무선 센서 네트워크 환경에서의 키 설립 프로토콜에 관한 비교 분석*

임태령 이화성 이동훈

고려대학교 정보경영공학전문대학원

imtr@cist.korea.ac.kr, {hwaseong, donghlee}@korea.ac.kr

Analysis on Pairwise Key Establishment Protocols for Wireless Sensor Networks

Im, Taeryung Lee, Hwaseong Lee, Dong Hoon

Graduate School of Information Management and Security, Korea University

요약

안정적인 무선 센서 네트워크 환경을 위해서는 각 노드 간에 전송되는 메시지의 암호화와 인증이 매우 중요하며 이를 위해서는 각 노드와 그 주변 이웃 노드 간에 안전하고 효율적인 키 설립이 필요하다. 현재 이를 위한 여러 프로토콜이 제안되었으며 각 프로토콜을 실제 시스템에 적용하기 위해서는 해당 네트워크의 규모에 알맞은 효율적인 프로토콜을 선택하여 적용할 수 있어야 한다. 이를 위해 본 논문에서는 대표적인 pairwise key 설립 기법인 SPINS와 LEAP을 설명한 후 기법의 특징을 비교분석 하고 네트워크 규모에 따라 합리적이고 타당한 키 설립 기법을 선택하기 위해 고려할 사항을 알아본다.

1. 서론

무선 센서 네트워크는 하나 이상의 베이스 스테이션(base station, sink node)과 여러 개의 센서 노드로 이루어져있는 네트워크이다. 센서 노드를 필요한 지역에 다수 배치시키기 위해서는 각각의 노드들의 가격이 상대적으로 저렴한 제한된 성능의 노드를 사용하여 네트워크를 구성해야 한다. 이런 노드들은 계산 능력과 저장 공간, 에너지, 통신 능력 등에 제한이 존재한다. 그럼에도 불구하고 무선 환경에서 브로드캐스트(broadcast) 방식으로 통신이 이루어지므로 공격자는 쉽게 통신 내용을 도청하고 패킷을 삽입하거나 재전송하는 등의 공격이 쉽게 이루어 질 수 있으므로 통신 데이터의 암호화와 인증이 필수이다. 하지만 이런 제한된 성능의 노드에서는 일반적인 공개키 기법을 이용한 키 설립 방식 보다는 각 네트워크 규모와 노드의 특성에 따른 합리적이고 타당한 키 설립 기법이 필요하다 [1, 3].

본 논문은 다음과 같이 구성되어있다. 먼저 2장에서 본 논문에서 언급되는 프로토콜의 표기를 정리하고 3장에서 SPINS[4]에 대해 간단히 설명하고 4장에서는 LEAP[5]에 대하여 간단히 소개한다. 5장에서 각각의 프로토콜에 대한 비교를 통해 결론을 도출한다.

2. 표기

본 논문에서 사용된 표기들을 정리하면 다음과 같다.

표기	설명
u,v	통신주체, 센서 노드
S	베이스 스테이션
N_u	노드 u가 선택한 임의의 값
K_{uv}	노드 u,노드 v 사이의 pairwise key(상호 공유키)
K_{uS}	베이스 스테이션 S와 공유된 노드 u의 비밀 값
K_{IN}	전체 네트워크의 비밀키인 초기키(initial key, LEAP에서 사용)
MAC(K,M)	대칭키 K를 이용한 M에 대한 MAC
$\{M\}_K$	대칭키 K로 M을 암호화
F	의사 난수 함수(pseudo random function)
T_{min}	공격자가 노드를 포획(capture)하여 노드의 비밀정보를 얻는데(node compromise) 걸리는 시간의 하한(minimum time)
T_{est}	새로 추가된 노드가 이웃 노드를 발견하여 키를 설립하는데 걸리는 예상 시간(estimated time)
n	네트워크의 전체 노드의 개수

<표 1> 논문에서 사용된 표기

3. SPINS

가. 프로토콜 소개 및 특징

SPINS는 크게 두 가지 부분으로 구성이 되어있다. 데이터 기밀성과 두 노드 사이에서의 데이터 인증, 무결성 및 데이터 freshness를 제공할 수 있는 SNEP과 데이터 브로드캐스트 시에 데이터 인증을 제공할 수 있는 μTESLA로 이루어져 있다.

SNEP를 사용하기 위해서는 통신하기를 원하는 두 노드 간에 pairwise key를 공유하고 있어야 하는데 이를 위해서 네트워크의 각 노드들은 배치 이전에 베이스 스테이션과 각각 유일한 대칭키인 개인키를 공유하고 이를 바탕으로 베이스 스테이션이 pairwise key 설립에 참여를 함으로서 노드 간에 키를 설립한다. 이 대칭키에 단방향 함수(one-way function)을 취함으로 노드 사이에 전송될 메시지에 대한 인증키를 각 노드가 스스로 유도해낼 수 있으며 이 키들을 이용하여

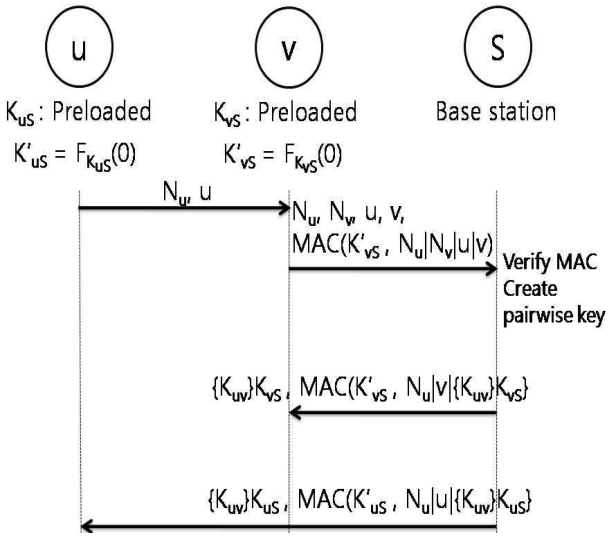
* "본 연구는 정보통신부 및 정보통신연구진흥원의 대학 IT연구센터 지원사업의 연구결과로 수행되었음" (IITA-2008-(C1090-0801-0025))

노드 간에 각각의 카운터를 교환하여 사용함으로 약한 데이터 freshness를 이룰 수 있다.

그리고 μTESLA를 이용하면 베이스 스테이션의 브로드캐스팅을 인증할 수 있는데 이는 시간의 지연을 두고 대칭키를 공표함으로 이루어진다. 이를 위해서는 우선 각 노드가 배치 이전에 공표되는 대칭키를 확인 할 수 있도록 단방향 키 체인의 첫 번째 키(commitment)를 저장하고 있어야하며 베이스 스테이션과 모든 노드 사이에 느슨한 시간의 동조화가 필요하다. μTESLA를 이용하여 라우팅 비콘(routing beacon)을 전송하게 되면 넓이 우선 신장 트리(breadth first spanning tree) 형태의 라우팅 토폴로지(routing topology)를 생성하는 인증된 라우팅이 가능하다.

나. SNEP을 이용한 이웃 노드간 키 설립

위에서 언급된 SPINS 상에서 두 노드간의 pairwise key의 설립은 다음과 같이 베이스 스테이션이 trusted third party 역할을 하여 각각의 노드에게 임의의 대칭키를 생성하여 배포하는 형태이다.



<그림 1> SPINS에서 pairwise key 설립

<그림 1>과 같이 만약 노드 u가 v와 pairwise key 설립을 하고 싶다면 u가 v에게 자신의 ID와 임의의 수 N_u를 전달하게 되고 v는 전송 받은 u의 ID값 및 임의의 수와 자신의 ID값, 자신이 생성한 임의의 값을 모두 포함하여 배치 전에 미리 저장되어있던 베이스 스테이션과의 비밀키를 사용, MAC을 첨부하여 u와 v사이의 pairwise key를 베이스 스테이션에 요청한다.

베이스 스테이션은 키를 생성한 후 키를 각각의 노드의 개인키로 암호화 하여 각각의 노드에 전송한다. 각 노드는 베이스 스테이션과 개인키를 공유하고 있으므로 위 과정에서 전송받은 pairwise 키의 복호화와 메시지의 출처가 신뢰 가능한 개체(베이스 스테이션)로부터 온 것인지 검사할 수 있다. 전체 과정에서 두 노드가 각각 생성한 난수를 포함함으로 해당 키는 strong key freshness를 만족한다.

4. LEAP

가. 프로토콜의 소개 및 특징

LEAP은 4가지 키를 이용하여 여러 가지 전송 형태를 지원하는 키 설립 프로토콜이다. LEAP에서는 메시지를 베이스 스테이션에 포워딩하는데 소요되는 에너지를 줄이기 위한 data aggregation이나 passive participation과 같은 in-network processing이 가능한 통신 형태를 고려하여 여러 통신 방식에 따라 다른 대칭키를 사용하여 안전한 통신을 하도록 제안하였으며 노드 추가 시 pairwise key의 설립이 베이스 스테이션을 경유하지 않고도 가능하다. 이 4가지 키는 다음과 같다.

INDIVIDUAL KEY 각각의 노드의 비밀 값으로 각 노드의 개인키(individual key)는 전체 네트워크의 비밀 값인 initial key(K_{IN})로부터 생성된다.

PAIRWISE KEY 두 노드간의 통신에 이용되며, 통신하려는 두 노드의 개인키를 이용하여 설립이 된다.

CLUSTER KEY 인증된 지역 브로드캐스트에 사용되며 설립된 pairwise key를 이용하여 각 노드가 모든 이웃 노드에게 임의로 생성하여 pairwise key로 암호화하여 배포한다.

GROUP KEY 전체 네트워크상으로 브로드캐스트 할 때 사용되는 키로 각 노드의 배치 전에 저장하고 추후 키의 갱신을 위하여 인증된 group key의 재배포 프로토콜이 필요하다.

LEAP의 다른 프로토콜과의 큰 차이점은 공격자가 노드를 포획하여 노드의 비밀정보를 얻는데 걸리는 시간이 새로 추가된 노드가 이웃 노드를 발견하여 키를 설립하는데 걸리는 시간보다 오래 걸린다 ($T_{min}>T_{est}$)고 가정을 한 상태에서 프로토콜이 진행이 된다는 점이다.

이런 성질을 이용하여 LEAP에서는 각 노드가 배치될 때 미리 K_{IN}을 저장해놓고 노드를 배치하여 T_{min}보다 짧은 시간 동안 베이스 스테이션의 참여 없이 이웃 노드를 발견하여 pairwise key를 설립할 수가 있으며 가능한 노드 포획에 대비하기 위해 T_{min}이후에 비밀 값들을 지운다. 즉, 노드가 포획 당하는데 걸릴 것이라 여겨지는 최소의 시간 전에 네트워크 전체의 비밀 정보를 이용하여 이웃 노드와의 키 설립을 효율적으로 하고 그 후에 바로 비밀 정보를 삭제하는 방식이다. 즉, 배치 초기의 안전성을 희생함으로써 베이스 스테이션의 참여 없이도 이웃 노드를 발견하고 키 설립을 효율적으로 가능하게 한 방식이다.

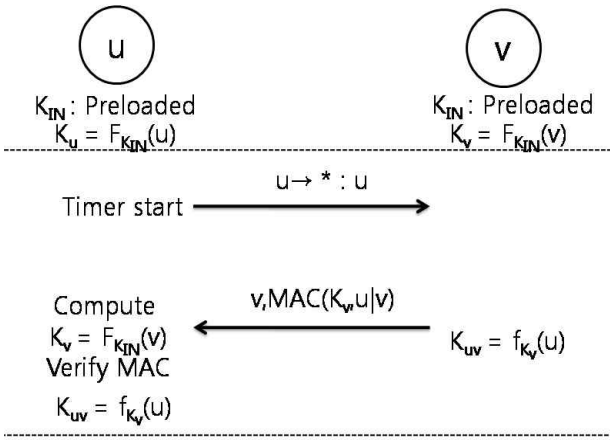
예를 들어, 센서 노드로서 4MHz CPU에 최대 40 Kbps의 전송속도를 가지는 Mica *mote*[6]가 사용되었다면 키 설립 과정에서 설치된 노드가 ID를 먼저 전송하고 응답으로 이웃 노드가 ID와 MAC을 보내므로 만약 ID가 4바이트이고 MAC이 8바이트라고 가정하면 이웃 노드들과의 키 설립 시 걸리는 시간이 수 초 이내이다. 현실적으로 공격자가 센서 노드를 포획하여 내부의 정보를 복제하는 일련의 작업을 수 초이내에 달성하기는 매우 어려우므로 여기서의 가정은 상당히 현실성 있는 가정이라고 할 수 있다. 실제로 [2]의 실험에 의하면 Mica mote의 메모리를 복사하는데 노드를 포획한 후 수십 초에서 수분이 걸린다는 것을 알 수 있다.

나. LEAP에서 이웃노드 발견 및 키 설립

KEY PRE-DISTRIBUTION. 노드의 배치 전에 네트워크의 비밀키 K_{IN}을 미리 저장하고 있고 이를 바탕으로 의사 난수 함수를 이용하여 각자의 개인키를 계산한다. <그림2>에서 같이 u가 추가되는 노드라면 $Ku= F_{K_{IN}}(u)$로 개인키를 계산할 수 있다.

NEIGHBOR DISCOVERY. 노드가 배치가 되면 u와 같이 새롭게 배치된 노드는 자신의 아이디 값을 브로드캐스트하고 이를 전송 받은 노드들의 응답을 받는다. 이때 K_{IN}을 이용하여 상대방의 개인키

를 계산하여 MAC을 검증함으로 메시지를 인증한다.



<그림 2> LEAP에서 pairwise key 설립

PAIR-WISE KEY ESTABLISHMENT. 서로 간에 전송받은 정보를 통하여 의사 난수 함수를 통해 대칭키를 생성해내는데 이때, <그림2>와 같이 응답하는 노드는 비밀키 K_{IN}가없이도 자신의 개인키를 이용하여 Kuv= F_{Kv}(u)로 계산할 수 있다.

KEY ERASURE. T_{min}이 되면 추가되었던 노드는 네트워크의 비밀값 K_{IN}과 키 설립과정에서 계산하였던 이웃 노드의 개인키를 모두 지움으로 추후 공격자가 노드를 포획하더라도 피해를 지역화 할 수 있게 다른 노드의 비밀정보와 전체 네트워크의 비밀 정보를 삭제한다. 또한 자신의 개인키는 저장하고 있도록 하여 다른 노드가 새롭게 추가 되었을 경우 키 설립을 할 수 있도록 한다.

5. 비교 및 분석

프로토콜	SPINS	LEAP
통신량	O(n)	O(1)
메모리	O(1)	O(1)
안전성	안전함	T_{min}>T_{est}라는 가정이 성립할 때 안전
확장성	소규모 네트워크에 적합, 확장이 쉽지 않음	대규모 네트워크에도 적용가능, 확장이 용이

<표2> 노드의 개수가 n인 네트워크에 노드 추가 시 두 프로토콜의 비교

SPINS에서의 키 설립 프로토콜에서는 베이스 스테이션이 직접 키 설립 과정에 참여를 하여 각 노드의 개인키로 암호화 및 인증을 수행하므로 당사자 노드들 이외에는 해당 pairwise key를 알 수 없으며 이는 각각의 개인키의 안전성에 의존하므로 안전하다. 또한 키 설립 요청 메시지에 임의의 값이 포함이 되므로 강한 key freshness를 보장할 수 있으며 노드 포획 시에는 해당 노드에 저장된 비밀 정보 밖에 얻을 수 없으므로 해당 노드의 개인키와 이웃 노드들과의 pairwise key 이외에 다른 키는 안전하다.

하지만 이렇게 노드간의 대칭키 설립을 하기 위해서는 센서 노드가 베이스 스테이션에 키 생성을 요청해야 하는데 일반적으로 센서 노드는 통신 반경이 크지 않으므로 베이스 스테이션에서 멀리 떨어진 노드들은 키 요청을 하기 힘들기 때문에 센서 네트워크를 대규모로 넓은 지역에 배치하기 어렵다. Mica *mote*를 예로 들면 통신 반경이 약 30M 정도 이므로 반경 30M이상의 넓은 지역에 센서 네트워크를 배치했을 경우에는 노드와 베이스 스테이션 간에 멀티홉(multi-hop) 방식으로 통신을 해야 하는데 이런 방식은 실제 구현이 까다롭고 노드 추가 및 네트워크의 확장 시에 모든 요청이 베이스 스테이션으로 전달(forwarding)되어야 함으로 전체 네트워크상에 많은 통신량을 요구한다. <표 2>에서와 같이 최악의 경우 통신 회수는 O(n)에 속하게 되므로 센서 노드들의 에너지 소비가 크게 될 것이다. 또한 요청이 베이스 스테이션으로 집중되는 형태이므로 베이스 스테이션 주변의 노드들에게도 통신상의 부하가 집중되게 되고 이로 인하여 빠르게 전력고갈이 될 가능성이 있다.

LEAP에서는 키 설립 과정에서 베이스 스테이션에 참여를 필요로 하지 않으므로 센서 노드의 통신 반경의 제약에서 비교적 자유롭고 그러므로 대규모로 넓은 지역에 노드를 효율적으로 배치 할 수 있다. 또한 노드의 아이디만을 서로 전송하므로 다른 방식에 비해 전송량도 크지 않고 이웃 노드 사이의 pairwise key 수립 과정이 지역적으로 진행되므로 <표2>와 같이 통신 횟수가 적은 장점이 있다. 이런 장점들은 위에서 살펴보았듯이 T_{min}>T_{est}라는 가정 하에서 안전한데 실제로 T_{est}는 수초 정도에 끝나므로 이 전에 노드를 포획하여 비밀 정보를 얻어내기 힘들다는 이 가정은 상당히 타당하다고 볼 수 있다. 만약 T_{min} 이후에 공격자가 노드를 포획하여도 이미 pairwise 키를 설립한 이웃 노드 외에는 통신을 할 수 없으므로 피해를 지역화 시킬 수 있다.

하지만 전체 네트워크가 하나의 비밀 키 K_{IN}에 의존하고 있으므로 계속적으로 노드를 추가 할 때마다 K_{IN}을 미리 저장하고 있는 노드가 추가가 되게 되므로 점점 K_{IN}이 노출될 가능성이 커질 수가 있기 때문에 보안상으로 취약한 단점이 있다. 즉, 장기적으로 계속 네트워크에 노드를 추가해나가는 경우에는 매 추가시마다 공격자가 노드를 포획하는데 걸리는 시간이 매번 동일하다고 할 수 없기 때문에 노드 추가의 횟수가 늘어나면 늘어날수록 공격자가 더욱 신속하게 노드를 포획할 수 있을 것이며 T_{min}<T_{est}이 될 수 가능성이 점점 커져 나중에는 공격자가 비밀키를 얻어 내어 전체 네트워크가 위험해질 수도 있다. 또한 위와 같은 공격자의 적극적인 공격이 아닌 설치되는 노드의 고장이나 여타 다른 보안 사고가 발생하여 K_{IN}이 노출된다면 전체 네트워크가 위험에 빠질 수도 있다.

그러므로 키 설립의 안전성 측면에서는 SPINS와 같이 trusted third party를 포함하여 안전하게 키 설립을 하고 비밀정보가 누설이 되더라도 그 피해가 지역적인 프로토콜이 더 좋으나 배치되는 지역과 네트워크의 규모나 센서 노드의 통신 반경의 제약을 고려한다면 LEAP과 같은 다소의 안전성을 희생을 하더라도 프로토콜을 적용하는데 있어서 효율적이고 키 수립과정에서 베이스 스테이션의 참여를 줄일 수 있는 프로토콜이 더 적당하다.

6. 결론

안전성과 효율성은 트레이드오프(tradeoff) 관계라고 할 수 있다. 그렇기 때문에 배치의 효율성이나 네트워크 어플리케이션에서 요구되는 보안 정도에 따라서 타당한 키 설립 프로토콜을 적용시켜야 될 것이다.

SPINS에서의 키 설립 방식이 베이스 스테이션을 통하여 키를 설립하므로 매우 안전하지만 센서 노드의 통신 반경 제약의 문제와 네트워크의 규모가 커지면 배치 준비과정이 복잡해지는 문제가 있으므로

소규모의 네트워크에 적합하며 LEAP는 약간의 보안상의 취약점이 있으나 센서 노드를 효율적으로 대규모로 효율적으로 배치할 수 있는 장점이 있다.

추후 계속적으로 높은 안전성을 제공하면서도 여러 제약이 많은 센서 환경에서도 효율적으로 사용할 수 있는 프로토콜이 계속적으로 연구가 되어야 할 것이다.

참고문헌

[1] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, “A survey on sensor networks”, In Proceedings of the IEEE Communications Magazine, Vol.40, No. 8, pp. 102-114, 2002.

[2] J. Deng, C. Hartung, R. Han and S. Mishra, "A practical study of transitory master key establishment for wireless sensor networks".First IEEE/CreateNet Conference on Security and Privacy for Emerging Areas in Communication Networks (SecureComm), pp. 289-299, 2005.

[3] D. Djenouri, L. Khelladi, and A. N. Badache, “A Survey of Security Issuesin Mobile Ad Hoc and Sensor Networks”, In Proceedings of Communications Surveys and Tutorials, Vol. 7, No. 4, pp. 2-28, 2005.

[4] A. Perrig, R. Szewczyk, V. Wen, D. Culler, and J. Tygar. “"SPINS: Security protocols for sensor networks,"" Wireless Networks, Volume 8 , pp. 521 - 534,.2002.

[5] S. Zhu, S Setia, and S. Jajodia, "LEAP: Efficient Security Mechanisms for Large-Scale Distributed Sensor Networks", ACM CCS'03, pp.62-72, 2003,

[6] http://www.xbow.com/Products/Product_pdf_files/Wireless_pdf/MICA.pdf