SNEP와 ECC를 이용한 RFID 보안 시스템 설계

박상현°, 한수, 최용식, 전영준, 신승호
인천대학교 컴퓨터 공학과
{tank1862°, pucktan, mars, 0961144}@incheon.ac.kr

Design of RFID Security System Using SNEP and ECC

Sang-Hyun Park°, Soo-Han, Yong-Sik Choi, Young-Jun John, Seoung-Ho Shin
Dept. of Computer Engineering, University of Incheon

요 약

IT 기술의 발달로 인간의 편이를 위한 많은 기술들이 생겨나고 21세기 IT분야만이 아닌 사회 전 분야에서 가장 주목을 받는 기술이 유비쿼터스이다. 유비쿼터스는 사용자의 인식없이 컴퓨터와 통신을 하는 기술이다. 주거환경의 개선 부분이나 구매의 편리를 위한 부분에서 가장 많은 적용이 시도 되고 있다. 하지만 무분별한 인식에 의한 개인의 프라이버시와 여러 가지 보안문제가 야기되고 있다. 일반 RFID 분야에서는 보안이 필요 없는 부분도 있지만 RFID가 더 많은 분야에서 시도가 되려면 보안요소가 꼭 필요하다.

본 논문에서는 저 전력과 낮은 메모리에서 사용하기 위해서 무선에서 사용하고 있는 보안 모듈인 SNEP와 ECC알고리즘을 RFID에 적용할 수 있는 시스템을 설계 및 제안한다.

1. 서 론

IT기술의 발달로 인하여 생활의 편이를 추구하는 많은 기술들이 생겨나고 21세기 가장 부각되고 있는 기술이 유비쿼터스 이다. 유비쿼터스는 사용자의 인식없이 컴퓨터와 통신이 가능한 환경이 가능한 기술이다. 이런 유비쿼터스의 핵심기술로 RFID가 주목을 받고 있으며, RFID를 적용하여 유비쿼터스 환경 구축을 위한 많은 연구가 진행중이다. 대표적으로 세계 굴지의 기업인 베네통과 월마트가 막대한 자본을 투자하여 RFID (Radio Frequency Identification)를 이용하여 구매와 판매에 대한 개선을 시도했다. 하지만 개인의 프라이버시를 무시한 방안으로 인하여 소비자에 대한 고소까지 들어오는 사례를 나았다[4]. RFID 사용에 대한 문제는 태그를 통하여 알려 질수 있는 익명성 문제, 태그의 개인정보에 대한 암호화의 정도에 따라 누설가능성이 상존하는 보안문제, 대량생산 공업제품이므로 복제나 위조 등의 가능성에 따른 위·변조 문제가 있다[5]. USN/RFID라는 핵심기술을 이용하기 위해서는 개인 프라이버시를 위한 정책적인 방안과 기술적인 연구가 이루어 져야 한다.

본 연구에서는 RFID 이용에 따른 개인 프라이버시 보호를 위한 방안으로 저전력과 낮은 메모리에서 사용이 가능하면서 보안성이 뛰어나고 기존에 무선에서 사용하고 있는 암호화 알고리즘인 ECC알고리즘을 이용하여 USN/RFID환경에 적용이 가능한 프로토콜을 설계 및 제안 한다.

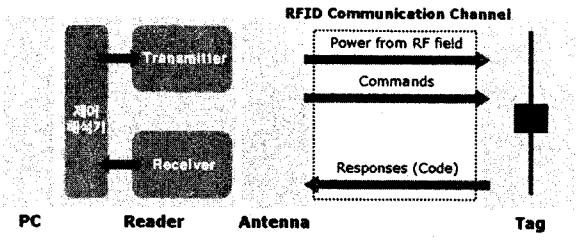
2. 관련연구

2.1 USN/RFID

USN/RFID란 필요한 모든 것(곳)에 RFID를 부착하고 이를 통하여 사물의 인식정보를 기본으로 주변의 모든 정보를 탐지하여 이를 실시간으로 네트워크에 연결하여 정보를 관리하는 것을 말하는 것으로 먼저 인식정보를 제공하는 RFID를 중심으로 발전하고 이에 감지능력이 추가되고 이들 간의 네트워크가 구축되는 USN 형태로 발전할 것으로 전망되고 있다.

2.2 RFID

마이크로 칩을 내장한 태그, 레이블, 카드 등에 저장된 데이터를 무선주파수를 이용하여 리더에서 자동인식 하는 기술이다. RFID는 비접촉식으로 여러 개의 태그를 동시에 인식할 수 있고, 인식시간이 짧고, 태그에 대용량의 데이터를 저장할 수 있으며, 반영구적인 사용이 가능한 장점이 있다. 그래서 RFID는 기존의 바코드나 자기인식 장치의 단점을 보온하고 사용의 편리성을 향상시켜 줄 차세대의 핵심기술이다[7].



[그림 1] RFID 통신 방법

RFID는 여러 가지 분류가 있다.

첫 번째, 태그와 리더 사이의 전송 방식에 따라 전자 결합 방식, 마이크로파 방식, 전자 유도 방식, 광 방식 등이 있다.

두 번째, 태그 내부의 전지 보유 유무에 따라 전지 없이 에너지를 공급 받아 작동하는 수동형 태그와 전지가 포함된 능동형 태그로 나눌 수 있으며, 칩의 종류에 따라 반도체 칩을 이용하는 태그와 LC소자 또는 플라스틱/폴리머 소자 등으로만 구성된 무칩(chipless)으로 구분되다.

세 번째, 이용 주파수에 따라 분류가 가능하며, 국내의 표준에 맞추어 나눈다면, 125, 134 Khz, 13.56 Mhz 433.92 Mhz, 860-960 Mhz, 2.45Ghz 대역으로 나누어 볼 수 있다[8].

[표 1] 무선 주파수별 적용 분야

이용주파수	인식거리	적용분야
125-134 Khz	< 10cm	동물이력 관리
13.56 Mhz	10-70 cm	신분증
433 Mhz	< 100 M	물류, 유통
860-960 Mhz	5-7m	물류
2.45 Ghz	< 1m	의류, 기밀문서

[표1]을 보면 433 Mhz 를 제외하고는 모두 거리가 7m이하이며 433 Mhz 역시 배터리가 들어있는 능동 태그를 사용할 경우에 적용되는 거리이다.

2.3 Sensor Network에서의 보안

1) 센서 네트워크 보안

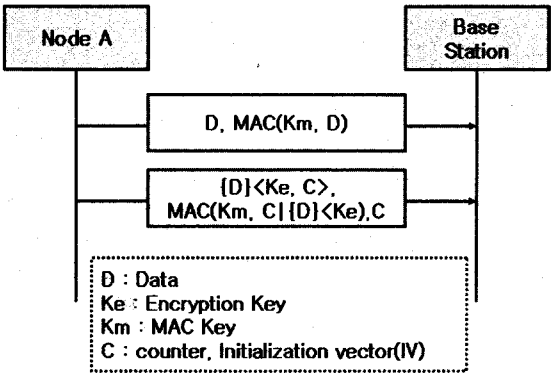
일반적으로 무선망을 이용한 센서 노드 방식은 Broadcasting방식이다. 이것은 센서 네트워크 서비스 특성상 최소한의 자원 소모에 적절한 보안 요구사항을 만족하기 위한 보안 수준을 제공하는 것이다. 일반적인 센서 네트워크에서의 통신 방식은 다음과 같다.

- node to base station 통신
- base station to node 통신
- base station to all nodes 통신

이러한 환경에서의 보안이 필요한 부분은 node간 통신 보안과 node broadcasting 등에 대한 안전성을 보장하는 것이다. 일반적으로 센서 네트워크를 위해 운영되는 센서 노드는 안전하지 않은 위치에 설치된다. 따라서 각 노드에 대한 신뢰성을 보장 받을 수 없기 때문에 한 노드의 보안 노출이 다른 노드에 영향력을 미치지 않도록 보안 사고의 최소화가 절대적으로 필요하다.

2.4 Security Protocols for Sensor Networks(SPINS)

1) SNEP (Secure Network Encryption Protocol)



[그림 2 SNEP의 구조]

SNEP에서 제공하는 보안사항은 다음과 같다.

- 데이터 비밀성 (Data Confidentiality) : 의도된 수신자마이 데이터를 소유할 수 있도록 데이터를 비밀키로 암호화하며 제 3자가 암호 메시지에서 원래 메시지를 추론할 수 없는 보안 기능을 보장한다.
- 양단간 데이터 인증 : 의도된 송신자가 정말로 해당 데이터를 보냈는지 검증하기 위해서 공유돈 키를 기반으로 MAC을 사용한다.
- 재사용 방지 : MAC에 counter값을 포함하여 공격자에 의해 재사용 공격이 이루어질 경우 counter정보를 판별한다.
- 데이터 신선성 (Data Freshness) : 해당 데이터가 가장 최근의 버전임을 의미하는 것으로 최근 데이터

임을 검증하기 위한 기능이다.
- 낮은 통신 부하 : Counter 상태는 각 end point에 유지되며, 각 메시지에 담아 전송할 필요가 없다.

2.5 ECC 암호화 알고리즘

타원곡선은 아래의 식을 만족하는 $(x, y) \in F_q \times F_q$들의 집합과 함께 무한점 (point at infinity)이라고 하는 특별한 점 o를 포함한 집합, 연산은 다음과 같이 덧셈을 정의한다.

$$(p>3 \text{ 일때}) E: y^2 = x^3 + ax + b,$$
$$(a, b \in F_q, 4a^2 + 27b^3 \neq 0 \in F_q)$$
$$(p=2 \text{ 일때}) E: y^2 + xy = x^3 + ax^2 + b,$$
$$(a, b \in F_{2^m}, b \neq 0)$$

다음 수식에 의하여 제곱근에 의한 공식을 이용하여 해를 키 값으로 이용하며, 역으로 값을 유추하기 어렵다는 점을 착안하여 개발되었다. 기존 보안 알고리즘보다 조금 더 복잡한 알고리즘을 요구한다.

하지만 <표 1>에서 대표적으로 사용하는 보안 알고리즘인 RSA와 DSA, ECC 시스템 매개변수와 키 크기를 비교하여 보면 ECC가 적은 키 값을 이용함을 알 수 있다.

[표 1] 시스템 매개변수와 키 크기 (단위: bit)

	시스템 매개변수	공개키	비공개키
RSA	n/a	1088	2048
DSA	2208	1024	160
ECC	481	161	160

ECC (Elliptic Curve Cryptography: 타원곡선 암호) 알고리즘이 짧은 키 길이를 이용하는 점은 메모리와 대역폭 및 CPU 처리능력이 제한된 이동 통신 기기 및 스마트 카드에서 효율적으로 작동될 수 있다는 것을 의미한다. 타원곡선암호(ECC)의 또 다른 이점은 비록 모든 사용자가 같은 기저체 K를 사용한다할 지라도, 각 사용자가 다른 곡선 E를 선택할 수도 있다는 것이다. 즉, 모든 사용자는 체 연산을 수행하기 위해 같은 H/W를 사용할 수 있으며, 추가 보안을 위해 주기적으로 곡선 E를 바꿀 수도 있다. 타원곡선에 대한 여러 정의가 존재 하지만 $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$의 해집합과 무한원점(o)을 말한다.

3. 제안프로토콜

3.1 개요

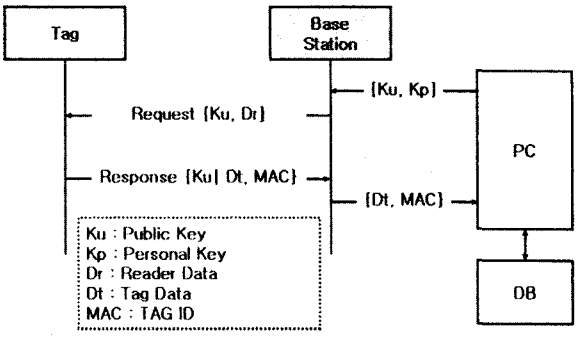
대칭키를 이용하는 방법은 앞에서 설명한 바와 같이 많은 메모리 공간을 요하기 때문에 Sensor Network 환경 내에서는 부적합하다. 그래서 본 논문에서는 공개키를 이용하는 방법을 제안하려 한다. 2.4절의 ECC의 특징에서 기존 암호화 방식인 DSA, RSA보다 적은 시스템 매개변수와 공개키 길이를 사용하기 때문에 적은 메모리와 CPU에서도 동작이 가능하다.

3.2 세부절차

암호화 방식은 ECC를 이용하여 기존의 공개키 방식에 이용되고 있는 알고리즘보다는 적은양의 메모리를 사용하며, SNEP 방식을 접목시켜 MAC을 ECC암호화를 이용하여 암호화 하여 전송한다. DB에서는 키 쌍과 MAC을 관리하여 해당 장비가 인가된 장비인가를 확인한다.

- PC에서 두 개의 키 쌍을 생성 {공개키 : Ku, 비공개키 : Kp} 한다.
- Reader에서 TAG로 {공개키 : Ku}와 작동을 위한 데이터 Dr로 보낸다.
- TAG의 정보와 고유 식별을 위한 MAC을 공개키로 암호화 하여 Reader로 보낸다.
- 정보를 받은 Reader에서는 복호화를 수행하고 TAG의 정보{Dt} 만을 PC로 보낸다.

3.3 주요 흐름도



[그림 3 주요 흐름도]

ECC암호화 알고리즘을 해당 PC에서 생성하여 Reader에서 송신을 할 때 동봉하여 보내며 TAG에서 암호화를 수행하며 보내며 Reader에서 복호화를 수행하여 MAC과 TAG의 Data (Dt)를 PC로 보내어 해당 장비의 인가를 확인한다.

4. 결론

유비쿼터스 환경은 먼저 RFID를 중심으로 발전하고 이에 감지기능이 추가되고 이들 간의 네트워크가 구축되는 USN 형태로 발전할 것으로 전망되고 있다. 그러나 이러한 자동화되고 손쉽게 정보를 얻을 수 있는 환경에서는 보안에 있어 심각한 결과를 초래 할 수 있다.

현재 단계에서 USN 환경에서의 공격의 형태나 공격자에 대한 명확한 추정은 아직까지는 센서 네트워크 자체가 미성숙한 단계에 있기 때문에 어렵다. 현재의 공격보다는 광범위한 범위와 대상을 목표로 하는 것으로 예상되고 있다.

센서 노드에 암호키를 탑재하는 방식은 물리적 공격에 대한 취약점이 일어날 수 있다. 그래서 본 논문에서는 Reader에서 TAG로 데이터를 전송할 때 키를 분배하는 방식을 사용하여 물리적 공격에 대한 방비를 하였고 ECC를 암호화 알고리즘으로 적용함으로써 기존보다 좀 더 나은 보안을 제공 받을 수 있다.

기술적인 방법들의 개발로 태그로 인한 개인 프라이버시 침해를 막는것도 중요하지만 태그와 리더에서의 정보보호 및 프라이버시 위협 이외에 베리사인의 EPC Trust Service 및 eTRON CA처럼 RFID 네트워크 보호를 위한 인증기술 및 체계가 마련되어야 하며, 법·제도, 기술개발이 상호 연계되는 RFID 정보보호 서비스가 고려되어야 할 것이다.

5. 참고문헌

[1] 센서 네트워크 보안 프로토콜 소개와 향후 과제, 서운석, 신순자, 김유정, 신상철, "정보과학회지", 2004. 12.

[2] 유비쿼터스 컴퓨팅의 핵심 RFID HANDBOOK, 이근호, 한호병, 강병권, 조영빈, "영진닷컴", 2004. 03.

[3] 정보통신부, 'u-센서 네트워크구축 기본계획', 2004. 2.

[4] 개인정보 보호를 위한 RFID 신뢰 확보가 중요하다, 강달천, 주학수, 권혁조, KISTI, 2004. 11.

[5] RFID 태그의 프라이버시를 위한 기술적인 접근, 조준혁, KISTI, 2005. 03.

[6] RFID/USN 정보보호 기술, 김광조, KISTI TTA저널 95호, 2004.

[7] 유승화, 유비쿼터스 사회의 RFID , 전자신문사, 2005.3, pp.59-60,

[9] 조대진, "RFID 이론과 응용," 홍릉출판사, 2005, pp.3-4

[9] A.Perrig, R.Szewczyk, V.Wen, D.Culler, J.D.Tygar, "SPINS : Security Protocols for Sensor Network", Wireless Networks Journal (WINET), 8(5) : 521-534, Sep 2002