무선 센서 네트워크에서의 향상된 키 분배 기법*

조정식° 여상수 김성권
중앙대학교 컴퓨터공학부
{mfg°, ssyeo}@alg.cse.cau.ac.kr, skkim@cau.ac.kr

Enhanced Key Distribution Scheme in Wireless Sensor Networks

Jung-Sik Cho° Sang-Soo Yeo Sung Kwon Kim
School of Computer Science & Engineering, Chung-Ang University

요 약

무선 센서 네트워크는 방대한 응용분야와 유비쿼터스 환경 하에서 중요한 한 부분을 차지하며 그 유용성을 입증하고 있다. 이런 무선 센서 네트워크의 센서 노드는 작은 크기를 바탕으로 목표 장소에 임의로 배치되어 다양한 데이터를 수집하는 능력이 탁월하다. 하지만 이런 장점은 센서 노드의 한정된 하드웨어 능력과 전원공급 문제, 물리적 노출 문제로 인해 스스로를 위험에 노출시키는 여지를 만들게 되었다. 즉 일반적으로 사용되어지는 네트워크 보안 방법을 무선 센서 네트워크에 적용하기에는 센서 노드 능력에 한계가 있으며, 환경적 요소로 인해 불가능하다. 따라서 무선 센서 네트워크의 특성을 감안한 효과적인 보안 방법이 필요하며, 이런 맥락에 본 논문은 무선 센서 네트워크의 하드웨어적인 한계를 감안한 대칭키(symmetric key) 기반의 키 분배 기법을 제안하고자 한다. 제안하는 기법에서는 모든 노드가 공통으로 소유한 전체 마스터 키(master key) 와 의사 난수 생성기(pseudo random number generator:PRNG), 그리고 특정 대상으로부터 분배되는 난수(random number)의 조합을 통해 임의의 키를 생성, 갱신함으로써 다양한 종류의 무선 센서 네트워크 모델에 유연하게 대처할 수 있도록 하였다. 또한 이를 위한 통신 회수를 최소화함으로써 효율성을 제공해 준다.

1. 서 론

"임의의 대상 혹은 환경으로 부터 수집된 다양한 데이터를 이용하여 인간에게 유용한 정보를 제공해준다." 이는 무선 센서 네트워크에서 추구하는 궁극적인 목표라 할 수 있다. 이를 위해서 작은 센서 노드들은 목표 대상 혹은 장소에 임의로 설치되고 자체적인 알고리즘을 통해 센서 네트워크를 형성한다. 무선 센서 네트워크를 통해 수집된 데이터들은 안전하고 믿을 수 있는 중앙 노드인 베이스 스테이션(Base station)으로 무선 통신을 통해 전달되어 인간에게 유용한 정보를 제공해 준다.

어떤 정보라도 그 정보를 생성함에 있어서 제공 되어지는 데이터는 정확하고 신뢰 되어야 한다. 마찬가지로 무선 센서 네트워크는 정확하게 데이터를 수집하고, 베이스 스테이션으로 안전하게 전달해줘야 한다.

만약 악의를 가진 공격자에 의해 전송되어지는 데이터의 유출 및 위/변조는 심각한 문제를 야기할 수 있다. 이러한 이유로 무선 센서 네트워크는 보안을 위해 통신의 암호화와 인증이 요구되어 진다. 이때 사용되어지는 암호화와 인증 방법은 키 방식에 따라 대칭키(symmetric key)방식과 비대칭키(asymmetric key)방식으로 나눌 수 있다. 하지만 센서 노드는 소형이라는 가장 큰 특징이면서 단점으로 인해 에너지와 계산능력, 통신능력 면에서 한계를 가지고 있다. 따라서 상대적으로 많은 양의 계산이 필요한 비대칭키 기반의 암호화 방식은 적용되기 어렵다. 현재 무선 센서 네트워크에서는 대칭키 기반의 암호화 방식이 활발히 연구되어 지고 있다.

대칭키 기반의 암호화 방식을 사용함에 있어서 가장 중요한 부분은 키 관리 문제이다. 키 생성부터 시작하여 분배, 갱신에 이르기까지 모든 부분들이 신뢰되어지고 안전하게 이루어져야 한다.

따라서 우선 본 논문은 기존에 연구되어진 무선 센서 네트워크에서 대칭키 기반의 키 관리 프로토콜인 G. Jolly의 논문[4]과 A. Perrig의 "SPINS"[1] 논문을 살펴보고 그 장단점을 분석하고, 나아가 향상된 키 분배 관리 기법을 제안하고자 한다.

또한 무선 센서 네트워크에서 중요한 고려사항 중 하나는 무선 센서 네트워크의 형태, 즉 무선 센서 네트워크 모델에 따라 키 관리 프로토콜이 상이하게 달라진다는 점이다. 본 논문에서는 이를 감안하여 특정 모델에 구애받지 않는 좀 더 유연한 키 관리 기법을 제안하고자 한다.

2. 관련 연구

무선 센서 네트워크는 군사, 환경, 가정, 의료, 상업 등 그 응용 분야에 있어서 매우 다양하며 그에 따른 요구 사항도 다양하다. 그러므로 무선 센서 네트워크가 어느 분야에 사용되고 어떤 요구 사항을 충족 하느냐에 따라 그 형태, 즉 무선 센서 네트워크 모델이 정해진다. 무선 센서 네트워크 모델은 구성원에 있어서 차이를 보인다. 센서 노드와 수집된 데이터가 모아지는 신뢰할 수 있는 중앙 노드인 베이스 스테이션이 기본 구성원이다. 이후 클러스터 형성 유무와 클러스터 헤드의 선출 방법에 따라 센서 네트워크 모델이 달라진다. 이렇게 센서 네트워크 모델이 다양하다 보니 현재 제안되어지고 있는 무선 센서 네트워크에서의 키 관리 프로토콜도 그 모델에 맞게 설계되고 다양한 방향으로 진행되어지고 있다. 결국 그 궁극적인 목적은 무선 센서 네트워크의 특성을 고려한 안전하고 효율적인 키 관리 프로토콜 개발이다.

본 장에서는 G. Jolly의 논문[4]과 A. Perrig의 논문[1] 을 분석하여 각 센서 네트워크 모델에 따른 키 관리 프로토콜과 그 장단점을 살펴보도록 하겠다.

2.1 G. Jolly의 논문

이 논문은 그림1과 같이 M. Younis[2] 이 제안한 네트워크 모델을 바탕으로 키 관리 프로토콜을 설계하였다.

* 본 연구는 한국과학재단 특정기초연구 (R01-2005-000-10568-0) 지원으로 수행되었음

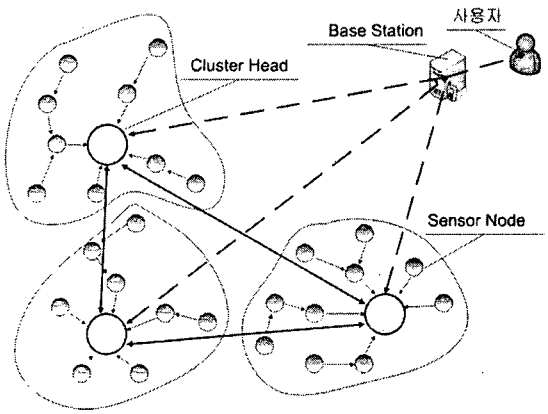

그림 1. M. Younis 이 제안한 네트워크 모델

이 논문에서 제안하는 키 관리 프로토콜은 무선 센서 네트워크에서 각 센서 노드에 키를 분배하는 방법 중 Identity Based Symmetric Keying(IBSK)[5]을 확장하고 있다. 즉 베이스 스테이션이 각 센서 노드의 ID를 기반으로 키를 유지, 분배하는 방법을 사용하고 있다. 이러한 G. Jolly 프로토콜의 장점은 다음과 같이 열거 할 수 있다.

- 센서 노드에게 최소의 통신 횟수만으로 키를 수립하고 있다는 점에서 에너지 효율면에서 높은 성능을 보여주고 있다.
- 노드의 추가, 폐기와 키의 갱신을 제공해줌으로써 노드의 물리적인 위험으로 부터의 복원력을 제공해주고 있다.

하지만 이에 반하여 다음과 같은 단점을 가지고 있다.

- 키의 종류가 단순하다는 한계점이 있다. 즉 다양한 통신 모델을 지원해주지 않고 있다.
- 게이트웨이 노드들이 키를 교환한다는 점에서 도청을 통한 키 정보 유출의 위험성이 존재하고 있다.
- 암호화를 통한 키 정보의 은익은 제공하고 있으나 이에 대한 인증을 제공해주지 못하고 있다.

즉 G. Jolly의 논문은 센서 노드의 하드웨어적인 면에 있어서 에너지 측면과 물리적인 위험을 고려한 훌륭한 프로토콜이지만 좀 더 다양한 통신 모델과 신뢰할 수 있는 통신을 제공해 주지 못하고 있다.

2.2 A. Perrig의 "SPINS"

이 논문은 SNEP(Sensor network Encryption Protocol) 과 μTESLA라는 두가지 Secure building block으로 이루어져 있다. 이중 SNEP 은 1 : 1 통신을 기본으로 데이터 기밀성, 통신자간 데이터 인증, 무결성을 제공해준다.

SNEP 은 센서 노드들이 설치 전 통신 당사자 간만의 공통된 마스터 키를 가지고 있다. 이를 바탕으로 다음과 같이 의사 난수 생성 함수 $F_K(x)$를 통해 각 노드는 키들을 생성하게 된다.

$$X_{AB} \Rightarrow \begin{cases} K_{AB} = F_{X_{AB}} \\ K'_{AB} = F_{X_{AB}} \\ K_{BA} = F_{X_{AB}} \\ K'_{BA} = F_{X_{AB}} \end{cases}$$

각 노드는 생성된 키 K_{AB}, K_{BA}를 통해 서로 암호화와 복호화를 수행하고 K'_{AB}, K'_{BA}를 통해 MAC을 생성, 검증을 수행한다.

SPINS의 장점들은 다음과 같이 나열할 수 있다.

- 마스터 키와 의사 난수 생성 함수를 통해 키를 만들어 냄으로써 키의 교환이 필요 없다. 이는 키 생성과 분배에 있어 키의 직접적인 이동이 없다는 점에서 안전한 방법이라 할 수 있다.
- 생성된 키를 바탕으로 데이터 기밀성과 MAC을 통한 두 노드간 데이터 인증, 무결성을 제공해준다.

이에 반해 SPINS의 단점은 다음과 같이 논할 수 있다.

- SPINS 역시 통신 모델이 다양하지 못하다.
- 정보의 유출과 센서 노드의 물리적인 위험부터 복원할 수 있는 방법, 즉 노드의 폐기, 추가, 키 갱신을 제공해주지 않고 있다.
- 키 생성이 단순하다. 즉 매개변수가 단순하여 마스터 키의 유출로 인해 통신에 사용되어지는 키들이 쉽게 노출될 수 있다.

3. 제안 키 분배 기법

본 논문은 특정 무선 센서 네트워크 모델을 구애받지 않고 그림 2와 같이 추상적인 네트워크 모델을 설정한다.

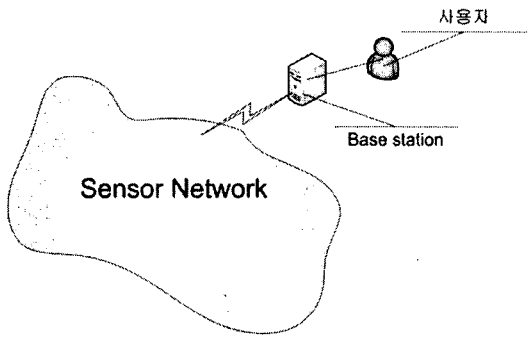

그림 2. 추상적 네트워크 모델

표 1은 본 논문에서 사용되어질 무선 센서 네트워크를 구성하는 기본적인 요소와 사용되는 수식에 대한 표기이다.

이 가정과 표기를 바탕으로 다음과 같은 가정을 추가한다.

- 모든 센서 노드는 자신의 ID number를 알고 있고 설치

표 1. 표기 설명

표기법	설명
B	Base Station
S	모든 Sensor node Group
S_i	Sensor node i
$ID_i\#$	sensor node ID number
N	Random number
$F_K(x)$	K를 키로 사용하고 x를 매개 변수로 하는 Pseudo Random Number Generator
K_M	전체 Master Key
K_{MAC}	전체 MAC Key

전 K_M과 K_{MAC} 그리고 $F_K(x)$을 저장한다.

- 키 관리를 위해 이루어지는 모든 통신은 암호화 하고 MAC 을 첨가하여 비밀성과 인증을 제공해준다.
- 공식 (1) 을 통해 각 센서 노드들은 자신의 개인 마스터 키와 공식 (2) 를 통해 개인 MAC 키를 생성하고 저장한다.

$$F_{K_M}(i) = K_{M_i} \quad \text{공식 (1)}$$

$$F_{K_{MAC}}(i) = K_{MAC_i} \quad \text{공식 (2)}$$

- 베이스 스테이션은 전체 마스터 키 K_M과 각 센서 노드의 아이디 $ID_i\#$, 개인 마스터 키, 개인 MAC키에 대한 정보를 DB에 저장해 둔다.

이를 바탕으로 각 센서 노드들은 그 응용분야에 적합한 형태로 설치되어지고 무선 센서 네트워크를 형성하게 된다.

본 논문이 제안하고자 하는 부분은 이때 어떤 형태의 네트워크 모델을 사용하더라도 실제 통신에 사용되어질 키들은 각 노드들이 가지고 있는 의사 난수 생성기와 각 마스터 키, 그리고 난수의 조합을 통해 생성하자는 것이다.

네트워크 모델에 따른 통신의 형태는 다양하나 크게 나누면 1:1 통신 혹은 지역적, 그룹 형태의 통신으로 나눌 수 있다. 이때 통신에 사용되어질 키와 MAC 키를 생성하기 위해 공식 (3),(4) 같이 난수를 이용하게 된다.

$$F_{K_M}(N) = K_{S,S,} \quad \text{공식 (3)}$$

$$F_{K_{MAC}}(N) = K_{MAC_{S,S,}} \quad \text{공식 (4)}$$

여기서 사용되어지는 난수는 두 가지 방법을 통해 각 센서 노드들에게 분배 될 수 있다. 첫 번째 방법은 통신에 참여하는 센서 노드 간 협의를 통해 분배할 될 수 있으며, 두 번째 방법은 신뢰되어지는 노드 즉 베이스 스테이션을 통해 분배될 수 있다. 이렇게 함으로써 키의 생성에 있어 네트워크 모델에 구애 받지 않고 유연하게 대처할 수 있으며, 실질적인 키의 이동없이 난수의 분배를 통해 통신에 사용되어질 키를 생성할 수 있다.

키의 갱신에 있어서는 베이스 스테이션이 난수 N을 생성하여 통신 (1) 과 같은 형태로 모든 노드들에게 전달해 주고, 이를 전달 받은 각 노드들은 공식 (5),(6)을 통해 전체 마스터 키와 전체 MAC 키를 갱신, 이후 파생적으로 공식 (1)~(4)를 수행함으로써 모든 키를 갱신 할 수 있게 된다.

$$ID_i\# \| E(K_{M_i}, N) \| MAC(K_{MAC_i}, ID_i\# \| N) \quad \text{통신 (1)}$$

$$F_{K_M}(N) = K_{M_{+N}} \quad \text{공식 (5)}$$

$$F_{K_{MAC}}(N) = K_{MAC_{+N}} \quad \text{공식 (6)}$$

이는 다음과 같은 이점을 가지게 된다.

- 키 정보를 저장하기 위한 부담이 매우 적다.
- 키 수립을 위한 통신 횟수가 현저히 적다.
- 키를 수립하는 과정에 MAC을 사용하여 인증을 제공해주고 있다.

이와 같은 키 관리 기법을 G. Jolly의 논문[4] 적용한 프로토콜이 논문[6]에 제안되어 있다.

또한 본 논문에서는 암호화 알고리즘으로 대칭키 암호화 알고리즘인 RC5 사용을 제안하며, 이를 의사 난수 생성기로도 사용한다. 이렇게 함으로써 센서 노드 안에 암호화 알고리즘을 구현하는데 있어 부담을 덜어 준다.

4. 결론

키의 생성과 갱신에 있어 마스터 키와 의사 난수 생성기 그리고 난수의 조합을 이용함으로써 다양한 무선 센서 네트워크 모델에 대해서 유연성 있게 대처할 수 있으며, 통신 키의 실질적인 이동이 없으므로 도청에 의한 키 유출을 방지할 수 있다. 또한 아무리 많은 센서 노드가 물리적인 위험으로 인한 키에 대한 정보가 유출 되었다 하여도 난수를 모를 경우 센서 네트워크 전체에 피해가 가지 않는다.

5.참고 문헌

[1] A. Perrig, R. Szewczyk, V. Wen, D. Culler, and J. D. Tygar,"SPINS: Security Protocols for Sensor Networks," Wireless Networks, vol. 8, no. 5, pp. 521-534, 2002.

[2]M. Younis, M. Youssef, and K. Arisha, "Energy-Aware Routing in Cluster-Based Sensor Networks," in Proceedings of the 10th IEEE/ACM MASCOTS2002, October, 2002.

[3]G. Gupta, M. Younis, "Performance Evaluation of Load-Balanced Clustering of Wireless Sensor Networks," in the Proceedings of the 10th ICT'2003, February 2003.

[4]G. Jolly, M.C. Kuscu, P. Kokate, and M. Younis, "A Low-Energy Key Management Protocol for Wireless Sensor Networks" in Proceedings IEEE ISCC'03. 2003.

[5]D. Carman, P. Kruus, and B. Matt, "Constraints and approaches for distributed sensor network security," Tech. Rep. 00-010, NAI Labs, September 2000.

[6] 조정식, 여상수, 김순석, 김성권, "무선 센서 네트워크에서 정보보호를 위한 키 관리 프로토콜", 한국정보과학회 2004년 가을 학술발표논문집(A), 제31권 2호, pp. 430~432 ,2004년 10월