Smart Dust Network에서 효율적인 키 분배*

박정형, 염대현, 이필중

포항공과대학교 전자전기공학과

Efficient Key Distribution in Smart Dust Networks

Jung Hyung Park, Dae Hyun Yum, Pil Joong Lee

Department of Electronic and Electrical Engineering, POSTECH

요 약

무선 센서 네트워크가 다양한 방면에서 활용됨으로써 그 중요성이 더해지고 있다. 이러한 센서 네트워크에서 각 노드 사이의 안전한 통신을 위해 각 센서 노드 사이에 pair-wise key를 설정하여야 한다. Anderson등은 smart dust network환경에서 현실적인 공격자 모델을 제시하였고, 그에 효율적인 key 교환 scheme을 제안하였다. 본 논문에서는 Smart dust network환경에서 computational cost와 communicational cost 측면에서 Anderson등의 scheme보다 효율적인 키 설정 scheme을 제안한다.

I. 서론

MEMS(micro-electro-mechanical system), 무선 통신과 디지털 전자공학 영역의 놀라운 발전은 소규모, 저전력, 저비용의 센서들의 개발을 주도하여왔다. 이러한 작은 센서들은 감지 기능, 데이터 처리 기능, 그리고 통신 기능을 가지며[8], 이러한 능력을 가진 센서들을 이용한 무선 센서 네트워크는 다양한 분야에 활용됨으로서 중요성이 더해지고 있다.

만약 군사 지역이나 전쟁터에 센서들이 배치되어 진다면 무선 센서 네트워크에서의 안전성은 중요한 문제가 될 것이다. 게다가 이러한 경우 적들은 센서 노드에 방해 전파를 보내거나 아니면 센서 노드를 임의로 조작하여 허위 정보를 제공하는 등 많은 공격들을 가할 것이다.

이렇듯 센서 네트워크를 설계할 경우 안전성은 고려해야할 중요한 문제이며, 안전한 센서 네트워크위해 각 센서 노드사이의 pair-wise key들을 안전하게 설정해야만 한다. 하지만 물리적인 센서 노드들의 제약으로 인해 전형적인 공개키 방식은 부적합하여 대칭키 암호 방식을 사용한다. 게다가 일반적으로 센서 노드들은 임의의 위치에 배치되므로 이웃하는 노드들에 대한 정보를 사전에 결정할 수 없다. 이러한 이유로 대부분의 센서 네트워크에서 key 설정 scheme들은 센서 노드들을 배치하기 전에 센서 노드들에게 잠재적인 키들을 배당하는 방법을 사용한다.

대부분의 센서 네트워크에서 key 설정 scheme들은 센서의 초기 배치 단계에 공격이 가능하다고 가정을 하며, 특히 공격자는 모든 노드를 포획할 수 있고, 모든 통신을 감시할 수 있다는 가정을 한다. 이는 상당히 강한 가정으

* 본 연구는 정보통신부 및 정보통신연구진흥원의 대학 IT연구센터 지원사업과 BK21의 연구결과로 수행되었음.

로 새롭게 제기 되고 있는 smart dust network 환경에서는 부적합하다. 따라서 현실적인 공격자 모델을 재정의 하고 효율적인 scheme을 설계할 필요성이 있다.

II. 선행 연구들

2.1 일반적인 센서 네트워크

전형적인 센서 네트워크는 매우 많은 수의 작고 저렴한 센서 노드들로 구성이 되며, 이러한 센서 노드들은 스스로 네트워크를 형성하기 위해 노드들끼리 서로서로 무선 통신을 한다.

무선 센서 네트워크를 이용한 많은 어플리케이션에서 센서 노드 사이의 신뢰성 있는 통신이 요구되어 지며, 이를 위해서 센서 노드 사이의 pair-wise key들은 안전하게 설정되어야 한다. 이 pair-wise key들은 센서 노드 사이에 인증 및 기밀성 같은 보안을 목적으로 사용되어진다.

충분한 계산 능력을 가진 객체들 사이의 pair-wise key 설정인 경우, Diffie-Hellman key agreement 또는 RSA-based key establishment[5, 6]와 같은 공개키 암호 방식을 이용한다. 하지만 센서 네트워크에서 사용되는 센서 노드들은 공개키 암호화를 수행할 만큼 큰 계산 능력 및 저장 공간을 가지지 않았으며, 배터리의 에너지도 제한되어 있어 공개키 암호 방식을 사용할 경우 battery-draining denial of service attack에 취약하다.

이러한 이유에서 대칭키 암호화 방식에 기반한 key distribution 방법들이 제안되었다.

가장 간단한 key distribution 방법은 모든 센서 노드들이 하나의 master key를 저장하고 그 키를 이용하여 센서 노드들 사이의 pair-wise key를 설정하는 방식이다. 하지만 이 경우 공격자가 하나의 센서 노드를 포획하여 master key를 알게 된다면, 이를 이용하여 모든 센서 노드들의 pair-wise key를 구할 수 있다.

Kerboros와 유사하게 KDC(key distribution center) 역할을 하는 base station을 통해 pair-wise key를 설정 방식[7]에서는 작은 메모리 공간을 요구하고, 센서 노드의 포획에 대한 강한 안전성을 보장한다. 그러나 센서 노드 수가 많아지면 base station 주위에 집중적인 자원 손실이 발생할 수 있어 대규모 무선 센서 네트워크에는 적합하지 않다.

Eschenauer과 Gligor[3]은 Random key pre-distribution scheme을 제안하였으며, Chan, Perrig, and Song[4]은 이를 확장한 key distribution scheme을 제안하였다. 이들 scheme에서 각 각의 센서 노드들은 배치 후 가질 수 있는 센서 노드들 사이의 키를 사전에 분배한다. 따라서 이 scheme들은 사전 계산 단계가 요구되어진다. 또한, 실제 사용되어지지 않는 많은 키들까지 저장하여야 하기에 많은 메모리 공간이 필요하므로 이러한 random key pre-distribution scheme들은 smart dust network에서는 실용적이지 않다.

2.2 Smart dust 네트워크

Tine 센서 개발 project중 하나인 "smart dust" project에 의해 크기, 소비전력과 가격등을 기존의 센서들에 비해 획기적으로 줄일 수 smart dust[2]가 개발되었다. 이로써 random scattering에 의해 거대한 양의 smart dust들을 분배할 수 있게 되었다.

대부분의 기존 센서 네트워크에서의 key 설정 scheme들은 센서 초기 배치 단계에도 공격이 가능하며, 네트워크 전체의 통신을 감시할 수 있다고 가정하고 있다. 이러한 가정은 매우 강한 가정이여서 이 가정에서 안전한 scheme은 경제적으로 많은 부하를 초래한다.

이러한 강력한 가정은 전략적으로 중요한 고가의 센서 네트워크에는 적당할지 몰라도 smart dust network의 응용의 경우에는 현실적이지 않다.

2.3 Smart dust network환경에서의 공격자 모델

[1]에서는 smart dust network 환경에서 smart dust의 초기 배치 될 때, 공격자는 smart dust 사이의 통신을 일정한 비율 감시 할 수 있다는 가정아래 다음과 같은 공격자 모델을 제시 하였다.

첫째, 공격자는 초기 배치 단계 동안에 배치

장소에 물리적인 접근을 할 수 없다.

둘째, 공격자는 초기 배치 단계 동안에 smart dust network의 일정 비율의 통신만을 감시할 수 있다. 키 교환이 끝난 후에는 공격자는 모든 통신을 감시할 수 있다.

셋째, 공격자는 초기 배치 단계 동안에 능동적인 공격(ex. jamming 또는 flooding)을 할 수 없다. 키 교환이 끝난 후에는 공격자는 어떤 종류의 공격도 할 수 있다.

2.4 Key Infection[1]

Key Infection은 다음과 같이 두 단계로 이루어진다.

1) smart dust 노드 i는 k_i를 생성한 후 broadcast하고, 이웃한 노드 j는 i의 메시지를 획득한다.

2) 노드 j는 pair-wise key를 만들고 자신의 ID와 함께 i가 보내준 k_i를 이용하여 암호화한 후 암호화된 메시지를 broadcast한다.

이러한 과정을 거침으로써 smart dust 노드 i와 j는 pair-wise key를 설정할 수 있다. Pair-wise key를 설정하는데 있어서 어떠한 보호도 없이 평문으로 k_i를 전송하는데는 다소 납득하기 어려움이 있다. 하지만 smart dust network환경에서 공격자 모델에서와 같은 공격자들에 대해서는 충분한 안전성을 보일 수 있다. 만약 공격자가 없는 지역에 smart dust 노드 i와 j가 배치되거나 공격자가 노드 사이에 key 교환을 마친 후에 도착한다면 i와 j는 안전한 링크를 형성할 수 있다. Smart dust 노드 i와 j의 통신을 엿들을 수 있는 위치에 공격자가 사전 배치되어져 있다면, 노드 i와 j 사이의 pair-wise key는 노출 될 것이다. 하지만 100개의 정당한 smart dust 노드가 배치될 곳에 사전에 1개의 공격 노드가 배치되어 있고, 각 smart dust 노드들은 평균적으로 이웃하는 노드를 4개 가진다면 전체 네트워크에서 약 2.4%의 링크만이 손실되므로 여전히 전체 네트워크는 충분한 안전성을 제공해준다.

하지만, 위와 같은 Key Infection은 smart dust 노드들 사이에 최소 2번의 데이터 전송이 필요하다. 만약 이웃하는 노드를 4개 가진 smart dust 노드가 있다면 이는 최대 5번의 데이터 전송을 필요로 하다.

III. 제안하는 Scheme

우리는 Smart dust network 환경에서 각 smart dust 노드 사이의 key 설정에 있어서 Key Infection에 비해 효율적인 scheme을 아래와 같이 제안한다.

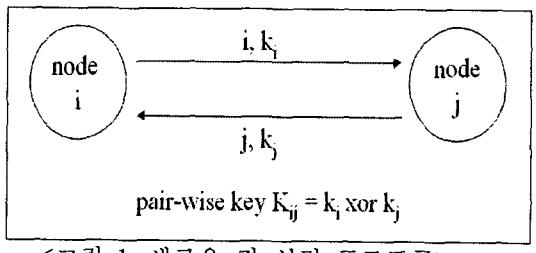
3.1 기존 사실

Smart dust network를 구성하는 노드들은 모두가 같은 종류이며, 이에 따라 모든 노드들의 송수신 반경은 동일하다. 제안하는 scheme은 이러한 사실과 [1]에서 제시한 공격자 모델을 이용한다.

3.2 새로운 키 설정 Scheme

Smart dust node가 분산되어 뿌려질 때, 각각의 smart dust node들은 자신의 ID와 랜덤한 키를 어떠한 암호화 과정 없이 broadcast한다. 그림1에서와 같이, 만약 smart dust node i와 j가 서로 이웃한 노드라고 하면 i는 j의 ID_j와 k_j를 수신하게 되고, j는 i의 ID_i와 k_i를 수신하게 될 것이다. 이렇게 이웃한 노드 j의 ID_j와 k_j를 수신한 i는 자신이 broadcast한 k_i와 j로부터 수신한 k_j를 XOR하여 pair-wise key($k_{ij} = k_i$ xor k_j)를 만든다. 노드 j 또한 i와 동일한 방식으로 pair-wise key를 만들게 된다.

Smart dust 노드 i와 j는 이후 k_{ij}를 이용하여 안전한 통신을 할 것이다.



<그림 1. 새로운 키 설정 프로토콜>

3.3 제안하는 Scheme vs. Key Infection

제안하는 scheme의 경우 이웃하는 노드의 수에 상관없이 key 설정을 위해 각 노드는 단

한번의 broadcast를 한다. 이에 비해 Key Infection의 경우는 broadcast해야 하는 횟수가 이웃하는 노드의 수에 비례하기 때문에 제안하는 scheme이 Key Infection에 비해 communicational cost측면에서 효율적이다. 또한 제안하는 scheme의 경우 각 노드는 xor연산만을 이용하여 pair-wise key를 설정하기 때문에 symmetric encryption을 이용하는 Key Infection에 비해 computational cost측면에서도 효율적이다. 하지만, Key Infection의 경우는 explicit key authentication을 제공하는 반면 제안하는 scheme은 implicit key authentication을 제공하는 단점이 있다. smart dust network에서 각각의 노드들은 유동성을 가지며, 이에 따라 전체 네트워크는 동적인 topology를 가진다.

Smart dust 노드가 최초 배치되었을 때 노드들은 자신의 이웃한 노드와 pair-wise key를 설정한다. 하지만 실제적인 네트워크 환경에서 노드들은 유동성을 가지고 있기 때문에 최초 배치되었을 때의 pair-wise key를 나누어 가졌던 이웃 노드가 항상 이웃 노드로 존재한다는 보장을 할 수가 없다. 따라서 최초 pair-wise key를 설정할 때 implicit key authentication을 제공하는 것만으로도 충분하다.

Key Infection의 경우는 explicit key authentication을 제공하기위해 2-pass 통신으로 이루어진다. 하지만 위에서 본 듯이 smart dust network환경에서 implicit key authentication을 제공하기는 것만으로도 충분하기에 각 smart dust 노드들은 한 번의 데이터 전송을 통해 효율적인 pair-wise key를 설정할 수 있다.

IV. 결론

본 논문에서는 [1]에서 제시한 현실적인 공격자 모델 아래에서 Key Infection에 비해 communicational cost 와 computational cost 측면에서 효율적인 scheme을 제안하였다.

제안하는 scheme은 매우 효율적이고 현실적인 공격 모델을 고려하고 있으며, Key Infection에 비해 cost측면에서 효율적이므로 실용적인 센서 네트워크 응용에서 다양하게 활용될 것이다.

[참고문헌]

[1] R. Anderson, H. Chan, and A. Perrig, "Key Infection: Smart Trust for Smart Dust," In 12th IEEE International Conference on Network Protocols, pp.206-215, October 2004.

[2] J. M. Kahn, R. H. Katz, and K. S. Pister, "Emerging Challeges: Mobile Networking for 'Smart Dust'," Journal of Communications and Networks, vol. 2, no. 3, pp. 188-196, September 2000.

[3] H. Chan, A. Perrig, and D. Song, "Random key predistribution schemes for sensor networks," In IEEE Symposium on Security and Privacy, May 2003.

[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, pp 41-47, Nov. 2002.

[5] W. Diffie and M. Hellman, "New directions in cryptography," IEEE Transactions on Information Theory, IT-22(6):644-654, Nov. 1976.

[6] R. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," Communications of the ACM, 21(2):120-126, Feb. 1978.

[7] A. Perrig, R. Szewczyk, V. Wen, D. Cullar, and J. D. Tygar, "SPINS: Security protocols for sensor networks," In Proceedings of the 7th Annual ACM/IEEE International Conference on Mobile Computing and Networking, pp.189-199, July 2001.

[8] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "A survey on sensor networks," IEEE Communications Magazine, Vol. 40, No. 8, pp.102-114, August 2002.