주 제

무선 센서 네트워크 보안

세종대학교 권태경, 신수연, 박상호, 박태진

차례

I. 서 론

무선센서네트워크는 다수의 소형 센서노드를 무선으로 연결한 통신망을 일컬으며 최근 유비쿼터스 컴퓨팅 환경을 구축하기 위한 핵심 기술로서 많은 관심을 끌고 있다. 이것은 대상 지역에 광범위하게 설치되어 동적인 센싱 작업을 수행하며, 센싱 데이터를 바탕으로 기존의 유무선 네트워크 인프라에 연결된 응용서비스 서버와 연동하는 기능을 수행한다. 따라서 측정, 수집, 가공 등 정보에 대한 기본적인 처리 기능이 광범위하게 분산되어야 한다. 센서네트워크는 다양한 응용분야를 갖는데, 야생환경 모니터링, 산업기계 계측, 건축구조물 안전 모니터링, 군사목적 계측 등 특수 응용 분야에서부터 교통 트래픽 모니터링, 공해 모니터링, 화재 감지, 건물 시큐리티, 수질 검사, 생체 의료 모니터링 등 생활 응용 분야에 이르기까지 그 범위가 방대하며, 대부분 대상 정보에 대한 정확한 측정과 안전한 수집 및 전달을 요구한다. 따라서 센서네트워크에서 보안 기능은 반드시 필요한 요구사항이다. 대상지역에 광범위하게 설치되어 동적인 동작을 수행하는 센서네트워크의 보안 기능을 위해서는 안전한 키분배, 암호, 인증, 프라이버시 보호, DoS 공격 방어, 안전한 라우팅, 노드 포획 방어 기술 등의 개발이 필요하다. 센서네트워크를 구성하는 기본요소인 센서노드는 주로 Atmel, ARM, Motorola 등의 CPU를 바탕으로 하는 시스템과 전력장치, 통신장치를 포함한 모트(mote) 부분과 각 종 센서를 장착하는 센서보드 부분으로 구성된다. 센서노드는 그 종류가 다양하며, 특히 스마트더스트와 같은 초소형 노드도 포함한다. 따라서 전력, 계산능력, 통신능력 등 모든 면에서 기존의 계산 장치와는 확연한 차이가 있으며 상대적으로 매우 취약한 성능을 갖는다. 또한 매우

많은 수의 노드가 오류 및 장애를 허용해야하며, 자율적인 ad-hoc 구성을 통해서 연결되므로 효과적인 관리 및 보안 기능 강화가 매우 어렵다. 센서네트워크를 구성하는 센서노드는 기능이 취약할 뿐만 아니라, 물리적으로 도난이 쉬운 외부 환경에 노출되며, 특히 외부 환경과의 물리적인 접촉을 필요로 하므로 기존의 정보보호 기술을 그대로 적용할 수 없다. 이러한 문제를 해결하기 위해 많은 연구가 진행 중에 있다.

본 고에서는 무선 센서 네트워크의 전반적인 사항과 활발히 연구되고 있는 보안 이슈 및 그 핵심 기술에 해당하는 키 분배 기법들에 대해서 소개한다. II장에서는 무선 센서 네트워크의 센서 노드와 응용에 대해서 논 한 후, III장에서는 무선 센서 네트워크의 보안 서비스를 위한 6가지 주요 이슈에 대해서 논한다. IV장에서는 잘 알려진 키 분배 기법들에 대해서 소개하고 V장에서 센서 네트워크 보안에 대한 전망과 함께 결론을 맺는다.

II. 무선 센서 네트워크 소개

무선 센서 네트워크는 유비쿼터스 환경의 중요한 기술이다. 이번 장에서는 센서 네트워크를 구성하는 센서노드들을 소개하고, 센서 네트워크의 응용분야들에 대해서 살펴본다.

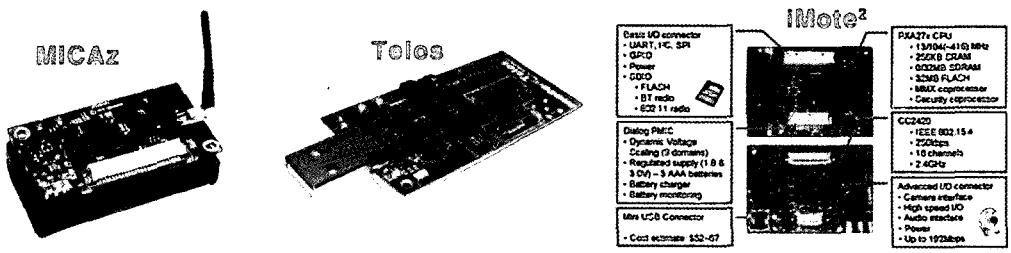
1. 센서 노드 개요

현재 학계에서 주로 연구 목적으로 가장 많이 사용되는 센서 노드는 U.C.Berkeley에서 개발하여 Crossbow사에서 상용화한 8비트 CPU 기반의 MICA 모트 시리즈이다. 현재 Zigbee 표준인 IEEE 802.15.4 라디오 통신을 지원하는 MICAz[17]까지 개발된 MICA시리즈는 센서 네트워크를 대표하는 센서노드이다. 또한 Moteiv사의 Telos[18]는 16비트 CPU를 채택하여 MICAz를 능가하는 계산 능력과 함께 USB 단자를 부착한 모트로 활용되고 있다.

한편 현재 연구 개발 진행중인 Intel iMote2[19]는 앞으로 구성될 센서네트워크의 패러다임을 완전히 바꾸고 발전된 센서네트워크의 모델을 완성시켜 줄 것이라 기대를 모으고있다.

인텔의 강력한 반도체 기술이 집적된 임베디드 칩인 PXA271은 13~104MHz(최대416MHz)의 속도와 256K SRAM 0~32MB의 SDRAM 그리고 32MB의 FLASH 메모리를 갖춤으로써 현재까지 나온 모트와는 비교도 할 수 없을 정도의 강력한 기능을 제공할 수 있을 것으로 기대되고 있다.

이 뿐만 아니라 다양한 외부 기기와의 연결을 이용해 현재 컴퓨터가 수행해주고 있는 강력한 기능까지도 하나의 센서노드가 제공해 줄 수 있을 것으로 기대를 모으고 있다.



(그림 1) 다양한 센서 노드들 [17], [18], [19]

(그림 2) 센서 네트워크의 다양한 응용들 [3]

2. 센서 네트워크 응용

센서 노드는 제한된 계산 능력과 통신 능력에도 불구하고 해당 지역의 온도, 습도, 빛 등의 환경을 센싱을 할 수 있다. 또한 원하는 프로그램을 센서 노드에 올림으로써 여러 센서노드들과 스스로 센서 네트워크를 구성할 수 있다. 이러한 특성들로 인해서 센서노드들은 현재 다양한 산업 · 연구분야에서 사용되고 있다.

대표적인 응용으로 2001년부터 진행되고 있는 삼나무 프로젝트가 있다. 미국 캘리포니아 지방에 있는 숲에 MICA 모트를 살포하여 숲의 생태를 모니터링하여 숲이 어떠한 변화가 있는지를 연구하는 해당 프로젝트에 센서 네트워크의 응용이 중요한 기술로 사용되고 있다. 또한 건축 분야에서도 센서 네트워크가 중요한 기술로서 사용되고 있다. 캘리포니아의 금문교의 교량 곳곳에 센서노드를 설치하여 바람의 세기에 대한 금문교의 반응과 진동을 모니터링하고 있다. 이 센서노드가 센싱하는 정보를 사용하여 바람에 대한 금문교의 반응과 안전성 등을 측정할 수 있다. 뿐만 아니라 산업분야에서도 이러한 센서 네트워크가 중요한 역할을 차지한다. 인텔의 반도체 칩 생산 라인에서도 이러한 센서노드가 사용된다. 각각의 베어링에 부착된 센서노드들은 베어링의 상태를 체크하여 베어링의 상태 정보를 전송해 주게 되는데 상태가 좋지 않은 베어링을 즉시 교체해 줌으로써 생산라인이 멈추는 것을 막는다. 생산라인의 중지로 인한 회사의 손실보다 센서 네트워크를 이용한 관리에 드는 비용이 훨씬 저렴하므로 이 방법이 다른 산업라인에도 긍정적인 영향을 끼칠 것으로 보인다. 이 밖에도 사람이 접근할 수 없는 위험 지역에 대한 연구와 탐사, 군사작전 등에도 중요한 응용 기술로 사용될 것이라 전망된다.

III. 무선 센서 네트워크의 보안 이슈

센서 네트워크는 무선 통신 사용, 자원의 제약성 등 네트워크 자체의 특성으로 인해 일반 네트워크에 비해 보안이 매우 취약하다. 우선, 센서네트워크를 구성하는 센서노드는 매우 제한된 통신, 계산 능력과 작은 메모리 공간을 가지므로 RSA 나 Diffie-Hellman key agreement 등 기존의 공개키 암호 기술을 그대로 적용하는 것은 불가능하다. 또한, 물리적으로 안전하지 않은 환경에 배치되고 매우 많은 수의 노드가 오류 및 장애를 허용해야하며, 자율적인 ad-hoc 구성을 통해서 연결되므로 효과적인 관리 및 보안 기능 강화가 매우 어렵다. 안전한 무선 센서 네트워크를 구축하기위해서는 다음 6가지의 보안 기술 개발이 필요하다[13].

1. 안전한 키 분배 및 확립

무선 센서 네트워크에서 정보보호 서비스를 구축할 때 우선적으로 해야 할 사항 중에 하나는 센서 네트워크 운영 시 사용될 암호 키를 설정하는 것이다. 지난 수십 년 동안 다양하고 효율적인 키 관리 프로토콜이 제안되었지만 기존의 프로토콜을 센서 네트워크에 적용하는 것은 한계가 있다. 이들의 대부분은 공개키 암호 방식을 사용함으로 연산량이 많아 배터리 소모가 많고, 메모리가 적은 센서 노드에 적용하기에는 적합하지 않기 때문이다. 더구나 수백, 수천 개의 노드로 구성되는 센서 네트워크에서의 키 관리 프로토콜은 확장성이 있어야 한다. 이에 대한 해결책은 대칭키 암호 방식을 사용하는 것이다. 대칭키 암호 방식을 사용한 가장 기본적인 프로토콜은 센서 네트워크를 구성하고 있는 모든 센서 노드가 단일 암호 키를 사용하는 것이다. 그러나 하나의 노드로부터 암호 키가 노출 되는 것은 네트워크 전체의 정보를 노출시키는 문제가 있다. 변형된 방법으로 하나의 암호 키를 이용하여 링크 계층의 단대단 암호화 세션 키를 설정하는데 사용하고 세션 키가 설정된 후 암호 키를 삭제하는 것이다. 그러나 이 방법 또한 초기 구축 후 그룹 멤버의 변경이 있을 경우 네트워크에 새로운 멤버를 추가하는 것은 불가능 하다. 발전된 방향으로 각각의 두 센서 노드 간에 유일한 암호 대칭키를 미리 설정하는 방법이 있다. 하지만 각각의 노드가 개의 키를 메모리에 저장하고 있어야 하므로 자원제약이 많은 센서 노드에겐 적합하지 않고 전체적으로 개의 키가 필요하므로 확장성이 떨어진다. 이러한 문제를 해결하기 위해 랜덤 키 사전 분배(RKP: Random Key Predistribution) 스킴과 위치 기반 스킴 등 다양한 키 설정 방식이 제안되었으며 다음 장에서 대표적인 RKP 스킴들과 위치나 배치 정보를 이용하는 스킴들에 대해 설명하고자 한다.

2. 암호와 인증

기존의 네트워크와 마찬가지로 대부분의 센서 네트워크 어플리케이션은 전송되는 정보의 도청이나 수정, 잘못된 정보의 삽입 등 다양한 공격으로부터 방어할 필요가 있다. 이를 위한 가장 기본적인 방법은 암호화이다. 센서 네트워크에서 기본적으로 고려해야 할 사항은 제한된 센서 노드를 최대한 효율적으로 사용하는 것이다. 따라서 센서 네트워크의 비밀성과 인증을 보장하기 위해서 적용하고자 하는 기술도 계산 능력과, 메모리, 통신, 에너지등이 제한된 센서 노드의 특성을 고려하여 적용시켜야 한다. 초기 센서 네트워크에서는 암호화 기술을 하드웨어적으로 지원할 수 있게 해 주었다. 링크 계층(Link Layer)에서 지원되던 하드웨어적인 암호화 기술은 암호화의 편의성은 제공해 주었지만, 그만큼의 효율성을 제공해주지는 못했다. 센서 네트워크에서 대부분의 에너지 소비는 통신 패킷의 송수신시에 일어난다. 하지만 하드웨어적인 암호 구현은 계산 비용만 줄여주기 때문에 그만큼의 효율성을 발휘하지는 못한다. 현재 센서 네트워크에서는 비밀성을 보장히기 위한 대칭키 암호 시스템과 해쉬 함수등의 소프트웨어적인 구현이 활발하게 이루어지고 있다. 대표적인 예로, 센서 네트워크의 대표적인 운영체제인 TinyOS를 만든 U.C.Berkeley에서는 TinySec이라는 암호화 응용 컴포넌트를 제공한다.

3. 프라이버시 보호

유비쿼터스 시대가 되면 센서 네트워크가 우리 일상의 중심이 될 것이다. 더불어 프라이버시에 대한 문제가 크게 대두될 것이다. 센서 노드들은 사람이 있는 어느곳에나 배치될 것이다. 이는 인간의 생활을 더 윤택하고 편리하게 바꿔줄 것이다. 하지만 드러나지 않

는 공격자에 의해서 개인의 정보가 쉽게 노출될 수 있다. 예를 들어, 옷 가게를 운영하는 주인은 센서 노드를 조작하여 고객의 정보를 쉽게 유출할 수 있다. 또한 마음만 먹으면 이웃집을 감시할 수 있고 법을 집행하는 기관에서는 용의자에 대한 감시를 하게 됨으로써 개인의 프라이버시를 침해할 수 있다. 기술의 발전으로 인해 센서노드는 작아지고 값은 더 저렴해질 것이다. 이로인해 센서노드들은 숨기기 쉬워지고 더 광대한 지역을 감시할 수 있게 될 것이다. 더 나은 서비스를 제공받기 위해서는 개인의 정보를 정확하게 더 많이 노출할 필요가 있다. 이로인해 지금까지 대처해 왔던 방식과는 다른 방식이 필요하다. 이는 단순히 기술적으로 해결될 수 있는 문제가 아니다. 프라이버시 보호를 위한 기술 발전이 필요할 뿐만 아니라 사회적인 규범과 법규가 제정되고 잘 지켜져야 할 것이다. 이미 유비쿼터스의 또다른 핵심 기술인 RFID 프라이버시를 위한 5가지 규정이 만들어진 상태이며, 센서 네트워크도 이와 유사한 규정이 제정될 필요가 있다. 센서 네트워크의 프라이버시 보호는 현재 미비한 상태이며 앞으로 더 연구해야 할 필요가 있는 분야로 남아있다.

4. DoS 공격 방어

공격자는 DoS (Denial-of-Service) 공격을 통해 무선 센서 네트워크의 성능을 저하시킨다. 가장 단순한 DoS 공격의 형태는 공격자가 높은 에너지 신호를 브로드캐스팅하여 네트워크의 동작과 기능을 혼란시키거나 마비시키는 것이다. 공격자가 802.11 매체 접근 제어 (MAC: Medium Access Control) 프로토콜을 방해하여 통신을 못하게 하는 더 강력한 공격도 가능하다. 이러한 공격을 방어하는 표준 중 하나는 스펙트럼 확산 통신(spread-spectrum communication)이다. 하지만, 이는 암호학적으로 안전하기는 하나 상용가능한 것은 아니며, 공격자가 노드를 직접 포획하여 암호학적인 키를 얻어낼 경우에는 안전하지 않다. 스펙트럼 확산 통신 이외에 센서 네트워크의 속성으로 인해 새로운 방어가 가능하다. 전파 방해가 단지 네트워크의 어떤 한 부분에만 영향을 미칠 경우, 전파 방해에 저항력있는 네트워크는 전파 방해와 영향받은 지역을 탐지하여 그 지역 주변을 라우팅함으로써 방어가 가능하다.

5. 안전한 라우팅

센서 네트워크에서 통신을 가능하기 위해서는 라우팅과 데이터 포워딩은 필수적인 서비스이다. 하지만, 현재 라우팅 프로토콜들은 많은 보안 취약성을 가진다[10]. 라우팅 프로토콜의 보안 취약성으로 인한 두 가지의 가능한 위협[8]은 외부 공격과 내부 손상 노드로 인한 위협이다. 외부 공격은 공격자가 잘못된 라우팅 정보를 삽입하거나 예전 라우팅 정보를 사용하는 것이다. 이러한 방법으로 공격자는 네트워크를 분리하거나 네트워크에 과도한 트래픽을 주는 등의 영향을 줄 수 있다. 내부 손상된 노드를 통한 위협은 공격자가 손상 시킨 노드를 이용하여 다른 노드에게 악의적인 라우팅 정보를 보내는 것이다. 외부 공격은 암호화나 단순한 인증 같은 암호학적 스킴으로 방어할 수 있지만, 내부 손상된 노드를 사용한 악의적인 라우팅 정보는 손상된 노드 또한 유요한 서명을 생성할 수 있으므로 탐지하기 힘들다. 따라서, 이러한 공격에 강력한 안전한 라우팅 프로토콜을 고안할 필요가 있다.

6. 노드 포획 방어 기술

센서 네트워크가 직면한 가장 도전적인 이슈는 어떻게 노드 포획 공격에 대한 회복력을 제공할 것인가

이다. 센서 네트워크의 대부분의 응용에서 센서 노드는 공격자가 쉽게 접근 할 수 있는 위치에 놓이게 된다. 이러한 노출은 공격자가 센서 노드를 포획하여 암호학적인 비밀을 얻어내고 프로그래밍을 수정 하거나 공격자의 통제 이래 악의적인 노드로 바꿀 가능성을 증가시킨다. 노드 포획에 회복력을 가지는 네트워크를 위해 네트워크 상태의 사본을 만들고, 네트워크의 잘못된 경우를 탐지하기 위해 다수 투표와 다른 기술들을 사용할 필요가 있다. 예를 들어, 모든 패킷을 여러 개의 독립적인 경로를 통해 보내고, 패킷을 받은 노드가 일관성을 검사하여 노드 포획에 대한 회복력을 어느 정도 얻을 수 있는 라우팅 프로토콜이 디자인되고 있다. 회복력을 얻기 위한 또 다른 방법으로는 환경에 대한 다중의 중복되는 정보를 얻는 것이다. 예를 들어, 네트워크는 이벤트에 반응하기 전에 여러 개의 이벤트 보고를 요구하여, 많은 데이터 값 중 비 정상적인 데이터는 버려버리는 것이다. 중복에 기초한 방어는 센서 네트워크에 적합하지만, 그럼에도 불구하고 노드 포획은 센서 네트워크 보안에 있어서 가장 성가신 문제이다.

IV. 무선 센서 네트워크를 위한 키 분배

센서 네트워크에 적합한 단순한 대칭키 암호 기술을 사용하는 경우의 문제를 해결하기 위해 랜덤 키 사전 분배 (RKP: Random Key Pre-distribution)스킴들이 제안되었다. 이 스킴들은 큰 키 풀(key pool)로부터 키의 부분 집합을 선택하고 각각의 노드의 메모리에 저장한다. 배치 된 후에, 센서 노드는 미리 저장된 키를 사용하여 키를 설정 할 수 있다. RKP 스킴들은 네트워크 크기에 상관없이 통신 오버헤드가 일정하다는 장점을 가지지만, 메모리 오버헤드가 증가하고, 랜덤 그래프 모델에만 적용할 수 있는 한계를 가진다. 또한, RKP 스킴들은 한정된 키를 배치 전에 센서 노드에 저장하므로 배치 후에는 모든 이웃 노드들과 공유 키를 갖는 것이 불가능하다. 이러한 스킴들의 안전성은 손상된 노드를 통해 손상될 수 있는 링크의 수 분석을 통해 이루어져왔다. RKP의 이러한 문제들을 해결 하기 위해, 위치 정보를 이용한 스킴들이 제안되고 있다.

1. 랜덤 키 사전 분배 (RKP : Random Key Pre-distribution) 스킴

Eschenauer와 Gligor[7]는 각각의 센서 노드가 큰 키 풀로부터 랜덤하게 m 개의 키를 선택하는 랜덤 키 사전-분배 스킴을 제안하였다. 두 이웃 노드가 적어도 하나의 공통 키를 공유하고 있을 경우에만 안전한 통신 확립이 가능하다. Chan et al.[2]는 Eschenauer과 Gligor의 기본 스킴[7]을 안전한 연결 확립을 위해선 적어도 q ($q > 1$)개의 키를 공유해야만 하는 q -합성수 스킴으로 확장하였다. 이 스킴을 공격하기 위해 공격자는 더 많은 링크를 손상시켜야 한다. 하지만, 희망하는 연결성을 얻기 위해서 더 많은 수의 키를 저장할 필요가 있다는 단점이 있다. Du et al.[5]은 기본 스킴과 Blom의 키 관리 스킴[1]을 조합하여 pairwise 키 스킴을 제안했다. Du의 pairwise 키 스킴에서 각각의 센서 노드들은 ϖ 개의 비밀 행렬로부터 랜덤하게 τ 열을 선택한다. 같은 비밀 행렬로부터 열을 선택했을 경우, 두 이웃 노드는 서로 안전하게 통신 할 수 있다. 또한, Blom 스킴의 λ -안전 속성으로 인해 임계치 보다 적은 노드가 손상되었을 때, 추가적인 링크가 손상되지 않는다.

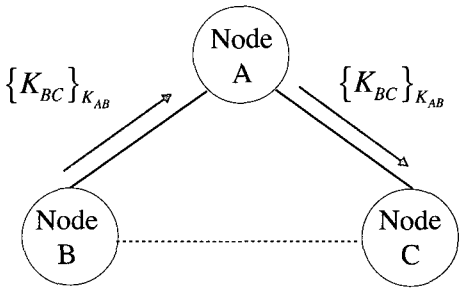
1.1 Eschenauer와 Gligor의 랜덤 키 사전분배

센서네트워크에 공개키 암호 방식을 적용했을 때

의 문제점과 단일키를 사용했을 때의 문제점을 해결한 연구들로는 Laurent Eschenauer와 Virgil D. Gligor가 제안한 랜덤-키 사전 분배[7]가 있다. 랜덤-키 사전분배기법은 모든 가능한 키들의 공간에서 매우 큰 대칭키 풀을 랜덤하게 선택하고 여기서 일정한 개수의 키를 랜덤하게 선택하여 각 센서 노드의 키 링에 저장한다. 대칭키 풀에 있는 모든 키는 유일한 ID를 가지며 키와 함께 키에 대한 ID도 노드의 키 링에 저장된다. 센서 노드들이 배치된 후 키 설정 과정이 수행된다.

각각의 센서 노드는 자신의 키 링에 있는 키의 ID를 브로드캐스트 한다. 인접한 노드는 브로드캐스트된 ID와 자신의 키 링의 ID와 비교하여 상대방과 같은 공통키를 소유하고 있는지 판단한다. 만약 동일한 키가 자신의 키 링에 있다면 Challenge Response 프로토콜을 통해 세션 키를 설정한다. 만약 키 링에 공통키가 없다면 세션 키를 설정한 인접 노드를 통하여 경로키를 설정한다.

(그림 3)은 경로키 설정하는 과정을 보여준다. 만약, 공격당한 노드가 있을 경우 그 노드의 키링은 취소 및 제거되어야만 한다. 컨트롤러인 키 설정 서버는 전자서명키를 생성하여 각 노드에게 유니캐스트를 하면 각 이웃노드들은 전자서명키를 획득한 후, 리스트 속에 있는 키들의 ID를 찾아서 자신들의 키 링에 있는 키들중 일치하는 것을 제거한다. 이로서 공격당한 노드들과의 연결은 없어지며, 이 키를 세션키로 가지고 있는 각 노드들은 자신의 키 링에서 관련 세션키를 제거함으로써 이웃노드들에게 크게 영향을 미치지 않는다. 또한, 보통 키 수명이 노드 수명보다 길지만, 만일 키 수명이 먼저 끝나는 경우가 있을 수 있다. 이러한 경우 키 재분배가 필요하다. 이것은 키를 제거한 뒤에 공유키를 발견하고 경로키 설치를 재시작 해야하므로 각 노드에서 키가 스스로 폐기 되는것과 동일하다.



(그림 3) 경로키 설정 과정

1.2 Chan의 랜덤 Pair-wise 키 사전분배

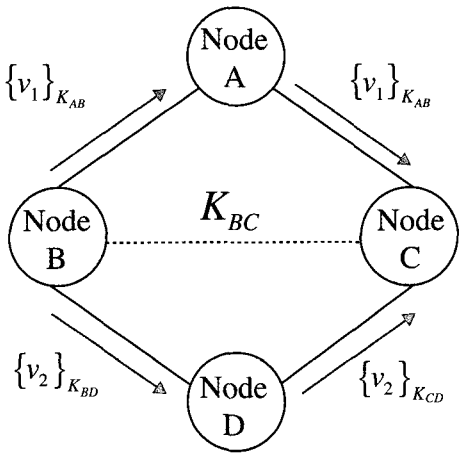
Chan et al.은 랜덤 키 사전분배의 두 노드가 공통키로 사용하려는 키를 인접한 다른 노드가 가지고 있을 가능성이 있으므로 이 키를 이용하여 두 노드 사이의 트래픽을 도청할 수 있는 결점을 보안하기 위해 q -합성수 랜덤 키 사전분배 스킴과 다중 경로 키 강화 스킴을 제안하였다. 더 나아가 노드 간 상호인증을 제공하고 안전성도 강화시킨 랜덤 Pair-wise 키 사전분배 스킴을 제안하였다[2].

가. q -합성수 랜덤 키 사전분배 스킴

q -합성수 랜덤 키 사전분배 스킴은 [7]의 랜덤 키 사전분배 프로토콜의 결점을 보안하기 위해 제안된 스킴으로 공통키를 하나 이상인 개를 사용한다는 점 외에는 랜덤 키 사전분배 프로토콜과 동일하다. 노드는 인접한 노드의 브로드캐스트를 통해 q 개의 공통키를 찾은 다음 그 q 개의 키를 이용하여 새로운 세션 키 $K = hash(k_1 \| k_2 \| \| \mathrm{L} \| k_q)$를 생성한다. 만약 인접한 노드와 공통으로 가진 키의 갯수가 q 개 미만인 경우에는 통신을 할 수 없다.

나. 다중 경로 키 강화 스킴

다중 경로 키 강화 스킴 또한 랜덤 키 사전분배 프로토콜의 결점을 보안하기 위해 제안되었다. 노드는 기본적인 세션 키 설정 후 독립적인 경로를 통하여 세



(그림 4) 다중 경로 키 강화

션 키를 강화한다. 예를 들어, (그림 4)에서 노드 B와 노드 C는 세션 키 K_{BC}를 강화하기 위하여 독립적인 두 경로, 노드 A를 통한 경로와 노드 D를 통한 경로를 이용한다. 노드 B는 키와 같은 길이를 갖는 v_1과 v_2를 랜덤하게 선택한 다음 독립적인 두 경로를 통해 노드 C에게 보낸다. 노드 C는 두 랜덤한 값을 받은 후 새로운 세션 키 $k' = k \oplus v_1 \oplus v_2 \oplus \mathrm{L} \oplus v_j$ (j: 독립적인 경로의 수)가 생성된다.

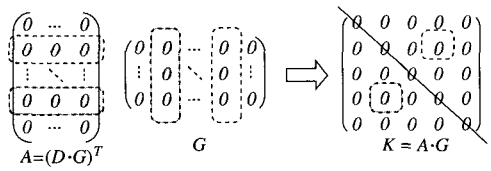
다. 랜덤 Pair-wise 키 사전분배 스킴

노드 간 상호 인증, 노드 캡쳐에 대한 완벽한 회복력을 가지고, 베이스 스테이션 없이도 손상된 노드를 감지하여 취소할 수 있는 기능 등 센서네트워크에서 중요한 정보보호 서비스를 제공한다. 배치 전, 센서 네트워크를 구성하는 센서 노드의 수가 이라고 할 때, 개의 유일한 노드 ID를 생성한다. 각각의 노드는 랜덤하게 선택한 개의 노드 ID를 갖는다. 생성된 각각의 노드 쌍에 대해서 Pair-wise 키를 생성하고 각각의 노드 키 링에 저장한다. 배치 후, 우선 각각의 노드가 자신의 ID를 인접한 노드들에게 브로드캐스트 하고, 이 브로드캐스트를 통해 인접한 노드들은 자신의 키 링과 비교하여 같은 ID를 찾아낸다. 같은 ID를 가진 경우에는 cryptographic handshake를 통해 공통의 Pair-wise 키를 가지게 된다. 일치하는 ID가 없을 경우에는 링크를 생성하지 못한다. 또한, 랜덤 Pair-wise 키 사전분배는 노드 취소를 제공하고 취소 공격과 노드 복제와 생성 공격에 대해서도 회복력을 가진다.

1.3 Du의 멀티 스페이스 키 사전분배

W. Du, J. Deng, Y. S. Han과 P. K. Varshney은 Blom 스킴[1]을 기반으로하여 기존의 스킴들에 비해 부분적으로 노드가 캡쳐 당했을 경우의 네트워크 회복력을 향상시킨 새로운 키 사전분배 스킴을 제안하였다[5].

가. Blom 스킴



(그림 5) Blom 스킴의 행렬

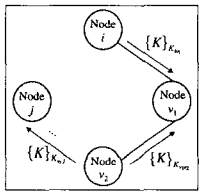
Blom은 네트워크상의 어떤 노드 쌍이 pairwise 비밀키를 찾을 수 있게 하는 키 사전분배 방법을 제안하였다[1]. 베이스 스테이션은 유한체 $GF(q)$를 통하여 $(\lambda+1)\times N$ 인 행렬 G와 랜덤한 $(\lambda+1)\times(\lambda+1)$의 대칭 행렬 D를 생성한다. 여기서, N은 네트워크 크기이고, G는 공개된 정보, D는 비밀 정보이다. 그 다음, 베이스 스테이션은 $N\times(\lambda+1)$인 행렬 $A=(D\cdot G)^T$ ($(D\cdot G)^T$: $(D\cdot G)$의 전치 행렬, A : 대칭 행렬)를 계산한다. D가 대칭 행렬이므로 다음의 식이 성립한다.

$$A \cdot G = (D \cdot G)^T \cdot G = G^T \cdot D^T \cdot G = G^T \cdot D \cdot G = (A \cdot G)^T \quad (1)$$

식 (1)을 통해, 만약 $K=A \cdot G$ 라면 K의 j행 i열인 $K_{ij} = K_{ji}$ 라는 것을 알 수 있다. 이 값 K_{ij}, K_{ji}을 노드 i와 j의 pairwise 키로 사용하고, 각각의 노드는 식 (1)에 따라서 상대적으로 K_{ij}와 K_{ji}를 계산 할 수 있다. 베이스 스테이션은 노드 k(k=1, 2, L, N)에게 행렬 A의 k번째 열과 행렬 G의 k번째 행을 저장한다. 노드들이 배치된 후, 만약 노드 i와 노드 j가 서로 pairwise 키를 찾고자 할 경우, 두 노드는 서로 G의 행을 교환하고 A의 비밀 열을 이용하여 K_{ij}와 K_{ji}를 계산한다. (그림 5)는 Blom 스킴의 행렬을 보여준다.

나. Multiple-스페이스 키 사전 분배 스킴

$$G = \begin{bmatrix} 1 & 1 & \cdots & \\ s & s^2 & \cdots & s^N \\ & & \vdots & \\ s^\lambda & (s^2)^\lambda & \cdots & (s^N)^\lambda \end{bmatrix}$$



(그림 6) (a) G 행렬의 예 [5] (b) 경로를 통한 키 동의 과정

Blom 스킴은 센서 네트워크에서 개발된 것이 아니고 하나의 키 스페이스를 사용한다. W. Du, J. Deng, Y. S. Han과 P. K. Varshney는 Blom 스킴을 센서 네트워크에 맞게 수정하고 다중 키 스페이스를 사용하여 노드 캡쳐에 대해 네트워크 회복력을 향상시켰다. Blom 스킴과 같이 공개되는 행렬 G와 ω개의 비밀 행렬 D를 생성하고, 노드 j에게 $G(j)$를 제공한다. $G(j)$의 λ+1개의 요소를 모두 저장하는

것이 아니라 행의 두 번째 요소를 씨드로써 저장한다. (그림 6 (a))는 G 행렬의 예를 보여준다. 각각의 튜플 $S_i = D_i \cdot G, (i=1,2,L,\omega)$를 키 스페이스라고 하고, 행렬 $A=(D \cdot G)^T$ 를 계산한다. 다음, 각각의 노드를 위해 ω개의 키 스페이스 중에서 τ개의 키 스페이스를 선택한다. 노드 j 에 의해 선택된 스페이스 S_i에서 A_i의 j 번째 열만 저장한다. 이 정보는 비밀 정보이고 노드 내에 안전하게 저장된다. 배치 후, 각각의 노드는 자신의 노드 ID, 어떤 스페이스를 선택했는지에 대한 정보와 행렬 G의 Seed가 포함된 메시지를 브로드캐스트한다. 만약 인접한 이웃 노드와 동일한 스페이스를 가졌다면 Blom 스킴을 사용하여 비밀 pairwise 키를 식 (2)와 같이 계산한다. 만약, 인접한 이웃 노드와 동일한 스페이스를 가지고 있지 않다면, 키 동의 과정을 통해 pairwise 키를 가진 다른 노드들을 통해서 랜덤 키를 공유한다. 즉, (그림 6 (b))와 같이 i 부터 j 까지의 경로를 통하여 키를 공유한다.

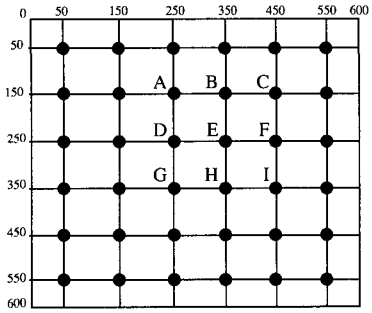
$$K_{ij} = K_{ji} = A_c(i) \cdot G(j) = A_c(j) \cdot G(i) \quad (2)$$

2. 위치 기반 키 사전 분배 스킴

Du et al.[6]는 센서 배치 정보를 이용한 키 사전 분배 스킴을 제안하였다. 이 스킴은 배치 정보를 이용하여 더 작은 메모리 공간으로도 더 높은 연결성을 얻을 수 있다. Huang et al.[9] 또한 배치 정보를 고려하고 Blom의 스킴[1]과 랜덤 키 사전 분배를 조합하여 위치-인지 키 관리 스킴을 제안하였다.

2.1 Du의 배치 정보를 이용한 키 사전 분배 스킴

W. Du et al.은 배치 정보를 이용한 새로운 랜덤 키 사전 분배 스킴을 제안하였다[6]. 이 스킴에서 센서 노드는 궁극적으로 $t \times n$ 그룹 $G_{i,j}$ 로 나뉜다 (i=1,L, t, j=1,L, n). 사이즈가 |S| 인 전체 키 풀 S와 배치 되는 곳의 포인트는 (그림 7)의 그리드와 같이 배열된다고 가정한다. 각각의 노드는 m 개의 키를 가진다. 키 사전 분배 스킴의 목적은 배치 후 센서 노드가 자신의 이웃 노드와의 공통된 비밀 키를 찾는 것이다. Du의 키 사전 분배 스킴은 키 사전 분배, 공유 키 발견, 경로 키 확립, 세 부분으로 나뉜다.



(그림 7) 노드 배치 포인트(각각의 점은 배치 포인트를 나타냄) [6]

가. 키 사전 분배

a. 키 풀 S 를 배치 그룹 $G_{i,j}$ 와 일치하는 $t \times n$ 키 풀 $S_{i,j}$로 나눈다.

b. 키 풀 설정 후, 배치 그룹 $G_{i,j}$ 의 각각의 노드에게 배치 그룹과 일치하는 키 풀 $S_{i,j}$ 로부터 랜덤하게 m 개의 키를 할당한다.

나. 공유 키 발견

배치 후, 센서 노드는 이웃 노드들과 공유한 키를 발견하기를 시도한다.

a. 각각의 노드는 자신이 가진 키의 인덱스를 포함하고 있는 메시지를 브로드캐스트한다. 만약 이웃 노드가 자신이 가진 키와 브로드캐스트한 노드가 가진 키 중 일치하는 것이 있다면 그 키를 두 노드의 안전한 통신 채널을 위해 사용한다.

b. 공유 키를 발견 후, 전체 센서 네트워크는 키 공유 그래프 G를 형성한다.

다. 경로 키 확립

공유 키 발견 과정에서 공유 키를 설정하지 못한 경우에는 키 공유 그래프 G에서 이미 확립된 경로를 이용한다. 공유 키를 발견하지 못한 두 노드는 G에서 서로에게 가는 경로를 찾고, 두 노드 중 한 노드가 랜덤 키 K를 생성하여 링크 별로 이미 확립된 키를 이용하여 암호화하여 보낸다. 나머지 한 노드에게 이 랜덤 키가 도착하면 이 키가 pairwise 키가 된다.

2.2 Huang의 위치 인식 키 관리 스킴

D. Huang et al.은 배치 정보를 이용하는 그리드 그룹 스킴을 제안하였다[9]. Du et al.[6]이 배치 정보를 이용한 pairwise 키 스킴과는 달리 센서를 넓은 지역에 균등하게 배치시킨다. 각각의 센서에게 큰 키 풀로부터 키를 랜덤하게 할당하는 대신, 구조화된 키 풀로부터 비밀키를 계획적으로 할당한다.

가. 그리드 그룹 배치 스킴

배치될 곳은 2차원 사각형의 지역이라고 가정하고, 사각형의 지역은 각각 $a \times a$ 크기의 $(i \cdot j)$ 배치 지역으로 나뉜다. 각각의 작은 배치 지역을 *zone* $Z(i \cdot j)$라고 한다. 각각의 센서는 배치 지역과 각각의 그룹에 균등하게 배치된다고 가정하고, 그룹의 센서의 수는 n_z 이다. 전체 배치 지역의 센서의 전체 수는 N으로 나타내고, $N = n_z \cdot i \cdot j$ 이다. 그룹의 ID가 (i, j) 이고 센서의 유일한 노드 ID가 $b(b=1,\mathrm{L}, N)$일 때, 센서는 $[(i, j), b]$로 식별된다. 센서 배치 방법은 다음과 같다. 먼저, N센서를 각각의 그룹에 n_z 센서씩 $(i \cdot j)$ 그룹으로 나누고, $G(i, j)$의 각각의 센서에게 식별자 $[(i, j), b]$를 할당한다.

나. 키 사전 분배 스킴

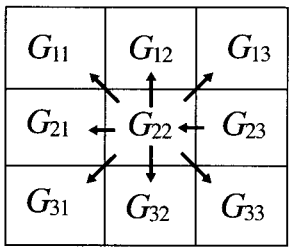
값 (i, j)은 그룹 혹은 지역 (zone)을 식별하기 위해 사용된다. 그룹의 관계에 따라 두 개의 키 사전분배 스킴을 제안한다. 그룹 내에서의 키 사전 분배 스킴을 I-스킴, 두 이웃 그룹간의 키 사전 분배 스킴을 E-스킴이라고한다.

a. I-스킴 : 주어진 지역 내에서의 키 사전 분배

$\tau = 2$는 초기 노드 캡쳐 임계치를 최대화시키고, λ

이상의 센서는 주어진 키 공간을 선택할 수 없다. 위의 두 제안의 결과로, 각각의 그룹의 센서의 수 n_z는 $|G(i,j)| \leq \lambda\omega/\tau$로 제한된다. 각각의 키 공간에 대해, 비밀 행렬 $A=(D \cdot G)^T$은 $N\times(\lambda+1)$ 행렬이다. 키 풀 P는 $P = L\times M$ 부분 키 풀들로 구성되며, 여기서 부분 키 풀은 i = 1,L, L, j = 1,L, M 인 $P(i,j)$로 나타낸다. 각각의 부분 키 풀은 ω개의 $N\times(\lambda+1)$ 키 행렬 A인 부분 키 공간으로 나뉜다. A 의 각각의 요소는 유일한 키이다. N개의 센서는 $L\times M$ 의 그룹들로 나뉜다. 그룹은 $G(i, j)$으로 나타낸다. 센서에게 $id=[(i,j), b]$ (b=1,L, N,(i,j) : 그룹 ID) 할당한다. 센서 $[(i,j), b]$에게 $P(i,j)$의 ω개의 부분 키 공간으로부터 τ개의 부분 키 공간을 랜덤하게 선택한다. 선택된 공간은 λ번 선택된 것이 아니어야한다. 센서에게 선택된 각각의 부분 키 공간에대해서 행렬 A의 b번째 열을 적재한다.

b. -스킴: 인접한 두 지역을 위한 키 사전분배



(그림 8) 그리드 구조에서의 센서 배치

(그림 8)과 같이, 하나의 지역은 최대 8개의 이웃 지역들을 가진다. 그룹 $G(i_1, j_1)$의 센서 i는 자신의 이웃 그룹들 중 하나의 그룹 ($G(i_2, j_2)$)으로부터 하나의 노드 (j)를 랜덤하게 선택한다. 키 k_{ij}는 유일하고, id_i, id_j는 i와 j의 식별자일 때, i의 듀플 $<k_{ij}, id_j>$를 j의 듀플 $<k_{ij}, id_j>$을 인스톨한다. 한 번 i가 그룹 $G(i_2, j_2)$의 동료 노드 j를 선택하면 같은 그룹에서 다른 노드를 선택할 수 없다.

다. Pairwise 키 확립 프로토콜

키 확립 프로토콜은 주어진 지역 내에서의 키 확립과, 인접한 지역들 간의 키 확립, 두 과정으로 나뉜다.

a. 같은 지역내에서의 키 확립: 각각의 센서는 자신의 식별자 $[(i, j), b]$와 자신의 키 공간 식별자 $[\tau_1, \tau_2]$를 브로드캐스트한다. 받은 ID와 일치하는 키 공간을 기반으로, 모든 이웃 노드의 ID를 점으로하여 키 그래프를 만든다. 각각의 이웃 노드 $[(i,j), u]$는 같은 키 공간을 가졌는지 검사하고, 만약 같은 키 스페이스를 가지고 있다면, [6]와 같이 pairwise 키를 확립한다. 각각의 센서는 같은 키 공간을 가진 이웃 노드들을 키 그래프에 추가하고, 키 공간을 공유하고 있는 이웃 센서들의 리스트를 브로드캐스트한다. 이 리스트를 받으면 각각의 노드는 자신의 키 그래프를 업데이트한다. 그 다음, 센서는 남은 이웃 센서들에게 request를 보내거나 pairwise 키를 확립하기 위해 소스 라우팅을 하고 자세한 키 경로를 키 그래프에 넣는다. 주어진 지역에서 모든 이웃 센서와 pairwise 키를 확립하지 않은 노드가 있을 수 있다. 비록 이런 노드가 존재할 확률은 작지만 만약 이런 노드가 존재하면 다중경로를 이용하여 pairwise 키를 설정한다.

b. 인접한 지역들 간의 키 확립

센서는 pairwise 키를 확립하고 싶은 노드 리스트를 브로드캐스트한다. Requestor와 같은 지역에 있는 이웃 노드는 이미 requestor와 키를 공유하고 있고, 프록시 처럼 작용한다. 이웃 노드는 쌍에 대한 pairwise 키를 선택하고, 선택된 키를 requestor와의 pairwise 키로, 목적 노드와의 pairwise 키로 각각 암호화하여 requestor에게 보낸다. Requestor는

목적 노드에게 암호화된 pairwise 키를 보낼 수 있다. 이 때, q개의 이웃 노드를 q개의 경로로 사용하고 q개의 키를 생성하여 인접한 지역의 이웃 노드와 pairwise 키를 생성한다: $k = k_1 \oplus \mathrm{L} \oplus k_q$.

3. LEAP: 로컬 암호화와 인증 프로토콜

S. Zhu, S. Setia와 S. Jajodia는 in-network 프로세싱을 제공하는 센서 네트워크를 위한 키 관리 프로토콜 LEAP (Localized Encryption and Authentication Protocol)을 제안했다[14]. LEAP은 다른 안전성 요구사항을 만족시키기 위해 4가지 형태의 키를 사용하고, 센서 네트워크의 실질적인 면을 고려했다는 점에서 의미가 있다. 네 가지 키는 개인 키, Pairwise 키, 클러스터 키, 그룹 키이다. N은 네트워크의 노드 수이고, u, v는 참여 노드이다. $\{S\}_k$는 키 k로 암호화한 메시지 s를 의미하고 $MAC(k, s)$는 키 k를 사용한 메시지 s의 메시지 인증 코드를 의미한다. 네 가지 키의 확립 기법 다음과 같다.

3.1 개인 키 확립

개인 키는 베이스 스테이션과 노드들 간에 공유하는 키이며 노드가 배치 되기 전에 Pre-load된다. 이 키는 베이스 스테이션과 각각의 노드와의 통신을 위해 사용하고 베이스 스테이션은 안전하다고 가정하므로 이 키의 안전성은 고려하지 않아도 된다. 이 키는. 노드 u에 대한 개인 키는 의사 난수 함수($f_k()$)와 베이스 스테이션의 마스터 키 K_m^s를 이용하여 베이스 스테이션이 $K_u^m = f_{K_m^s} A(u)$과 같이 생성하고 배치 되기 전에 노드에게 미리 적재된다.

3.2 Pairwise 공유 키 확립

Pairwise 키는 어떤 노드가 인접한 이웃 노드와 공유하는 키이며 프라이버시와 소스 인증과 같은 안전한 통신을 위해 사용된다. 이는 노드에게 미리 적재된 초기 키를 통해 배치된 후에 생성된다.

가. 키 사전 분배 : 노드를 배치하기 전에 동일한 초기 키 K_I를 메모리에 저장시키고 각 노드는 그 K_I로부터 의사 난수 함수를 이용하여 자신의 마스터 키 $K_u = f_{K_I}(u)$를 생성한다.

나. 이웃 노드 발견 : 노드가 배치 된 후 노드 u는 자신의 아이디를 브로드캐스트한다. 이를 받은 각각의 이웃 노드 v는 자신의 아이디와 마스터 키 K_v를 통해 생성된 MAC을 전송한다. 노드 u는 K_v를 계산하여 노드 v의 ID를 검증할 수 있다.

다. Pairwise 키 확립 : 의사 난수 함수을 이용하여 동일한 Pairwise 키 $K_{uv} = f_{K_v}(u)$를 생성한다.

라. 키 제거 : 마지막 단계로 초기 키 설정이 끝난 후 저장된 초기 키와 중간에 사용된 모든 키를 완전히 삭제한다.

3.3 클러스터 키 확립

클러스터 키는 한모든 이웃 노드들 간에 공유하는 키이고 Pairwise 키 생성 후 Pairwise 키로 암호화되어 이웃 노드에게 전송된다. 그래서 결국 Pairwise 키의 안전성이 이 프로토콜의 안전성을 보장한다. 노드 u가 인접한 모든 이웃 노드 v_1, v_2, L, v_m과 통신이 필요할 경우 클러스터 키를 확립한다. 노드 u는 먼저 랜덤한 키 K_u^c를 생성하고 각각의 이웃 노드와의 pairwise 키로 암호화하여 보낸다. $u \rightarrow v_i : (K_u^c)_{K_{uv_i}}$

3.4 그룹 키 확립

그룹 키는 베이스 스테이션과 센서 네트워크의 모든 노드가 공유하는 키로 전체 센서 네트워크의 노드들에게 브로드캐스트 할 경우 메시지를 암호화하기 위해 사용된다. 그룹 키도 개인 키와 마찬가지로 미리 적재된다. 그룹 키는 센서 네트워크 전체에서 공유되

는 키이므로 손상된 노드가 취소된 후에 키를 업데이트하기 위한 효과적인 리킹 메카니즘이 필요하다. 그룹 키는 모든 노드에게 배치되기 전에 미리 적재하고 후에 안전하게 업데이트한다. 손상된 노드의 노드 취소가 이루어진 후에 베이스 스테이션은 각각의 노드에게 노드와의 개인 키로 암호화하여 유니캐스트함으로써 그룹 키를 업데이트 할 수 있지만 이는 오버헤드가 네트워크 사이즈에 비례하여 증가하므로 LEAP는 클러스터 키 기반의 효과적인 키 업데이트 스킴을 제공한다.

V. 결 론

센서 네트워크에서의 안전한 통신을 위해 대칭키 암호에 기반을 둔 보안 프로토콜들이 많이 개발되었다. 안전한 키 분배 및 관리를 위한 LEAP[14]과 브로드캐스팅 메시지 인증을 위한 μTesla[12]등이 그것이다. 대칭키 암호가 암 · 복호에 효율적임에도 불구하고 센서 네트워크의 특성상 물리적인 공격에 의해서 키가 쉽게 노출될 수 있다. 또한 대칭키 기반의 암호 프로토콜들은 공유키 설정과 브로드캐스팅 메시지 인증을 위해서 복잡한 과정을 거쳐야 할 뿐 아니라 과도한 트래픽을 발생시킨다. 이러한 문제점을 해결하기 위해 공개키 암호를 센서 네트워크에 적용하고자 하는 노력이 계속되고 있다. 1024bit의 RSA 암호를 센서 네트워크에 적용하기에는 센서노드 자원의 제약이 있다. 이러한 센서노드 자원의 제약으로 인해 타원 곡선 암호가 무선 센서 네트워크의 공개키 암호 시스템의 기반이 될 것으로 전망된다. 타원 곡선 암호의 160bit 키는 RSA의 1024bit키 만큼의 안전성을 제공한다.[15] 현재 센서노드에서 타원 곡선 암호를 올리기 위한 시도들이 계속되고 있다. NCSU의 Peng Ning et al.은 TinyECC[16]를 구현하여 소스 코드와 실험 결과를 홈페이지에 공개해 놓았다. 센서 노드에 적합한 $GF(p)$상에서의 타원 곡선 암호를 구현한 Peng Ning은 MICAz에 최적화된 assembly code가 포함된 컴포넌트들을 공개 함으로써 센서 네트워크에서의 타원 곡선 암호 연구의 시작점이 되었다. Havard univ의 David J. Malan도 EccM 2.0[11]을 구현하여 소스 코드를 홈페이지에 공개하였다. EccM 2.0은 MICA2 모트에 적합한 $GF(2^m)$ 상에서의 타원 곡선 암호를 하나의 모듈에 구현해 놓았다. 두 개 모두 타원 곡선 기반의 Diffie-Hellman (ECDH)과 타원 곡선 기반의 전자 서명(ECDSA)을 구현해 놓았으며 이후로 나오는 타원 곡선 기반의 공개키 암호 시스템들의 비교점이 되고 있다. 또한 Dublin City univ.의 Barry Doyle et al.은 수학 라이브러리인 MIRACL을 ARM7에 맞추어 컴파일 하여 해당 이미지 올린 FPGA를 센서노드인 Tyndall Mote에 연결 시켜서 타원 곡선 암호를 구현하였다[4]. 이 외에도 Telematik의 Erik-Oliver Blaβ는 160bit 보다는 작지만 현재 안전성이 보장되는 113bit의 키를 사용한 타원 곡선 암호 프로토콜을 개발하였다. 한편, 이미 Ⅱ장에서 소개한 바와 같이, 고성능 모트 개발이 최근 활발히 이루어지고 있으며, 예를 들면, PXA271~3 CPU를 기반으로 한 iMote2와 같이 공개키 암호를 수행 할 수 있는 모트들이 속속 등장할 전망이다. 하지만, 이와 같은 고성능 모트도 가격, 공개키 암호 수행 시 요구되는 전력 등의 부담으로 인하여 여전히 기존의 극소형 저전력 모트를 기반으로 한 연구도 계속될 전망이다.

[참 고 문 헌]

[1] R. Blom, "An Optimal Class of Symmetric Key Generation Systems," In Proceedings

of Advances in Cryptology EUROCRYPT' 84, LNCS, vol. 209, Springer- Verlag, pages 335-338, 1985.

[2] H. Chan, A. Perrig, and D. Song, "Random Key Predistribution Schemes for Sensor Networks," In Proceedings of IEEE Symposium on Research in Security and Privacy, pages 197-213, 2003.

[3] David E. Culler, "Wireless Sensor Networks - the Next IT Revolution," KES 2004, Oct 7, 2004.

[4] B.?Doyle, "S. Bell, A. F. Smeaton, K. McCusker, and N. O'Connor, Security considerations and key negotiation techniques for power constrained sensor networks," In Proceedings of the Computer Journal (Oxford University Press), vol. 49, no. 4, pages 443-453, 2006.

[5] W. Du, J. Deng, Y. S. Han, and P. K. Varshney, "A Pairwise Key Predistribution Scheme for Wireless Sensor Networks," In Proceedings of ACM CCS' 03, 2003.

[6] W. Du, J. Deng, Y. S. Han, S. Chen, and P. K. Varshney, "A key management scheme for wireless sensor networks using deployment knowledge," In Proceedings of IEEE INFOCOM, March 2004.

[7] L. Eschenauer and V. D. Gligor, "A key-management scheme for distributed sensor networks," In Proceedings of the 9th ACM conference on Computer and communications security, pages 41-47, November 18-22 2002.

[8] Fei Hu, Jason Tillet, Jim Ziobro, and Neeraj K. Sharma, "Secure Wireless Sensor Networks: Problems and Solutions," Journal on Systemics, Cybernetics and Informatics (Best Paper Award), Vol.1, No.9, 2004.

[9] D. Huang, M. Mehta, D. Medhi, and L. Harn, "Location-aware key management scheme for wireless sensor networks," In Proceeding of 2nd ACM workshop on Security of Ad Hoc and Sensor Networks, 2004.

[10] C. Karlof, and D, Wagner, "Secure routing in wireless sensor networksL Attacjs abd ciybterneasyres," In Proceedings of the 1st IEEE International Workshop on Sensor Network Protocols and Applications, 2003.

[11] D. J. Malan, M. Welsh, and M. D. Smith, "A public-key infrastructure for key distribution in TinyOS based on elliptic curve cryptography," In Procedings of The First IEEE International Conference on Sensor and Ad Hoc Communications and Networks, Santa Clara, California, October 2004.

[12] A. Perrig, R. Szewczyk, V. Wen, D. Culler, and J. D. Tygar, "SPINS: Security protocols for sensor networks," In Proceedings of ACM International Conference on Mobile Computing and Networks (MobiCom), 2001.

[13] A. Perrig, D. Wagner, and J. Stankovic,

"Security in Wireless Sensor Networks," In Proceedings of Communications of the ACM, page 53-57, 2004.

[14] S. Zhu, S. Setia and S. Jajodia, "LEAP: Efficient Security Mechanisms for Large-Scale Distributed Sensor Networks," In Proceedings of the 10th ACM Conference on Computer and Communication Security, pages 62-72, 2003.

[15] "Key management guideline-workshop document," draft. Available at http://csrc.nist.gov/encryption/kms/keymanagement-guideline-(workshopt)%.pdf, NIST, 2001.

[16] "TinyECC: Elliptic Curve Cryptography for Sensor Networks (Version 0.1)," Available at http://discovery.csc.ncsu.edu/software/TinyECC/, North Carolina State University.

[17] MICAz : Wireless Measurement System, http://xbow.com/Products/Product_pdf_files/Wireless_pdf/6020-0060-01_A_MICAz.pdf, 2004, Crossbow.

[18] Telos rev.B : Enabling Ultra-Low Power Wireless Research, http://www.moteiv.com/products/docs/an002-telos.pdf, 2004, tmoteiv.

[19] Intel Mote2 Overview, http://www.intel.com/research/downloads/imote_overview.pdf, 2005, intel-research.

권태경

1992년 연세대학교 컴퓨터 과학과 학사
1994년 연세대학교 컴퓨터 과학과 석사
1999년 연세대학교 컴퓨터 과학과 박사
1999년 ~ 2000년 UC Berkeley EECS 포스트닥 연구원
2000년 ~ 2001년 (주)데이터웨이브시스템 이사
2001년 ~ 2003년 세종대학교 컴퓨터공학부 전임강사
2003년 ~ 현재 세종대학교 컴퓨터공학과 조교수
관심분야 : 정보보호, 암호 프로토콜, 센서 네트워크 보안, 무선 네트워크 보안, 임베디드 시스템 보안, 바이오정보보호, DRM, 컴퓨터 네트워크, 유비쿼터스 컴퓨팅

신수연

2004년 세종대학교 컴퓨터 공학과 학사
2006년 세종대학교 소프트웨어공학과 석사
2006년 ~ 현재 세종대학교, 컴퓨터공학과 박사 과정
관심분야 : 정보보호, 센서 네트워크 보안, 암호 프로토콜

박상호

2004년 세종대학교 컴퓨터, 소프트웨어학과 졸업
2006년 세종대학교 소프트웨어 공학과 석사
2006년 ~ 현재 세종대학교 컴퓨터 공학과 박사 과정
관심분야 : DRM, 저작권 보호, 임베디드 시스템 보안, 센서 네트워크 보안

박태진

2006년 세종대학교 컴퓨터, 소프트웨어학과 졸업
2006년 ~ 현재 세종대학교 컴퓨터 공학과 석사 과정
관심분야 : 컴퓨터 네트워크, 센서 네트워크 보안, 암호 프로토콜