

공개암호키를 사용한 센서네트워크에서의 키 분배 구현†

*오경희 **김태성 **김호원

한국전자통신연구원

*khoh@etri.re.kr

Implementation of Publickey-based Key Distribution in Wireless Sensor Network

*Oh, Kyunghee **Kim, Taesung **Kim, Howon

Electronics and Telecommunications Research Institute

요약

센서네트워크는 넓은 지역에 무선 인프라로 묶여 설치된 센서들을 사용하여 상황 인지로 감지된 데이터를 응용서비스 서버와 연동하는 기술이다. 이는 환경 감시, 대상 추적, 환자 모니터링, 군사적 목적 등 매우 다양한 분야에 사용될 수 있다. 센서네트워크 역시 기존 네트워크에서 필요로 하는 보안 기능을 요구한다. 그러나 센서네트워크에 사용되는 노드들이 사용할 수 있는 자원에 제약이 있어, 기존의 암호기술을 그대로 적용하는데 어려움이 있다. 이러한 센서네트워크에서의 키 분배 문제를 해결하기 위하여 인증센터를 사용하는 기법, 랜덤 키 사전 분배 기법, q -합성수 랜덤 키 사전 분배 기법, Blom 스킴, 위치 기반 키 사전 분배 기법 등이 제안되어 있다. 한편, 공개키 연산의 많은 부하로 인하여 공개키 기법을 센서네트워크에 적용하기에 적합하지 않으리라 여겨져 왔으나, 최근의 연구결과들에 의하면 PKI처럼 복잡한 시스템을 구현하는 것은 부적합할지라도 공개키를 이용한 키 분배 기법을 센서네트워크에 적용하는 것이 실효성이 있다는 것을 보여준다. 본 논문에서는 TinyOS 플랫폼에서 공개키를 이용하여 센서 노드 간 상호 인증 및 세션키를 생성하여 암호 데이터 통신을 수행하는 센서네트워크 플랫폼을 구현한 결과를 제시한다.

1. 서론

유비쿼터스 컴퓨팅 시대의 필수 기반 기술로 센서네트워크의 중요성이 부각되고 있다. 센서네트워크는 넓은 지역에 무선 인프라로 묶여 설치된 센서들을 통하여 상황 인지를 하여 감지된 데이터를 응용서비스 서버와 연동하는 기술이다. 이는 환경 감시, 대상 추적, 환자 모니터링, 군사적 목적 등 매우 다양한 분야에 사용될 수 있다.

센서네트워크 역시 기존 네트워크에서 필요로 하는 보안 기능을 요구한다. 그러나 무선 통신의 공통된 취약점만이 아니라 센서네트워크 고유의 특성으로 인하여, 보안 기능 구현에 있어 고려해야 할 사항들이 있다. 우선 센서네트워크에 사용되는 노드들의 하드웨어들은 주로 작은 메모리를 가지고 전력 사용에 제한을 가지고 있어, PKI와 같은 고급 보안 기능을 사용하는데 제한이 있으며 기존의 암호기술을 경량화하여 구현하여야 한다. 또한 노드들이 공개된 장소에 배치될 수 있으므로, 네트워크에 대한 물리적 보호가 불가능한 경우들이 많다. 따라서 노드 캡처에 의한 공격에 쉽게 노출될 수 있으며, 이를 대비하여 물리적 침입을 방어할 수 있는 하드웨어를 구현하고, 노드 캡처에 의한 내부자 공격을 방어할 수 있는 체계가 필요하다.

만일 이러한 방어 체계가 구축되지 않는다면, 정보의 누출

에 의하여 개인의 프라이버시가 침해되거나 기업의 기밀 정보가 누출될 수 있으며, 공격자가 의도적으로 생성된 잘못된 데이터가 주입되어 기계가 오작동할 수도 있다.

이러한 위협으로부터 데이터를 보호하기 위하여, 센서네트워크에서도 암호화 통신이 꼭 필요하다. 그중 암호화 통신에 사용될 키를 분배하는 것은 센서네트워크에서의 보안 문제를 해결하기 위하여 선결되어야 할 문제들 중 하나이다. 센서네트워크에서의 키 분배 문제를 해결하기 위한 다양한 방법들이 제안되어 있으며, 인증센터를 사용하는 기법, 랜덤 키 사전 분배 기법, q -합성수 랜덤 키 사전 분배 기법, Blom 스킴, 위치 기반 키 사전 분배 기법, 공개키 방식 등이 있다. 본 논문에서는 센서네트워크의 특성을 고려한 키 분배 방식에 관한 것으로, 기존에 제안된 키 분배 방식을 살펴보고, 특히 공개키 기법을 사용하는 키 분배방법에 대하여 센서 노드들이 서로 인증하고 키를 분배할 수 있는 방법을 제시하고 구현한 결과에 대하여 논의한다.

2. 센서네트워크 보안

센서네트워크에 대한 공격 유형을 살펴보면, 우선 단순히 센서 노드간의 통신을 도청하는 공격이 있다. 이는 데이터를 암호화하여 전송함으로써 방지가 가능하다. 이를 위하여 노드 간

† 본 연구는 정보통신부 및 정보통신연구진흥원의 IT신성장동력핵심기술개발사업[2005-S-088-03, 안전한 RFID/USN을 위한 정보보호 기술] 사업의 일환으로 수행하였음

암호화 키 분배의 문제가 해결되어야 한다.

노드 캡처는 물리적으로 노드를 침입하여 키와 같은 비밀 정보를 획득하거나, 노드의 기능을 장악하여 내부자 공격에 활용하는 공격이다. 이러한 공격의 한 유형으로 SPA 혹은 DPA와 같이 노드 내부 회로의 전력 사용의 특성을 분석하는 기법을 사용하여 노드 내의 비밀 정보를 알아낼 수 있다. 이에 대비할 수 있는 하드웨어 및 소프트웨어 설계가 필요하다. 또한 물리적인 침입을 감지하고, 비밀 정보가 포함된 메모리를 삭제하는 등의 대비책도 가능하다.

센서네트워크 내에 허위 노드가 침입하게 되면, 공격자는 이 노드를 통하여 허위 정보를 유발하거나 실제 데이터의 전송을 방해할 수 있다. 침입한 허위 노드를 통하여 라우팅 경로 조작 등으로 여러 가지 공격들을 수행할 수 있다. 공격 노드가 라우팅 메시지의 경로 비용을 조작하여 주위 노드들의 라우팅 경로가 공격 노드로 향하게 한다면, 주위에서 센싱된 정보들을 도청할 수 있을 뿐만 아니라, 조작도 가능하다. 이러한 공격 유형으로 Selective forwarding, Wormhole attack, Sink hole attack 등이 있다. 또한 공격 노드가 여러 개의 ID를 가장하는 Sybil attack 도 가능하다. 만약 공격 노드로 노트북 컴퓨터와 같은 수준의 강력한 장비를 사용한다면, 다른 노드들에 비하여 강한 전파를 사용하는 공격도 가능한데, Hello flood attack이 그러한 공격의 한 예이다. 이러한 공격들은 허위 노드의 침입이나 노드 캡처 공격에 의하여 이루어지므로, 센서네트워크는 노드 인증 등의 과정과 같은 접근제어를 통하여 허위 노드의 침입을 방지할 수 있어야 하며, 제어 메시지를 암호화하고, 노드 캡처를 막기 위한 tamper-proofing을 통하여 방지하여야 한다. 또한 침입을 탐지하기 위하여 라우팅 경로를 다변화 하는, 비대칭 라우팅 경로 설정이나 다중 경로 설정 기법을 사용할 수 있다.

공격자가 허위 노드와 같은 내부자 노드를 사용할 수 없고 데이터 프레임들이 암호화되어 보호될지라도 공격자는 트래픽 분석만으로도 센서네트워크 환경에 대한 어느 정도의 정보 수집이 가능하다. 이에 대처하기 위해 정상적인 센서 노드들에서 허위 패킷을 발생시켜 트래픽 분석이 불가능하도록 하는 방법도 있다.

이러한 센서네트워크에서의 보안 위협 특성을 고려할 때, 이에 특화된 보안 기법이 필요하다. 노드 인증과 암호화 통신을 위해 노드들이 사용할 키를 분배하는 기능은 꼭 필요하다.

센서 노드의 자원 제약 특성으로 인하여 비대칭 키의 사용이 쉽지 않음으로 인해, 임의의 두 노드 사이에 대칭키를 분배하기 위한 연구들이 많이 이루어졌다. 만약 동일한 키를 여러 노드에서 같이 사용한다면, 노드 캡처 공격에 의하여 센서네트워크 전체의 비밀 정보들이 유출될 수 있는 위험에 처해질 수 있다. 반대로 임의의 두 노드 간 통신에서 모두 다른 키를 사용한다면 센서네트워크 전체에서 모든 노드 수의 제곱에 해당하는 키가 필요하며, 센서네트워크와 같이 많은 수의 노드가 사용되는 환경에서 각 노드에서 필요한 모든 키들을 노드들이 저장하고 관리한다는 것은 불가능하다. 이를 해결하기 위한 방법들을 살펴보면 다음과 같다.

우선 임의 키 사전 분배 기법이 있다. 임의 키 사전 분배 기

법은 모든 가능한 키 공간에서 매우 큰 대칭키 풀을 임의로 선택하고, 각 노드들마다 여기서 일정한 개수의 키를 임의로 선택하여 노드의 키 저장 공간에 저장한다. 이후 두 노드가 키를 공유하기 위해서, 자신의 키 저장 공간에 있는 키들의 ID를 이웃 노드들에게 브로드캐스트하고, 이웃 노드들에서 받은 키 ID 값과 자신이 가진 키들의 ID를 비교하여 공통된 키를 찾는다. 만약 동일한 키가 발견되면, 이 키를 사용하여 challenge response 과정을 거쳐 세션키를 생성한다. 만약 공통된 키를 발견하지 못한다면, 이미 세션키를 생성한 다른 이웃 노드로 우회하여 경로키를 생성할 수 있다[1]. 이러한 방법은 birthday paradox 개념을 응용한 것으로, 완벽하지는 않더라도 임의의 두 노드 사이에 성공적으로 키를 생성할 확률이 매우 높다.

그러나 이러한 방법은 어느 한 노드가 공격자에게 노출되었을 때, 센서네트워크의 키 풀 일부가 공격자에게 누출되고, 따라서 노출된 키 풀의 양에 따라 센서네트워크 내의 다른 통신 내용들도 공격자에게 노출되는 단점이 있다. 이를 보완하기 위한 방법들 중 하나로, q-합성수 임의 키 사전 분배 기법이 있다. 위의 임의 키 사전 분배 기법에서 두 노드 사이에 단 하나의 공통키를 사용하여 세션키를 생성했던 것과는 달리, q개의 공통키를 찾은 다음 이를 조합하여 세션키를 생성한다. 만약 공격자가 어느 정도의 키들을 알고 있다 하더라도, 두 노드 사이에 사용된 q개의 공통키들을 모두 알고 있어야만 도청이 가능하게 된다[2]. 그러나 두 노드 사이에 공통키가 q개 미만이라면 세션키를 생성하는 것이 불가능하다는 단점이 있다.

Blom 스킴은 네트워크상의 어떤 임의의 두 쌍이라도 두 노드 사이의 비밀키 생성이 가능하며 노드 캡처에 대해서도 이전의 방법보다 우수한 저항력을 가진다. $(\lambda+1) \cdot N$ 의 공개 행렬 G와 $(\lambda+1) \cdot (\lambda+1)$ 의 개인 행렬 D를 기본으로, $A=(DG)^T$ 를 비밀 행렬로 한다. 이때 D는 대칭행렬이어서, $AG=(AG)^T$ 의 특성을 가진다. 각 노드_i는 A의 i번째 열과 G의 i번째 행을 저장하고, 노드 배치 후 노드_i와 노드_j가 키를 생성하고자 할 때, 서로 G의 행을 교환한 후, 각각 $K_{ij}=A_iG_j$, $K_{ji}=A_jG_i$ 를 계산한다. $K_{ij}=K_{ji}$ 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[3].

이러한 방법 이외에도 노드의 배치 정보를 적용하여 메모리 효율과 연결성을 높인 방법들도 제안되었다[4,5].

IEEE 802.15.4[6]을 기반으로 하는 ZigBee[7]의 경우, Trust Center를 사용하여 키를 분배한다. 새로운 노드가 네트워크에 결합하기 위해서는 그림 1과 같이 노드가 라우터에 association을 맺은 후, 이를 경유하여 Trust Center로부터 인증 및 링크키를 분배 받는 방식이다. 그리고 두 노드 사이의 링크키를 생성하는 경우에도 그림 2와 같이 Trust Center가 개입한다. 이렇게 Trust Center를 사용한 인증 및 키 분배 방법은 인증 과정에서 아직 인증 받지 않은 노드로부터 여러 홉의 라우터를 거쳐 Trust Center까지 통신이 이루어져야 한다는 점에서, 노드의 수가 많은 센서네트워크에서는 인증 비용이 많이 소요되며, 공격 노드가 다수의 노드 ID를 가장하는 것과 같은 방법의 서비스 거부 공격을 할 수 있다는 점에 취약하다.

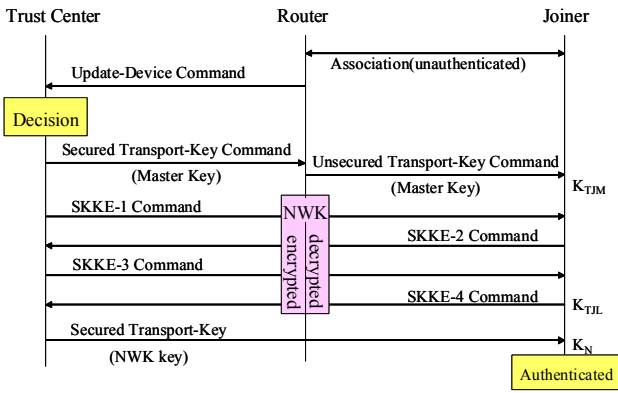


그림 1. Trust Center와 링크키 생성 과정

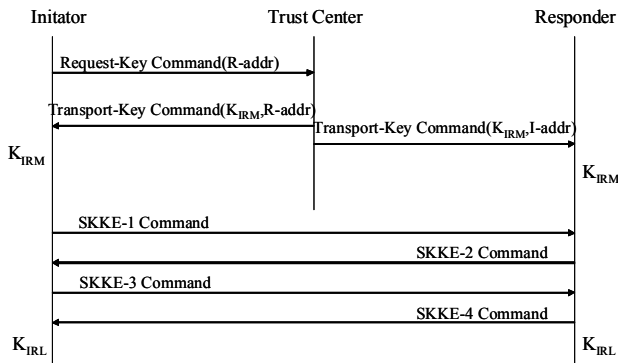


그림 2. 노드 사이의 링크키 생성 과정

무선랜 규격의 사례를 참조하면, IEEE 802.11 WLAN의 경우, 데이터 보안의 취약점을 제거하기 위하여, 단말의 접속 권한을 인증하고, 데이터 프레임을 새로운 암호 알고리즘을 사용하여 보호하도록, 기존 규격의 보안 기능 항목들이 수정되었다 [8]. 그러나 수정된 규격에서 데이터 프레임들에 대한 암호화 기능만을 지원하고, 관리프레임에 대한 무결성, 기밀성, 인증, 재전송 방지 등의 보안 기능을 제공하지 않았다. 이로 인하여 관리 프레임을 사용한 서비스 거부 공격 혹은 서비스 가로채기 공격 등이 여전히 가능하였다. 이에 IEEE 802.11 Task Group w에서 일부 관리 프레임에 대하여 암호화 및 인증 등의 보안 기능을 제공하는 방안들이 연구되고 있다[9].

IEEE 802.15.4 WPAN의 경우에도, WLAN의 관리 프레임에 해당하는 명령 프레임들을 사용한 공격이 가능하다. WPAN 규격에 명령 프레임에 대한 보안이 따로 정의 되어 있지 않으나, 데이터 프레임의 암호화와 동일한 방식으로 명령 프레임에 대한 보안을 적용할 수 있을 것이다. 그러나 ZigBee 규격에서 여러 수준의 보안 레벨을 정의하고 있으나, 가장 높은 수준의 보안을 적용한다하더라도 처음 association이 이루어지기 이전에는 노드 사이에 바로 적용할 수 있는 키가 존재하지 않는 문제점이 있다. 초기에 노드가 가질 수 있는 키는 Trust Center와 공유하고 있는 마스터키 밖에 없기 때문이다. 따라서 association 과정과 링크키 생성 과정이 완료되기 이전까지는 두 노드 사이에 주고받는 프레임들을 보호할 방법이 존재하지 않는다. 임의의 두 노드 사이에 키를 공유하는 방법을 제시하는 앞에 소개된 센서네트워크의 키 분배 방법들을 적용할 수 있다. 그러나 이러한 방법들은 노드의 자원을 추가로 요구하거나, 노드 캡처에 의하여 다른 노드 간의 비밀 정보까지 함께 유출될

가능성이 있는 등의 부담이 있다.

3. 공개키를 사용한 센서네트워크 키 분배

공개키를 이용한 키 분배 방법은 RSA 혹은 ECC와 같은 공개키 암호 알고리즘을 사용하여 Trust Center와 같은 제3자의 개입 없이 두 노드가 직접 안전하고 신뢰성 있게 키를 생성하는 방법이다. 공개키 알고리즘에서는 각 노드들이 자신 고유의 공개키와 비밀키 쌍을 가지고 있으며, 키를 생성하고자 하는 상대방의 공개키와 자신의 비밀키를 사용하여 두 노드 사이에 공유되는 키를 생성할 수 있다.

타원곡선 암호 알고리즘 ECC를 사용하여 키를 분배하는 ECDH의 경우, 노드 A가 비밀키 a와 공개키 a*G를, 노드 B가 비밀키 b와 공개키 b*G를 가지고 있을 때, 서로 공개키를 알려준 후, 각각 자신의 비밀키를 사용하여 두 노드 사이에 공유되는 키 $a*(b*G) = b*(a*G)$ 를 연산할 수 있으므로, 공유키 $a*b*G$ 가 생성된다.

기존 망에서 널리 사용되었으나, 센서네트워크에 사용되는 디바이스들의 자원제약으로 인하여 연산량이 많은 공개키 암호화 방식이 적합하지 않으리라 여겨졌다. 그러나 최근의 연구결과들은 공개키 암호화 방식이 센서네트워크 보안에서도 여전히 유효함을 보여준다. TinyOS 기반에 ECC 알고리즘을 구현한 TinyECC의 경우, ECDSA를 이용하여 전자서명에 3.17초, 검증에 4.04초가 소요된다[10]. 이는 대칭키 기반의 연산시간에 비하면 여전히 긴 시간이지만, 실제 응용에 키 분배 방법으로 구현되어 사용된다하더라도 충분히 실효성이 있는 시간으로 볼 수 있다.

또한, Trust Center를 이용하는 Kerberos 기반의 노드 키 분배 방법과 타원곡선 암호 알고리즘을 이용한 공개키 암호 프로토콜 ECDH/ECMQV 기반 키 분배 방법의 비교에서, Trust Center와 노드간의 연결 홉수가 3홉 이상이 되면 오히려 공개키 기반의 방식에 비하여 에너지 소모가 더 많아짐을 보여준다[11].

본 연구에서는 트리 구조의 센서네트워크 형성과정에서 그림 3과 같이 부모 자식 노드 사이에 키를 생성하는 과정을 개발하였다. 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 1은 브로드캐스트 되는 접속 정보 프레임이 송신된 이후, 세션키를 생성할 때까지의 각 단계별 소요시간을 측정된 값이다. 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.

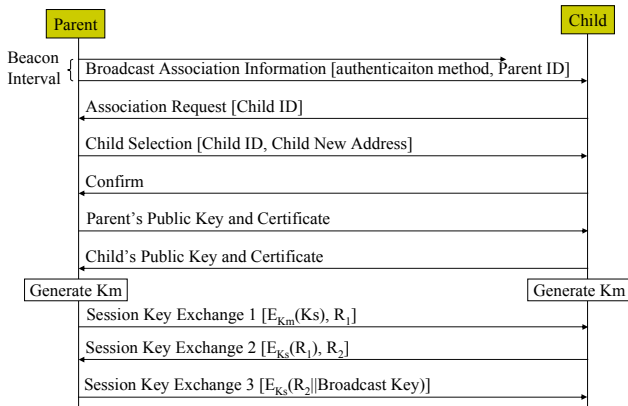


그림 3. 공개키 기반 키 생성 과정

표 1. 단계별 키 생성 소요 시간 (단위: 초)

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

표 2. 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

표 2는 동일한 조건에서 반복하여 실시한 시험에서, 키를 생성하는데 소요된 시간이다. 시험에 사용된 센서 노드 하드웨어는 MSP430 MCU를 탑재한 TmoteSKY이다.

4. 결론

공개키 기반의 키 분배 기법은 랜덤 키 사전 분배 기법과 Blom 스킴에 비하여 노드 캡처에 의한 비밀정보 유출 공격에 강하다는 장점이 있으나, 많은 연산량이 필요하다는 단점이 있다. 기존의 컴퓨팅 환경에 비하여 센서 노드에 사용되는 MCU가 공개키 암호 알고리즘의 많은 연산량을 처리하기에 부담이 전혀 없는 것은 아니다. 그러나 구현 결과에서 볼 수 있듯이 노드 사이에 키를 생성하는데 필요한 시간이 14~15초 정도로 그리 길지 않고, 키 생성이 센서네트워크의 초기화 과정에서만 필요한 점을 고려할 때, 공개키 암호 알고리즘을 사용한 센서네트워크 키 분배 기법도 충분히 실효성이 있다고 볼 수 있다. 또한 연결을 맺고자 하는 두 노드간의 통신 이외의 별도 통신 없이 키 분배가 이루어지므로, Trust Center 기반의 키 분배 방식과 비교하여 확장성이 있다. 단지 시험에 사용된 MSP430에서 제공하는 48Kbyte 프로그램 영역 중 공개 암호 알고리즘 관련 코드가 약 13Kbyte를 사용하여, 상대적으로 비중이 컸다.

센서네트워크는 건축물 관리나 환경 감시 등을 위하여 공개된 장소에 배치될 가능성이 매우 높다. 따라서 외부 위협에 대한 노출도 많아 이에 대한 대비가 꼭 필요하다. 전통적인 정보보호 기술들을 센서네트워크에 적용하는 방법 중 하나로, 기존의 네트워크 환경에 널리 사용되고 있는 공개키 기반의 정보보호 기법도 센서네트워크에 적용할 수 있음을 확인하였다.

참고 문헌

- [1] 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
- [2] H. Chan, A. Perrig, and D. Song. "Random key predistribution schemes for sensor networks," In IEEE Symposium on Security and Privacy, May 2003
- [3] 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
- [4] W. Du, J. Deng, Y. S. Han, S. Chen, and P. Varshney, "A Key Management Scheme for Wireless Sensor Networks Using Deployment Knowledge," IEEE INFOCOM 04, Hong Kong, March, 2004
- [5] D. Huang, M. Mehta, D. Medhi, L. Harn. "Location-aware Key Management for Wireless Sensor Networks," 2nd ACM Workshop on Security of Ad Hoc and Sensor Networks, 2004
- [6] IEEE 802.15.4-2003, IEEE Standard for Information technology--Telecommunications and information exchange between systems--Local and metropolitan area networks--Specific requirements Part 15.4: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low Rate Wireless Personal Area Networks (LR-WPANs)
- [7] ZigBee Specification, ZigBee Document 053474r06, Version 1.0, ZigBee Alliance, June 27, 2005
- [8] IEEE 802.11i-2004, Amendment to IEEE Std 802.11, 1999 Edition. IEEE Standard for Information technology--Telecommunications and information exchange between system--Local and metropolitan area networks--Specific requirements--Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications--Amendment 6: Medium Access Control (MAC) Security Enhancements
- [9] Protected Management Frames, http://grouper.ieee.org/groups/802/11/Reports/tgw_update.htm
- [10] 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.
- [11] J. Johann Großschadl, A. Szekeley, and S. Tillich, "The Energy Cost of Cryptographic Key Establishment in Wireless Sensor Networks," ASIACCS 2007, pp. 380 - 382. ACM Press, 2007.