情 報 保 護 學 會 誌
第18卷 第2號, 2008. 4

센서네트워크 보안 기술 개발 동향

김 호 원*, 이 석 준**, 오 경 희**

요 약

최근 유비쿼터스 환경을 실현하는 기술로서 사물 및 환경 정보를 센싱하여 무선으로 통신하여 필요한 정보를 수집 및 분석, 처리하는 센서네트워크 기술에 대한 관심이 고조되고 있다. 특히, 최근 국내에서는 u-City와 u-Port 사업 등, 범국가적으로 유비쿼터스 환경을 실현하고자 하는 사업이 진행되고 있기 때문에, 센서네트워크 기술에 대한 관심이 더욱 크다. 센서네트워크 기술은 기본적으로 상황 정보 인지 기능을 갖춘 센서 노드들이 무선 통신 인프라를 구성하여 환경 정보 모니터링이나 산업체 기기 제어 및 모니터링, 홈 자동화, 보안 및 군사용, 자산 및 물류 응용 등, 다양한 응용을 수행할 수 있는 기술이다. 하지만, 센서네트워크 기술은 본질적으로 무선통신 인프라를 기본으로 하고 있으며, 높은 자원 제약성(낮은 컴퓨팅 능력과 제한된 전원 공급 능력, 저가로 구현해야 한다는 제약성)으로 인해, 일반적으로 높은 보안 취약성을 가지는 것으로 알려져 있다. 본 고에서는 현재 국내의 센서네트워크 산업 분야에서 특히 취약한 것으로 알려져 있는 보안 기술 관점에서 센서네트워크 동향을 살펴보고, 센서네트워크 보안 기술 개발 현황을 살펴보고자 한다.

Ⅰ. 서 론

최근 무선 통신 기술과 칩 설계 기술, IT 기술의 급속한 발전은 사물의 지능화와 네트워크화를 골격으로하는 유비쿼터스 환경을 실현 가능하게 하고 있다. 특히, 유비쿼터스 환경을 실현하는 대표적인 기술인 센서네트워크 기술은 최근 국내의 산업계와 학계, 연구소에서 핵심 기술 개발과 응용 기술 개발 등, 활발한 연구 개발 및 시범 서비스 개발이 진행되고 있다. 국내에서 개발이 진행되고 있는 센서네트워크 핵심 기술 개발 분야로는 센서네트워크용 운영체제 기술과, 무선 통신 기술, 센서 기술, 노드 기술, 네트워크 기술 (라우팅, MAC 기술 등), 위치인식 기술, 에너지 harvesting 기술 등이 있으며, 개발되는 이러한 핵심 기술은 u-청계천, u-세종 도시 등, 다양한 시범 서비스에 적용되고 있다. 물론 범국가적인 사업인 u-City나 u-Port와 같은 응용에서도 핵심 기술로 사용될 것이다.

한편, 핵심 기술 개발 분야 중에서 국내에서 연구/개발이 활발히 진행되지 않는 분야로는 센서네트워크에서의 보안 분야와 저전력 분야를 대표적으로 손꼽을 수 있다. 하지만, 이 두 분야는 실제 센서네트워크의 상용화 및 산업화에 있어서 매우 중요하므로 앞으로도 많은 연구/개발이 진행되어야 할 것으로 보인다. 먼저 센서네트워크 저전력 기술 분야를 살펴보면, 센서네트워크를 구성하는 노드는 제한된 전원을 사용하여 정보 센싱 및 처리, 통신을 하기 때문에, 우선 센서가 저전력 특성을 가져야 하며, 또한, 센싱된 정보를 처리하는 센서노드 프로세서가 저전력 특성을 가져야 한다. 또한, 통신 프로토콜, MAC, 라우팅 등, 네트워크 요소도 저전력 특성을 가져야 한다. 이 뿐만 아니라, 센서노드에 탑재되는 센서노드용 운영체제도 저전력 동작 특성 및 전력 제어 기능을 가져야 하며, 센서노드용 하드웨어 보드(Mote)도 소비전력을 관리하는 기법이 구현 되어야 한다. 하지만, 현재 국내의 센서네트워크 기술 개발자 및 응용 서비스 개발자들은 복합적인 지식과 경험을 필요로 하는 센서네트워크 저전력 기술 개발에 대해선 많은 노력을 기울이지 못하고 있다.

또한, 센서네트워크 보안 기술 개발 현황을 살펴보면, 현재 국내 산업계의 기술 수준은 초기 단계에 머물러 있다. 대표적인 보안 요구 사항인 기밀성과 무결성도 센서네트워크에서 제대로 제공하지 못하고 있기 때문에 센서네트워크 응용 환경에 대한 도청과 통신 데이터에

* 부산대학교 정보컴퓨터공학부 (howonkim@pusan.ac.kr)
** 한국전자통신연구원 정보보호연구본부(junny@etri.re.kr, khoh@etri.re.kr)

대한 위변조가 용이한 상황이다. 더욱이, 센서네트워크는 통신 방식이 무선이며, 정형화된 네트워크 토폴러지를 가지지 않기 때문에, 유선 네트워크보다 더욱 다양한 보안 취약성을 가진다. 이에, 센서네트워크에 대한 활발한 연구/개발이 필요하며, 개발된 보안 기술을 시범 서비스 및 응용 서비스에 사용 되어야 할 것이다. 본 고에서는 센서네트워크 보안 기술 개발 현황을 다루기로 한다. 이를 위해 먼저 센서네트워크에 대한 다양한 보안 취약성을 분석하고 이를 막을 수 있는 보안 기술을 소개한다.

Ⅱ. 센서네트워크의 보안 취약성 및 방지 방안

2.1. 도청

먼저 센서네트워크에서는 센서노드간에는 IEEE 802.15.4 LRWPAN 등과 같은 무선 통신으로 이뤄진다. 이 때문에, 센서노드간 통신 정보에 대한 기밀성이 제공되지 않는다면 어떤 정보가 전송되는지를 쉽게 알 수 있다. 이는 즉, 도청이 용이함을 뜻한다. 무선 통신 정보는 브로드캐스팅 되기 때문에, 이러한 도청은 더욱 손쉽게 가능하다. 도청을 방지하기 위해서는 전술한 것처럼 센서노드간에 통신되는 데이터에 대하여 암호화를 통해 기밀성이 보장되어야 한다. 이를 위해 IEEE 802.15.4 표준 규격에선 AES 암호를 사용하여 기밀성을 보장하도록 하고 있다. 센서노드의 RF 통신 칩으로 시장에서 가장 많이 사용되고 있는 TI사의 CC2420(구 Chipcon사)과 같은 칩에선 IEEE 802.15.4의 표준 규격을 따르기 때문에, AES 암호 알고리즘을 하드웨어 블록으로 제공하고 있다. 사용자는 이를 이용하면 최소한 센서노드간 통신 데이터에 대한 기밀성은 보장할 수 있다. 하지만, AES와 같은 암호 알고리즘을 사용하기 위해선 키 분배 문제가 발생하는데, 이에 대해선 표준 규격 등에서 구체적으로 제안하는 기술이 없다. 이 때문에, 개발자가 자체적으로 안전한 키 분배 문제를 해결해야 한다. 본 고에서는 다음 장에서 안전하게 키를 분배하는 기술 개발 현황을 소개하고 본 연구자가 공개키 암호 알고리즘을 기반으로 개발한 사례를 소개한다[1].

2.2. 데이터 위변조

센서네트워크를 구성하는 노드에 대한 인증 기능이 없는 경우, 공격용 노드가 쉽게 네트워킹에 참여할 수 있게 된다. 이 경우, 공격용 노드는 도청으로부터 수집한 패킷 정보, ID 정보를 활용하여 정보에 대한 위변조 공격을 할 수 있다. 이를 방지하기 위해선 전송 되는 정보가 위변조 되어 있는지 무결성 검증 기능이 필요하며 또한, 인증 절차를 통해서만 네트워킹에 참여할 수 있도록 해야 한다.

2.3. 라우팅 공격

센서네트워크 환경에선 노드의 ID를 위장하거나 가짜 라우팅 정보를 제공하고, 라우팅 프로토콜을 조작함으로서 쉽게 공격 받을 수 있다. 몇 가지 사례를 보면 다음과 같다. 공격용 노드는 다수 노드의 ID를 가장하여 무선 통신 대역을 많이 확보하게 된다. 이 경우, 타 노드는 공격용 노드로 라우팅을 시도하게 되어 정상적인 네트워킹이 불가능하게 된다. 이를 막기 위해선 사전에 비밀키를 분배하거나, 인증 프로토콜을 통해 노드의 identity를 확인할 수 있어야 한다. 또한, 공격용 노드는 라우팅 프로토콜의 헛점을 악용하여, 가짜 acknowledge 응답을 주위 노드에 보낼 수도 있다. 이 경우, 주위 노드는 공격용 노드에 계속적인 통신 시도를 할 것으로 보인다. 또한, RF 신호 강도와 같은 라우팅 정보를 조작하여 보냄으로서 주위 노드들이 공격용 노드에 접속을 선호하도록 가장할 수 있다. 즉, 가짜 라우팅 비용 정보를 제공하여 정상적인 네트워킹을 막는 방법이다. 이는 노드에 대한 인증을 통해서 가짜 노드가 해당 네트워크에 join하지 못하게 하여 막을 수 있으며, 또한, 링크 계층 프로토콜에 대한 메시지 인증 등을 통해, 정상 메시지로부터 추출한 명령에 대해서만 대응할 수 있도록 할 수 있다.

2.4. 물리적 공격

센서네트워크는 옥외에 설치되어 외부 환경 정보를 센싱하여 이를 처리하는 목적으로 많이 사용되기 때문에, 쉽게 외부의 물리적인 공격에 노출되기 쉽다. 센서네트워크에 대한 물리적인 공격으로는 물리적인 손상이나 절취 등이 가능하다. 이러한 경우에는 전류 센서 등을 사용해서 절취 등을 발견하여 대응할 필요가 있다.

이 외에 또 다른 형태의 물리적 공격으로 소비전력이나 방사되는 전자파 정보와 같은 부채널 정보(side

channel information)를 사용하여 키 값과 같은 주요 정보를 알아내는 방법이 있다. 이 기법으로는SPA(simple power analysis attack)와 DPA(differential power analysis attack), EM(electromagnetic attack) 공격 등이 있다. 이를 방지하기 위해선 키 값을 사용하는 암호 알고리즘, 보안 프로토콜, 소프트웨어 등에 대한 부채널 공격 방지 기법(side channel tamper resistant technique)이 구현되어야 할 것이다. 또 다른 물리적 공격 기법으로는 SPI 버스나 JTAG 포트, EEPROM에 대한 공격으로 주요 데이터나 시스템 프로그램, 하드웨어 설계 데이터에 대한 공격 및 역공학적 공격 기법이 있다.

Ⅲ. 센서네트워크 보안 기술 개발 현황

본 장에서는 센서네트워크에서의 주요한 보안 취약성인 도청 문제와 키 분배 문제, 라우팅 공격 문제, 물리적 공격 문제에 대한 개발 현황에 대해 소개하고자 한다.

3.1. 도청 문제 해결

도청 문제를 해결하기 위해선 전술한 것처럼 센서네트워크의 저전력 통신 특성과 컴퓨팅 능력에 적합한 형태의 암호 알고리즘을 사용하여 기밀성을 제공할 수 있다. 센서간 RF 통신 칩으로 많이 사용되고 있는 CC2420 칩에선 AES-128 암호 알고리즘을 하드웨어 IP로 제공하고 있는데, 이를 사용하면 통신 데이터에 대한 기밀성이 보장된다. CC2420에서 제공하는 암호 기능을 살펴보면 다음과 같다[2].

- Counter 모드와 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 변경을 필요로 함
- 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

〔표 1〕 CC2420 칩에서 제공한 암호의 동작 특성

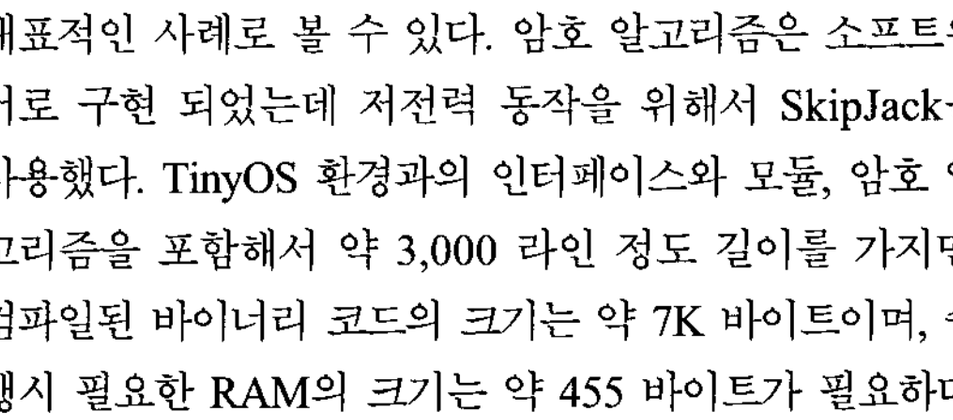
mode	L(a)	L(m)	L(MIC)	Time(us)
CCM	50	69	8	222
CTR	-	15	-	99
CBC	17	98	12	99
stand-alone	-	16	-	14

* a: authentication payload
* m : message
* MIC: message integrity code
* i.e. L(a) : byte length of authentication payload

CC2420에서 제공하는 각 암호의 동작 모드(mode of operation)의 성능을 보면 아래와 같다. 각 동작을 보면, AES-CCM 동작 성능이 222 usec로 WPAN 환경에서 충분히 사용할 수 있음을 알 수 있다. 즉, AES-CCM 모드를 사용하더라도 기존의 데이터 전송에 영향을 주지 않음을 의미한다.

센서네트워크 환경에서 도청 문제를 해결한 또 다른 개발사례로는 TinySec을 예로 들 수 있다[3]. TinySec은 TinyOS 1.1.0에서 구현된 것으로서 MICA와 MICA2, MICADot 모트와 호환성을 가진다. 사용한 RF 칩 환경은 Chipcon사의 CC1000과 RFM TR1000으로서 현재의 TinyOS 2.0 환경에선 호환되지 않는다. TinySec은 센서네트워크 환경에서 도청 및 위변조 방지 기능이 구현된 대표적인 사례로 볼 수 있다. 암호 알고리즘은 소프트웨어로 구현 되었는데 저전력 동작을 위해서 SkipJack을 사용했다. TinyOS 환경과의 인터페이스와 모듈, 암호 알고리즘을 포함해서 약 3,000 라인 정도 길이를 가지면, 컴파일된 바이너리 코드의 크기는 약 7K 바이트이며, 수행시 필요한 RAM의 크기는 약 455 바이트가 필요하다. 아래 그림은 TinySec 컴포넌트 그림을 보여주고 있다.

TinySec에선 기밀성 제공 뿐만 아니라 데이터 위변조에 대한 방지 기능을 제공하는데, 보안성을 높이기 위해선 통신 패킷에 대한 오버헤드를 유발한다. 즉, MIC



〔그림 1〕 TinySec component diagram

값을 패킷에 덧붙이면 그 만큼 패킷의 위변조 방지 기능이 없는 경우보다 더 패킷의 길이가 늘어나게 된다. 이는 센서네트워크의 메모리 사용량이 많아진다는 것을 의미하는 것 외에도 센서네트워크에 있어서 매우 중요한 요소인 소비 전력량이 많아진다는 것을 의미한다. TinySec에선 개발한 기술의 통신 오버헤드 특성을 분석했는데, 그 결과를 보면 다음과 같다.

- 보안 기능(기밀성, 무결성)을 제공하지 않은 경우: 37 바이트(CRC 포함)
- 무결성을 제공하는 경우(TinySec-Auth 모드) : 38 바이트
- 무결성 및 기밀성을 제공하는 경우(TinySec-AE 모드) : 42 바이트

즉, TinySec에선 무결성 및 기밀성을 제공하는 경우라도 보안 기능을 제공하지 않은 경우보다 약 8%의 정도의 패킷 오버헤드를 가진다. 비록 계산 및 통신시 소비되는 전력량에 대한 정확한 데이터를 제공하지는 않았지만, 일반적으로 통신 패킷 길이와 통신 소비 전력은 비례하므로, 이를 통해 보안 기능이 구현되었을 때도 상대적으로 그다지 많지 않은 소비 전력이 추가됨을 알 수 있다. 한편, TinySec에선 대칭키 암호 알고리즘을 사용할 때 필수적으로 해결해야 할 문제인 키 분배 문제에 대해선 언급하지 않고 있다.

3.2. 키 분배 문제 해결[1)]

키 분배 문제는 센서네트워크에서 기밀성 및 무결성을 보장하기 위해서 암호 알고리즘을 사용하는 경우에는 반드시 선행되어야 할 문제다. 현재 키 분배 문제를 해결하기 위한 많은 노력이 학계 등을 중심으로 행해지고 있다. 예를 들어, 인증센터를 사용하는 기법이 IEEE 802.15.4 표준 문서에도 언급 되어 있으며, 랜덤 키 사전 분배 기법, q-합성수 랜덤 키 사전 분배 기법, Blom 스킴, 위치 기반 키 사전 분배 기법 등 많은 연구 논문이 나와 있다. 또한, 최근에는 그 동안 많이 다루지 않던 타원곡선 암호 알고리즘과 같은 공개키 암호를 센서네트워크 환경에 사용하여, 안전하게 키를 분배하는 방식에 대한 연구/개발 결과물도 있다. 본 논문에선 대표적인 키 분배 기법인 사전 키 분배 기법과 Blom 스킴, 그리고 공개키 암호 알고리즘을 사용한 키 분배 사례를 보이고자 한다.

임의 키 사전 분배 기법은 정의된 키 공간에서 매우 크기가 큰 대칭키 풀을 임의로 선택하고, 이 풀로부터 일정한 갯수의 키를 임의로 선택하여, 각 노드에게 분배한다. 이렇게 되면 각 노드는 임의의 키 세트를 가지게 되며, 통신을 원하는 두 노드 사이에는 자신이 가지고 있는 키 세트 중에서 동일한 키 값을 가질 수도 있고 그러지 못할 수도 있다. 만일, 통신을 하고자 하는 두 노드가 동일한 키를 가질 경우에는 이 키를 가지고 안전한 통신을 수행하면 된다. 하지만, 만일, 두 노드에는 동일한 키를 공유하지 않는 경우에는 통신을 원하는 노드들은 자신의 키 세트와 동일한 키를 가지는 다른 노드를 찾아, 우회 통신을 하면 된다[4]. 이 키 분배 기법은 birthday paradox 개념을 응용한 것으로, 완벽하지는 않더라도 임의의 두 노드 사이에 성공적으로 키를 생성할 확률이 매우 높다[1].

한편, Blom 스킴은 임의 키 분배 방식에 비해 물리적인 노드 캡쳐에 의한 공격에 높은 보안성을 가진다. Blom 스킴은 $(\lambda+1) \cdot N$의 공개 행렬 G와 $(\lambda+1) \cdot (\lambda+1)$의 개인 행렬 D를 기본으로, A=(DG)T를 비밀 행렬로 한다. 이때 D는 대칭행렬이어서, AG=(AG) T의 특성을 가진다. 각 노드i는 A의 i번째 열과 G의 i번째 행을 저장하고, 노드 배치 후 노드i와 노드j가 키를 생성하고자 할 때, 서로 G의 행을 교환한 후, 각각 Kij=AiGj, Kji=AjGi 를 계산한다. Kij = Kji 이므로 두 노드는 동일한 키를 가지게 된다. Blom 스킴은 λ-security의 특성을 갖는다. 이는 개인 행렬에서 노출되는 열의 수가 λ 이하이면 행렬 D를 기반으로 생성된 다른 키들의 안전이 보장됨을 의미한다[1],[5].

한편, 위에서 제시된 기법 외에도 그 동안 센서노드의 높은 자원 제약성 때문에, 많은 연구가 진행되지 않았던 공개키 암호 알고리즘을 사용한 사례가 있다. 국외 개발 사례를 먼저 살펴보면, North Carolina 주립대학에선 타원곡선 암호 알고리즘(ECC)를 TinyOS 상에서 구현하여 키를 안전하게 분배하고 있으며, 실제 사용을 위해 타원곡선 기반 암호화 프로토콜인 ECIES와 키 분배 프로토콜인 ECDH, 서명 기법인 ECDSA 프로토콜을 구현하였다[6]. 해당 기술은 MICAz와 Telosb, Tmote Sky에서 사용할 수 있으며, SECG에서 추천하는 128 비트와 160

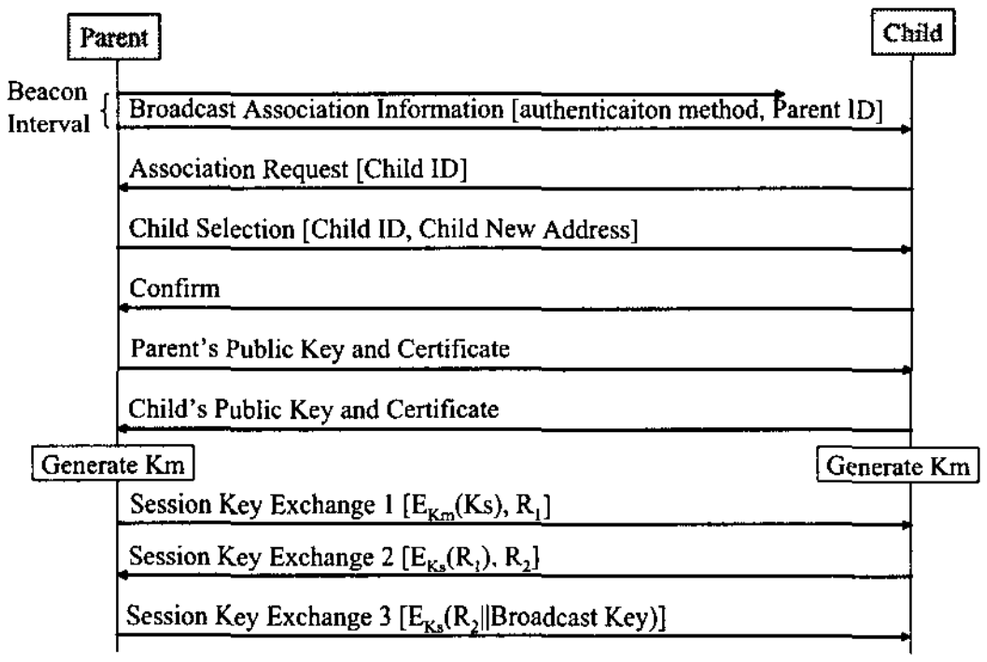
1) 본 절에 소개된 키 분배 문제 해결기법 중에서 공개키 암호 알고리즘을 사용한 기법은 본 저자의 다른 논문 [1]에 상세한 내용이 소개되어 있다.

비트, 192비트 타원곡선을 사용하고 있다. 성능을 보면, 전자서명에 3.17초, 검증에 4.04초가 소요된다. 이는 비록 대칭키 암호 알고리즘 기반의 키 분배 기법보다는 다소 긴 시간이지만, 실제 응용에 사용되는 경우에도 충분히 실제 사용할 수 있는 시간이다.

저자도 공개키 암호 알고리즘을 센서네트워크에 적용하여 실제 환경에서 안전한 키 분배 실험을 완료했다. 트리 구조의 센서네트워크 형성과정에서 [그림 2]와 같이 부모 자식 노드 사이에 키를 생성하는 과정을 개발하였다[1]. 부모 노드가 주기적으로 송신하는 정보를 자식 노드가 수신하고 자식 노드가 접속을 요청한다. 부모 노드는 다수의 접속요청들 중 하나를 선택하여 네트워크 주소를 할당한 후, 공개키를 주고받아 ECDH 키 생성과정을 수행한다. ECC 연산 모듈은 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. [표 2]는 브로드캐스트 되는 접속 정보 프레임이 송신된 이후, 세션키를 생성할 때까지의 각 단계별 소요시간을 측정한 값이며, [표 3]은 키 생성시 필요한 총 소요시간을 보이고 있다. 공개키 인증서의 마지막 프레임을 수신한 이후, 세션키 생성 과정을 시작하는 단계까지, 즉 Km을 생성하는 시간이 전체 과정의 대부분을 차지한다. 이는 공개키 암호알고리즘의 많은 연산량 때문이다.

현재 타원곡선 암호를 사용하는 경우, 프로토콜 구성 여하에 따라 4초에서 14초 정도의 시간이 소요된다. 키 분배는 센서네트워크의 설정 단계에서 필요로 하는 단계이므로, 이 정도의 시간도 실제 사용할 수 있는 정도의 수준이다. 만일 더 빠른 시간을 필요로 할 경우에는 공개키 암호 알고리즘을 수행할 수 있는 FPGA (혹은 칩)를 전용으로 센서노드에 구현하여 고성능을 얻을 수 있다.



〔그림 2〕 공개키 기반 키 생성 과정

〔표 2〕 단계별 키 생성 소요 시간 (단위: 초)

	누적 시간	소요 시간
Broadcast Frame	0.000	
Confirm	0.748	0.748
Last Certifcate Frame	1.253	0.505
SKE 1	14.500	13.347
SKE 3	14.681	0.181

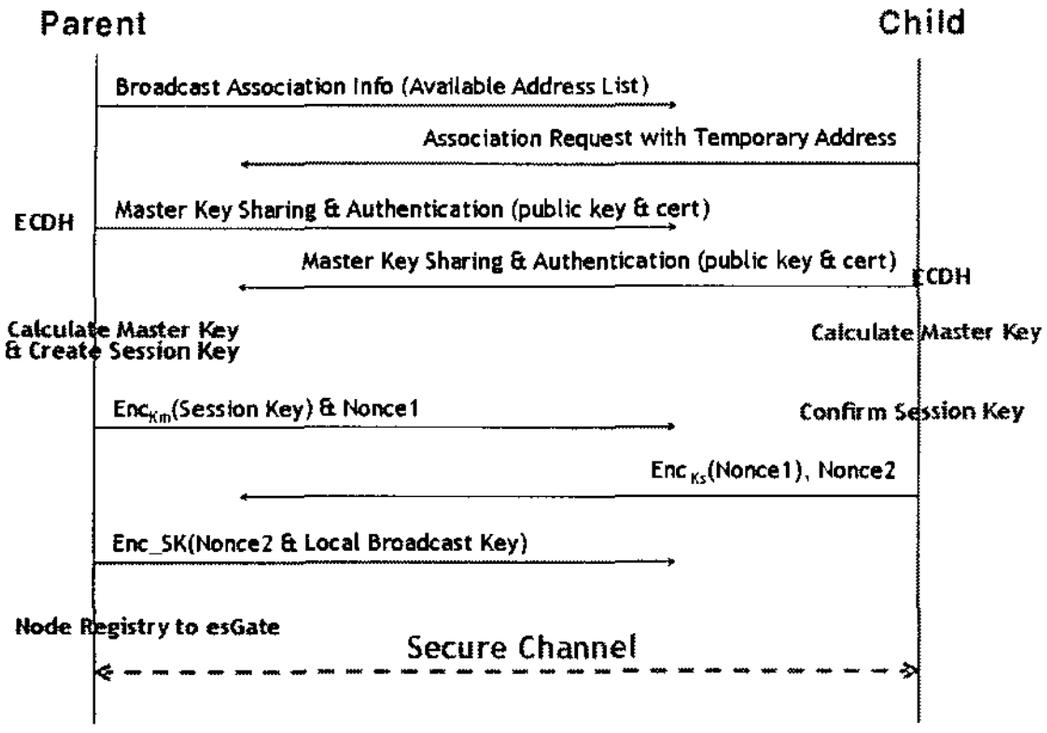
〔표 3〕 키 생성 총 소요 시간 (단위: 초)

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

3.3. 라우팅 공격 방지

전술한 것처럼 센서네트워크의 네트워크 라우팅 레벨에서는 다양한 공격 기법이 존재한다. 여기서, 노드 ID 값을 가장하는 sybil attack이나 허위 acknowledge 응답을 통해 공격하는 ACK spoofing 공격, 라우팅 비용 등을 허위로 제공하여 라우팅을 교란하는 sinkhole attack 등은 통신하고 있는 상대 센서노드의 신원(identity)을 확인하는 인증 기능을 추가함으로서 막을 수 있다. 이를 위해, 본고에서는 ETRI의 최근 연구 결과물을 소개한다[1]. 주요 특성으로는 인증을 받지 못한 센서노드는 기존의 라우팅이 수행되고 있는 센서네트워크의 통신 도메인에 참여할 수 없다. Secure association이라는 이 기법은 ECDH 공개키 암호 프로토콜을 사용하여 센서 노드간 인증을 수행하며, 인증을 통과한 노드만 상호 통신이 가능하다. 동작 을 기술하면 다음과 같다.

- 네트워크로 join하고자 하는 child 노드가 있을 경우, parent 노드는 association을 위한 절차를 시작하라는 명령을 child 노드에 보낸다(이때, 네트워크 라우팅 구조는 트리기반 라우팅 구조를 가정하고 있다).
- child 노드는 임의로 자신의 주소 정보를 parent 노드에 제공하여, network에 association하겠다는 의사를 보인다.



(그림 3) ECC 기반 Secure Association 절차

- 이때, parent 노드는 child 노드의 신원을 확인하기 위해, 공개키와 인증서를 제공한다.
- child 노드도 이에 대한 응답으로 자신의 공개키와 인증서 값을 전송한다.
- ECDH 프로토콜을 통해 안전하게 상대 노드와 키 분배가 완료된 노드는 인증서 정보를 통해, child 노드가 인증된 노드인지를 확인할 수 있게 된다.
- 인증 과정을 통과한 child 노드는 네트워크 라우팅 도메인에 참여하게 되어 세션키, nonce 값 등을 발생하여, 안전한 보안 통신이 가능하게 된다.

해당 연구 결과는 네트워크가 설정된 상태에서 새로운 노드가 들어올 경우 인증을 수행하는 것으로서 네트워크 보안 도메인을 구성할 수 있다는 장점을 가진다.

3.4. 물리적 공격 방지

물리적 손상이나 절취와 같은 물리적인 공격은 tampering 회로 등을 사용하여 이를 확인하여 물리적 공격에 대처할 수 있다. 또한, 현실적으로 센서노드 등을 옥외에 설치할 때, 물리적 구조물을 같이 설치하는데, 이를 통해서 물리적 공격을 방지할 수 있다.

소비전력과 같은 부채널 정보를 활용하여 공격하는 부채널 공격기법에 대한 방지 기술은 현재 암호학계를 중심으로 많은 연구가 진행되고 있다. 대표적인 연구 방향으로는 side channel resistant한 비밀키/공개키 암호 알고리즘에 대한 연구가 있다. 타원곡선 암호 알고리즘의 scalar multiplication 단계에 있어서 SPA/DPA resistant한 인코딩 기법에 대한 연구가 그 예에 해당한다.

또한, 센서노드 등을 구현하는데 있어서 디버깅 목적으로 사용하는 JTAG 포트에 대해 사후 서비스 론칭시에는 security bit를 활성화하여 내부 데이터와 프로그램을 유출하지 못하도록 해야 한다. 하지만, 이 경우에는 더 이상 디버깅이 불가능하다는 단점도 있다. 이를 위해 최근에는 freescale사를 중심으로 암호 기술을 사용하는 back-door key 기술을 사용하며, Xilinx나 Altera와 같은 경우에는 FPGA 설계 데이터에 대한 on-chip encryption 기법을 활용하여 FPGA 설계 데이터에 대한 보안성을 제공하고 있다. 실제 응용에 있어서는 물리적인 보안성이 그 무엇보다도 우선적으로 해결해야 할 분야이기 때문에, 향후 이 부분에 대한 연구가 많이 필요할 것으로 보인다.

Ⅳ. 결 론

본 고에서는 최근 국내에서는 이슈화 되고 있는 u-City와 u-Port 사업의 핵심 기술은 센서네트워크의 보안 취약성을 분석해보고 이에 대하여 기술적인 관점에서의 대책 및 기술 개발 현황에 대해 알아보았다.

센서네트워크 분야는 무선 통신 특성과 네트워크의 비정형성, 그리고 높은 자원 제약성으로 인해, 도청, 데이터 위변조, 네트워크 라우팅 공격, 물리적인 보안 취약성 등 다양한 보안 취약성을 가진다. 이를 해결하기 위해선 기밀성과 무결성으로 대표되는 기존의 보안 요구 사항을 센서네트워크에 적용할 수 있어야 하며, 또한, 센서네트워크의 고유한 특성으로 부터 발생하는 네트워크 라우팅 공격 문제와 물리적 보안 취약성, 부채널 공격 문제 등에 대한 적절한 대응 기술 개발이 필요하다. 본 고에서는 이와 관련하여 최근 국내외의 기술 개발 현황에 대해 간략히 소개하였다.

참고문헌

[1] 오경희, 김태성, 김호원, “공개암호키를 사용한 센서 네트워크에서의 키 분배 구현”, 한국방송공학회 동계학술대회 pp.95-98, 2008.2

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

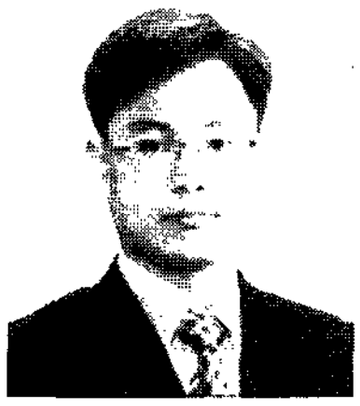
[3] Chris Karlof, Naveen Sastry, David Wagner, “TinySec : A Link Layer Security Architecture for Wireless Sensor Networks”, Sensys 2004

[4] L. Eschenauer and V. D. Gligor, "A key-management scheme for distributed sensor networks", In Proceedings of the 9th ACM Conference on Computer and Communication Security, pages 41--47, Nov. 2002

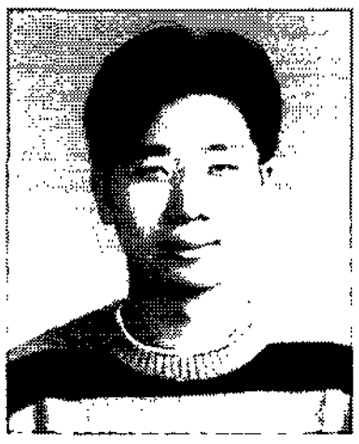
[5] R. Blom, "optimal class of symmetric key generation systems", EUROCRYPT 84 workshop on advances in cryptology: theory. and application of cryptographic techniques, pp. 335-338, Dec. 1985, Paris

[6] 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.

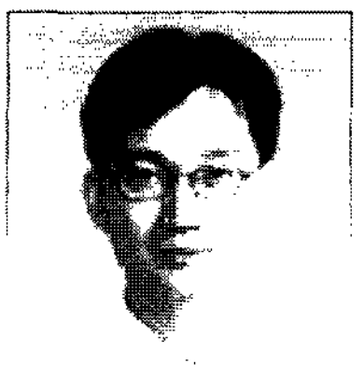
〈著者紹介〉



김 호 원 (Howon Kim)
종신회원
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 정보보호연구단 팀장/선임연구원
2008년 3월 ~ 현재 : 부산대학교 정보컴퓨터공학부 조교수
<관심분야> 센서네트워크 보안, RFID 보안, 프라이버시 보호, 공개키 암호, 저전력 기술



이 석 준 (Sokjoon Lee)
1998년 2월서울대학교 컴퓨터공학과 졸업
2000년 2월 : 서울대학교 컴퓨터공학과 석사
2000년 2월 ~ 현재 : 한국전자통신연구원 정보보호연구본부 선임연구원
<관심분야> 센서네트워크 보안, RFID 보안, 인증 프로토콜, 무선 침입탐지기술



오 경 희 (Kyunghee Oh)
1999년 2월 : 연세대학교 컴퓨터과학과 졸업
2001년 2월 : 연세대학교 컴퓨터과학과 석사
2000년 12월 ~ 현재 : 한국전자통신연구원 정보보호연구본부 선임연구원
<관심분야> 센서네트워크 보안, RFID 보안, 무선랜 보안