# 안전한 USN을 위한 정보보호기술 동향

## Trend of Secure USN Information Protection Technology

21세기를 대비하는 정보보호 특집

이신경 (S.K. Lee) RFID/USN보안연구팀 선임연구원
이해동 (H.D. Lee) RFID/USN보안연구팀 선임연구원
정교일 (K.I. Jung) RFID/USN보안연구팀 책임연구원
최두호 (D.H. Choi) RFID/USN보안연구팀 팀장

목 차



* 본 연구는 지식경제부 및 정보통신연구진흥원의 IT핵심기술개발사업[2005-S-088-04, 안전한 RFID/USN을 위한 정보보호 기술] 사업의 일환으로 수행하였음

다수의 센서 노드들이 무선 네트워크로 구성된 센서 네트워크상에서 전송되는 정보를 안전하게 보호하기 위한 방법은 내부적으로 센서 노드의 보안 기능을 추가하는 것 뿐만 아니라 전체 네트워크를 보호하기 위한 계층적인 보안 요구사항을 만족하여야 한다. 이에 본 고에서는 센서 네트워크의 보안 요구사항을 분석하고, 관련 암호 알고리듬과 네트워크 프로토콜, 그리고 표준화 동향을 살펴본 후 센서 네트워크의 특성을 고려한 안전한 정보보호기술을 소개한다.

# Ⅰ. 서론

USN은 다수의 센서 노드로 구성된 무선 네트워크로써 다양한 위치에 설치된 센서 노드들로부터 사람과 사물, 그리고 환경 정보를 인식하고, 인식한 정보를 통합·가공해 언제, 어디서나, 안전하고 자유롭게 이용할 수 있게 하는 정보서비스 인프라를 뜻한다. 센서 네트워크는 다양한 환경에서 주변상황을 모니터링하고 필요한 정보를 센싱하는 용도로 사용되기 때문에 센서 노드의 정보 신뢰성이 매우 중요하다[1].

그러나 수많은 센서 노드들이 감지된 정보를 베이스스테이션으로 보내는 데 있어 각 센서 노드들의 제한된 전력은 빈번한 네트워크의 진입과 탈퇴를 발생하여 잦은 토폴로지의 변화를 가져오고, 이는 수집되는 정보의 신뢰성을 떨어뜨리는 결과를 가져온다[2]. 이러한 가운데 악의적인 노드가 센서 노드로 가장하여 네트워크에 진입하게 되면 잘못된 정보를 전파하거나 라우팅 정보를 혼란시켜 센서 네트워크의 보안 취약점을 가중시킬 수 있다. 특히 노드들이 배치된 물리적 환경이 공격에 그대로 노출되어 전송되는 정보가 변경되거나 유출되어 정보의 기밀성 및 무결성을 쉽게 무너뜨릴 수 있다[1]-[3].

더욱이 이러한 공격의 파급 효과는 단순히 센서 노드만의 문제만이 아니라 USN 서비스를 사용하는 일상 생활까지 확대 가능하여 그 파급효과는 매우 클 것으로 예상된다. 이렇다 보니 보안을 강화하기 위한 방법으로 내부적으로 센서 노드의 보안기능을 추가하는 것 이외에도 외부적으로 보안위협으로부터 전체 네트워크를 보호하기 위해 네트워크의 모든 부분에 보안 기능을 도입하는 계층적 보안이 관심을 모으고 있다[4].

이에 본 고에서 안전한 USN 환경을 위한 정보보호 기술의 개발 동향을 소개한다. 이를 위해 먼저 센서 네트워크의 보안 요구사항을 분석하고, 관련 암호 알고리듬과 네트워크 프로토콜, 그리고 표준화 동향을 살펴본 후 센서 네트워크의 특성을 고려한 안전한 정보보호기술을 소개한다.

# Ⅱ. USN의 보안 요구사항

## 1. USN Cryptographic Algorithms

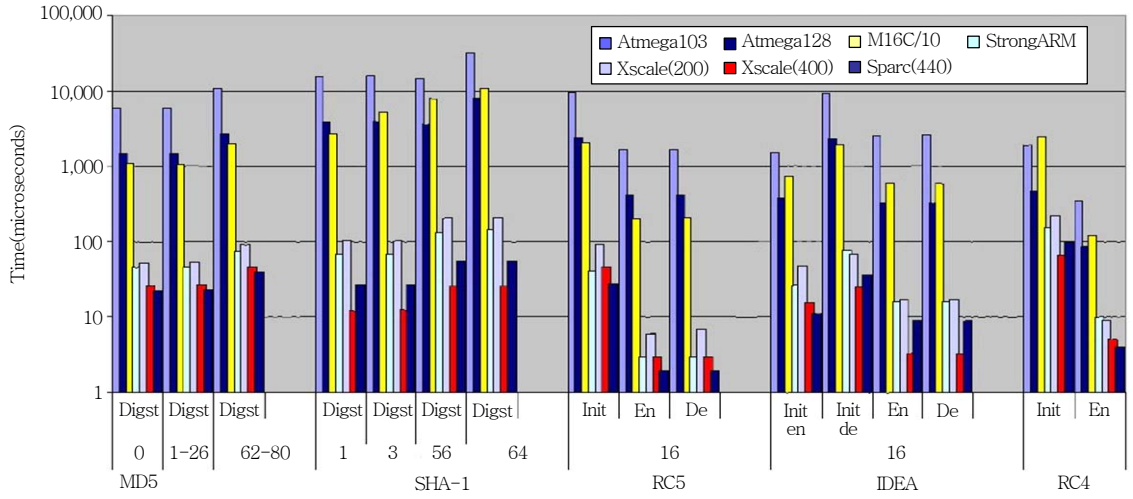
USN의 안전한 서비스 제공 및 보안 응용 서비스의 출현을 위해서, 일반적인 보안 요구사항인 기밀성, 무결성, 인증, 부인방지를 구현하는 암호학적 방법이 적용되며, 자원제약성이라는 USN 환경에 적합한 경량의 저전력 특성을 가지는 암호 알고리듬이 필요하다. 본 절에서는 USN 환경에 사용되거나, 사용될 목적으로 연구되고 있는 대칭키 암호 시스템과 공개키 암호 시스템으로 구분하여 암호 알고리듬을 소개한다.

### 가. USN을 위한 대칭키 암호 알고리듬

USN 시스템은 작은 임베디드 기기상에서 구현되며, 이러한 임베디드 장치는 다양한 CPU 플랫폼을 가진다. CPU의 종류에 따라 연산은 8bit, 16bit, 32bit 단위로 수행된다. (그림 1)은 Atmega 103, Atmega 128, M16C/10, StrongARM SA-1110, XScale PXA250, UltraSPARC Ⅱ 등의 플랫폼상에서, 보안에서 폭넓게 사용되고 있는 암호 알고리듬인 RC4, IDEA, RC5, MD5, SHA-1의 성능을 비교하였다[5].

그 결과 Atmega 103에서는 RC5에 비해 RC4가 다소 빠른 성능을 보였으며, StrongARM에서는 RC5가 RC4보다 3배 빠른 성능을 보였다. 이러한 성능 차이는 RC5가 32bit 워드단위로 동작하며, RC4가 8bit 워드단위로 동작하기 때문이다. Atmega 103에서 RC5와 IDEA를 비교할 경우, RC5가 1.5배 빠른 성능을 보인다. 결과적으로 저사양의 프로세서상에서는 RC4가 RC5보다 좋은 성능을 보여준다. 센서 네트워크 시스템의 CPU 종류에 따라 적절한 알고리듬을 선택하는 것이 필요하다.

TinyOS 기반 Mica2 센서 모트는 링크 레벨의 암호 및 기밀성 제공을 위해서 TinySec[6]을 사용하였다. TinySec에서 사용되는 알고리듬은 64bit 블록 암호인 SkipJack과 RC5 대칭키 암호 시스템




(그림 1) 알고리듬, 플랫폼에 따른 암호 연산시간 비교[5]

이다. 상기 알고리듬은 저전력 동작을 위해서 선정되었으며, C 언어 단독 혹은 C와 어셈블리어를 함께 사용하여 소프트웨어로 구현되었다. <표 1>에서 알 수 있듯이 RC5(C)의 경우 0.90ms의 연산시간을 필요로 하며, 계산복잡도가 큰 연산에서 어셈블리어를 함께 사용함으로써 암호연산을 0.26ms 내에 처리할 수 있다.

USN 센서 노드의 통신에 가장 널리 사용되는 RF 통신 칩으로는 TI사의 CC2420[7], CC2430 등이 있다. 상기 RF 칩에서는 AES-128 암호 알고리듬을 하드웨어 가속기로 제공한다. 이를 사용하여 센싱 데이터 통신에서의 기밀성을 보장받을 수 있다. CC2420에서 제공하는 AES 암호 가속기는 <표 2>와 같이 Counter 모드, CBC-MAC 모드, CCM 모드를 지원하며, AES-CCM 동작 성능이 222 $\mu$sec로 USN 환경에서 충분히 사용할 수 있음을 알 수 있다. 즉, AES-CCM 모드를 사용하더라도 기존의 데이터 전송에 영향을 주지 않음을 의미한다[8].

[9]에서는 RFID 태그 혹은 USN 센서와 같은 유비쿼터스 컴퓨팅 기기에 적합한 64bit 블록 길이와 128bit 키 길이를 가지는 새로운 블록 암호(HIGHT)를 제안하였다. <표 3>은 AES와 HIGHT의 성능비교표로 HIGHT는 0.25$\mu$m technology에서 3048 gate 면적으로 구현되었으며, 최대동작 주파수 80

〈표 1〉 TinySec Cipher Performance[6]

| Cipher & Implementation | Time(ms) | Time(byte times) |
|---|---|---|
| RC5(C) | 0.90 | 2.2 |
| SkipJack(C) | 0.38 | 0.9 |
| RC5(C+ assembly) | 0.26 | 0.6 |

〈표 2〉 CC2420 AES 가속기 동작 특성[8]

| Mode | L(a) | L(m) | L(MIC) | Time($\mu$s) |
|---|---|---|---|---|
| CCM | 50 | 69 | 8 | 222 |
| CTR | - | 15 | - | 99 |
| CBC | 17 | 98 | 12 | 99 |
| Stand-aloned | - | 16 | - | 14 |

* a: authentication payload, m: message, MIC: Message Integrity Code, L(x): byte length of x

〈표 3〉 AES와 HIGHT 성능 비교[9]

| Algorithm | Technology ($\mu$m) | Area (GEs) | Throughput (Mbps) | Max Frequency (MHz) |
|---|---|---|---|---|
| AES[10] | 0.35 | 3400 | 9.9 | 80 |
| HIGHT | 0.25 | 3048 | 150.6 | 80 |

MHz상에서 150.6Mbps throughput의 좋은 성능을 보이고 있다[9],[10].

### 나. USN을 위한 공개키 암호 알고리듬

USN 네트워크의 자원 제약성 때문에 초기 센서

네트워크 보안은 대칭키를 기반으로 연구되어 오다가 현재 공개키 시스템을 적용하려는 시도가 활발히 진행되고 있다. 공개키 시스템으로 폭넓게 사용되는 암호 알고리듬인, 인수분해의 어려움에 기반한 RSA 알고리듬이나 ElGamal은 서버나 개인 PC와 같은 플랫폼의 자원을 요구하므로 USN 환경에서는 적용하기에 어려움이 있다. RSA와 동일한 암호 안전성을 제공하면서도 작은 키를 사용하는 다양한 공개키 알고리듬이 소개되어 있다. 본 절에서는 USN 정보보호에 사용되는 공개키 알고리듬을 살펴본다.

미국 매사추세츠의 WPI에서는 경량 센서 노드에 탑재 가능한 저전력 공개키 암호로 Rabin, Ntru을 구현하고 성능 특성을 분석하였다. 상기 공개키 암호 알고리듬은 RSA와 동일한 보안 안전성을 제공하면서도, ECC 연산의 다소 낮은 저전력 구현 특성을 보완할 수 있다. Rabin 기법은 RSA의 특별한 하나의 형태로써, 인수분해 문제의 어려움에 기반한 공개키 암호 시스템으로 1979년 Rabin이 제안하였으며, NtruEncrypt는 SVP의 어려움에 기반한 공개키 암호 시스템으로 1996년 Hoffstein, Pipher와 Silverman이 제안하였다. <표 4>는 Rabin 기법과 Ntru 성능 특성을 보여주고 있다. 적절한 알고리듬과 구현 파라미터를 선정하고 저전력 기술을 적용할 경우, 전력 소비를 20$\mu$W 이하로 암호 연산을 수행할 수 있다. 이는 배터리 전지를 사용하는 센서노드 환경에서 충분히 사용할 수 있음을 보여준다.

〈표 4〉 Rabin's Scheme과 Ntru 성능 특성[11]

| | Rabin | Ntru(k=1) | Ntru(k=84) |
|---|---|---|---|
| Equivalent security | 60bits | 57bits | 57bits |
| Area[eqv. gates]<br>- combinational<br>- storage elements | 16,726<br>8,875<br>7,851 | 2,850<br>523<br>2,327 | 16,200<br>7,000<br>9,200 |
| Delay(avg. # cycles) | 1,440 | 29,225 | 433 |
| Avg.power@500kHz<br>- static(%)<br><br>- dynamic(%)<br><br>- peak power | 148.18$\mu$W<br>117.5$\mu$W<br>(79.3%)<br>30.68$\mu$W<br>(20.7%)<br>169.8$\mu$W | 19.13$\mu$W<br>15.10$\mu$W<br>(78.9%)<br>4.03$\mu$W<br>(21.1%)<br>20.22$\mu$W | 118.7$\mu$W<br>103.06$\mu$W<br>(86.8%)<br>15.64$\mu$W<br>(13.2%)<br>n/a |
| Energy<br>- per bit encrypted | 426.76nJ<br>833.5pJ<br>(512bits) | 1,118.15nJ<br>4,235.41pJ<br>(264bits) | 102.79nJ<br>389.4pJ<br>(264bits) |
| Throughput | 177.8<br>kbits/s | 4.52<br>kbits/s | 304.85<br>kbits/s |

노스캐롤라이나 주립 대학에서 타원 곡선 암호 알고리듬을 TinyOS 상에서 구현하여 키를 안전하게 분배하고 있으며, 실제 사용을 위해 타원 곡선 기반 암호화 프로토콜인 ECIES와 키 분배 프로토콜인 ECDH, 서명 기법인 ECDSA 프로토콜을 구현하였다[8],[12]. 해당 기술은 MICAz와 Telosb, Tmote Sky에서 사용할 수 있으며, SECG에서 추천하는 128bit와 160bit, 192bit 타원곡선을 사용하고 있다. 성능을 보면 전자서명에 3.17초, 검증에 4.04초가 소요된다. 이는 비록 대칭키 암호 알고리듬 기반의 키 분배 기법보다는 다소 긴 시간이지만, 실제 응용에 사용되는 경우에도 충분히 실제 사용할 수 있는 시간이다[8].

XTR 공개키 암호 알고리듬은 Crypto2000에서 처음 소개되었고, 안전성의 관점에서 볼 때, 부분군에서의 DLP 문제에 기반을 두고 있다. 그러나 XTR은 부분군의 원소를 표현하고 계산하는 데 표준적인 방법을 사용하지 않으며, 전통적인 방법보다 대폭적인 통신상/계산상의 이점을 갖는다. 1024bit RSA의 안전성과 동일한 XTR은 ECC에 기반을 둔 암호 시스템과 속도 및 안전성 면에서 비슷하다. XTR의 공개키는 ECC보다 두 배 정도 크지만 RSA와 ECC의 파라미터 초기화 시간보다 무시할 만큼 작은 시간이 소요된다. 따라서 XTR은 센서 네트워크 환경에서 RSA와 ECC의 좋은 대안이 될 수 있다[13].

## 2. USN Network Protocol

센서 네트워크의 네트워크 계층은 다수의 노드로 구성되며, 이동성을 고려할 경우 네트워크의 토폴로지의 빈번한 변화로 라우팅 정보의 갱신을 필요로 한다. 무선 센서 네트워크의 전송거리 제약으로 센서 노드들의 통신은 멀티 홉 통신방식을 기본으로 라우팅을 하게 되며, 제한된 용량의 배터리를 사용하기 때문에 에너지 상태를 염두한 통신방법도 고

려할 필요가 있다[14].

센서 네트워크의 보안을 위한 네트워크 계층에서의 프로토콜로는 SPINS가 제시되어 있다. SPINS는 크게 두 가지 기술인 SNEP와 $\mu$TELSA로 나뉘어지고, SNEP는 데이터의 비밀성, 양단간의 데이터 인증, 재사용방지, 무결성 등을 제공하는 역할을 하며, $\mu$TELSA는 데이터 브로드캐스트에서의 인증을 담당한다[14].

암호 프로토콜에 대해서는 수많은 논의가 있었고, 암호화 방식이 네트워크 보안에 얼마나 중요한지 또한 자주 거론되어 왔다. 하지만 암호화 프로토콜 자체만으로 센서 네트워크의 안전성을 보장할 수는 없다. 아무리 보안 프로토콜이 잘 갖추어 있더라도 내부로부터의 보안 위험에서 자유로울 수는 없기 때문이다. 게다가 현재의 센서 네트워크는 응용되는 분야의 특성에 따라 ZigBee, IEEE802.15.5, IP-USN, WiBEEM 등 다양한 무선 접속 기술이 적용되기 때문에 그에 따른 보안의 적용도 단순하지만은 않을 전망이다[4],[14].

### 3. 표준화

USN 기술의 표준화는 이제 시작단계라 할 수 있다. 해외의 USN 표준화 접근 방향이 기존의 기술로부터 USN으로의 기술을 접근하고 있다면 국내의 경우 USN 기반 기술을 시범사업으로 활용하면서 기술과 응용서비스 모델의 표준화를 맞춰가고 있다. USN이 여러 기술의 결합인 만큼, 각각의 기술들이 적용되는 비즈니스 모델에 따라 요구하는 프로토콜이 모두 달라 개별적으로 표준을 갖춰가고 있다. USN과 관련된 주요 국제표준화 기구는 ITU-T, ISO/IEC JTC 1/SC 6, IETF, IEEE, 지그비 얼라이언스 등이 있으며, 각각의 전문 분야에 대한 표준화를 추진하고 있다[15].

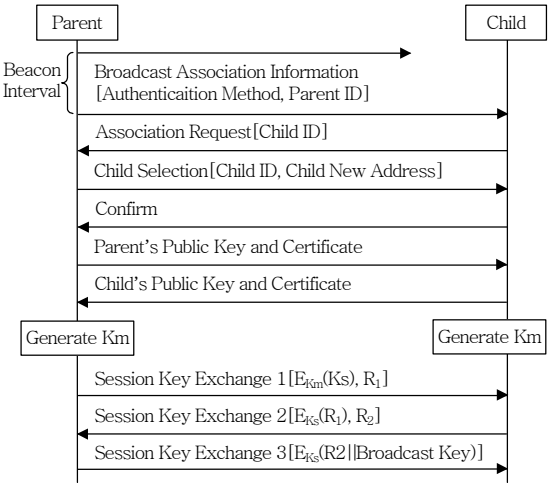
국내 표준의 경우 2007년 12월에 2008년 추진되는 USN 중점 확산사업에 공통으로 적용되는 주파수와 정보보호 등의 표준, 응용서비스별 수요자 요구사항, USN 시스템 구축에 필요한 가이드라인 등 표준화 전반에 걸친 협의를 진행하기로 결정했다[15].

## Ⅲ. 안전한 USN을 위한 정보보호 기술 개발

### 1. USN 보안 노드

현재 ETRI에서는 보안 센서 노드에 필요한 키 분배 프로토콜 및 이에 필요한 ECC 연산 모듈을 TinyOS 상에서 소프트웨어 구현[8] 및 전용 하드웨어[16]를 개발하였다.

(그림 2)는 트리 구조의 센서 네트워크에서 센서 노드들이 부모-자식 관계로 키의 생성과정을 보여준다. 부모 노드와 자식 노드는 공개키를 교환하면서 ECDH 키 생성과정을 수행하며, ECC 연산은 TinyECC 0.3을 기반으로 수정하였다. 부모 노드가 데이터 암호화에 사용할 세션키 Ks를 난수로 생성한 후, ECDH로 공유된 키 Km을 사용하여 자식 노드에게 안전하게 전달한다. 이때 난수 R1, R2를 사용하여 Km의 동일성을 검증하므로 세션키 생성과정을 통하여 노드 상호간의 인증과정도 이루어지게 된다. 키 생성시간은 14~15초 정도로 센서 네트워크 설정 단계에서 충분히 적용할 수 있는 시간이다.




(그림 2) 공개키 기반 키 생성과정[8]

〈표 5〉 ECC 연산 시간[16]

| Operation | Time |
|---|---|
| Scalar Multiplication(Np) | 49ms |
| ECC Addition(P+ G) | 220$\mu$s |

또한 위의 설정시간을 줄이기 위해서 ECC 연산을 전용 하드웨어로 구현하였다. ECC 연산은 사용 좌표에 따라 설계 구조 및 성능이 달라지며, 저면적/저전력 구현을 위해서 affine 좌표로 사용하여 설계하였다. 설계된 ECC 모듈은 0.25$\mu$ 삼성 공정으로 하드웨어 합성시 22k 게이트의 면적으로 구현되며, MSP430 MCU 기반의 USN 보안 노드의 시스템 클럭인 4MHz로 동작시 연산 성능은 <표 5>와 같다.

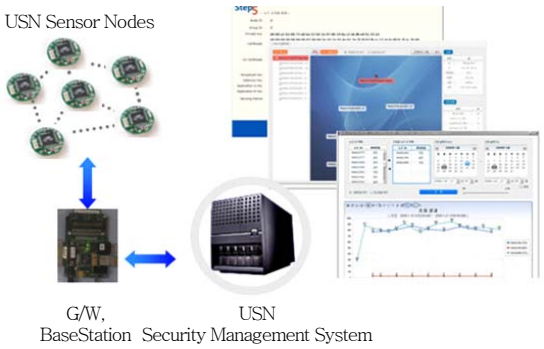
## 2. USN 보안관리시스템

센서 네트워크의 다양한 위협으로부터 데이터를 보호하기 위해서 노드의 인증과 센서 노드들간의 암호화 통신이 이루어져야 한다[17]. 노드의 인증과 암호화 통신이 정보의 무결성과 기밀성을 제공하기 위한 링크 계층 및 네트워크 계층에서의 보안이라면 보안관리는 보다 상위계층에서의 보안기술을 의미한다.

현재의 센서 네트워크는 네트워크 자체의 구성과 응용서비스들의 구현에 연구개발이 집중되어 있어 매니지먼트(관리)라는 개념을 고려하고 있지 않는 실정이다. 그러나 점차 엔드-투-엔드 보안이 확장되고 있으며, 이에 따라 보안도 네트워크처럼 계층화되는 움직임을 보이고 있다[4],[9].

일반적인 의미의 보안 관리는 외부 침입에 대한 단순한 모니터링을 나타내고 있다. 하지만 근래에는 보안을 계층적으로 구현하여 네트워크 각 부분의 보안을 적용하는 동시에 이렇게 네트워크 내에 퍼져 있는 보안 기능을 통합 관리하여 새로운 보안 위협으로부터 네트워크를 보호한다는 통합적인 보안 관리 서비스를 지칭한다.

기존 유선 망의 경우 관리서비스는 초기 네트워크 토폴로지가 구성되면 그 변화가 많지 않아 설치된 장비의 고장이나 장비들의 성능에 초점을 두고



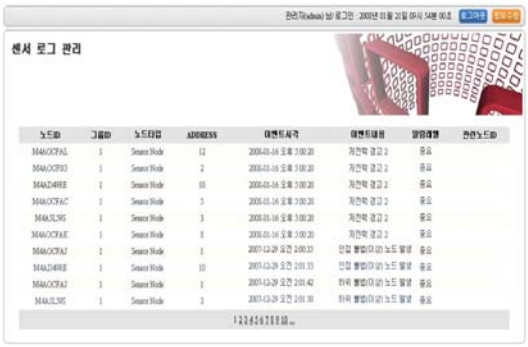

(그림 3) 센서 네트워크의 기본 구성도[3]

관리를 하였지만 센서 네트워크의 경우 관리대상이 네트워크 장비들이 아닌 센서가 분포된 지역과 그 지역에서 올라오는 정보를 중요시하기 때문에 좀 더 다른 측면에서의 서비스를 제공하여야 한다[2].

USN 보안관리시스템은 사용자나 네트워크 관리자가 센서 노드와 센서 게이트웨이로 구성된 센서 네트워크를 보다 쉽고 용이하게 관리하기 위한 시스템으로 보안에 특화된 기능을 중심으로 다루고 있다. USN 보안관리시스템은 센서 네트워크의 모든 관련 정보를 한눈에 볼 수 있으며, 공격의 예비단계인 스캐닝을 경고하고, 실제 공격 시에는 적절한 제어가 가능한 기반을 제공하는 것을 목적으로 하고 있다.

센서 네트워크의 기본구성은 다수의 센서와 베이스스테이션으로 이루어져 센서들이 감지한 정보를 중앙의 베이스스테이션으로 전송하며 이는 다른 유선 망과의 연동을 위해 게이트웨이를 거쳐 사용자나 관리자에게 웹 인터페이스를 통해 전달하게 된다. (그림 3)에서와 같이 본 고에서의 게이트웨이는 베이스스테이션 노드가 포함된 형태로 센서 노드들로부터 데이터를 전송 받아 이를 보안관리시스템으로 보내거나 보안관리시스템으로부터 데이터를 받아 필요시 각 센서 노드로 명령을 전달하는 기능을 수행한다[2],[3].

보안관리시스템은 센서 노드들이 배치되기 전에 노드 초기화 과정을 실행하여 인증서를 발급하고 노드간 키 생성을 위한 Km을 공유하게 된다. 이렇게 설정된 노드들은 공개된 장소에 배치되어 라우팅 경




(그림 4) 보안관리시스템의 이벤트 로그관리 화면

로가 결정되는 시점에 노드들의 인증이 이루어지고, 이로써 인증을 통과한 노드들만 상호 통신이 가능하고 인증을 받지 못한 센서 노드는 센서 네트워크의 통신 도메인에 참여할 수 없도록 하여 네트워크 공격으로부터 방어를 할 수 있도록 한다[8].

센서 네트워크가 유지되는 동안에도 공격 노드가 다른 노드와 통신을 시도하려고 하면 관련 노드들은 보안 이벤트를 발생시켜 이를 보안관리시스템에게 전달한다. (그림 4)는 보안 관리시스템에서 웹을 통해 보안 이벤트를 확인하는 화면으로 인접노드의 인증과 관련된 보안 이벤트와 센서 네트워크의 토폴로지 변화에 큰 영향을 끼치는 전력소모의 이벤트 정보 등을 수집하여 경고 및 이력 정보를 제공하고 있다.

## Ⅳ. 결론

2008년도 부산시의 U-시티 사업을 비롯하여 U-헬스, U-응급의료확산서비스, 온천천 홍보 예경보 시스템 구축 등 전국적으로 총 602억 원 규모의 RFID/USN 사업을 추진할 것으로 조사됐다. 이렇게 다양한 곳에서 USN에 대한 시범 및 확산 서비스가 진행되고 있음에도 불구하고 USN에 적용되는 네트워크 프로토콜은 표준화된 인터페이스 없이 여전히 다양하게 적용되고 있으며, 자원제약으로 PKI와 같은 고급 보안 기능을 적용하기 힘들기 때문에 보안 기능이 강화된 센서 노드들은 찾아보기 어려운 현실이다.

이에 본 고에서 USN 환경에 사용되거나, 사용될 목적으로 연구되고 있는 암호 알고리듬을 소개하였으며 네트워크 계층의 보안 요구사항과 표준화에 대하여 살펴보았다. 더불어 안전한 USN 환경에서의 정보보호를 위해 센서 노드의 키 분배 프로토콜, TinyOS 기반의 소프트웨어 및 전용 하드웨어 ECC 모듈을 설명하였다. 특히 센서 노드의 인증과 암호 알고리듬을 적용하는 것만으로 모든 센서 네트워크의 공격이 방어됨을 의미하지는 않기 때문에 USN의 보안 관리 시스템을 통해 관련된 정보를 관리하고 센서 노드들을 제어함으로써 비합법적인 노드들의 진입을 탐지하거나 암호화 방식의 적용, 네트워크 계층에서의 공격을 감지하여 보다 안전한 센서 네트워크에 대한 관리를 가능할 수 있도록 하였다.

### ● 용어해설 ●

TinyOS: UC 버클리에서 진행해 온 스마트 더스트(Smart Dust) 프로젝트에 사용하기 위하여 개발된 컴포넌트 기반 내장형 운영체제

타원 곡선 암호 방식(ECC): 밀러와 코블리츠가 제안한 타원 곡선 기반 암호로써, 이산대수에서 사용하는 유한체의 곱셈군을 타원 곡선군으로 대치한 암호방식

## 약 어 정 리

| | |
|---|---|
| μTELSA | 'micro' version of the Timed, Efficient, Streaming, Loss-tolerant Authentication protocol |
| ECC | Elliptic Curve Cryptography |
| ECDH | Elliptic Curve Diffie-Hellman |
| ECDSA | Elliptic Curve Digital Signature Algorithm |
| ECIES | Elliptic Curve Integrated Encryption |
| SECG | Standards for Efficient Cryptography Group |
| SNEP | Secure Network Encryption Protocol |
| SPINS | Security Protocols for Sensor Networks |
| SVP | Shortest Vector Problem |
| WiBEEM | Wireless Beacon-enabled Energy Efficient Mesh network |
| WPI | Worcester Polytechnic Institute |
| XTR | Efficient Compact Subgroup Trace Representation |

# 참 고 문 헌


[1] 이병길, 김호원, "센서 노드 관리를 위한 보안 인터페이스 설계," IPIU2008, 2008, p.184.

[2] 이신경, 이석준, 김호원, "센서 네트워크 관리를 위한 라우팅 공격 모델 설계," IPIU2008, 2008, p.208.

[3] S.H. Lee, N.J. Park, and D.H. Choi, "Security Management for Sensor Network," ICHIT2008, HanNam Univ., 2008.

[4] 신동윤, "보안기술의 변화 이끄는 네트워크컨버전스," http://www.ionthenet.co.kr/newspaper/view.php?idx=12001, 2007. 4.

[5] Ganesan et al., "Analyzing and Modeling Encryption Overhead for Sensor Network Nodes," WSNA'03, Sep. 2003.

[6] Chris Karlof et al., "TinySec: A Link Layer Security Architecture for Wireless Sensor Networks," SenSys'04, Nov. 2004.

[7] CC2420 DataSheet, "CC2420, 2.4GHz IEEE 802.15.4/ZigBee-ready RF Transciever," Chip-con, 2006.

[8] 김호원, 이석준, 오경희, "센서네트워크 보안 기술 개발 동향," 정보보호학회지, 제18권 제2호, 2008. 4.

[9] Deukjo Hong et al., "HIGHT: A New Block Cipher Suitable for Low-Resource Device," CHES'06, LNCS 4249, 2006.

[10] M. Feldhofer, J. Wolkerstorfer, and V. Rijmen, "AES Implementation on a Grain of Sand," *IEE Proc. on Information Security*, Vol.152, Issue 1, 2005, pp.13-20.

[11] Gunnar Gaubatz et al., "Public Key Cryptography in Sensor Networks|Revisited," ESAS'04, 2004.

[12] TinyECC: A Configurable Library for Elliptic Curve Cryptography in Wiress Sensor Networks, Ver 1.0, http//discovery.csc.ncsu.edu/software/TinyECC, 2007. 2. 11.

[13] 한동국, 장상운, 윤기순, 장남수, 박영호, 김창한, "XTR을 가장 효율적으로 구성하는 확장체," 한국정보보학회논문지, 제12권 제6호, 2002.

[14] 이재용, "RFID/USN," 표준기술동향, TTA 저널, 제 100호, 2005. 8.

[15] 이수진, "국내외 USN 표준화 단체 동향," http://www.ionthenet.co.kr/newspaper/view.php?idx=12734, 2008. 2.

[16] 최용제, 김호원, "센서 네트워크용 타원곡선 암호 프로세서 구현," IEEK, 2007.

[17] 오경희, 김태성, 김호원, "공개 암호 키를 사용한 센서 네트워크에서의 키 분배 구현," 한국방송공학회, 2008, pp.95-98.