무선 센서 네트워크에서의 다중 채널을 사용한 안전한 키 설립 방법

유기백° 김종권
서울대학교 컴퓨터공학부
{kbyoo°, ckim}@popeye.snu.ac.kr

Secure Key Establishment Scheme using Multi-Channel in Wireless Sensor Networks

Kibaek Yoo, Chongkwon Kim
School of Computer Science and Engineering, Seoul National University

요 약

무선 센서 네트워크의 사용이 증가함에 따라, 센서 네트워크의 보안에 대한 연구가 중요한 이슈가 되고 있다. 그 중 센서 노드들 사이의 키 설립 방법에 대한 연구가 매우 활발히 진행되었으며, 그에 따라 다양한 연구 결과들이 제시되었다. 하지만 기존의 연구 결과들은 강력한 보안성을 제공하기는 하나 키 설립과정이 매우 복잡하기 때문에 현실적으로 이용되기에는 어렵다는 단점이 있다. 즉, 이는 실제 센서 노드에 대한 구현을 어렵게 하며, 다양한 응용 분야에서 요구하는 보안성의 제공 역시 보장하지 못한다.

이에 본 연구에서는 다중 채널을 사용한 간단한 키 설립 방법을 제시하였다. 제시된 방법은 필요한 저장 공간과 통신 횟수, 계산 횟수를 최소화 한 반면, 다중 채널을 사용함으로서 보안성은 강화하였다. 이는 다양한 분야에서 제시된 방법이 활용될 수 있음을 의미한다. 1장의 서론에 이어 2장에서는 관련연구를 설명한다. 3장에서는 배경지식을 설명하고 4장에서 제안한 프로토콜을 설명한다. 마지막으로 5장에서는 분석을 통하여 이를 증명한다.

1. 서 론

무선 센서 네트워크의 사용이 증가함에 따라, 센서 네트워크 보안의 중요성에 대한 관심 역시 증가하고 있다. 이에 따라 센서 네트워크의 보안 기술에 대한 많은 연구가 최근 몇 년간 활발하게 진행되어 왔다. 그러나 센서 네트워크에서의 보안 문제는 기존의 유선 통신 네트워크뿐만 아니라, 무선 통신 네트워크의 보안 문제와도 접근방법이 크게 다르다. 그 이유는 센서 네트워크만이 가지고 있는 다음 특징 때문이다.

· 센서 노드는 자원이 제한적이다 : 센서 노드는 일반 PC와 비교하여 연산속도, 저장 공간, 통신 파워와 전송 대역폭, 소모 에너지 등에서 극히 제한된 자원만을 가지고 있다.

· 네트워크 규모가 매우 광범위하다 : 일반적으로 센서 네트워크는 수천~수만 개의 센서 노드들이 매우 광범위한 지역에 자유롭게 분포된다.

· 물리적인 공격방법이 존재 한다 : 센서 노드는 매우 작고 숫자가 많으며, 응용 분야에 따라 위험 지역이나 적군 지역과 같은 네트워크 관리자의 손이 닿지 않는 곳에 뿌려지는 경우가 많다. 이는 공격자가 물리적인 방법을 통하여 노드 안에 저장되어 있는 정보를 알아내고, 합법적인 노드인 것처럼 가장하여 네트워크 안에서 공격하는 것을 가능하게 해 준다.

· 토폴로지를 예측할 수 없다 : 일반적으로 센서 노드는 넓은 지역에 비행기나 헬리콥터 등을 이용하여 분포된다. 이는 노드의 개수와 통신 거리, 장애물 등에 의해 토폴로지가 랜덤하게 정해진다는 것을 의미한다.

위와 같은 특징들로 인해 효율적인 키 생성 방법에 대한 연구는 센서 네트워크 보안에서도 가장 중요한 이슈이다. 이론적으로는 단 하나의 공통된 키를 이용하여 모든 노드들이 통신이 가능하다. 하지만 이 경우 단 하나의 노드만 공격자에 의해 노출 되어도 모든 노드들의 키가 노출된다. 반대로 모든 노드들이 각각 고유한 키를 공유할 경우 통신하고자 하는 노드의 개수만큼의 키를 저장하고 있어야 한다. 이것은 센서 노드의 제한된 저장 공간을 생각할 때 매우 비효율적이다. 따라서 기존의 많은 연구들이 이 양 극 사이를 절충할 수 있는 다양한 키 생성 프로토콜을 제안하였는데, 대부분의 연구결과들은 대칭 키를 1-hop 떨어진 이웃들 간에 분배하는 방식을 선택하고 있다. [1,2,3,4,5]

그러나 기존에 제시된 대부분의 키 설립 방법들은 강력한 보안성을 제공하기는 하나, 키 설립 과정이 너무 복잡하여 센서 네트워크 전체의 성능과 수명을 저하시킬 수 있으며, 실제로 구현하여 적용시키기 어렵다는 문제점이 존재한다.

또한 센서 네트워크는 매우 다양한 분야에 활용될 수 있으며, 이는 각 분야에 따라 요구하는 보안 수준이 다를 수 있다는 것을 의미한다. 예를 들어 위험지역이나 군 관련 분야와 같은 강력한 보안을 필요로 하는 분야도 있는 반면, 홈 네트워크의 가정 내부와 주변의 온도, 습도, 조도 모니터링과 같이 보안이 크게 중요하지 않는 분야도 있다. 그리

고 후자의 경우 기존의 복잡한 키 설립 방법들을 사용하는 것은 매우 큰 과부하가 될 것이다.

이에 본 연구에서는 매우 간단한 키 설립 방법을 제안하였다. 이 방법은 기존의 연구들에 비해 적은 저장 내용, 통신 횟수와 계산 횟수를 요구한다. 또한 다중 채널을 사용하여 키 설립 방법의 복잡성에 비해 높은 보안성을 제공함으로서 다양한 분야에서 활용될 수 있도록 하였다. 그리고 키 설립 방법에 대한 자세한 설명과 분석을 통하여 이를 증명하였다.

2. 관련연구

[1]에서는 센서 노드가 분포되기 전에, 노드에 키 생성에 필요한 정보를 미리 저장하는 키 설립 방법을 제시하였다. 센서 노드는 분포되기 전에 master key pool에서 랜덤하게 일정수의 키를 선택하여 저장한다. 센서노드는 분포된 이후 자신이 소유한 몇 개의 키 중에 자신의 이웃 노드와 공통된 키를 하나라도 가지고 있다면 그 키를 사용하여 안전하게 통신할 수 있다. [2]에서는 [1]의 방법을 확장한 q-composite라는 방법을 제시하였다. 각 노드는 하나의 공통된 키가 아닌, 최소한 q개의 공통된 키를 가지고 있어야 키 설립이 가능하다. 이 방법은 기존 연구에 비해 보안성을 증가시킬 수가 있지만, 센서 노드에 저장되어야 하는 정보가 많아질 수가 있으며, 네트워크 연결성이 떨어질 수가 있다. [3]에서는 polynomial을 사용한 키 설립 방법을 제시하였다. 이 방법은 [1]과 유사하지만 key pool 대신에 polynomial pool을 사용한다. 가장 최근의 연구인 [4]에서는 다중채널을 이용한 키 설립 방법을 제시하였다. 각 노드는 다중채널을 사용하여 미리 저장되어 있던 유일한 키들을 원본으로 브로드캐스트한 후, 서로 공통적으로 가지고 있는 키들을 사용하여 키 설립을 할 수 있다.

위에서 제시된 방법들은 모두 강력한 보안성을 제공한다. 그러나 사전에 저장되어야 하는 정보가 많거나, 키 설립 과정이 너무 복잡하며, 추가적으로 배치되는 센서 노드와의 키 설립을 위해 유지해야 하는 정보의 양이 많다는 등의 단점들도 존재한다. 이는 사용할 수 있는 자원이 극히 제한된 센서 노드에 있어서 과부하가 되며, 실제 구현이 어려울 수도 있다.

[5]는 본 연구의 기초가 된 연구로서 매우 간단한 키 설립을 통하여 센서 노드에 대한 과부하를 최소화 하였다. 그러나 [5]는 키 설립 과정이 동작하는 동안 공격자의 수가 극히 적을 경우에만 보안성이 보장된다는 단점이 존재한다. 본 연구는 다중채널을 사용함으로서 키 설립 방법의 간결성을 유지하면서도 동시에 공격자의 수가 증가하더라도 일정 수준 이상의 보안성을 제공하는 키 설립 방법을 제시한다.

3. 배경지식

3.1 Key Infection

R. Anderson, H. Chan 그리고 A. Perrig는 [5]를 통하여 매우 간단한 키 설립 방법을 제시하였다. 이 연구에서는 센서 네트워크의 사용 용도에 따라 요구되는 보안 수준이 다르며, 센서 노드들이 분포된 초기에는 공격자에 의한 공격방법이 매우 제한적이라고 가정하였다. 먼저 노드 i와 j가 존재하며 서로가 전송범위 안에 있다고 한다. 센서 노드가 분포된 직후, 노드 i는 키 k_i를 만들어 브로드캐스트 한다. 이를 받은 노드 j는 $\{j,k_{ij}\}_{ki}$를 통하여 노드 i에게 응답한다. 이 때 $\{\}_k$는 {}안의 내용을 키 k로 암호화 하였다는 것을 의미하며, k_{ij}는 노드 i와의 통신을 위하여 노드 j가 임의로 생성한 키이다. 이 과정 이후 노드 i와 j는 키 k_{ij}를 통하여 안전하게 통신할 수 있다.

3.2 네트워크 모델

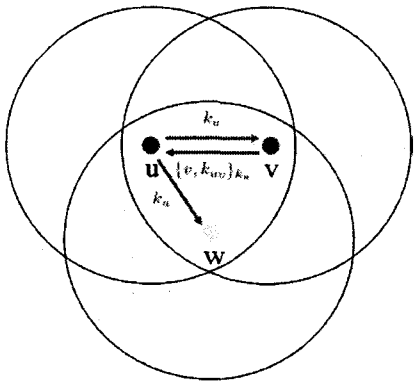
센서 노드들은 특정 지역에 랜덤하게 분포된다고 가정한다. 이 때, 센서 노드들은 충분히 밀집되어 있으며, 전송 범위는 약 10m 정도이다. 따라서 한 노드 입장에서 여러 개의 이웃 노드들이 존재한다.

센서 노드는 키 설립이 안 될 경우를 대비한 표준 채널을 포함한 여러 개의 채널 중 하나를 사용할 수 있으며, 원하는 때에 채널 변경이 가능하다고 가정한다.

3.3 공격 모델

센서 노드들이 분포된 직후의 일정한 짧은 기간 동안에는 공격자에 의한 공격이 극히 제한적이라고 가정한다. 이 시간동안 1. 공격자는 센서 노드에 대한 물리적 공격이 불가능하다. 2. 분포 지역에 미리 배치되어 있던 공격 노드들에 의한 도청이 가능하다. 이 때 공격 노드들은 분포되는 센서 노드들과 성능이 비슷하다. 3. 공격 노드들은 도청 이외의 키 설립 과정에 참여하거나 거짓 정보의 플러딩 공격과 같은 다른 적극적 공격이 불가능하다. 이 기간이 지난 이후 공격자는 어떠한 공격 방법도 사용할 수 있다.

4. 프로토콜 설명



(그림 1)

먼저 노드들은 느슨하게 동기화되어 있다고 가정한다. 각 노드는 사용할 수 있는 채널 중 하나를 랜덤하게 선택한다. 그리고 키를 하나 생성하여 브로드캐스트 한다. 이 때 충돌을 피하기 위하여 CSMA/CA나 타이머 사용과 같은 방법을 택한다. (그림 1)을 예로 들어본다. 노드 u는 임의로 키 k_u를 생성한 후 브로드캐스트 한다. 이를 수신한 이웃 노드들은 이에 대한 응답 메시지를 전송한다. 노드 v와 노드w는 노드u의 이웃 노드이다. v는 u와 같은 채널을 선택하여 v가 브로드캐스트한 메시지를 수신하였으며, w는 다른 채널을 선택하여 수신하지 못하였다. v는 u에게 u와 사용할 키 k_{uv}를 생성하고, 여기에 자신의 아이디를 포함하여 메시지를 만든다. 그리고 이것을 u에게서 받은 키로 암호화 한 후 u에게 유니캐스트 한다($\{v, k_{uv}\}_{k_u}$). 반면 w는 메시지를 수신하지 못하였으므로 그에 대한 응답을 수행할 수 없다.

모든 노드들이 메시지를 브로드캐스트하고 응답을 받을 수 있는 충분한 시간이 지난 후, 각 노드는 다시 채널들 중 하나를 랜덤하게 선택한다. 그리고 위의 키 교환 과정을 반복한다. 이 때, 이미 두 노드 사이의 키 설립이 완료된 경우에는 메시지를 수신하여도 그에 대한 응답을 수행하지 않는다. 노드 u를 보자. u는 새로운 키 k_u'를 생성하여 브로드캐스트 한다. 이번에는 v와 w 모두가 u가 브로드캐스트한 메시지를 수신하였다고 하자. v는 u와 이미 키 설립이 완료되었으므로, 수신한 메시지에 대한 응답을 보내지 않는다. 반면 w는 u와의 키 설립이 완료되지 않았으므로, $\{w, k_{uw}\}_{k_u}$ 로 응답 한다.

총 사용채널의 개수만큼 위의 과정을 수행한 후에도 키 설립이 안 된 경우, 각 노드는 사전에 정해진 표준 채널(default channel)을 통하여 키 설립 과정을 수행한다. 이는 채널의 개수가 증가할 경우 감소할 수 있는 네트워크 연결성을 보장하기 위해서이다. 이 과정을 마지막으로 프로토콜의 수행이 완료된다.

다음 장에서는 분석을 통하여 여러 개의 채널을 사용하는 것이 보안성 증가에 도움이 된다는 것을 증명한다.

5. 분석

본 장에서는 먼저 공격 방법을 공격 노드들이 연합하는 경우와 연합하지 않는 경우 두 가지로 나누었다. 그리고 각 경우에 대해 공격 노드에 의해 키가 노출될 가능성을 upper bound에 대해 계산하였다.

키 설립 과정이 끝난 이후 공격자가 공격을 시작한다면, 본 연구에서 제공된 프로토콜은 키 설립에 대해 완벽한 보안성을 보장한다. 여기서는 공격자가 합법적인 센서 노드가 특정지역에 분포되기 전에, 미리 해당 지역에 공격 노드를 랜덤하게 분포해 놓았으며, 표준 채널에 사용되는 채널에 대해 알고 있다고 가정한다. 이 때, 센서의 평균 전송 거리는 r, 센서 노드가 분포될 지역의 넓이는 s, 공격 노드의 개수는 n, 채널의 개수는 c로 나타낸다.

5.1 키 설립 가능성

먼저 키 설립 가능성을 계산해보자. 한 노드가 이웃 노드가 전송한 정보를 듣지 못할 확률은 $1-(1/c)$ 이다. 따라서 표준 채널을 사용하기 전까지 키를 설립하지 못할 확률을 p_c라 하면 p_c는 (1)번식으로 나타낼 수 있다.

$$p_c=(1-\frac{1}{c})^c \qquad (1)$$

<표 1>은 채널 개수에 따른 키 설립 가능성을 나타낸다. 채널의 수가 증가할수록 키 설립 가능성이 낮아지므로 이를 통하여 표준 채널의 필요성을 유추할 수 있다.

<표 1>

c	p_c
1	0
2	0.25
3	0.296
4	0.316
5	0.327

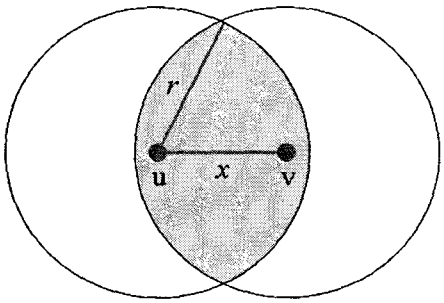
5.2 공격 노드가 연합하는 경우

먼저 공격 노드가 도청할 수 있는 최대 영역을 계산하면 $\pi r^2 n$으로 나타낼 수 있다. 이 때 키가 노출되기 위해서는 공격 노드 역시 키 설립에 참여한 노드들과 같은 채널을 사용해야 한다. 따라서 공격 노드에 의해 키가 노출될 확률은 $\pi r^2 n/sc$ 이다. 따라서 공격 노드에 의해 키가 노출될 확률을 p_a 라 하면 p_a는 (2)번식으로 나타낼 수 있다.

$$p_a=(1-p_c)^{\frac{\pi r^2 n}{sc}}+p_c\frac{\pi r^2 n}{s} \qquad (2)$$

이는 다중 채널을 사용하지 않았을 경우에 비해 최대 $(1-p_c)$c배 정도의 보안성이 향상된다는 것을 보여준다.

5.3 공격 노드가 연합하지 않는 경우



(그림 2)

공격 노드가 연합하지 않는 경우, 키가 노출되기 위해서는 공격 노드가 반드시 두 노드의 겹쳐지는 전송 범위에 위치하고 있어야 하며, 키 설립 당시의 두 노드와 같은 채널을 사용하고 있어야 한다. (그림 2)를 예로 들어 본다. x는 두 노드 사이의 거리를 나타낸다. 그림에서 어두운 부분이 노드 u와 노드 v의 전송 범위 중 겹쳐지는 부분이다. 이 부분을 $S(x)$라고 하자. 이 때 $S(x)$의 계산은 (3)번식과 같다.

$$2r^2\cos^{-1}\left(\frac{x}{2r}\right)-x\sqrt{r^2-\frac{x^2}{4}} \qquad (3)$$

두 노드 사이의 거리에 대한 확률 분포 함수는 $F(x)=x^2/r^2$ 이고, 확률 밀도 함수는 $f(x)=F'(x)=2x/r^2$이다. 이를 통하여 겹쳐지는 부분의 예측 넓이를 계산하면 (4)번식과 같다[2].

$$\int_0^r S(x)f(x)dx=\left(\pi-\frac{3\sqrt{3}}{4}\right)r^2=0.586\pi r^2 \qquad (4)$$

따라서 (2)의 식에 πr^2에 $0.586\pi r^2$을 대입하면 키가 노출될 확률을 계산할 수 있다. 그 확률을 p_b라 하면 p_b는 (5)번식으로 나타낼 수 있다.

$$p_b=(1-p_c)^{\frac{0.586\pi r^2 n}{sc}}+p_c\left(\frac{0.586\pi r^2 n}{s}\right) \qquad (5)$$

6. 결론

본 연구에서는 다중 채널을 사용한 안전한 키 설립 방법을 제시하였다. 이는 기존에 제시된 키 설립 방법들에 비해 매우 간단하며, 키 설립에 따른 과부하가 적다. 따라서 이 방법은 높은 보안 수준을 요구하지 않는 센서 네트워크 분야에 적용하여 활용할 수 있을 것이다.

참고 문헌

[1] L. Eschenauer and V. D. Gligor, "A Key-Management Scheme for Distributed Sensor Networks," in *ACM Computer and Communication Security (CCS) 2003*, October 2003

[2] H.Chan, A. Perrig, and D. Song, "Random Key Predistribution Schemes for Sensor Networks," in *IEEE Security and Privacy Symposium 2003*, May 2003

[3] D.Liu and P. Ning, "Establishing Pairwise Keys in Distributed Sensor Networks," in *ACM Computer and Communication Security (CCS) 2003*, October 2003

[4] J. Miller and H. Vaidya, "Leveraging Channel Diversity for Key Establishment in Wireless Sensor Networks," in *IEEE INFOCOM 2006*, April 2006

[5] R. Anderson, H. Chan and A. Perrig, "Key Infection: Smart Trust for Smart Dust," in *IEEE International Conference on Network Protocols (ICNP) 2004*, October 2004