RFID/USN 보안을 위한 프로토콜 설계

박 상 현* · 박 상 민** · 신 승 호*
*인천대학교 컴퓨터공학과 · **인천대학교 산업경영학과

Design of protocol for RFID/USN security

Sang Hyun Park* · Sang Min Park** · Seung Ho Shin*
*Department of Computer Science & Engineering, University of Incheon
**Department of Industrial and Management Engineering, University of Incheon

Abstract

Payment and security requirement are playing an increasingly critical role in RFID system, allegedly the core of the ubiquitous, especially in logistics. Therefore, security technology has been playing essential role gradually unlike the past when only the perception of equipment was considered an important technology. The current encoding system allows the access only to the user who has the secret key.

Many encoding algorithm has been studied to ensure the security of secret key. Security protocol is the most typical way to authorize appropriate user perception by using the data and secret key to proceed the encoding and transmit it to the system in order to confirm the user.

However, RFID system which transmits more than dozens of data per second cannot be used if the algorithm and protocol of the existing wired system are used because the performance will degrade as a consequence. Security protocol needs to be designed in consideration of property of RFID and hardware.

In this paper, a protocol was designed using SNEP(Sensor Network Encryption Protocol), the security protocol used for the sensor similar to RFID- not the current system used in wired environment- and ECC (Elliptic Curve Cryptography: oval curve encoding), the encoding algorithm.

Keywords : RFID, ECC, SPIN, Security

1. 서 론

인간의 편의를 위하여 발전해온 많은 과학기술 중 현재 가장 부곽되고 있는 기술이 유비쿼터스 이다. 이런 유비쿼터스를 만들어 주기 위한 핵심 기술로 RFID와 USN(Ubiquitous Sensor Network)이 주목 받고 있다. RFID는 이미 오래전에 개발된 기술로 갑자기 주목받는 이유는 여러 굴지의 기업에서 이를 이용한 물류, 유통의 혁신을 꾀하고, 433MHz를 이용한 미국의 컨테이너 관리, 걸프전에서의 군사물자 관리 등 큰 기업과 국가에서 주목받기 시작하면서 이다. 하지만 세계 굴지의 기업인 베네통과 월마트에서 막대한 자본으로 RFID를 이용한 구매와 판매에 대한 개선을 시도했으나 개인의 프라이버시를 무시한 방안으로 인하여 소비자에 대한 고소까지 들어오는 사례를 나았다[1].

RFID를 사용하게 되면 태그를 통하여 개인정보가 여과 없이 알려 질수 있는 익명성 문제, 태그의 개인정보에 대한 암호화의 정도에 따라 누설가능성이 상존하는 시큐리티 문제, RFID가 대량생산 공업제품이므로 복제나 위조 등의 가능성에 따른 위변조 문제가 있다[2]. RFID/USN 핵심 기술로 이용하기 위해서는 개인 프라이버시를 위한 정책적인 방안과 기술적인 연구가 이루어 져야 한다.

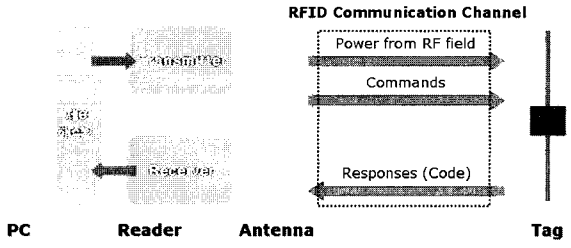
† 본 논문은 2006년도 인천대학교 학술연구 조성비 지원에 의하여 수행되었음.
2007년 5월 접수; 2007년 6월 수정본 접수; 2007년 6월 게재확정

본 연구에서는 개인 프라이버시 보호를 위한 방안으로 기존에 비대칭키 암호화 방식의 ECC알고리즘과 SNEP(Secure Network Encryption Protocol)를 이용하여 USN환경에 적용이 가능한 프로토콜을 설계 및 제안 한다. 논문의 구성은 다음과 같다. 2장에서는 RFID/USN에 대한 소개와 RFID/USN에서 사용이 가능한 보안 모듈에 대해서 소개를 하고, 3장에서는 본 논문에서 제안하는 프로토콜을 소개하고, 4장에서 결론과 발전 방향에 대해서 언급한다.

2. 관련 연구

2.1 USN/RFID

마이크로 칩을 내장한 태그, 레이블, 카드 등에 저장된 데이터를 무선주파수를 이용하여 리더에서 자동으로 인식 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 자기인식장치의 단점을 보완하고 사용의 편리성을 향상시켜 줄 차세대의 핵심기술이다[3][9][10].



<그림 1> RFID 통신 방법

RFID는 크게 3가지 방식으로 분류가 가능하다[11][12].

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

둘째, 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 구분된다.

셋째, 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[4]. <표 1>을 보면 433 Mhz 를 제외하고는 모두 거리가 7m이하이며 433 Mhz 역시 배터리가 들어있는 능동 태그를 사용할 경우에 적용되는 거리이다.

<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

2.2 Sensor Network의 보안

일반적으로 무선망을 이용한 센서 노드 방식은 Broadcasting방식이다. 이것은 센서 네트워크 서비스 특성상 최소한의 자원 소모에 적절한 보안적 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 보안 요구사항은 node간 보안, 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.

2.2.1 센서네트워크 표준화 동향

현재 센서 네트워크 표준화 동향은 Ad-hoc 망을 기반으로 센서 네트워크를 구축하는 표준이 주를 이루고 있다. IEEE를 중심으로 표준화가 이루어지고 있으며 Bluetooth, IEEE802.15.4, Zigbee, P1451.5(Wireless Sensor Interface Standard)등이 진행 중인 주요 표준이다. 앞의 3개의 표준은 기존의 무선환경에서 네트워크 구축을 위한 Topology를 구성하는 관점에 주안점을 두고 연구가 진행 중에 있다.

1993년에 IEEE P1451은 그 생성 자체가 센서 네트워크를 목표로 하여 탄생되었으며 P1451.0~P1451.5로서 총 6개의 표준으로 나뉘어 진행 중이다. 센서 내부

Transducer간의 통신과 Transducer와 NCAP(Network Capable Application Processor)간의 통신을 위한 인터페이스와 기능에 대한 표준화가 진행 중에 있다. 하지만 Ad-hoc 네트워크의 P2P방식으로 수많은 기기들을 연결하기 위해서는 프로토콜이 한계를 가지며 또 오작동하는 기기들까지도 일일이 관리하여야 하는 문제점을 갖고 있다.

소형 센서기기의 개발을 주요 목표로 하고 있는 버클리에서는 TinySec 프로젝트를 수행하여 안전한 그룹관리 SPIN(Security Protocol for Sensor Network)프로토콜을 개발하였다. 이 프로토콜은 멀티캐스팅 보안 프로토콜인 TESLA(Timed Efficient Stream Loss-tolerant Authentication)를 간소화시켰으며, 개발로 m/TESLA와 SNEP(Secure Network Encryption Protocol)로 구성된다. m/TESLA는 다수로 구성된 센서 네트워크의 기기들의 인증을 담당하며, SNEP는 데이터의 기밀성, 인증, 초기성(Freshness)을 보장한다. 링크계층에서 동작하는 프로토콜 성능 측면에서 5 ~10%의 오버헤드를 유발한다.

2.3 센서 네트워크 보안 프로토콜 (SNEP: Secure Network Encryption Protocol)[14]

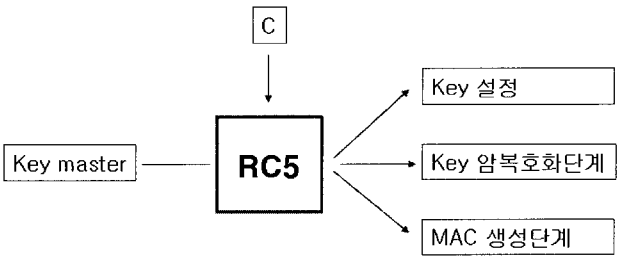
센서 네트워크의 보안 요구사항을 만족하는 보안 프로토콜로 SNEP이 있다. 이 프로토콜은 대칭형 암호방식만을 사용하며, 무선 센서네트워크와 같은 자원이 제한된 환경에서 보안 프로토콜을 제공할 때 자원의 오버헤드를 최소화하는 것을 목표로 한다.

센서 노드에서 기지국으로의 통신과 같은 유니캐스트 통신에서는 송수신자가 비교적 명확하기 EOans에 두 통신 당사자가 서로 비밀을 공유하고, 각 패킷에 공유된 키로 계산한 메시지 인증 코드(Message Aythentication Code : MAC)를 덧붙임으로써 비교적 충분한 보안을 제공할 수 있는데, 이와 같은 목적으로 사용되는 프로토콜이 SNEP이다. SNEP은 일반적으로 키 설정 단계, 암호화단계, MAC 생성단계로 구성된다.

2.3.1 SNEP의 키 설정, 암호화 및 MAC 생성

1) 키 설정 단계

SNEP은 일반적으로 RC5 대칭 키 암호화 알고리즘을 이용하여 다양한 목적의 키 값을 유도한다. 마스터키(Master Key)는 기지국과 센서 노드사이에서 사전에 나누어 가지며, 마스터키를 기반으로 암호화를 위한 암호화 키, MAC 값 생성을 위한 키 값, 랜덤 키 값 등을 생성한다.



<그림 2> 키 생성 메커니즘

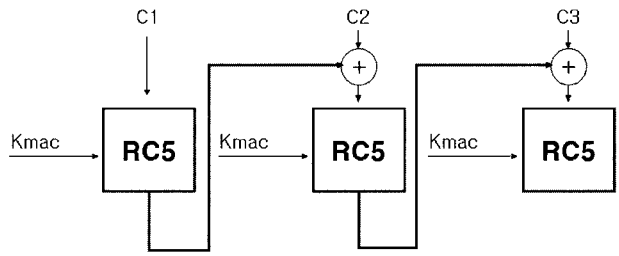
2) 암·복호화 단계

암호화는 전 단계에서 생성한 암호키를 카운터 모드(Counter Mode)로 암호화하여 Chain으로 연결하는 구조이다.

E{(Bn_Key. Counter) P} = C를 이용해 암호화 루틴을 반복하여 암호화 및 복호화를 수행한다.

3) MAC 생성단계

그리고 메시지 인증코드{MAC} 생성키를 이용하여 <그림 3>과 같이 CBC 모드로 암호화된 메시지에 대한 메시지인증코드를 생성한다.



<그림 3> SNEP의 MAC 생성메커니즘

2.3.2 SNEP 프로토콜의 보안서비스

SNEP 프로토콜은 다음과 같은 보안 서비스를 제공한다.

- 데이터 기밀성 : 데이터 교환 시 암호화를 통하여 데이터 기밀성을 제공한다.
- 확고한 보안성 : 공격자가 같은 키로 암호화된 평문-암호문 쌍을 알고 있다 하더라도 암호화된 메시지의 평문을 추출해 낼 수 없도록 한다.
- 양단간 데이터인증과 무결성 : MAC (메시지 인증코드)을 사용하여 양단간 데이터 인증과 무결성을 제공한다.
- 재사용 방지 : MAC에 카운터(Counter) 값을 포함하여 공격자에 의한 재사용 공격을 방지한다.
- 데이터 신선성 : 해당 데이터가 가장 최근의 버전임을 검증하기 위한 기능을 제공한다.
- 낮은 통신 부하 : 각 블록이 끝난 후 카운트를 하나씩 증가시켜서, 카운터를 메시지에 포함하지 않고 증가시켜서, 낮은 통신 부하 및 기밀성을 제공한다.

2.4 Zigbee

Zigbee의 어원은 표준화를 위한 모임의 초기에 여러 제안 및 결정을 위한 혼선의 모양을 빗대어 Zig Zag에서의 Zig와 가장 경제적으로 통신을 한다는 벌(Bee)의 개변을 도입하여 Zigbee (IEEE 802.15.4)로 명명하였다[5].

<표 2> Zigbee 주파수와 데이터 전송율

주파수	밴드	영역	데이터전송율	채널수
2.4 Ghz	ISM	전세계	250 kbps	16
868 Mhz		유럽	20 kbps	1
915 Mhz	ISM	미국	40 kbps	10

ZigBee는 근거리 (10cm-30m)에서 낮은 데이터 전송율을 갖는 저가격이면서 전력 소모측면에서 효율성이 있어 배터리가 수개월에서 수년간 지속될 수 있는 장점을 갖는 무선 네트워크 (네트워크 당 255개의 노드 연결)기술이다[6].

Zigbee는 <표 2>와 같이 PHY로 2.4 Ghz대역 (QPSK변조방식)의 16채널, 915 MHz대역 (BPSK 변조방식)의 10 채널, 868 Mhz대역의 1개 채널을 이용한다.

Zigbee는 공장 자동화 시스템, 농장 살수 장치 또는 가정용 온도 조절기와 같은 산업용 및 홈 오토메이션 응용으로 고안된 표준이지만 응용범위를 넓혀 장난감, 게임기, 가전 제품의 디바이스 및 PC 주변기기 제조업체에게도 큰 호응을 얻고 있다.

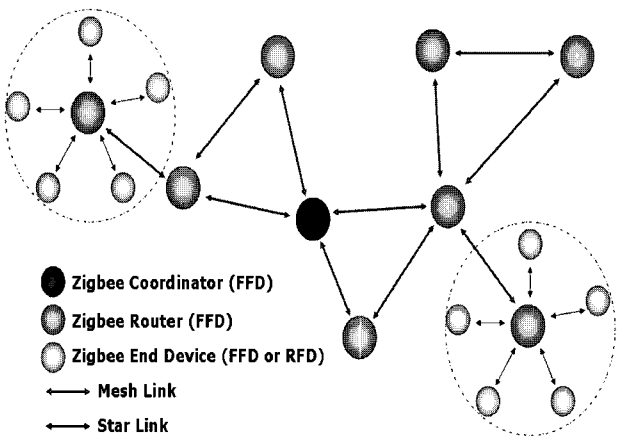
2.4.1 기술배경

ZigBee는 802.15.4 표준에 의해 제작되어 802.15.4와 유사한 특징을 가진다[8].

- 205 kb/s와 20 kb/s의 데이터 전송율
- 마스터 슬레이브 혹은 피어 투 피어 동작
- 최대 254개 네트워크 기기 혹은 64516개 분개점
- 조이스틱과 같은 보조 기기에 대한 지원
- CSMA/CA 채널 액세스
- 코디네이터에 의한 자동 네트워크 설치
- 동적 어드레싱 기기
- Fully Agreed upon protocol for transfer reliability
- 저전력 소모를 보증하는 전력 관리
- 채널이용 <표 2>

2.4.2 Zigbee 네트워크

모든 Zigbee 네트워크는 <그림 4>와 같이 적어도 하나의 RFD또는 FDD를 갖는 네트워크 코디네이터와 확장된 네트워크 토폴로지에 의해 요구되는 링크와 폼 브리지에 FDD와 네트워크 코디네이터를 사용하게 된다. Zigbee 네트워크는 연결성과 기능에 기초하여 자율적으로 모양을 이룰 수 있다.



<그림 4> Zigbee 네트워크

2.5 프라이버시

U-Commerce환경은 상거래 정보의 질을 높여 인센티브 체계를 세우는 효과를 이끌지만 반대로 역효과를 낳을 가능성을 가진다. 체계적 정보 저장이 프라이버시 침해로 이어질 가능성을 지니고 있기 때문이다.

그러나 아무리 인센티브 체계를 잘 정립하여 각각의 경제주체들에게 이익과 효용을 제공한다 할지라도 프라이버시가 심각하게 침해될 요인이 존재한다면 U-Commerce에 참여하지 않은 소비자들이 생길 것이다.

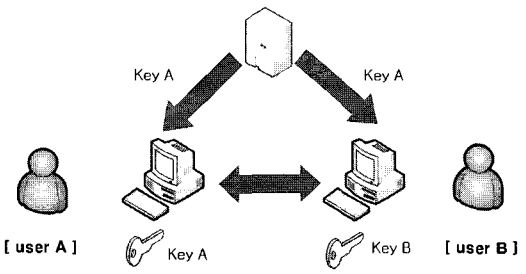
이탈자들이 많이 생겨난다면 디지털 네트워킹에서 중요한 네트워크 효과가 발생하지 않게 될 것이므로 사용이 활성화될 가능성이 줄어든다.

따라서 프라이버시를 보호할 수 있는 방안이 반드시 제공되어야 할 것이다.

많은 유비쿼터스 컴퓨팅 연구에서 프라이버시를 보호하기 위한 방안을 제안하였다. 주로 원칙 혹은 요구사항(principle or requirement)을 제시하거나 유저 모델링을 제안하였는데, 원칙이나 요구를 제시하는 연구로는 Bellotti & Sellen (1993), Langheinrich (2002, 2001), Jiang (2002), Holtjona & Fiona (2004) 등이 있고, 유저 모델링을 제안한 연구는 Jiang et al. (2002), Lederer et al. (2002) 등이 있다[13].

2.6 공개키 암호

비밀키 암호화 시스템의 가장 큰 문제점은 바로 메시지의 송신자와 수신자가 비밀키를 사전에 서로 주고받아야 한다는 것이며 또한 송신자와 수신자가 단 2명일 경우는 상관이 없지만 그 수가 늘어날수록 보관하여야 할 암호키가 기하급수적으로 늘어난 다는 것이다.

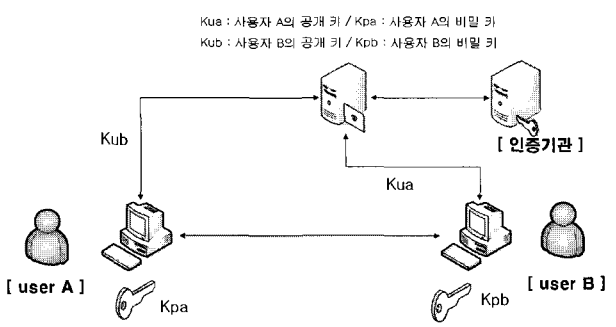


<그림 5> 비밀 키 기반구조

예를 들면 4명이 서로 정보를 주고받을 경우에는 6개의 공통키(비밀키)가 필요하며, 6명일 경우는 10개, 6명일 경우는 15개, 50명일 경우는 1000개 이상의 공통키가 필요하게 된다 (N명이 서로 통신을 할 경우에는 [N(N-1)/2]개의 공통키가 필요하다). 게다가 공통키가 중복되지 않도록 키 생성에 주의해야 한다. 이렇듯 공통키 암호화는 키관리에 상당한 문제가 있다.

이러한 점을 해결한 암호화 시스템이 공개키 암호화 시스템이다. RSA (Rivest, Shamir, Adleman) 암호 시스템은 매우 큰 정수의 소인수분해가 어렵다는 것을 기초로 이론화된 것이다.

공개키 암호화 시스템에서 각 개인은 개인키와 공개키의 쌍을 만들고 공개키는 전화번호처럼 외부에 공개하고 개인키만 자신이 비밀로 간직한다. 메시지의 전송시 송신자는 수신자의 공개키로 메시지를 암호화하여 보내면 수신자는 자신의 개인키로 그것을 복호화하여 내용을 확인하는 방식이다. 또한 여기서 공개키의 안전성을 위하여 인증기관이 필요하다.



<그림 6> 공개키 기반 구조

2.7 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.

$$(p>3 \text{ 일 때}) E: y^2 = x^3 + ax + b,$$
$$(a, b \in F_q, 4a^2 + 27b^3 \neq 0 \in F_q) \quad (1)$$
$$(p=2 \text{ 일 때}) E: y^2 + xy = x^3 + ax^2 + b,$$
$$(a, b \in F_{2^m}, b \neq 0) \quad (2)$$

<표 3> 시스템 매개변수와 키 크기 (단위: bit)

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

짧은 키 길이를 가지고도, 존재하는 공개키 스킴과 동등한 안전도를 제공한다. <표 3>에서는 키 쌍과 시스템 매개변수 저장에 드는 비트 크기를 제공하였다.

ECC 알고리즘이 짧은 키 길이를 갖는다는 것은 메모리와 대역폭 및 CPU 처리능력이 제한된 이동 통신기기 및 스마트 카드에서 효율적으로 작동될 수 있다는 것을 의미한다. 타원곡선암호(ECC)의 또 다른 이점은 비록 모든 사용자가 같은 기저체 K를 사용한다할지라도, 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[7].

3. 제안 프로토콜

RFID/USN환경은 정보를 전달하는 노드들의 수가 무수히 많다. 2.6절에서 설명한 바와 같이 대칭키의 경우는 노드들의 수가 늘어날수록 관리하는 키가 많아지는 문제가 있어 무선 환경에 적합하지 않아 비대칭키

방식이 적합하다. 비대칭키 방식은 현재 유선 전자서명에서 가장 많이 사용되는 방식으로 RSA 방식이다. 하지만 무선의 특성인 소형, 경량, 저전력의 환경에는 유선과는 다른 방식을 이용해야 한다. <표 3>에서 언급한 바와 같이 동일 성능을 위하여 필요한 공개키와 비공개키의 크기가 ECC가 가장 적다.

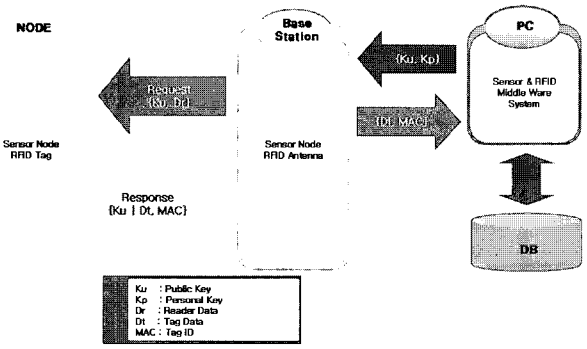
무선 환경에서의 안전한 보안을 위한 방안이 필요하다. 무선을 위한 방안으로 2.3절에서 언급한 SNEP방안이 있다. SNEP에서는 키 관리를 위한 방안으로 RC5를 사용하고 있다. 어떤 환경에서 사용하느냐에 따라 차이가 있겠지만 해쉬를 이용하는 RC5방법은 간단한 데이터 보안을 위한 방안에는 충분하지만 중요한 데이터 보안에는 사용하기에는 문제가 있다.

이에 무선을 위한 프로토콜로 SNEP와 암호화 알고리즘으로 ECC를 사용한 프로토콜을 제안한다.

3.1 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 확인하는 절차를 수행한다.

수행 단계는 다음과 같다.



<그림 7> 주요 흐름도

첫 번째, 임의의 필드로 설치되는 노드들은 설치 전 관리 시스템에 노드들의 고유 정보 식별을 위하여 MAC 정보를 저정한다.

두 번째, PC에서 설치를 위한 Node A의 두 개의 키 쌍을 생성 {공개키 : Ku, 비공개키 : Kp} 한다. 이 중 비밀키를 Node A에 저장한다.

세 번째, 설치가 완료된 Node와의 통신을 위해서는 BaseStation에서 각각의 Node로 Request 데이터 {Rpc}를 전송한다. (이 작업은 배터리 보호를 위하여 일반적으로 sleep 상태에 있는 장비들을 깨우기 위한 작업이다.)

네 번째, 암호화 데이터를 받은 해당 Node A는 고유 정보인 MAC을 공개키로 암호화한 데이터 [Kp(MACa + Rpc)] 를 BaseStation으로 보낸다.

다섯 번째, 정보를 받은 BaseStation에서는 복호화를 수행하고 해당 Node A의 정보{MACa} 만을 PC로 보낸다.

여섯 번째, Node A에서 전송 받은 MACa을 전송 받은 PC의 DB에 저장되어 있는 MACa의 정보를 확인하여 인가된 Node임을 확인한다.

일곱 번째, 인가된 Node임을 확인 하였다면 통신한다.

ECC암호화 알고리즘은 클럭수가 최대 140MHz까지 동작을 하며 이 경우의 성능은 약 64kbps며 이는 하나의 163-비트 데이터 프레임을 처리하는데 2.5msec가 소요됨을 의미한다.[15]

무선 에서도 이런 ECC 암호화 알고리즘을 이용하는 시스템은 효율적이다. 하지만 데이터가 노드 수에 따라 기하급수적으로 증가하는 USN 시스템에서 모든 데이터를 암호화 한다면 데이터 처리와 전력면에서 비효율적인 시스템이 될 것이다.

그래서 본 논문에서는 센서가 설치된 환경 하에서 통신을 위한 프로토콜을 제안 하였다.

통신을 하기 전 노드의 고유 정보인 MAC만을 암호화를 통하여 전송받고 이를 인증하여 인증된 Node임을 파악하고 파악된 노드와 통신을 한다. 지속적으로 통신이 이루어지지 않는 경우 일정 시간을 두어 이런 인증 절차를 통하여 다시 인증 받게 한다.

4. 결 론

유비쿼터스 환경은 먼저 RFID를 중심으로 발전하고 이에 감지기능이 추가되고 이들 간의 네트워크가 구축되는 USN 형태로 발전할 것으로 전망되고 있다. 그러나 이러한 자동화시켜 정보를 손쉽게 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.

본 논문에서는 센서를 대상으로 유선에서 사용하고 있는 인증 방법을 무선에서 사용이 가능하도록 SNEP와 암호화 알고리즘으로 ECC를 이용하여 설계 하였다.

하지만 현재 논문의 단계에서는 Basestation과 노드

와의 통신을 설명 하였다. 2.4절에서 설명한 Zigbee의 경우 Node와 Node간의 통신이 주가 된다.

현재 RFID/USN의 보안 표준이 존재하지 않기 때문에 향후 기술적인 표준이 되기 위해서는 Node와 BaseStation간의 인증 부분과 더불어 Node간 통신에 대한 부분, 인증을 할 때 적합한 Node가 아닌 경우에 어떻게 Node를 제외시킬 것인가에 대한 부분, 그리고 통신이 이루어지는 중간에 데이터의 변조나 침입 시도와 같은 불법적인 행위에 대한 판단 기준역시 필요하다.

5. 참 고 문 헌

[1] 강달천, 주학수, 권혁조, "개인정보 보호를 위한 RFID 신뢰 확보가 중요하다", KISTI, (2004. 11)

[2] 조준혁, "RFID 태그의 프라이버시를 위한 기술적인 접근" , KISTI, (2005. 03)

[3] 유승화, 유비쿼터스 사회의 RFID , 전자신문사, (2005. 03) :59-60,

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

[5] Klaus Finkenzeller, "유비쿼터스 컴퓨팅의 핵심 RFID HandBook," 영진출판사, (2002)

[6] http://www.zigbee.org/en/index.asp, Zigbee 포럼

[7] 박창섭, "암호이론과 보안," 대영사, (1999) :129-136,

[8] IPV6포럼코리아, "차세대 인터넷 프로토콜 IPv6," 다성출판사, (2002)

[9] 서운석, 신순자, 김유정, 신상철, "센서 네트워크 보안 프로토콜 소개와 향후 과제", 정보과학회지, (2004)

[10] 정보통신부, "u-센서 네트워크구축 기본계획," (2004. 02)

[11] 김광조, "RFID/USN 정보보호 기술," KISTI TTA 저널 95호, (2004).

[12] 조대진, "RFID 이론과 응용," 홍릉출판사, (2005) :3-4

[13] 조위덕, 이경전, 이호근, 권오병, 김경규, 이은종, "유비쿼터스 패러다임과 u-소사이어티," JinhanM&B, (2006. 10) :91

[14] 이성재, 김학범, 염흥열, "무선 센서 네트워크를 이용한 무인 경비 시스템에서의 OMAC-SNEP 기술에 관한 연구," 한국정보보호학회, 16(1), (2006) :105-114

[15] 정용진, 김종만, 김영필, 김성두, 이석용, 전신우, "스마트카드용 다원곡선 암호 알고리즘(ECC) 하드웨어 설계에 관한 연구," 광운대학교, 정보통신부, (2001. 07)

저 자 소 개

박 상 현

인천대학교 공학 학사와 석사를 취득하였으며, 현재 인천대학교 컴퓨터 박사과정 중. 관심분야는 RFID/USN, 암호학, 컴퓨터 통신

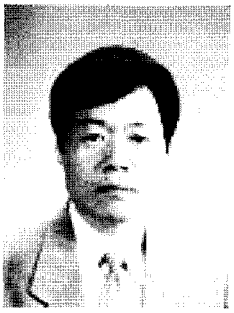
주소: 인천시 계양구 계산동 계산주공아파트 105동 1010호

박 상 민

한양대학교 산업공학과 공학사를 취득하였으며, 한양대학교에서 산업공학과 공학 석사와 박사를 취득하였으며, 현재 인천대학교 산업경영공학과 교수로 재직중이다. 관심분야는 e-Logistics

주소: 서울시 강남구 대치동 896-21

신 승 호



경희대학교에서 전자공학과 공학사를 취득하였으며, 경희대학교에서 공학석사와 박사를 취득하였으며, 현재 인천대학교 컴퓨터공학과 교수로 재직중이다. 관심분야는 컴퓨터 통신, 신호처리, 암호학

주소: 서울시 서대문구 남가좌동 173-18