USN 공격 기법 및 보안 기술 동향

이 석 준* 오 경 희** 김 호 원*** 정 병 호****

◈ 목 차 ◈

1. 서 론

최근 칩 설계 기술, 무선 통신 기술, IT 기술의 급속한 발달로 시간과 공간의 제약없는 자유로운 컴퓨팅 환경이 생기면서, 이러한 기술과 환경에 기존의 다양한 서비스 인프라를 접목한 u-청계천, u-시티, u-항만과 같은 유비쿼터스 서비스의 출현을 앞두고 있다. 유비쿼터스 서비스의 핵심 기술이라고 할 수 있는 USN(Ubiquitous Sensor Network)는 언제 어디서나 정보 시스템을 활용한 서비스를 제공받을 수 있는 유비쿼터스 사회를 위한 필수 네트워크이다. 이 기술은 기본적으로 상황 정보를 인지하는 기능을 가진 센서 노드들이 무선 통신 인프라를 구성하여 환경 정보 모니터링, 보안 관제, 군사 응용,Health-care와 같은 다양한 응용을 수행할 수 있다.

그러나, USN 기술은 무선으로 데이터를 주고받으며, 통신 주체인 각 센서 노드의 자원 제약성이 높다는 단점을 지니고 있다. 무선으로 데이터 통신을 한다는 것은 곧, 공격자가 물리적인 제약없이 네트워크에 참가할 수 있어 도청 및 데이터 위변조와 같은 다양한 공격 기법에 쉽게 노출될 수 있음을 뜻하며, 노드의 자원 제약성이 높다는 것은 이러한 공격에 방어하기 위하여 보안 기술을 적용하는 것이 쉽지 않음을 뜻한다.

현재 국내 산업계에서는 보안 기술에 대한 개발 수준이 초기 단계에 머무르고 있으며, 기술에 대한 관심도 역시 매우 낮은 편이다. 대표적인 네트워크 보안 요구 사항이라고 할 수 있는 기밀성과 무결성이 지원되지 않아 무선상에서 이루어질 수 있는 다양한 공격에 무방비로 노출되어 있으며, 이러한 상황은 유비쿼터스 서비스 확산에 있어 많은 기업체들이 큰 위험 요소를 가지고 있음을 뜻한다.

본 논문에서는 센서 네트워크에서 이루어지는 각종 공격 기법에 대하여 살펴보고, 이러한 공격에 대응하기 위한 보안 기능 및 각 기능별로 어떤 공격들을 무력화할 수 있는지를 기술한다. 또한, USN 보안 기술 개발 동향과 함께, 현재 ETRI에서 공개키 암호 알고리즘을 기반으로 개발한 사례에 대해 소개한다.

2. USN 공격 기법

2.1 USN 공격 모델

USN에서 공격자는 센서 노드보다 계산 능력이 뛰

* 한국전자통신연구원 정보보호연구본부
** 한국전자통신연구원 정보보호연구본부
*** 부산대학교 정보컴퓨터공학부
**** 한국전자통신연구원 정보보호연구본부
본 연구는 지식경제부 및 정보통신연구진흥원의 IT핵심기술 개발사업[2005-S-088-04, 안전한 RFID/USN을 위한 정보보호 기술] 사업의 일환으로 수행하였음

어난 노트북 수준의 장비를 이용한다고 가정할 수 있다. 이 경우, 공격자는 정상적인 노드에 비해 유리한 위치에 점하게 되는데, 이는 공격자의 장비가 CPU와 메모리 등 계산 능력에 있어서 더 뛰어나며, 고출력의 전파 전송 및 뛰어난 수신 능력을 가지기 때문이다.

공격은 일반적으로 외부자 공격과 내부자 공격의 2가지 범주로 분류할 수 있다. 외부자 공격은 네트워크에 참여할 권한이 없는 공격자의 공격을 의미하며, 내부자 공격은 어떠한 방식으로든 네트워크에 참여할 권한을 취득하여 시도하는 공격을 의미한다. 내부자 공격은 적법한 노드에 악성 코드를 동작시키거나, 적법한 노드로부터 네트워크 참여를 위한 보안 키, 인증 데이터 등을 취득하여 노트북과 같은 장비를 활용하는 공격 등이 가능하다.

내부자 공격은 공격자가 적법한 노드와 권한이 동일하기 때문에 보안 기법을 적용하더라도 공격을 원천적으로 봉쇄할 수는 없다. 그러나, 공격자가 처음부터 내부자로서 네트워크 참여 권한을 가지고 있다고 가정하는 것은 무리가 있으므로, 공격 초기에는 외부자 공격만 가능하다고 생각할 수 있다. 이 경우 외부자 공격은 그 자체로서 도청, 데이터 위변조와 같은 공격의 목표를 이룰 수 없다면 기본적으로 내부자 공격을 위한 정보 획득이 목표가 될 수 있다. 또한 내부자 공격이 이루어지더라도 공격으로부터 받는 피해의 범위를 최소화할 수 있는 보안 기법을 고려해야 할 것이다.

2.2 USN 공격의 종류

2.2.1 도청

USN 네트워크를 구성하는 각 센서 노드들은 일반적으로 IEEE 802.15.4와 같은 무선 통신을 구성한다. 따라서 무선 통신 상에서 주고받는 데이터에 대한 기밀성이 제공되지 않을 경우, 외부 공격자는 매우 손쉽게 도청을 할 수 있다.

IEEE 802.15.4 규격에서는 AES 암호 알고리즘을 이용한 기밀성 보장 방법을 기술하고 있으며, 센서 노드의 RF 칩으로 가장 널리 사용되고 있는 TI사의 CC2420 칩은 AES 하드웨어 모듈을 탑재하고 있다.

2.2.2 데이터 위변조

센서 노드들은 무선으로 통신을 하기 때문에 공격자가 네트워크에 참여하기 위한 물리적인 제약이 없으므로, USN 네트워크에서 공격자가 데이터 위변조 공격을 시도하는 것이 상대적으로 매우 쉽다. 이는 곧, USN 네트워크에서는 주변의 상황 정보를 인지하여 싱크 노드 혹은 게이트웨이 등을 통하여 응용 시스템으로 전달하는 것이 그 목적인데, 특히 상황 정보의 정확성이 매우 중요한 응용 서비스에서 그 정확성이 크게 왜곡될 수 있음을 뜻한다.

데이터 위변조 공격에 대처하기 위해서는 기본적으로 공격자가 아닌 정상 노드만이 네트워크에 참여할 수 있는 방법을 제공함과 함께, 특정 노드로부터의 메시지가 그 노드로부터 변조되지 않은 채 전달되었음을 확인할 수 있는 메시지 인증 기법이 필요하다.

2.2.3 서비스 거부 공격

서비스 거부 공격(DoS; Denial of Service)은 일반적으로 특정 서비스를 제공하는 네트워크에 대하여 서비스를 위하여 기대하는 기능과 성능이 원활하게 혹은 전혀 이루어지지 못하도록 하는 모든 종류의 공격을 포괄한다. 여기에는 하드웨어적인 파괴, 소프트웨어상의 버그, 혹은 전파 방해와 같은 다양한 방법을 포함할 수 있다.

USN 네트워크에서 센서 노드들은 응용 서비스에 따라 매우 열악한 환경에 설치될 수 있으며, 굳이 공격이 일어나지 않더라도 배터리 소실, 홍수 등과 같은 자연/인공 재해에 의한 노드 유실 등의 가능성이 항상 존재한다. 여기에 공격자가 고의적으로 노드를 파괴할 가능성까지 생각한다면, 특정 노드들이 네트워크 상에서 탈락하더라도 라우팅 경로를 자동적으로 재설정하는 등 결함 감내(Fault Tolerance) 기능을 포함하고 있어야 할 것이다.

이러한 결함 감내 기능을 제대로 설계하기 위해서는 다양한 계층에서 이루어질 수 있는 서비스 거부 공격의 가능성을 충분히 고려하여야 한다. Anthony D. Wood et al[1]은 센서 네트워크에서 일어날 수 있는 서비스 거부 공격과 대응 방안을 표 1과 같이 계층별로 정리한 바 있다.

(표 1) 센서 네트워크 계층별 서비스 거부 공격

Network Layer	Attacks	Defenses
Physical	Jamming	Spread-spectrum, Priority messages, Lower duty cycle, Region mapping, Mode change
	Tampering	Tamper-proofing, Hiding
Link	Collision	Error-correcting code
	Exhaustion	Rate limitation
	Unfairness	Small frames
Network and Routing	Neglect and greed	Redundancy, Probing
	Homing	Encryption
	Misdirection	Egress filtering, Authorization, Monitoring
	Black Holes	Authorization, Monitoring, Redundancy
Transport	Flooding	Client puzzles
	Desynchronization	Authentication

2.2.4 라우팅 공격

USN 네트워크에서 이루어지는 라우팅 공격은 메시지가 정상적인 경로를 통하여 싱크 노드에게 전달되는 것을 방해하고자 하는 것이다. 공격자는 라우팅 공격을 이용하여 응용 서비스가 정상적으로 이루어지지 않도록 할 수 있으며, 또한 다른 종류의 공격을 시도하기 위한 준비 단계로서의 공격 효과도 가능하다.

일반적인 USN 라우팅 기법들은 제한된 능력을 가진 노드들이 센싱된 데이터를 얼마나 효율적으로 보내는가에 초점을 맞추고 있으나, 보안을 고려하지는 않았기 때문에 여러 종류의 라우팅 공격에 취약할 수 밖에 없다.

라우팅 공격의 종류는 라우팅 정보의 위변조 공격, 메시지의 선택적 전달 공격, 싱크홀/웜홀 공격, Sybil 공격, HELLO flood 공격 등 여러 종류가 있으며, 공격의 상세한 내용은 C. Karlof 등의 논문[2]에 나와 있다.

2.2.5 물리적 공격

물리적으로 센서 노드를 파괴하여 네트워크 내부에 있는 일부 노드가 동작하지 못하도록 만드는 공격은 그리 심각한 위협은 아니다. 2.3에서도 언급한 바와 같이 일반적으로 USN 네트워크는 노드 유실, 배터리 소진 등 다양한 이유로 특정 노드의 사용이 불가능할 경우 라우팅 경로를 재할당할 수 있는 매커니즘과 같은 결함 감내 기능을 포함하기 때문이다.

그러나 센서 노드를 탈취하여 노드 내부의 중요한 정보를 획득하는 경우는 심각한 위협이 될 수 있다. 예를 들어, 기초적인 수준의 보안성을 제공하기 위하여 어떤 USN 네트워크에서는 모든 노드들이 동일한 암호키를 사용하고 있다고 가정해보자. 이 경우, 단지 하나의 노드를 탈취하여 키 정보를 획득하는 것만으로도 전체 네트워크를 손쉽게 도청할 수 있는 효과가 있으며, 또한 공격용 코드를 삽입하여 내부자 공격에 이용할 수도 있다. 이를 막기 위해서 tamper-resistant 기술을 적용할 수 있으나, 하드웨어비용이 매우 커지는 단점이 있다.

또 다른 형태의 물리적 공격으로 노드가 동작하고 있을 때 사용하는 소비전력 혹은 방사되는 전자파 정보 등을 이용하여 노드 내부에 있는 암호 키와 같은 중요한 정보를 알아내고자 하는 부채널 공격이 있다. 부채널 공격에는 SPA(Simple Power Analysis) 기법과 DPA(Differential Power Analysis) 기법, EM(Electro-Magnetic) 공격 등이 있다.

3. USN 보안 기술 동향

3.1 링크 계층에 대한 보안 기법의 적용

2.2에서 언급한 공격 중에서 공격 비용이 저렴하면서도 네트워크에 손쉽게 영향을 줄 수 있는 공격은 2.2.1의 도청, 2.2.2의 데이터 위변조와 2.2.4의 라우팅 공격이다. 따라서 USN 네트워크의 취약점을 노리는 대부분의 공격은 이들 형태를 띄게 된다.

이러한 외부자의 공격에 가장 손쉽게 대처하는 방법은 링크 계층에 보안 기법을 적용하는 것이다. 많은 종류의 외부자 공격들은 링크 계층의 암호화 및 메시지 인증 코드의 삽입만으로도 방어가 가능하다. 외부에서는 암호화 및 메시지 인증용 암호 키를 알 수 없다는 가정이 있다면, 이 방법을 적용하는 것만으로도 도청, 메시지 위변조 공격과 함께 라우팅 공격의 일부인 선택적 전달, 싱크홀 공격, Sybil 공격 등에 대해 방어할 수 있다.

최근 센서 네트워크 노드의 하드웨어 플랫폼으로 많이 각광을 받고 있는 Moteiv사의 Tmote Sky[3]와 Crossbow사의 micaz[4] 등은 모두 RF 칩으로 TI CC2420 칩을 사용하고 있다. CC2420 칩은 내부적으로 링크 계층에서의 AES 128bit 암복호화(CTR, CBC-MAC, CCM 모드)를 지원하므로, 이를 이용한 메시지 암호화 및 인증 코드 삽입이 가능하다. CC2420 칩이 제공하는 암호 기능을 살펴보면 다음과 같다.

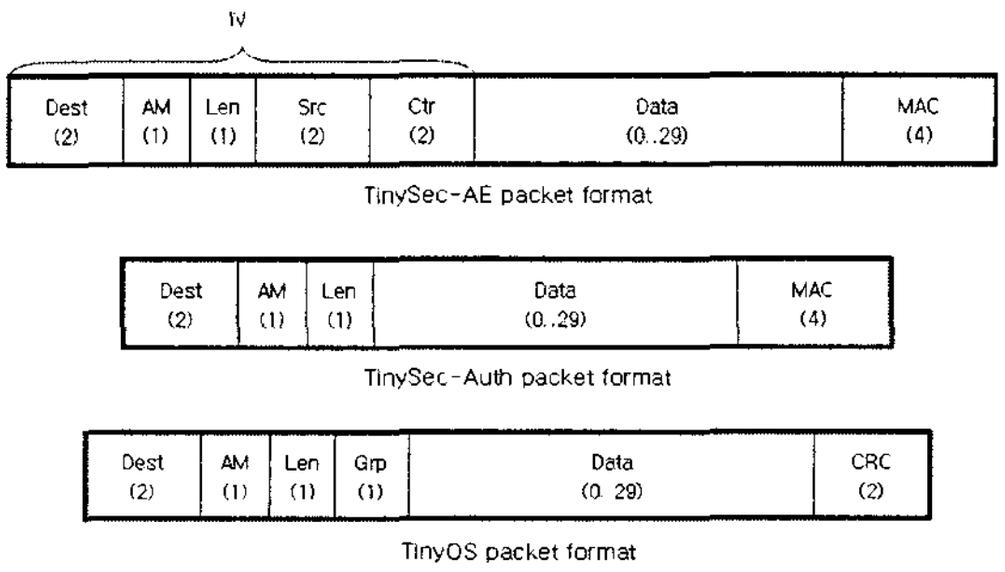
- CTR 모드, CBC-MAC 모드, CCM 모드 지원
- 2개의 키 값을 가질 수 있으며, 1개의 전송 nonce 값, 1개의 수신용 nonce 값을 설정할 수 있음
- 전송때마다 nonce 값에 대한 변경 필요
- IEEE 802.15.4에서 정의된 보안성이 강화된 commercial 모드에선 link key를 사용하는데, 이를 위해선 프레임 송수신 때마다 key를 재설정해야 함. CC2420에선 이를 위한 command 제공 및 버퍼 구조를 가짐
- Header length를 설정할 수 있기 때문에, NWK 계층과 APS 계층(zigbee security 규격에 정의된 계층)에서 기밀성을 제공할 수 있음

CC2420에서 제공하는 각 암호의 동작 모드별 성능을 보면 표 2와 같다. 표에 따르면 AES-CCM 동작 성능이 222 usec로 USN 환경에서 사용하기에 충분한 속도이며, 기존의 데이터 전송에 영향을 주지 않음을 의미한다.

(표 2) CC2420 칩에서 제공하는 암호의 동작 특성

mode	L(a)	L(m)	L(MIC)	Time (us)
CCM	50	69	8	222
CTR	-	15	-	99
CBC	17	98	12	99
Stand-alone	-	16	-	14

링크 계층에 대한 보안 기법을 적용한 다른 예로 TinySec[6]이 있다. TinyOS 1.1.0에서 구현된TinySec은 암호 알고리즘을 소프트웨어로 구현하였으며, 저전력 동작을 위해SkipJack을 사용했다. TinyOS 환경을 위한 인터페이스와 모듈, 암호 알고리즘 모듈은 컴파일된 바이너리 기준으로 약 7K 바이트, 필요한 RAM의 크기는 약 455 바이트였다.



(그림 1) TinySec과 TinyOS 패킷 형식

TinySec은 그림 1과 같은 패킷 형식을 지닌다. 그림 1에서 보면 기존의 TinyOS 패킷에 비해 TinySec 패킷이 약간의 오버헤드를 더 지님을 확인할 수 있다. 즉 그림 1에서 TinySec-AE(기밀성과 무결성 동시 지원)모드의 경우는 5 바이트가 증가하며, TinySec-Auth (무결성만 지원) 모드에서는 1바이트가 추가적으로 더 필요하게 되며, 이는 보안 기능을 지원하지 않는 경우에 비하여 평균적으로 각각 8%, 1.5%의 패킷 오버헤드 및 지연이 있음을 뜻한다.

메시지 무결성에 대해서 4바이트의 MAC 코드로 지원하므로, 일반적으로 사용되는 8바이트 혹은 그 이상의 길이를 가진 MAC 코드보다는 보안성이 약하다. 공격자는 단순한 bruce-force 공격의 경우 평균 231번 만큼의 시도로 공격에 성공할 수 있으며, 이는 USN 네트워크의 낮은 대역폭을 고려하면 허용할 만한 보안성으로 볼 수 있다.

TinySec에서는 대칭키 암호 알고리즘에 있어 중요한 키 분배에 대해서는 기본적으로 다루지 않고 있으며, [6]의 7장에서 원론적인 수준에서 간단히 언급하고 있다.

3.2 응용 계층에 대한 보안 기법의 적용

링크 계층은 노드와 노드 사이의 안전성(Hop-by-Hop Security)을 유지하는 것으로 노드와 게이트웨이 혹은 싱크 노드 사이의 종단간 보안(End-to-End

Security)을 보장하지는 않는다.

따라서 노드 제작시 미리 게이트웨이와 종단간 보안을 위한 키를 입력해두고, 이를 이용하여 응용 계층에서 암호화 및 메시지 인증 코드를 삽입하는 방법을 생각할 수 있다. 이는 데이터가 전송되는 경로 중간에 내부자 공격을 위한 노드가 있더라도 데이터가 도청되거나 위변조되지 않도록 하는 효과가 있다.

응용 계층 보안 기법은 링크 계층 보안 기법과 유사하게 구성할 수 있다. 앞서 언급한 CC2420 칩은 AES 알고리즘을 단독으로 동작시키는 것이 가능하므로, 응용 계층에서도 이 칩의 AES 모듈을 활용할 수 있다.

3.3 키 분배 기법

3.1에서는 도청과 데이터 위변조 등에 있어 링크 계층에 대한 보안 기법을 적용하는 것이 매우 효과적임을 언급하였다. 그러나 노드간 통신을 위해서는 대칭키를 사용하게 되는데, 이때 반드시 키 분배 문제가 해결되어야 한다. 가장 단순하게 생각할 경우 전체 네트워크 상에서 동일한 암호 키를 사용하는 방법이 있으나, 이는 단지 하나의 노드로부터 키가 유출되기만 하여도 네트워크 전체의 보안성이 깨지는 결과를 얻게 된다.

따라서 노드와 노드 사이에 각기 다른 연결이 맺어질 때마다 새로운 키를 생성할 수 있는 방법이 필요하다. 이를 위하여 신뢰할 수 있는 인증 센터를 통한 키 분배 기법[10]이라든지, 랜덤 키 사전 분배 기법, q-합성수 랜덤 키 사전 분배 기법, Blom Scheme[9], 위치 기반 키 사전 분배 기법 등 다양한 연구 결과가 있다.

또한 타원곡선 암호 알고리즘과 같은 상대적으로 가벼운 공개키 암호 알고리즘을 이용한 키 교환 기법에 대한 연구 결과[7, 8]도 나오고 있는 추세이다. TinyECC[8]의 경우, 소프트웨어적으로 구현된 ECDSA를 이용하여 전자 서명에 3.17초, 서명 검증에 4.04초가 소요된다고 밝히고 있다. 이는 대칭키 기반의 연산 시간에 비하여 매우 긴 시간이지만, 키 교환 자체가 자주 일어나지 않음을 고려하면 충분히 받아들일 수 있는 시간으로 보여진다.

3.4 노드 간 상호 인증

인증은 네트워크에 불법적으로 참여하려는 외부자 공격에 대응하는 가장 기본적인 수단이다. Sybil 공격[11]과 같이 multi-ID를 생성하는 공격에 대응하기 위하여 노드간 상호 인증을 수행하는 것이 필요할 수 있다.

일반적으로 암호학적으로 안전한 상호 인증을 수행할 경우, 인증과 동시에 링크 계층 보안을 위한 키를 할당받을 수 있는 매커니즘을 적용하는 것이 효율적이다.

3.5 서비스 거부 공격 대응 기법

서비스 거부 공격은 2.2.3에서 언급한 바와 같이, 그 종류와 방법이 매우 다양하므로 대응 기법 역시 그 종류에 따라 다를 수 있다. 큰 맥락에서 보면, 네트워크 일부 혹은 전체적으로 서비스 거부 공격이 이루어지기 위해서는 공격자가 지속적으로 고출력의 전파 전송을 시도하여야 한다. 서비스 거부 공격이 일어날 경우, 센서 노드들은 다른 노드들과의 통신시 송수신 실패, 메시지 에러의 비율이 평소에 비해 매우 커질 수 있다. 이 경우, 센서 노드는 소비 전력의 낭비를 막기 위하여 잠시 sleep 모드로 들어가거나, 메시지 송수신 시도 자체를 줄이는 방법 등으로 대응할 수 있다. USN 네트워크에서 결함 감내 기능을 포함하고 있다면 일부 노드가 sleep 모드로 들어가는 등 기능이 동작하지 않더라도 큰 문제가 되지 않을 수 있다.

다만, 효율적인 공격을 위하여 서비스 거부 공격이 싱크 노드 혹은 게이트웨이에 집중될 가능성이 있다. 싱크 노드가 서비스 거부 공격으로 인하여 정상 동작을 하지 못한다면 응용 서비스에서 노드들의 상황 인지 정보를 안정적으로 수집하지 못하게 될 것이다. 꼭 싱크 노드가 아니더라도 서비스 가용성/지속성이 중요한 응용의 경우 일반 노드들에 대한 서비스 거부 공격에 능동적으로 대처할 수 있어야 한다. 능동적인 대처를 위하여 침입 탐지(Intrusion Detection) 기능을 구현하는 방법[15, 16]을 생각해 볼 수 있다.

3.6 기타

USN 네트워크에서는 일반적으로 응용 서버에서 싱크 노드 혹은 게이트웨이를 통하여 브로드캐스트하는 제어/명령 메시지를 포함한다. 이 메시지는 반드시 위변조되지 않아야 하며, 암호학적으로 매우 높은 보안성을 요구한다.

따라서 브로드캐스트 메시지 인증도 USN 보안에 있어서 매우 중요한 연구 분야이다. 메시지 무결성을 위하여 공개키 방식의 전자 서명을 이용하기에는 패킷 크기가 지나치게 커지는 단점이 있으므로, 해쉬 체인을 사용하는 기법들이 많이 시도되고 있다. 대표적인 브로드캐스트 메시지 인증 기법으로는 u-Tesla[12]가 있으며, 센서 노드의 OS 프로그램을 네트워크 상에서 재프로그래밍하는데 있어 무결성을 제공하는 논문[13]도 참고할 만하다.

이 외의 연구 분야로 라우팅 공격에 대응하기 위한 Multi-path 라우팅 기법[14] 등도 있다.

4. ETRI USN 보안 기술

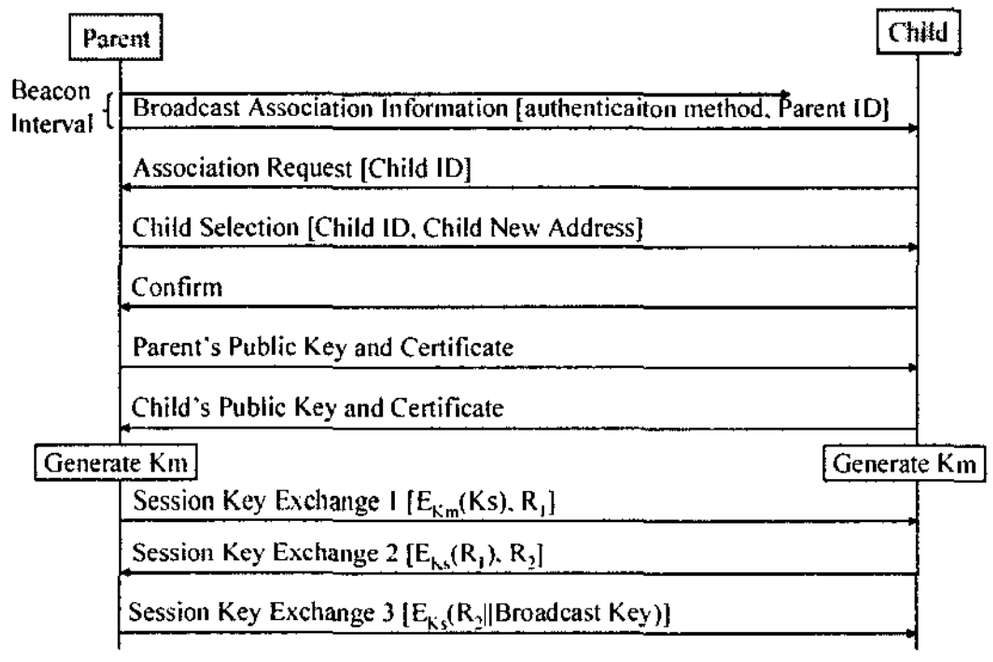
현재 ETRI에서는 USN에 적합한 보안 기술을 개발 중에 있다. ETRI의 USN 보안 기술은 3장에서 언급한 보안 기법들을 고려하여, 센서 노드의 열악한 하드웨어 환경에 적합하도록 가벼우면서 적절한 수준의 보안성을 제공하고자 한다. ETRI 보안 기술의 특징은 다음과 같다.

- 소프트웨어
  - Secure Association (ECC 기반 인증 및 동적 키 분배)
  - 링크 계층 보안
  - 응용 계층 보안
- 하드웨어
  - ECC 경량 하드웨어 모듈

4.1 Secure Association

ETRI에서는 USN 네트워크의 기본적인 보안을 위하여 노드간 상호 인증 및 동적(dynamic) 키 교환이 필수적이라고 보고, 이 절차를 Secure Association라고 정의하였다. ETRI에서는 이를 위해 ECC 알고리즘을 사용하였는데, ECC 알고리즘 연산이 보안성이 뛰어난 한편 이 절차는 일반적으로 연결 초기에 한 번 이루어지면 되는 것이므로 오랜 연산시간에도 불구하고 실효성이 있다고 보았기 때문이다.

Secure Association의 절차는 트리 구조의 센서 네트워크 형성 과정에서 부모와 자식 노드 사이에 인증을 맺고 키를 생성하는 과정으로, 그림 2를 통해 보인다. 부모 노드는 주기적으로 송신하는 정보를 자식 노드가 수신하여 접속을 요청한다. 부모 노드가 이 접속 요청을 받으면 자식 노드에게 네트워크 주소를 할당한 후, ECC 공개키 인증서를 주고 받아 검증 후 이를 바탕으로 ECDH 키 생성 과정을 수행한다. 부모 노드는 추후 4.2에서 사용할 링크 계층 보안용 세션키 Ks를 랜덤하게 생성하여 ECDH로 공유된 Km을 사용하여 자식 노드에게 안전하게 전달하고 이를 확인하는 절차로 Secure Association은 마무리된다.



(그림 2) Secure Association 절차

표 3은 브로드캐스트 되는 Association Information 프레임이 송신 된 후부터 세션키를 생성, 확인할 때까지의 단계별 소요 시간을 측정한 값이다. 여기에서 보면 최종 ECC 인증서 프레임을 수신하여 최초의 세션키 교환 메시지인 SKE 1을 보내기까지 걸리는 시간이 전체 연산 시간의 대부분을 차지한다. 이는 ECC 인증서 검증(ECDSA 연산으로 ECC 스칼라 곱 2회 이내의 시간 소요)과 Km 계산(ECDH 연산으로 ECC 스

칼라 곱 1회 시간 소요)에 필요한 연산량이 매우 크기 때문이다.

표 4는 동일한 조건에서 반복하여 실시한 시험에서 키를 생성하는데 소요된 시간이다. 시험에 사용된 센서 노드 하드웨어는 MSP430 MCU를 탑재한 Tmote Sky[3]이다.

(표 3) 단계별 키 생성 소요 시간 (단위: 초)

절차	누적 시간	소요 시간
Broadcast Frame	0.000	0.000
Confirm	0.748	0.748
최종 Certificate Frame	1.253	0.505
SKE 1	14.500	13.347
SKE 2	14.681	0.181

(표 4) 키 생성에 필요한 총 소요 시간 (단위: 초)

1회	2회	3회	4회	5회	평균
14.681	15.047	14.170	14.233	14.438	14.514±0.359

4.2 링크 계층 보안

USN 네트워크에서 널리 사용되는 무선 통신 기술인 IEEE 802.15.4를 지원하는 TI CC2420 칩은 AES 하드웨어 모듈을 포함하고 있으며, IEEE 802.15.4 패킷상에서 AES-CTR, AES-CBCMAC, AES-CCM 모드를 적용하여 송수신이 가능하다. ETRI에서는 CC2420 칩을 포함하고, TinyOS가 포팅되어 있는 Tmote Sky에서 AES-CCM 모드로 암복호화하는 기능을 구현하여 링크 계층 수준(Hop-by-Hop Security)의 메시지 기밀성과 무결성을 지원하고 있다.

여기에서 암호키는 4.1의 Secure Association에 따라 생성된 Ks를 사용하게 된다.

4.3 응용 계층 보안

TI CC2420 칩의 AES 하드웨어 모듈은 802.15.4 패킷 암복호화에 이용할 수 있을 뿐 아니라, AES 알고리즘을 단독(stand-alone)으로 사용하는 것이 가능하다. 이는 곧 링크 계층이 아닌 다른 계층에서도 이 칩의 AES 모듈을 이용할 수 있음을 의미하며, 따라서 ETRI에서도 응용 계층 보안을 위하여 이 모듈을 활용하고 있다.

ETRI의 응용 계층 보안은 소프트웨어적으로 AES-CCM 모드와 유사하게 동작하도록 구성하였으며, 응용 계층에서 보호하는 메시지는 센서 노드와 싱크 노드 사이의 종단간 보안(End-to-End Security)을 보장한다. 즉, 중간에 메시지를 전달하는 노드가 적법한 노드라 하더라도 메시지의 실제 내용을 알아낼 수는 없다. 이는 적법한 노드를 가장하고 있는 내부자 공격에 대응할 수 있는 방법이 된다.

센서 노드와 싱크 노드간 암호키는 처음 센서 노드를 초기화할 때 미리 저장해두는 것으로 한다. ETRI에서는 응용 서버(혹은 보안 관리 서버)에서 Global Master Key에 해당하는 GMK를 안전하게 저장하고 있으며, 각 노드들을 초기화할 때 다음과 같이 노드별 암호키 KID를 생성하여 입력한다.

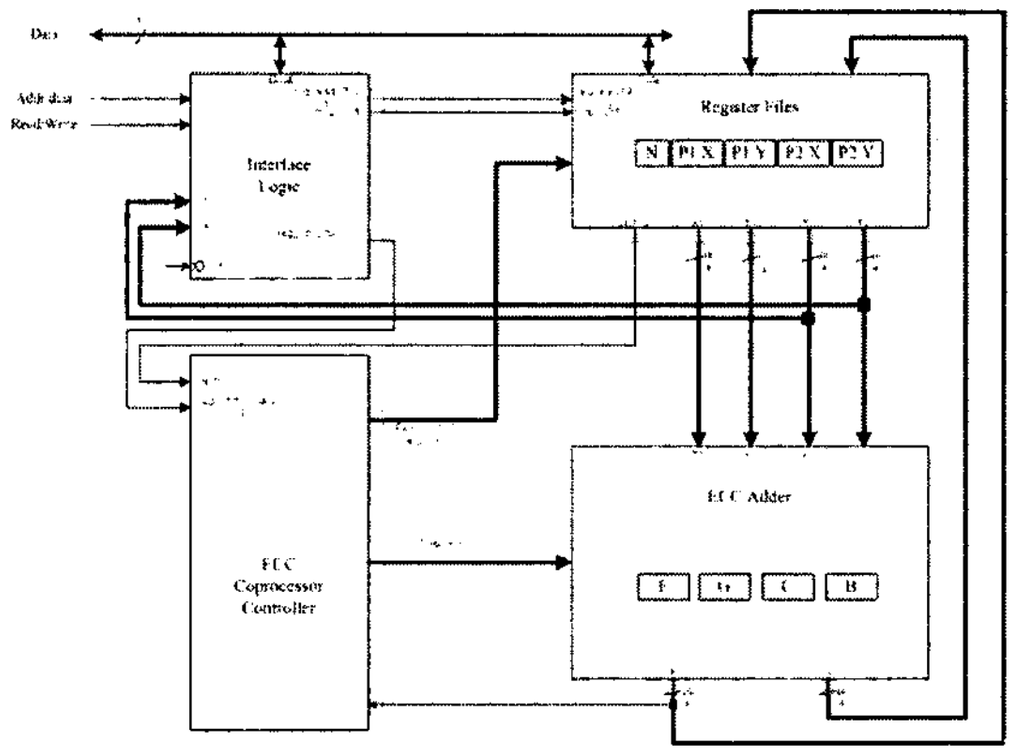
K_{ID} = Hash(GMK, Node ID)

따라서 GMK가 안전하게 저장이 되어 노출되지 않는다면, 공격자가 특정 노드에 대한 응용 계층 보안키인 K_{ID}를 알아낸다 하더라도, Hash 함수의 일방향성으로 다른노드에 대한 보안키를 알아낼 수 없게 된다.

4.4 ECC 경량 하드웨어 모듈

소프트웨어로 구현된 ECC(타원 곡선 암호 시스템)를 이용한 키 분배 기술[7, 8]은 키 분배에 걸리는 시간이 수 초이상 걸리는 단점이 있다. 따라서 ECC를 하드웨어 코프로세서로 구현하여 센서 노드의 하드웨어 플랫폼에 내장할 경우, 키 분배에 걸리는 시간을 상당 부분 단축시킬 수 있다.

ETRI에서는 ECC 경량 하드웨어 모듈을 FPGA칩과 0.25u ASIC 공정으로 모두 구현하였다[17]. 0.25u 삼성 공정으로 하드웨어 합성시 22k 게이트 면적 수준으로 구현되었으며, 프로세서 구조는 그림 3에서 볼 수 있다. 연산 시간에 대한 테스트 결과는 표 5과 같다.



(그림 3) 저면적 타원곡선 암호 코프로세서 구조

(표 5) 암호 코프로세서 연산 시간

ECC 연산 종류	연산 시간
스칼라 곱셈 연산 nP	49 ms
타원곡선 덧셈 연산 P+G	220 s

표 3에서 보는 바와 같이 ECC 연산에서 중요한 것은 스칼라 곱의 횟수이다. 4.1의 Secure Association에서 ECC 인증서의 검증(ECDSA 서명 검증)과 키 교환(ECDH)에서 필요한 연산은 스칼라 곱 3회 이내이므로 센서 노드에서 키 교환에 필요한 연산 시간이 대략 0.15초 수준 이내가 될 것이다. 이는 소프트웨어 구현 결과에 비하여 상당한 연산 시간 단축을 볼 수 있다.

4.5 부채널 공격 방지

ETRI에서는 부채널 공격 대응 기법을 적용한 하드웨어 및 소프트웨어 설계 기술을 USN 보안 기술에 적용할 계획이다. 4.4에서 개발한 ECC 경량 하드웨어 모듈에 부채널 공격 대응 기법을 적용한 결과를 2008년 완료할 예정이며, 소프트웨어 모듈에 부채널 공격 대응 기법을 적용하는 부분도 지속적으로 검토하고 있다.

5. 결 론

본 논문에서는 u-청계천, u-시티, u-항만과 같은 유비쿼터스 서비스의 핵심 기술이라고 할 수 있는 USN에 대한 공격 기술들을 검토하고, 이러한 취약점에 대응하기 위한 보안 기술의 종류와 동향에 대해 살펴보았으며 현재 ETRI의 연구 개발 현황에 대해서도 언급하였다.

USN은 센서 노드의 높은 자원 제약성과 무선 통신으로 인하여 본질적으로 안전성 측면에서 취약점을 지니게 된다. 유선 인터넷, 무선랜 등에서 사용하던 기존의 보안 기법을 적용하는 것은 센서 노드의 계산 능력, 저장 능력 등을 고려할 때 불가능하다고 볼 수 있으며, 반드시 센서 노드의 환경에 적용 가능하도록 경량화를 포함하는 customization이 필요하다. USN의 본질적인 취약점을 고려하지 않은 서비스는, 서비스의 안정성을 보장할 수 없는 심각한 문제점을 지닌다. 특히 보안 관제, 군사 응용, Health-care와 같이 상황 인지 정보의 정확성/기밀성이 중요하고 안정적인 서비스가 이루어져야 하는 곳에서는 반드시 다양한 각도에서 위험성을 검토하여 그에 맞는 보안 기술을 적용하여야 할 것이다.

참 고 문 헌

[1] A. Wood and J. Stankovic, "Denial of Service in Sensor Networks", IEEE Comp., Oct. 2002, pp. 54 - 62.

[2] C. Karlof and D. Wagner, "Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures", Proc. 1st IEEE Int'l., Wksp. Sensor Network Protocols and Applications, May 2003.

[3] Tmote Sky, http://www.moteiv.com

[4] MicaZ, http://www.xbow.com

[5] CC2420 DataSheet, "CC2420, 2.4GHz IEEE 802.15.4 / ZigBee-ready RF Transciever", Chipcon

[6] C. Karlof, N. Sastry, D. Wagner, "TinySec : A Link Layer Security Architecture for Wireless Sensor Networks", Sensys 2004

[7] 오경희, 김태성, 김호원, "공개암호키를 사용한 센서네트워크에서의 키 분배 구현", 한국방송공학회

동계학술대회 pp.95-98, 2008.2

[8] TinyECC: A Configurable Library for Elliptic Curve Cryptography in Wireless Sensor Networks, Ver 1.0, http://discovery.csc.ncsu.edu/software/TinyECC/, 11-02-2007.

[9] R. Blom, "optimal class of symmetric key generation systems", EUROCRYPT 84 workshop on advances in cryptology: theory. and application of cryptographic techniques, pp. 335-338, Dec. 1985, Paris

[10] ZigBee Specification, ZigBee Document 053474r06, Version 1.0, ZigBee Alliance, June 27, 2005

[11] J.R. Douceur, "The Sybil attack", 1st International Workshop on Peer-to-Peer Systems (IPTPS '02), 2002.

[12] Adrian Perrig, Robert Szewczyk, Victor Wen, David Culler, and J.D. Tygar. SPINS: Security protocols for sensor networks. In The Seventh Annual International Conference on Mobile Computing and Networking (MobiCom 2001), 2001.

[13] Prabal K. Dutta , Jonathan W. Hui , David C. Chu , David E. Culler, Securing the deluge Network programming system, Proceedings of the fifth international conference on Information processing in sensor networks, April 19-21, 2006

[14] D. Ganesan, R. Govindan, S. Shenker, D. Estrin, Highlyresilient, energy-efficient multipath routing in wireless sensor networks, Mobile Computing and Communications Review 4 (5) (2001) 11 - 25.

[15] A. Silva, M. Martins, B. Rocha, A. Loureiro, L. Ruiz, and H. Wong, "Decentralized intrusion detection in wireless sensor networks", Proc. of ACM IWQoS, 2005.

[16] K. Ioannis, T. Dimitriou, and F. C. Freiling, "Towards intrusion detection in wireless sensor networks", Proc. of the 13th European Wireless Conference, 2007.

[17] 최용제, 김호원, "센서네트워크용 타원곡선 암호 프로세서 구현", 전자공학회 추계학술대회, 2007

◐ 저 자 소 개 ◑

이 석 준

1998년 2월 : 서울대학교 컴퓨터공학과 졸업
2000년 2월 : 서울대학교 컴퓨터공학과 석사
2000년 2월~현재 : 한국전자통신연구원 정보보호연구본부 선임연구원
관심분야 : 익명 인증, 프라이버시 보호, 센서네트워크 보안, 무선 침입탐지기술

오 경 희

1999년 2월 : 연세대학교 컴퓨터과학과 졸업
2001년 2월 : 연세대학교 컴퓨터과학과 석사
2000년 12월~현재: 한국전자통신연구원 정보보호연구본부 선임연구원
관심분야 : 센서네트워크 보안, RFID 보안, 무선랜 보안

김 호 원

1993년 2월 : 경북대학교 전자공학과 졸업
1995년 2월 : 포항공과대학교 전자전기공학과 석사
1999년 2월: 포항공과대학교 전자전기공학과 박사
2003년 7월~2004년 6월 : 독일 Ruhr University Bochum Post Doctorial
1998년 12월~2008년 2월: 한국전자통신연구원 정보보호연구본부 팀장/선임연구원
2008년 3월~현재 : 부산대학교 정보컴퓨터공학부 조교수
관심분야 : 센서네트워크 보안, RFID 보안, 프라이버시 보호, 공개키 암호, 저전력 기술

정 병 호

1988년 2월 : 전남대학교 컴퓨터과학과 졸업
2000년 2월 : 충남대학교 컴퓨터과학과 석사
2006년 2월 : 충남대학교 컴퓨터과학과 박사
1988년~2000년 : 국방과학연구소 선임연구원
2000년 6월~현재 : 한국전자통신연구원 정보보호연구본부 책임연구원
관심분야 : 익명 인증, 네트워크 보안, 프라이버시 보호