함으로써 인증과 프라이버시가 안전하게 보장된다. 해쉬함수와 공개키 알고리즘만을 사용함으로써 효율적이며 저비용으로 구현 가능하다.

본 연구의 구성은 다음과 같다. 2장에서는 관련연구로서 RFID 기술과 Privacy 그리고 Sensor Network의 보안에 대하여 기술하고 3장에서는 제안된 Hash Lock과 PKI을 이용한 인증 프로토콜의 설계를 하고 4장에서 결론을 맺는다.

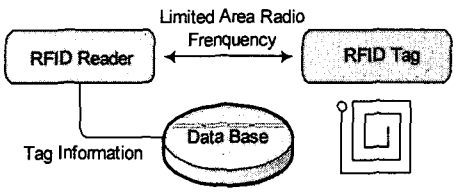
2. 관련연구

2.1 RFID 기술

RFID Tag를 이용한 기존과 다른 근접 공감감지가 가능하다. RFID는 [그림 1]과 같이 RFID Reader를 통하여 무선통신에 의해 접촉하지 않고 Tag의 정보를 기록하거나 판독하는 시스템이다. 안테나가 포함된 RFID Reader, 정보를

본 연구는 산업자원부 지정 동북아전자물류센터의 지원에 의한 것입니다.

교환하는 RFID Tag, Data Base로 구성된다. [5].



[그림 1] RFID 시스템

RFID가 보편화 되기 위해서는 낮은 비용의 생산과 빠른 인식 속도, 다중 Tag의 인식 등의 기술적인 측면과 위조불가(Unforgeability)와 추적불가(Non Tracking)와 같은 안성적 측면이 확보되어야 한다.

2.2 USN의 보안

일반적으로 USN의 노드는 안전하지 않은 위치에 설치된다. 따라서 각 노드에 대한 신뢰성을 보장 받을 수 없기 때문에 한 노드의 보안 노출이 다른 노드에 영향력을 미치지 않고 보안사고의 최소화가 필요하다.

2.2.1 Hash lock 방식

일방향 해시 함수의 역함수 계산 어려움에 기반한 Hash Lock 방식은 인가받지 않은 Reader기가 Tag를 읽는 것을 방지 할 수 있다. Spoofing은 방지하지 못하지만 탐지는 가능하다. 이 방식은 해쉬 함수만을 요구하므로 저비용으로 구현될 수 있으나, meta ID가 고정되어 공격자는 meta ID를 이용하여 해당 Tag의 위치를 추적할 수 있는 문제가 있다.

[그림 2] Hash Lock의 Unlocking 프로토콜

[그림2]와 같이 Reader는 Tag에게 metaID를 질의하고 DataBase는 (metaID, Key)를 조사하여 Reader는 Tag에게 Key를 전송한다. 만약 Hash(key)와 metaID가 일치하면 잠긴 상태에서 빠져나온다. [4].

2.2.2 Randomized hash lock 방식

이 방식은 Hash lock 방식을 개선한 것으로 고정된 meta ID를 갖게 하지 않기 위하여 난수 생성기를 통하여 접근할 때마다 Tag에서 다른 출력 값을 가지게 한다. 그러므로 Tag에 대한 추적은 불가능하다. 그러나 해쉬 함수와 난수가 동시에 생성되어야 하므로 저비용으로 구현하기 어렵다.

[그림3] Randomized Hash Lock의 Unlocking 프로토콜

[그림 3]와 같이 Reader는 Tag에게 질의를 보낸다. Tag는 랜덤한 난수를 생성하고, hash(ID || R) 값을 계산하고 Tag는 Reader에게 전송하여 hash(IDi || R) == hash(ID || R)을 만족하는 IDi를 찾으면 전송하고 잠긴 상태에서 빠져나온다. [4].

2.3.3 Hash-chain 방식

이 방식은 Randomized hash lock 방식의 문제점, 즉 Tag안의 정보가 노출되면 이전의 위치 정보가 추적되는 것과 해쉬함수와 난수생성으로 인한 고비용을 개선한 것이다. Tag안에서 해쉬 함수만으로 Tag정보의 보호가 가능하나 Tag의 위조 문제와 서버에서 Tag ID를 식별할 경우 해쉬 함수를 계속해서 반복, 수행해야 되므로 Randomized hash lock 방식보다 더 많은 연산이 요구되는 문제가 있다. [4].

3. 기 제안된 인증 프로토콜의 설계

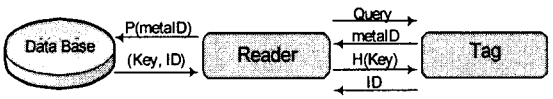
유비쿼터스 컴퓨팅 환경에서는 각 디바이스들이 생활의 곳곳에 널리 퍼져 있고 이러한 디바이스들을 통하여 어느 곳에서나 정보의 이동이 용이하다. 이것은 어디서든지 쉽게 정보가 유출 될 수 있음을 의미하고 개인의 프라이버시에 심각한 문제가 발생할 수 있다. 센서 디바이스는 통신 능력, 계산 능력, 전원 능력이 제한되어 있으며 종종 물리적으로 취약한 곳에 설치 될 수 있다. 또한 주변의 환경이나 사람과 상호 작용을 한다. 이것은 새로운 보안 문제들이 야기된다. 따라서 좀더 강력한 보안 체계가 필요하다. 이것은 기술적인 발전과 더불어 사회 전반적인 합의가 필요하다. 이에 효율적이며 안전하며 저비용으로 구현 가능한 인증 프로토콜을 제안한다.

3.1 인증 프로토콜

일방향 해시 함수의 역함수 계산 어려움에 기반한 Hash Lock에 PKI방법을 적용하여 MetaID를 비밀키로써 사용한다. Hash Lock 방식은 인가받지 않은 Reader기가 Tag를 읽는 것을 방지 할 수 있으며 탐지가능하며 Hash Function만을 요구하므로 저비용으로 구현가능하다. [그림 4]에서

의 Reader는 미리 등록된 공개키(meta ID를 이용하여 생성된)로 Tag를 인증하고 meta ID로 각 Tag의 유일한 키(k)를 생성하며 이에 해당하는 meta ID = H(k)를 가지고 있다. 이 때 H()는 해쉬함수이다.

Tag는 자신의 비밀키를 이용하여 생성된 meta ID를 Reader에 보내고 Reader는 해당되는 키(k)를 만들어내고 Tag에 보낸다. 이때 Tag는 Reader로부터 보내어진 키(k)를 해쉬값과 자신의 meta ID를 비교하여, 그 값이 동일하면 자신의 ID를 전송한다.



[그림 4] 인증 프로토콜

(1) Reader는 Tag에게 질의를 보낸다

(2) Tag는 미리 생성된 비밀키를 이용한 생성된 Meta ID를 보낸다.

(3)Reader는 P(meta ID) 인증키를 생성한다. Reader는 Data Base에서 값을 조사하고 일치하면 Key와 ID를 Tag에게 전송 한다.

meta ID는 PKI와 관련하여 사용할 수 있는 장치들에 대하여 단일 접속이 가능하며 다중 요소 인증을 사용하여 지역 환경에서 접속가능 하다.

기 제안된 방법은 고정된 meta ID를 이용하여 공격할 수 있는 방법에 대하여 안전하고 인가 받지 않은 사용자를 접근을 방지하고 합법적인 Reader기에 의해서는 식별 가능하다. 공개키에 의해 암호화된 암호문의 주어진 Tag의 연결성을 감소시키기 위하여 주기적으로 재암호화를 수행함으로써 인증과 프라이버시가 안전하게 보장된다. 그리고, 해쉬함수와 공개키 알고리즘만을 사용함으로써 효율적이며 저비용으로 구현 가능하다.

4. 결론 및 향후 계획

유비쿼터스 컴퓨팅 환경에서는 언제 어디서나 네트워크에 접근하여 경제적이고 편리하게 정보를 교환할 수 있다. 각 디바이스들이 생활의 곳곳에 널리 퍼져 있고 이러한 디바이스들을 통해서 어느 곳에서나 정보의 이동의 용이하다. 유비쿼터스 환경을 위한 핵심기술인 RFID를 통하여 사물의 인식정보 및 주변의 환경 정보까지 센싱하고 이를 연결하여 정보를 관리한다. 즉 이와같은 USN은 RFID를 지닌 물체나 동물, 사람 등을 판독, 추적 및 관리가 가능하다. 유비쿼터스 관련 서비스는 환경 정보 센싱, 자동차 분야, 환경 관리 분야, 물류 유통 분야에 사용 가능하다. [1][3].

RFID/USN의 도입에 따라 개인 프라이버시 위협을 비롯한 다양한 보안 문제점들이 제기되고 있다. 전통적인 네트워크와 다른 특징을 가지고 있다. 센서 디바이스는 통신 능력, 계산 능력, 전원 능력이 제한되어 있으며 종종 물리적으로 취약한 곳에 설치 될 수 있다. 또한 주변의 환경이나 사람과 상호 작용을 한다. 이것은 새로운 보안 문제들이 야기되며 기존의 보안 기술을 그대로 적용시키기 어렵다. 즉, Tag 정보의 위변조, 위장 Reader, DoS 공격, 네트워크에서 개인 추적 정보 유출 등의 보안 위협에 노출될 우려가 있다. RFID/USN 기술의 활성화를 위해서는 보안 기술이 필수적인 요소이다. [4].

따라서 본 연구에서는 유비쿼터스 환경에서 효율적이며 저비용 구현 가능한 Hash Lock과PKI를 사용한 인증 프로토콜을 설계하였다. 즉, 일방향 해시 함수의 역함수 계산 어려움에 기반한 Hash Lock기법과 PKI를 이용하여 인가받지 않은 사용자를 접근을 방지하고 합법적인 Reader기에 의해서는 식별 가능하도록 한다. PKI에 의해 암호화된 암호문의 주어진 Tag 연결성을 감소시키기 위하여 주기적으로 재암호화를 수행함으로써 인증과 프라이버시가 안전하게 보장된다. 그리고, 해쉬함수와 PKI만을 사용하여 효율적이고 저비용으로 구현 가능하다. 보안 없이는 유비쿼터스 비즈니스의 활성화가 이루어 질 수 없다. 강력한 보안 체계가 필요하며 사회 전반적인 합의가 필요하다. 유비쿼터스 시대에는 사용자가 처한 시공간적 위치와 상황, 그리고 각종 시스템과 단말기 간의 상호작용을 기반으로 각자의 취향에 맞는 다양한 비즈니스가 창출될 것이다

참고문헌

[1] 최재귀, 박지환, "효율적인 식별 기능을 가진 위조불가 RFID Tag 가변 ID 방식", 한국정보처리학회 논문지 C VOL. 11 NO. 04 pp. 447~454 2004.

[2] Klaus Finkenzeller, "RFID Handbook" second edition, John Wiley & Sons, 2003

[3] 장병준, 안선일, 이윤덕, "RFID/USN 기술개발 동향", 한국정보과학회 학회지 VOL. 23 NO. 2 pp. 83~87 2005.

[4] 홍도원, 장구영, 박태준, 정교일, "유비쿼터스 환경을 위한 암호 기술 동향", 전자통신동향분석 제20권 제1호 pp.65~68 2005.

[5] 송석현, 신상철, "RFID/USN 표준화 동향 및 이슈", 한국정보과학회 학회지 VOL. 22 NO. 12 pp. 67~74 2004.