센서 네트워크 보안 연구 동향

Research Trend for Sensor Network Security

나재훈(J.H. Nah) IPv6보안연구팀 책임연구원, 팀장
채기준(K.J. Chae) 이화여자대학교, 교수
정교일(K.I. Chung) 정보보호기반그룹 책임연구원, 그룹장

센서 네트워크는 많은 수의 센서 노드들로 구성된 네트워크로 센서를 통한 주변 정보 감지 및 감지된 정보를 처리하는 기능을 수행한다. 최근 유비쿼터스 컴퓨팅 개념의 도입과 함께 이를 실생활에 구현하기 위한 기반 기술의 하나로 센서 네트워크가 큰 관심을 모으고 있다. 그러나 유비쿼터스 컴퓨팅을 통한 삶의 편리성을 추구함과 동시에 네트워킹을 통해 제공되는 정보를 신뢰할 수 있어야 하며 개인의 프라이버시 또한 보장되어야 함은 기본적인 요구 사항이다. 센서 네트워크는 기존의 네트워크와 여러 모로 다른 특성을 갖고 있어 기존의 보안 기법을 그대로 적용하기 어렵다. 이러한 필요성에 의해 다양한 센서 네트워크 보안 관련 연구가 진행되고 있는데 본 고에서는 최근 가장 활발히 연구되고 있는 센서 네트워크 보안에 관련된 인증, 키관리, 네트워크 구조 등을 중심으로 연구 동향을 살펴본다.

I. 서 론

센서 네트워크는 유비쿼터스(ubiquitous) 컴퓨팅 구현을 위한 기반 네트워크로 초경량, 저전력의 많은 센서들로 구성된 무선 네트워크이다. 이는 특히 네트워크를 구성하는 센서의 수가 매우 많고 각 센서 노드들은 제한된 전력과 컴퓨팅 능력을 가지며, 빈번한 센서 노드들의 삽입과 제거에 의해 센서 네트워크의 토폴로지가 쉽게 변화될 수 있다는 특성을 갖는다. 이러한 센서 네트워크는 센서를 통한 정보 감지 및 감지된 정보를 처리하는 기능을 수행함으로써 우리의 삶을 자동화시키고 편리함을 제공하지만 일상 생활의 시스템에의 의존도가 높아질수록 이로 인한 위험성 또한 높아질 수 밖에 없다. 그러므로 센서 네트워크를 통해 제공되는 정보들을 신뢰하고 동시에 개인의 프라이버시를 보장 받을 수 있도록 하기 위한 보안 연구가 반드시 병행되어야 한다. 즉, 보다 현실적이고 안전한 유비쿼터스 컴퓨팅 환경을 구현하기 위해서는 센서 네트워크의 활용 방안 및 센서 기술 개발과 함께 감지된 정보를 안전하게 처리하고 관리할 수 있는 센서 네트워크 상에서의 보안 메커니즘 개발이 반드시 함께 연구되어 적용되어야 한다.

유비쿼터스 컴퓨팅 보안에 관한 연구에서 센서 네트워크와 더불어 흔히 언급되는 또 하나의 개념으로 RFID(Radio Frequency Identification)가 있다. RFID는 radio frequency를 이용한 전자 태그로 사람 또는 사물 등에 부착되어 대상에 관한 정보를 제공하는 것으로, 환경을 감지하고 감지된 정보를 네트워킹을 통해 전달하여 다음 단계의 오퍼레이션을 유도하는 센서 네트워크보다 훨씬 축소된 개념이다. 특히 향후에는 RFID의 기능이 점차 확대되어 단순한 태그의 기능으로서가 아니라 센서의 기능으로까지 확대될 것으로 예상되므로 본 고를 통해서는 좀 더 다양한 환경에서 다양한 기능을 수행할 수 있는 확장된 기능의 센서에 관련된 최근의 보안 연구 동향에 대해 살펴보기로 하겠다.

본문의 구성은 다음과 같다. II장에서는 센서 네트워크의 특성 및 보안상의 취약성에 대해 살펴보고, III장에서는 실제적으로 진행되고 있는 다양한 센서 네트워크 보안 연구 동향의 보안을 위한 인증 기법, 키관리 기법, 센서 노드간 pairwise 키 설정

기법, 네트워크 구조 연구, 기타 보안 연구 등으로 나누어 살펴보고 Ⅳ장에서 결론을 맺는다.

Ⅱ. 센서 네트워크 특성 및 보안상의 취약성

센서 네트워크는 일반적으로 특정 지역에 수없이 많은 센서들이 무작위로 뿌려져서 대상에 대해 감지하고 감지된 데이터를 중앙의 베이스 스테이션으로 전송하는 구조를 갖는다. 각 센서 노드가 다른 노드의 데이터를 중계해주는 기능을 한다는 점에서 기존의 모바일 애드혹 네트워크의 한 특수한 형태로 인식하는 경우도 있지만 센서 노드는 일회성을 갖는 경우가 많아 가격도 매우 저렴하고 크기도 작아야 하며 작은 기억 공간, 제한된 계산 능력 등을 특성으로 하므로 사실상 애드혹 네트워크보다도 훨씬 제약사항이 많다. 센서 네트워크는 수많은 노드들이 감지된 정보를 베이스 스테이션에게 보내야 하므로 중복된 데이터도 많고 베이스 스테이션이 각각의 데이터를 일일이 취합하기에 어려움이 많을 뿐 아니라 불필요한 트래픽의 증가로 이를 중계해야 하는 노드들에게 부담이 되어 수명을 줄이는 결과를 가져올 수 있으므로 중간에 aggregator(또는 게이트웨이)를 두는 구조를 취하는 형태가 대부분이다. 즉, 제한된 능력을 갖는 일반 센서 노드들과 이 센서 노드들로부터 데이터를 전송 받아 취합하여 베이스 스테이션으로 보내거나 베이스 스테이션으로부터의 쿼리를 센서 노드로 전달하는 aggregator 노드, 각 aggregator로부터 데이터를 받아 이를 취합하여 다음 기능을 수행하거나 필요 시 데이터 쿼리를 각 aggregator로 전달하는 베이스 스테이션으로 구성된 형태를 갖는다.

센서 네트워크는 네트워크가 갖는 근본적 특성으로 인해 일반 네트워크보다 훨씬 보안에 취약하다는 특성을 갖는다. 우선 센서 노드의 제약으로 인해 다양한 보안 스킴을 적용하기 힘들 뿐 아니라 노드가 배치된 물리적 환경이 공격에 그대로 노출되어 전송되는 정보가 쉽게 변경되거나 정당하지 않은 노드가 데이터를 전송함으로써 전체 정보의 무결성을 쉽게 무너뜨릴 수 있다. 뿐만 아니라 악의적인 노드가 센서 노드로 가장하여 불필요한 정보를 계속 발생시켜 중간 노드의 자원을 소모시킴으로써 네트워크의 수명을 단축시킬 수도 있다. 이처럼 간단한 공격만으로도 네트워크 전체를 쉽게 와해시킬 수 있을 뿐 아니라 특히 센서 네트워크의 목적에 따라서는 그 위험성이 상상을 초월할 수도 있다. 이처럼 보안에 취약함에도 불구하고 센서 네트워크의 보안 연구에 관한 필요성이 간과되는 경우가 많을 뿐 아니라 기존 보안 기법을 그대로 적용하기도 힘들다. 그러므로 센서 네트워크 기반 기술 연구의 초기 단계인 지금 이 센서 네트워크의 특성에 적합한 보안 기술 연구가 같이 진행되어야 하는 시점이다.

Ⅲ. 센서 네트워크 보안 연구 동향

현재 이루어지고 있는 대부분의 센서 네트워크 보안 기술 연구는 키분배 및 관리, 인증, 보안을 위한 네트워크 구조, 라우팅 등 다양한 보안 요소들이 결합된 형태로 이루어진다. 여러 가지 보안 요소가 동시에 포함되므로 다양한 기준으로 분류할 수 있으나 본 고에서는 편의상 가장 강조된 개념을 중심으로 인증 메커니즘, 그룹키 위주의 키관리 메커니즘, pairwise 키설정 메커니즘, 보안을 위한 네트워크 구조, 기타로 분류하여 소개한다.

1. 인증 기법

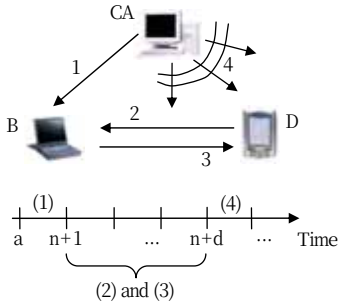
먼저 센서 네트워크 보안을 위해 초기에 제안된 대표적인 인증 메커니즘으로 A. Perrig, R. Szewczyk, V. Wen, D. Culler, J.D. Tygar의 SPINS(Security Protocols for Sensor Networks) 보안 구조를 들 수 있다[1]. 이 방법은 데이터의 기밀성을 제공하기 위한 SNEP(Secure Network Encryption Protocol) 구조와, 브로드캐스팅되는 데이터의 인증을 제공하기 위한 μTESLA 스킴으로 구성되어 있다. 이때 베이스 스테이션은 안전하며 센서 노드들은 베이스 스테이션과 공유하는 하나의 마스터 키 K를 사

전 분배 받는다고 가정한다. 먼저 SNEP 구조에 대해 살펴보면 A가 B에게 메시지 D를 보내고자 하면, A는 D를 마스터 키로부터 유도된 암호화 키 K_{encr}와 카운터 C를 이용하여 데이터를 암호화하고, 암호문에 C를 붙여 MAC 키로 MAC 값을 만들어 (1)과 같이 전송한다.

$$A \rightarrow B: \{D\}_{(K_{encr},C)}, MAC(K_{mac}, C|\{D\}_{(K_{encr},C)}) \quad (1)$$

μTESLA는 TESLA 방식을 센서 네트워크에 적용 가능하도록 응용한 것으로 인증 키 체인 생성이나 브로드캐스트 데이터 생성 방식은 TESLA와 유사하다. 단, 베이스 스테이션만이 센서 노드들에게 브로드캐스트할 수 있으며 센서 노드간 직접적인 브로드캐스팅은 지원되지 않는다. 따라서, 베이스 스테이션에서만 데이터 패킷 인증을 위한 키 체인을 생성하여 유지하며 초기 패킷 인증을 위한 전자 서명은 사용되지 않는다. 이 메커니즘은 해시 체인을 이용하여 효과적으로 데이터 인증을 제공할 수 있고 수신 노드들의 입장에서 중간에 패킷 분실이 발생하더라도 다음 패킷을 통해 이전 패킷들을 검증할 수 있는 장점을 갖는다. 그러나 모든 노드들이 "시간 동기화"가 되어 있어야 하고 실제 네트워크 전송 지연이 있을 수 있으므로 이를 고려한 키 노출 지연 시간의 설정 및 패킷의 저장을 위한 공간이 추가로 필요하다는 단점을 갖는다.

Mathias Bohge, Wade Trappe는 센서 네트워크 구조를 고전력의 AP(Access Point), 중전력의 이동성 전달 노드, 저전력의 이동성 센서 노드의 3계층의 애드혹 네트워크 토폴로지를 갖는 구조로 설정하고 이들간의 효율적 인증을 위해 TESLA를 이용한 인증서 방식을 제안하였다[2]. 이 구조를 기본으로 가장 상단에 존재하는 애플리케이션에 의해 브로드캐스트된 데이터를 인증하기 위해, 그리고 센서 노드의 이동 후에 필요한 엔티티 인증을 위해 TESLA 방식을 응용한 TESLA 인증서를 사용한다. 이 방식의 경우, 센서 노드 간에 직접적 통신은 없으며 중간에 위치한 전달 노드는 전달 기능만을 갖는 단순한 노드이고 모든 노드와 AP는 RSA 키 쌍을 가지며 TTP(Trusted Third Party)의 공개키를 알



(그림 1) TESLA 인증서 사용 단계

고 있다고 가정한다. 먼저 TESLA 인증서 발급 방식을 살펴보면 (그림 1)에서 보는 바와 같이 CA (Certificate Authority)는 주기적으로 B에 대한 TESLA 인증서를 발급하며 B는 이를 보관하고 있다가 D라는 말단의 센서 노드로부터 서비스 요청이 들어오면 이에 대해 자신을 인증하기 위해 인증 패킷을 발급한다. 이 패킷에는 B의 인증서와 TESLA 키를 이용한 MAC 값이 포함된다. $n+d$ 주기에 CA가 TESLA 키를 공개하면 D는 이 키를 이용하여 B로부터의 인증 패킷을 검증하고 패킷 내에 포함된 B의 인증키 및 MAC을 검증한다.

이 TESLA 인증서를 사용하는 인증 프레임워크는 AP를 통해 애플리케이션으로 도착하는 데이터가 검증된 센서로부터 왔는지, 이 데이터가 변조되지 않았는지를 확인하는 것을 목적으로 한다. 이 프레임워크를 통해 제공되는 인증 서비스는 다음과 같다.

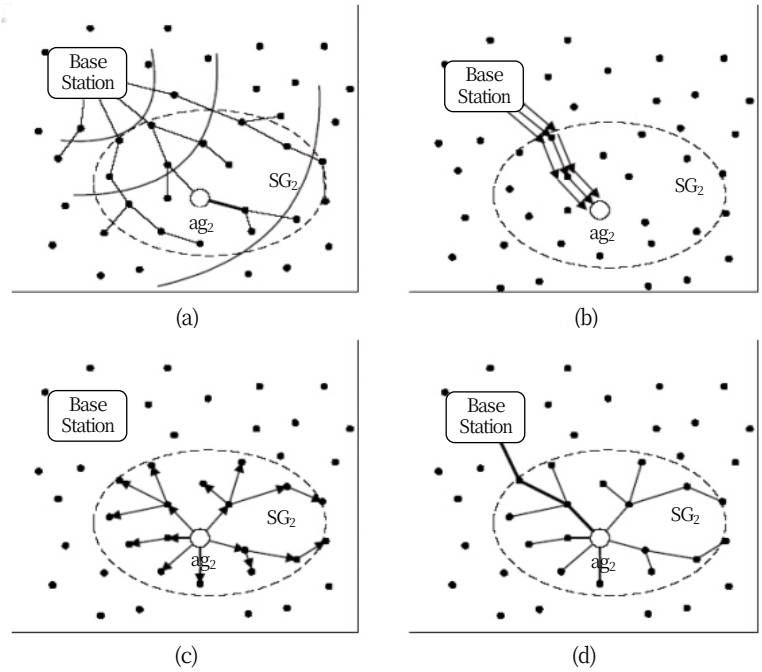
① 새로 가입하는 노드 인증: AP나 센서 노드가 네트워크에 참여하기 위해서는 TTP로부터 발행된 초기 인증서(*iCert*)를 제출한다.
② 새로 가입한 노드와 애플리케이션 간의 공유키 설립: 네트워크에 참여를 원하는 AP나 센서 노드는 애플리케이션에 TTP로부터 발급받은 *iCert*를 제출하고 유효한 것으로 판명되면 애플리케이션과 AP, 혹은 애플리케이션과 센서 노드 사이에 공유키가 설립된다.
③ 토폴로지의 변화 추적: 노드가 이동하여 기존에 설립된 공유키를 사용할 수 없는 경우를 위해 애플리케이션은 주기적으로 실시간 인증서(runtime certificate)를 발행한다.

④ 데이터의 근원지 인증 등의 서비스 제공: 각 노드와 키에 대해 인증을 수행하고 나면 데이터 근원지에 대해 인증할 수 있다.
특히 이 연구는 초기 인증서 분배 이후에도 주기적으로 실시간 인증서를 다시 분배함으로써 센서 노드의 이동 시에도 보안을 유지할 수 있다는 장점을 갖는다.

2. 키관리 기법(그룹키 기반)

베이스 스테이션과 클러스터 구조를 중심으로 중간에 aggregator를 두는 기본 구조를 기반으로 한 그룹키 관리 연구 중 Jing Deng, Richard Han, Shivakant Mishra의 연구가 있다[3]. 이 연구에서 각 센서 노드는 사전에 베이스 스테이션과의 1대1 비밀키를 갖는다는 가정 하에 단방향 해시 함수와 μTESLA를 사용하여 안전한 그룹키를 전달하기 위한 세 단계의 메커니즘을 제시하였다.

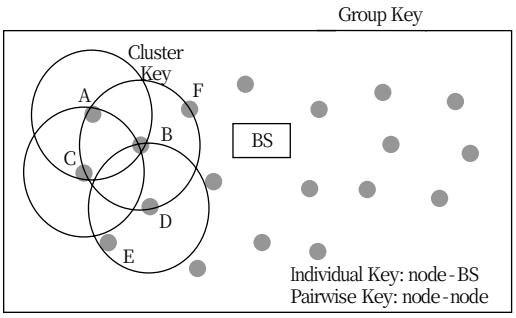
먼저 (그림 2)의 (a)그룹 선언(group announcement) 단계에서는 베이스 스테이션이 모든 센서 그룹의 정보와 각 그룹의 aggregator의 정보를 모든 센서 노드들에게 브로드캐스트한다. 두번째 단계 (b)에서 베이스 스테이션은 각 센서 그룹의 aggregator에게 해당 센서 그룹에 포함되는 모든 노드와 각 노드의 서브키를 유니캐스트로 전달한다. 이때 전송되는 서브키는 베이스 스테이션과 해당 aggregator간의 비밀키로 암호화되고 둘 간의 공유키로 생성한 MAC 값을 같이 보낸다. 마지막 단계 (c)에서 각 그룹의 aggregator는 자기가 속한 그룹의 멤버 각각에게 그룹의 ID, 서브키 정보, MAC 값을 유니캐스트로 전송한다. 이 메시지를 받으면 각 센서 노드는 자신이 속한 센서 그룹을 알게 되고 자신이 사용할 서브키를 계산할 수 있으며, 이 키를 이용하여 생성한 MAC 값을 확인함으로써 메시지가 변조되지 않았는지 인증한다. 마지막으로 받은 값에 해시 함수를 적용함으로써 정당한 aggregator로부터 온 메시지인지를 인증한다. 이와 같이 각 aggregator를 통해 베이스 스테이션으로부터 효율적으로 키를 분배할 수 있으며 베이스 스테이션과 aggregator로부터의 메시지를 각 센서 노드가 인증할 수 있을 뿐 아니라, 각 센서로부터 전달된 메시지를 상위



(그림 2) 계층적 센서 네트워크 구조

레벨에서 효과적으로 인증할 수 있는 방안을 제시하였다.

Sencun Zhu, Sanjeev Setia와 Sushil Jajodia는 일부 노드의 노출이 근접 이웃 노드까지 노출시키는 위협을 최소화하기 위한 LEAP이라는 키관리 프로토콜을 제안하였다[4]. LEAP은 각 센서 노드를 위한 네 가지 형식의 키에 대한 설정 구조와 노드 간 인증 프로토콜을 제시하였는데 구조를 그림으로 나타내면 (그림 3)과 같다.



(그림 3) LEAP 구조

■ 표기

u, v: 센서 노드

$\{f_k\}$: Pseudo Random 함수

$\{s\}_k$: 키 K로의 암호화

$MAC(k, s)$: 대칭키 K를 사용한 MAC 값

① 개인키 설정

모든 센서는 베이스 스테이션과 공유하는 개인키를 가지며 노드 u를 위한 키는 (2)와 같이 생성된다.

$$K_u^m = f_{K_s^m}(u) \quad (2)$$

② Pairwise Key 설정

노드 u,v간의 키를 설정하기 위해 우선 베이스 스테이션은 노드 u에게 초기키를 미리 할당하고 u는 이 키로부터 마스터키를 도출한 다음 hello 메시지를 브로드캐스트한다. 이웃 노드 v로부터 마스터키 K_v를 사용한 인증 코드와 ID를 포함한 응답 메시지를 받으면 v로부터의 hello 메시지를 인증하고 노드 u는 자신의 이웃 v를 찾은 pairwise key K_{uv}를 (3)과 같이 계산한다.

$$K_{uv} = f_{K_v}(u) \quad (3)$$

③ Cluster Key 설정

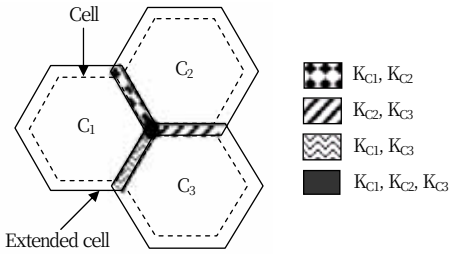
노드 u가 자신의 모든 이웃 노드와 cluster key를 설정하고자 한다면, 우선 랜덤키 K를 생성하고 생성된 키를 각각의 이웃 노드와의 pairwise key로 암호화하여 전달한다.

④ Group Key 설정

Group key는 노드가 배치되기 전에 각 노드에게 할당된다.

LEAP은 베이스 스테이션과의 인증뿐만 아니라 단방향 키 체인을 기반으로 한 노드 간 인증 프로토콜도 제공하는데 우선 모든 노드가 단방향 키체인을 생성하여 체인의 commitment 값을 각 이웃과의 pairwise key로 암호화하여 전송한 다음, 나중에 메시지를 보낼 때 다음 인증 키 값을 같이 보내면 이웃이 처음에 받은 commitment 값과 비교함으로써 인증을 수행한다. LEAP의 가장 큰 장점은 제안하는 키관리 메커니즘을 통해 in-network 프로세싱이 가능함과 동시에 이웃 노드가 보안 위협에 노출된 경우라도 노드의 보안을 유지할 수 있다는 점이다.

다음으로 Sasha Slijepcevic, Miodrag Potkonjak, Vlasios Tsiatsis, Scott Zimbeck, Mani B. Srivastava는 전송되는 데이터를 그 중요도에 따라 다양한 보안 레벨을 적용하여 이 레벨에 따라 다른 암호화 키를 사용하는 방안을 제시하였다[5]. 모든 노드는 초기의 마스터 키 집합을 가지며 각 레벨 별로 사용되는 키는 그 순간에 활성화 되어 있는 하나의 마스터 키로부터 유도된다는 가정 하에 네트워크를 통해 전달되는 데이터를 크게 이동 코드 정보, 센서 노드 위치 정보, 애플리케이션 데이터의 세 가지로 분류하였다. 가장 높은 레벨을 갖는 이동 코드(portable code)를 포함하는 데이터는 발생 빈도수는 낮지만 높은 수준의 보안을 요하므로 오버헤드가 높더라도 강도가 높은 암호화를 위해 현재의 마스터 키를 암호화 키로 사용한다. 다음의 보안 레벨은 센서 노드의 위치정보를 포함하는 데이터로 네트워크를 지역화하는 보안 메커니즘을 포함한다. 즉, 네트워크의 보안 위협을 최소화하기 위해 네트워크를 셀



(그림 4) 셀, 확장된 셀, 다중 키를 가진 영역

단위로 분할하고 각 셀 별로 지역키(location based key)를 사용한다((그림 4) 참조). 이는 암호화 키를 획득한 악의적인 노드에 의해 네트워크가 공격 당하더라도 일부 지역만 노출됨으로써 전체 네트워크의 보안을 유지할 수 있다는 장점을 갖는다.

마지막으로 가장 낮은 레벨의 보안 강도를 갖는 데이터는 애플리케이션 관련 데이터로 상대적으로 약한 암호화 기법을 사용하며 사용되는 키는 마스터 키로부터 MD5를 이용하여 유도된다. 이 메커니즘에서 각 센서 노드는 완전한 시간 동기화가 필요하고 자신의 위치를 정확히 알고 있어야 한다는 제한점을 갖는다.

3. 센서 노드간 Pairwise Key 설정 기법

먼저 L. Eschenauer, V. Gligor가 센서 네트워크에서 센서 노드간 pairwise key 설정을 위해 제안한 프로토콜을 살펴 본다[6]. 베이스 스테이션이 먼저 다량의 랜덤 키를 생성하여 이를 키 풀(pool)에 저장하고 키 풀에서 무작위로 임의의 키 집합을 선택하여 키 링을 생성하여 이를 각 센서 노드에게 분배한다. 센서 노드들은 자신이 갖고 있는 키 링의 키 정보를 이웃 노드들에게 브로드캐스팅함으로써 무선 통신 반경 내에서 자신의 이웃하는 노드들과 공유키를 찾는다. 두 링크 또는 그 이상 떨어져 있으면서 서로 공유하는 키가 없는 임의의 두 노드가 공유키를 갖기 위해서는 path key를 생성하여 공유한다. Path key를 설정하고자 하는 두 노드는 두 노드 간의 direct link path를 통해 키를 교환하여 공유키를 설정한다. 하나의 센서 노드가 자신의 키 링에서 사용하지 않은 키 중 하나를 path key로 설정한 후, 해당 노드까지 이르는 path 상에 있는 중간 노드들을 거쳐 상대 노드에게 전송한다. 이때, path 키 정보는 중간 노드들 간의 공유키로 암호화되어 전송된다. 이 스킴은 센서 노드의 개수가 매우 많더라도 수백 개 정도의 키로 기존의 pairwise key와 동일한 안전성을 제공한다는 장점을 갖는다.

D. Liu, P. Ning은 센서 노드간 pairwise key를 설정하는 방식에 있어서 기존의 랜덤 키를 이용하는 방식과 같이 키 풀을 사용하나 실제 키 값을 센서 노드들에게 할당하는 것이 아니라 키를 유도할 수 있는 다항식을 생성하여 분배하는 방식을 제안하였다[7]. 임의의 두 센서 노드가 동일한 t차 이변 다항식(bivariate polynomial)을 공유하면 두 노드는 그 다항식으로부터 서로 공통되는 키 값을 유도할 수 있다는 점을 이용한 다항식 기반의 pairwise key 설정 프로토콜로 기본 개념 및 좀더 향상된 방안들을 제시하였다.

① 기본 개념

키 셋업 서버는 소수 q에 대한 유한체 F_q 상에서 $f(x,y) = f(y,x)$의 성질을 만족하는 임의의 t차 이변 다항식을 (4)와 같이 생성한다.

$$f(x,y)=\sum_{i,j=0}^{t} a_{ij}x^i y^j \qquad (4)$$

다음으로 키 셋업 서버는 각 센서 노드 i에 대해서, x변수에 각 센서 노드의 ID를 입력값으로 하여 얻은 결과인 polynomial share인 $f(i,y)$를 해당 센서 노드에게 분배한다. 임의의 두 노드 i와 j는 각각 자신의 polynomial share의 y변수에 상대 노드의 ID를 입력함으로써 두 노드 간의 공유키를 얻을 수 있다.

② Polynomial Pool-Based Key Predistribution

안전성을 높이기 위해 하나의 polynomial 대신 다수의 랜덤 t차 이변 다항식을 생성하여 polynomial share를 분배한 다음, 임의의 두 센서 노드가 동일한 polynomial로부터 생성된 polynomial share를 갖고 있다면 기본 개념에서 설명된 방식으로 공유키를 생성하며, 동일한 polynomial을 공유하지 않는 경우 path key를 생성하여 pairwise key로 사용한다.

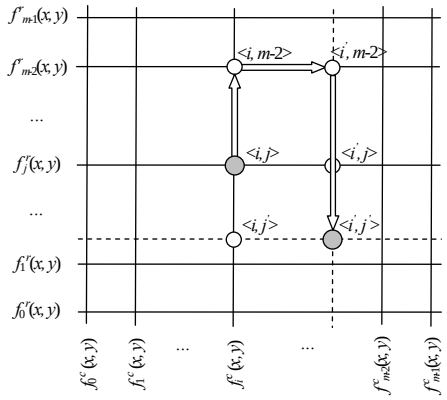
③ Grid-Based Key Predistribution

센서 노드들이 $m \times m$ grid 상의 행과 열이 교차하는 지점에 위치된다고 가정하면 보다 효율적으로 pairwise key를 생성할 수 있다. 셋업 서버는 $2m$개의 다항식을 생성하여 i 열 j 행에 있는 센서 노드에게 (그림 5)와 같이 두 개의 다항식 $f_i(x,y)$와 $f_j(x,y)$를 배분하여 동일한 행 또는 열에 위치한 노드들끼리는 바로 pairwise key를 생성할 수 있도록 한다. 동일한 행이나 열에 위치하지 않는 두 노드가 pairwise key를 설정하는 경우에도 각 센서 노드의 ID를 통해 센서 노드의 위치를 바로 파악할 수 있고, 센서 위치 정보를 이용하여 상대 센서 노드에 이르는 path를 보다 쉽게 찾을 수 있다는 장점을 갖는다.

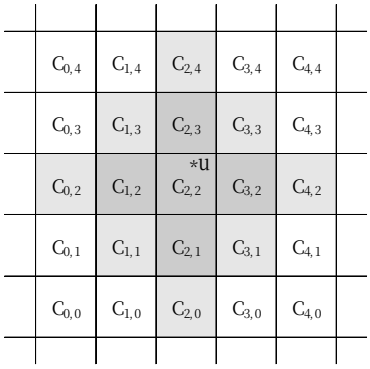
D. Liu, P. Ning이 제안한 또 다른 방식의 pairwise key 설정 프로토콜은 이들이 grid-based key predistribution에서 사용하였던 방식처럼 다항식을 분배하되 센서 필드를 셀 단위로 나누고 그 셀과 고유한 다항식을 연관시킨다[8]. 특정 셀에 위치하는 센서는 그 위치에 해당하는 다항식과 인접 4개 셀에 해당하는 4개의 다항식을 할당 받아 이웃 셀에 배치된 센서와 pairwise key를 생성하는 방식으로 이를 그림으로 표현하면 (그림 6)과 같다.

셋업 서버는 센서 u에게 좌표(2,2)를 할당하고 u가 위치한 셀과 인접한 네 개의 셀에 해당하는 polynomial share $f_{2,2}(u,y)$, $f_{2,1}(u,y)$, $f_{1,2}(u,y)$, $f_{2,3}(u,y)$, $f_{3,2}(u,y)$를 분배한다. 센서 배치 후 특정 두 센서가 pairwise key를 셋업하고자 하면, 우선 같은 공통의 다항식이 있는지 확인하여 공통의 다항식이 있으면 이전 연구에 설명되어 있는 polynomial-based key predistribution 방법으로 키를 설정한다. 이 방식은 기존의 랜덤 키 기반보다 이점이 있으나 다항식을 공유하는 센서의 수가 많아지면 다항식을 공유하는 센서의 수도 많아지므로 다항식이 노출될 수 있는 위험이 있다.

H. Chan, A. Perrig, D. Song는 센서 네트워크에서의 키 설정에 있어서 보안성을 강화하기 위한 세 가지 메커니즘을 제안하였다[9]. 첫번째는 노드사이에 q개 만큼의 키를 공유하는 q-composite 스킴,



(그림 5) Grid 기반 키 사전분배



(그림 6) 위치기반 키 사전분배

두번째는 두 노드 사이의 보안성을 높이기 위한 multipath reinforcement 스킴, 마지막으로 랜덤하게 pairwise 키를 분배하는 스킴이다.

먼저 q-composite 스킴은 키 스페이스에서 s개 만큼의 키가 선택되어 키 풀을 이루고 각각의 노드는 키 풀에서 m개 만큼의 키를 선택하여 키 링을 이룬 다음, 다른 노드와의 통신을 위한 키 설정을 위하여 이웃 노드와는 적어도 q개 이상의 키를 공유한다는 가정 하에 (5)와 같이 새로운 키 K를 형성함으로써 보안성을 강화한 방식이다.

$$K = \text{hash}(k_1||k_2||\ldots||k_q) \quad (5)$$

Multipath key reinforcement 방식은 두 노드 사이의 보안성을 강화하기 위하여 두 노드 사이의 다양한 경로를 통해 새로운 경로 키를 설정한다. 즉, 노드 A와 노드 B 사이에 j 개의 경로가 존재한다면 A가 B 에게 j 개의 값을 생성하여 다양한 경로를 통

하여 전달하고 이를 받은 B는 이 값들과 기존의 A, B 사이의 키와 함께 (6)과 같은 방법을 통하여 새로운 키 k'을 형성한다.

$$k' = k \oplus v_1 \oplus v_2 \oplus \cdots \oplus v_j \quad (6)$$

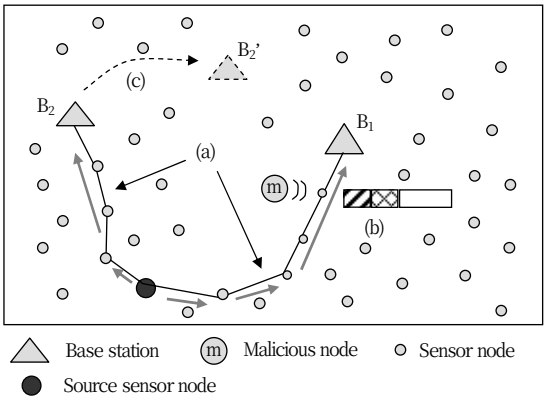
마지막으로 random pairwise 키 스킴은 기존의 pairwise 키 스킴을 수정한 방법으로 두 노드 사이의 연결 가능 확률 p에 따라 한 노드가 가질 키의 개수 m(키 링의 크기)을 $m = n \times q$로 계산한다. 그럼으로써 기존의 방식이 네트워크 크기가 증가함에 따라 노드의 키 링 크기 또한 커져야 한다는 단점을 가지는 것에 비해 좀더 향상된 방식이라 할 수 있다.

G. Jolly, Kuscu, P. Kokate가 에너지 효율을 고려하여 제안한 키 관리 방법에서 센서는 게이트웨이(aggregator)와 커맨드 노드(베이스 스테이션) 사이의 통신을 위한 두 개만의 키를 저장한다[10]. 게이트웨이는 자신을 포함한 클러스터 내의 센서들과의 통신이 가능한 키와 게이트웨이 사이의 그룹 키를 가지고 있다. 커맨드 노드는 안전하고 충분한 메모리를 가지고 있어서 게이트웨이의 수와 센서 노드 수만큼의 키를 저장하고 있다고 가정한다. 초기 단계에서 센서 노드와 게이트웨이가 배치되면 센서는 자신의 ID, 자신과 게이트웨이 간의 통신에 사용될 공유키를 포함하는 게이트웨이의 ID, 위치 등을 담은 정보를 브로드캐스트한다. 게이트웨이는 자신의 클러스터 내의 센서 정보를 게이트웨이 그룹키를 이용해 암호화하여 자신의 ID 정보와 함께 다른 게이트웨이들에게 전달한다. 다른 게이트웨이의 정보를 받은 게이트웨이는 갖고 있는 그룹키로 정보를 복호화 한 후, 자신의 키로 통신할 수 있는 센서가 있는지의 여부를 확인한다. 만약 그러한 센서가 있다면 역시 그룹키를 이용하여 자신에게 해당 센서와 통신할 수 있는 공유키가 있다는 정보를 암호화하여 자신에게 처음 정보를 보냈던 게이트웨이에게 알려 준다. 자신이 속한 센서와 통신할 수 있는 키를 받은 게이트웨이는 그 공유키를 이용하여 자신의 클러스터 내의 센서와 메시지를 주고 받는다.

이 스킴은 통신하려는 노드간의 pairwise 키를 사용하지 않고 센서는 게이트웨이, 커맨드 노드와의 통신을 위한 두 개의 키만 가지므로 기존 pairwise 스킴보다 에너지 면에서 효율적이며, 게이트웨이 노드는 게이트웨이 노드들끼리의 그룹키와 커맨드 노드와의 통신을 위한 키, 그리고 자신의 클러스터 내의 센서 노드들과의 통신을 위한 키만 저장하므로 만약 게이트웨이 노드가 노출되어도 위험성을 줄일 수 있다는 장점을 갖는다.

4. 보안을 위한 센서 네트워크 구조 연구

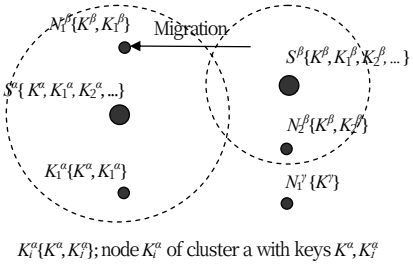
Jing Deng, Richard Han, Shivakant Mishra에 의해 제안된 보안 메커니즘에서는 베이스 스테이션을 계산 능력 및 보안 상의 제약 사항을 갖지 않는 특수한 노드로 설정하는 일반적인 보안 연구에 반하여 오히려 큰 보안상의 허점이 될 수 있는 베이스 스테이션에 대한 보안을 강화하기 위해 다중의 베이스 스테이션을 두는 네트워크 구조를 제안하였다[11]. 즉, 여러 개의 베이스 스테이션을 두어 베이스 스테이션까지의 다중의 경로를 설정하고 일부 경로에 문제가 생겼을 때 다른 경로로 우회할 수 있도록 하는 방안과 베이스 스테이션의 ID를 은폐시키는 방법, 베이스 스테이션을 재배치하는 세 가지 방법으로 구성된 보안 메커니즘이다. 다중의 베이스 스테이션을 두어 베이스 스테이션으로부터 시작되는 경로 탐색 과정을 거쳐 각 베이스 스테이션들이 네트워크의 토폴로지를 파악하고 나면 서로간에 정보를 공유함으로써 공통의 데이터 전송 테이블을 구성한다. 특히 노드가 동일한 데이터를 중복하여 다른 경로를 통해 전송할 때 기본 정책은 가능한 한 서로 멀리 떨어져 있는 경로를 사용함으로써 지역적 인접성을 이용한 외부 공격을 피해갈 수 있도록 하였다. 또한 통신중에 전달되는 패킷의 근원지와 목적지 주소를 간단한 함수를 적용하여 은폐함으로써 수동적 공격자가 근원지와 목적지를 파악할 수 없도록 하였으며, 마지막으로 가능한 한 오버헤드를 최소화 할 수 있는 방법으로 베이스 스테이션들을 재배치하고 재배치된 베이스 스테이션이 네트워크의 토폴로지를 재구성하여 전송 테이블을 갱신한다. 이를 그림으로 표현하면 (그림 7)과 같다.



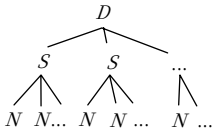
(그림 7) (a) 다중 베이스 스테이션으로의 다중 경로
(b) 헤더 주소 은폐 (c) 베이스 스테이션 재배치

Yee Wei Law, Ricardo Corin, Sandro Etalle, Pieter H. Hartel은 센서 네트워크의 특성을 고려하여 비용, 공간 및 에너지 절약, 시간 효율성 등을 고려한 분산된 네트워크 구조 및 키관리 구조를 제안하였다[12]. 네트워크를 supervised realm과 unsupervised realm으로 구분하고 supervised realm은 다시 supervisor와 supervised node로 구성하여 supervisor는 에너지, 보안, 계산 능력 및 전파 반경 면에서 좀 더 좋은 성능을 갖는다고 가정한다. Unsupervised realm은 unsupervised node로만 구성된다. 이와 같이 네트워크의 구조를 정의하고 supervised realm의 경우 supervised realm 내에서와 supervised realm 간에 노드 통신 시의 키 관리, unsupervised realm의 경우 unsupervised realm 내 키 관리, 그리고 supervised realm 내에서 unsupervised realm으로의 노드 이동 시 키 관리 기능 등을 정의하였다. 키 관리 및 도메인간 계층 구조는 (그림 8)과 같다.

Supervised realm의 경우 클러스터 α내에는 supervised node N_i^α마다 유일 키 K_i^α가 주어지고 supervisor S^α는 모든 멤버에 대한 노드 키를 가지며 S^α, N_1^α, ..., N_n^α는 동일한 클러스터 키 K^α를 갖는다. 이 클러스터 키는 supervised realm이 unsupervised realm으로 바뀔 때만 사용된다. 한 클러스터 내의 노드가 또 다른 클러스터로 이동할 때는 "이주(migration)" 프로세스가 수행된다. Unsupervised realm의 경우 모든 노드는 동일한 클러스터



(a) 키 분배



D=Domain, S=Supervisor, N=Node

(b) 3계층 구조

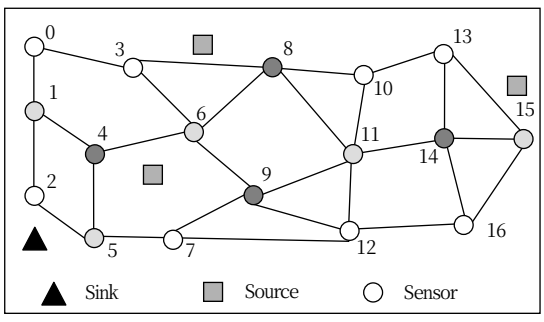
(그림 8) 키 관리 및 도메인간 계층 구조

키 K^γ를 공유한다. 이와 같이 구조를 설정하고 이를 바탕으로 supervised realm 내에서의 키 설정 과정, supervised realm 간의 노드 이동 시 세션키 설정 과정, unsupervised realm 내에서 supervised realm으로의 노드 이동 시 키 설정 과정 등을 명시하였는데 기본적으로 supervisor에게 키를 요청하되 데이터 교환 시 nonce 값을 임의로 생성하여 미리 할당 받은 키로 암호화하고 MAC을 계산하여 주고 받음으로써 인증을 수행한다. 최종적으로 CoProVe라는 공인된 보안 툴을 이용하여 보안성을 검증하였다.

Malik Tubaishat, Jian Yin, Biswajit Panja, Sanjay Madria는 센서 노드의 레벨을 기반으로 하여 계층화된 구조를 정의하고 이웃의 수(NBR)와 계층 클러스터에서의 레벨을 이용하여 에너지 효율을 높이는 동시에 최단 거리 통신을 가능하도록 하는 방안을 제시하였다[13]. 또한 안전한 센서 네트워크 라우팅 프로토콜(SRPSN)을 제안하였고, 이 구조에 적합한 그룹 키관리 스킴 또한 제시하였다. 이 연구에서 센서는 움직이지 않는 것으로 가정하며 모든 센서들이 타이머와 GPS를 갖고 있다고 가정한다. 또한 sink 노드(베이스 스테이션에 해당)는 일반 노드에 비해 저장 공간이나 계산 능력이 뛰어나며 모든 센서 노드들에 대해 각각의 대칭키를 갖고 있

다. 먼저 계층적 구조를 살펴보면, 센서 네트워크는 쿼리를 내보내거나 정보를 모으는 sink, 감지의 대상이 되는 source, 그리고 이들 간의 인터페이스 역할을 하는 센서로 구성된다. 각 센서는 배치된 후 자신의 ID와 NBR(이웃의 수)을 브로드캐스트하여 주변에서 가장 높은 NBR을 가진 센서가 클러스터헤드가 된다. 일반 센서, 클러스터헤드, 두 개 이상의 클러스터헤드를 연결하는 root 순으로 레벨 1,2,3으로 점차 높아지는데 센서 노드의 색깔이 진해질수록 레벨이 높은 센서를 의미한다((그림 9) 참조).

Sink로부터 각 센서로의 쿼리는 플러딩을 통해 전달되며 쿼리를 받은 센서는 자신이 감지한 정보를 sink에게 전달하되 가능한 한 가까운 노드 중 자신과 레벨이 다른 노드들을 먼저 고르고 이들 중 NBR이 가장 높은 노드를 선택하여 전송한다. (그림 9)에서 보면 source를 감지한 노드 15는 14로, 14는 11로 데이터를 전송한다. 이 구조를 기본으로 이들은 SRPSN(Secure Routing Protocol for Sensor Network)을 제안하였는데 이를 이용하여 모든 패킷은 중간에 악의적인 노드가 존재하여도 sink 노드까지 전달됨을 보장할 수 있다. 이와 같은 방식으로 sink 노드가 네트워크 토폴로지를 파악하고 나면 그룹키를 생성하여 각 센서 노드에게 암호화하여 전송한다. 그룹키 생성을 위해 이 연구에서는 Multi-party Diffie-Hellman 프로토콜을 응용하였는데, 각 센서 노드가 말단 노드로부터 상위 노드로 자신의 부분키를 내놓으면 부모 노드가 이를 취합하고 다시 부모 노드들이 내놓은 부분키를 그 상단에서 취합함으로써 그룹의 가장 상단의 노드가 전체 그룹키를 최종적으로 확정하여 이를 암호화한 다음 각 센서 노드에게 보내는 방법을 취한다.



(그림 9) 레벨 기반 계층적 라우팅 프로토콜

5. 기타 연구

본 고에서 소개한 연구 이외에도 다양한 센서 네트워크 관련 연구가 이루어지고 있는데 그 중 한 분야가 privacy 관련 연구이다. Privacy도 하나의 큰 연구 분야로서 특히 RFID를 중심으로 다양한 연구가 진행되고 있는데 여기서는 대표적으로 센서 네트워크 privacy에 관련된 하나의 예만을 소개한다.

M. Gruteser, G. Schelle, A. Jain, R. Han, D. Grunwald에 의해 제안된 방법은 센서 네트워크를 기반으로 한 위치 기반 서비스에서 이용자 프라이버시를 보호하기 위한 스킴이다[14]. 이 연구는 분산된 in-network 환경에서 위치 정보를 활용하되 사용자 익명성을 제공하는 방법으로 사용자의 정확한 위치 파악이 목적이 아니라 특정 위치별 인구 밀도나 이동 분포 등 통계적 자료를 얻는 데 응용될 수 있다.

센서 노드들은 건물 구조에 따라 계층적으로 분포되며 감지한 정보를 계층적으로 aggregation하여 계층별 위치 서버로 전송하는데 위치 정보를 그대로 전송하는 것이 아니라 data cloaking 알고리듬을 통해 수정된 형태로 전송한다. 정보의 익명성을 높이기 위해 데이터를 수정하는 방법은 두 가지인데 먼저, 센서가 감지한 객체의 수가 사전에 정의된 익명성 계수보다 크면 센서 노드의 ID는 사실대로 노출하고 데이터만을 cloaking하여 상위 노드에게 전송하고, 그렇지 않은 경우에는 센서 노드의 ID를 cloaking하고 데이터 값은 사실대로 노출하여 상위 노드에게 전송한다. 즉, 객체 수가 많은 경우는 이 위치에 속해 있는 개인의 ID를 노출하여도 프라이버시에 큰 해를 미치지 않으나 수가 적은 경우 개인의 ID가 노출되면 프라이버시가 침해당할 수 있는 위험성을 갖기 때문이다. ID cloaking과 데이터 cloaking은 실제 감지된 객체의 신원 또는 데이터 값을 정확하게 전송하지 않고 대략적인 값을 전송함으로써 정확한 정보가 노출되는 것을 방지하고 통계적 자료만을 제공한다.

Ⅳ. 결 론

유비쿼터스 사회로의 진입을 위해 최근 이에 대한 기반 구조로서 센서 네트워크에 대한 관심이 고조되는 가운데 센서 네트워크의 보안에 관한 연구 동향을 인증, 키관리, pairwise 키 설정, 보안을 위한 네트워크 구조 연구 등으로 나누어 살펴 보았다.

센서 네트워크는 특히 그 기본 특성과 목적이 기존의 네트워크와 여러 모로 많이 다르기 때문에 이에 대한 다양한 연구가 필요한 분야이다. 현재로서는 센서 네트워크 기반 기술에 대한 연구에 치중되어 보안에 대한 중요성이 많이 강조되지 않고 있는 게 사실이다. 그러나 점차 삶의 편리성을 추구하는 과정에서 시스템에 대한 의존도가 높아지면서 개인의 프라이버시 보호나 신뢰성 있는 서비스 제공에 대한 필요성 역시 높아지고 있으며 이를 위한 보안 관련 연구가 반드시 필요함은 분명한 사실이다. 특히 점차 시스템에 대한 보안 위협은 높아지고 그로 인한 부작용이 심각해지는 현 상황에서 보안 연구가 기반 기술 연구와 병행하여 초기부터 이루어지지 않는다면 보안상의 노출 위협으로 인해 센서 네트워크를 실제적으로 응용하는 데 많은 어려움이 따를 것으로 예상된다. 센서 네트워크 보안 연구는 그 필요성 및 중요성을 감안해 볼 때 많은 발전의 가능성을 갖고 있다.

참 고 문 헌

[1] A. Perrig, R. Szewczyk, V. Wen, D. Culler, and J.D. Tygar, “SPINS: Security Protocols for Sensor Networks,” *Proc. of the 7th ACM/IEEE International Conference on MobiCom*, 2001.

[2] Mathias Bohge and Wade Trappe, “An Authentication Framework for Hierarchical Ad Hoc Sensor Networks,” *Proc. of WiSE'03*, 2003.

[3] J. Deng, R. Han, and S. Mishra, “Security Support for In-Network Processing in Wireless Sensor Networks,” *Proc. of the 1st ACM Workshop on the Security of Ad Hoc and Sensor Networks(SASN)*, 2003.

[4] Sencun Zhu, Sanjeev Setia, and Sushil Jajodia, “LEAP: Efficient Security Mechanisms for Large-Scale Distributed Sensor Networks,” *Proc. of the 10th ACM Conference on Computer and Communication Security(CCS)*, 2003.

[5] S. Slijepcevic, M. Potkonjak, V. Tsiatsis, S. Zimbeck, and Mani B. Srivastava, “On Communication Security in Wireless Ad-Hoc Sensor Network,” *Proc. of WETICE'02*, 2002.

[6] L. Eschenauer and V. Gligor, “A Key-Management Scheme for Distributed Sensor Network,” *Proc. of the 9th ACM Conference on Computer and Communications Security*, 2002.

[7] D. Liu and P. Ning, “Establishing Pairwise Keys in Distributed Sensor Networks,” *Proc. of the 10th ACM Conference on Computer and Communication Security(CCS)*, 2003.

[8] D. Liu and P. Ning, “Location-Based Pairwise Key Establishments for Static Sensor Networks,” *Proc. of the 1st ACM Workshop on the Security of Ad Hoc and Sensor Networks(SASN)*, 2003.

[9] H. Chan, A. Perrig, and D. Song, “Random Key-Assignment for Secure Wireless Sensor Networks,” *Proc. of the 1st ACM Workshop on the Security of Ad Hoc and Sensor Networks(SASN)*, 2003.

[10] G. Jolly, Kuscu, and P. Kokate, “A Low-energy Key Management Protocol for Wireless Sensor Networks,” *Proc. of the 8th IEEE International Symposium on Computers and Communications*, June 2003.

[11] J. Deng, R. Han, and S. Mishra, “Enhancing Base Station Security in Wireless Sensor Networks,” *Technical Report CU-CS-951-03,* Department of Computer Science, University of Colorado, Apr. 2003.

[12] Yee Wei Law, Ricardo Corin, Sandro Etalle, and Pieter H. Hartel, “A Formally Verified Decentralized Key Management Architecture for Wireless Sensor Networks,” *Proc. of PWC'03*, Sep. 2003.

[13] Malik Tubaishat, Jian Yin, Biswajit Panja, and Sanjay Madria, “A Secure Hierarchical Model for Sensor Network,” *Proc. of SIGMOD*, Mar. 2004.

[14] M. Gruteser, G. Schelle, A. Jain, R. Han, and D. Grunwald, “Privacy-Aware Location Sensor Network,” *9th Workshop on Hot Topics in Operating Systems(HotOS IX)*, 2003.