# 무선 센서 네트워크에서 정보보호를 위한 키 관리 프로토콜

조정식°*,여상수*, 김순석**, 김성권*
*중앙대학교 컴퓨터공학부,**한라대학교 정보통신공학부
{mfg°*,ssyeo*}@alg.cse.cau.ac.kr, {sskim**}@halla.ac.kr,{skkim*}@cau.ac.kr

# Key Management Protocol for Information Security in Wireless Sensor Networks

Jung-Sik Cho°*, Sang-Soo Yeo*, Soon-Seok Kim**, Sung-Kwon Kim*
*School of Computer Science & Engineering, Chung-Ang University, Seoul, Korea
**School of Information & Communication Engineering, Halla University, Wonju, Korea

**요 약**

무선 센서 네트워크는 특정 관심 대상이나 환경으로부터 데이터를 수집하여 사용자에게 전달해 줌으로써 결정수단이나 연구를 목적으로 이용되어 지기 때문에 효과적인 보안이 요구되어 진다. 기존의 존재하는 많은 네트워크 보안은 센서 노드의 특성상 센서 네트워크에 적용될 수 없다. 본 논문은 이런 센서 네트워크의 특성을 감안하여 대칭키(symmetric key)를 기반으로 한 키(key) 관리 프로토콜을 제안한다. 제안 프로토콜은 키의 직접적인 이동 없이 마스터 키(Master Key), 의사 난수 생성기(Pseudo Random Number Generator:PRNG), 난수(Random Number:RN)의 조합을 통해 임의의 키를 생성함으로써 보안성을 강화함과 동시에, 다양한 통신 모델에서 사용되어지는 키들을 생성하고, 또한 통신 모델의 따라 프로토콜 축소와 확장이 가능하며, 다양한 네트워크 모델에 맞도록 변형이 용이하게 설계되었다. 그리고 센서 노드의 에너지 소비를 감안하여 프로토콜 수행에 필요한 통신회수를 최소화하였다.

## 1. 서 론

무선 센서 네트워크는 특정지역이나 환경으로부터 데이터를 수집하기 위해 해당지역에 다량의 센서 노드들이 임의로 설치되고, 서로 협력하여 자체 알고리즘과 프로토콜을 통해 형성된 네트워크를 말한다.

센서 네트워크로부터 수집된 데이터는 중앙에 신뢰되어지는 노드(base station)로 전송되어 사용자에게 해당 지역의 정보를 제공해 준다. 이때 악의를 가진 공격자에 의해 전송되어지는 데이터의 유출 및 위/변조는 심각한 문제를 야기할 수 있다. 이러한 이유로 센서 네트워크는 보안을 위해 통신의 암호화와 인증이 요구되어 진다.

이를 위해 사용되어지는 키 방식에 따라 대칭키(symmetric key)방식과 비대칭키(asymmetric key)방식으로 나눌 수 있다. 하지만 센서 노드는 에너지와 계산, 통신능력 면에서 한계를 가지고 있어, 상대적으로 많은 양의 계산이 필요한 비대칭키 기반의 암호화 방식은 비효율적이다. 현재 센서 네트워크에서는 대칭키 기반의 암호화 방식이 연구되어 지고 있다.

본 논문은 대칭키를 기반으로 무선 센서 네트워크에서 정보보호를 위한 키 관리 프로토콜을 제안하고자 한다. 제안 프로토콜은 계층적 마스터 키(Master key)와 공통된 의사 난수 생성기(Pseudo Random Number Generator:PRNG) 그리고 계층적 난수(Random Number:RN) 의 조합을 통해 암호화를 위한 키와 메시지 인증 코드(Message Authentication code:MAC)를 위한 키를 생성하며 그 특징은 다음과 같다.

- 통신에 대한 기밀성과 인증을 지원
- RN을 사용함으로써 랜덤 키를 생성
- 다양한 통신 모델을 지원해주며, 통신 모델에 따라 프로토콜의 축소와 확장가능
- 다른 네트워크 모델에 대한 변형이 용이
- 직접적인 키의 이동없이 RN을 통해 새로운 센서 노드의 추가, 폐기, 키 갱신을 제공

본 논문에서는 특정 네트워크 모델[2][3]에 대해 가능한 모든 통신 모델을 지원할 수 있도록 설계하였다.

## 2. 네트워크 모델

적용 네트워크 모델은 Younis 에 의해 제안된 모델[2][3]로써 그림1같이 관심지역에 많은 수의 센서 노드가 설치된다. 하지만 베이스 스테이션과의 위치가 멀리 떨어져 있어 직접적인 통신대신 클러스터 헤드(Cluster Head)가 클러스터링(Clustering) 알고리즘[2][3]을 통해 센서 노드들을 분할,관리하고 클러스터내에 수집된 데이터를 베이스 스테이션에 전송하는 형태를 가지고 있다. 표1은 구성요소의 특징을 나열한 것이다.

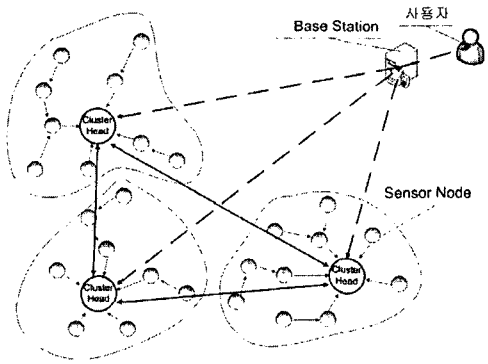


그림 1 네트워크 모델

| Sensor Node | Cluster Head | Base Station |
|---|---|---|
| - 짧은 거리 통신<br>- 클러스터 형성 후 움직이지 않는다.<br>- 특정한 형태를 가지지 않는다.<br>- 다른 sensor 로부터 data 중계 | - 긴 거리의 통신<br>- Cluster 당 하나 존재<br>- 해당 Cluster 내의 sensor node를 다룬다.<br>- Sensor node 보다 energy, hardware 적인 제약이 적다. | - Cluster head 로 부터 받은 data 처리<br>- 외부 network 와 연결<br>- Hardware 적 충분한 power 와 능력 보유 |

표 1 센서 네트워크 구성 요소 특징

### 3. 가정 및 전제

본 논문에서 사용되는 표기법에 대한 설명은 표 2에서 보여 주고 있다.

| 표기법 | 설명 |
|---|---|
| B | Base Station |
| C | 모든 Cluster Head Group |
| $C_i$ | Cluster Head j |
| S | 모든 Sensor node Group |
| $S_i$ | Sensor node i |
| $ID_i\#, ID_j\#$ | sensor node 또는 cluster head 의 ID number |
| N | Random number |
| $F_K(N)$ | Pseudo Random Number Generator |

표 2 표기 설명

i 는 sensor node를 j는 cluster head 를 나타낸다.

- 모든 센서 노드와 클러스터 헤드는 자신의 ID number를 알고 있고 설치 전 $K_M$을 저장한다.
- 프로토콜에서 이루어지는 모든 통신은 암호화하고 MAC 을 첨가하여 비밀성과 인증을 제공해준다.
- 프로토콜에서 이루어지는 bootstrapping 과 클러스터링(clustering)은 [2][3]을 이용한다.

### 4. Key 설명

본 논문에서 제안하는 키들은 모두 마스터 키 $K_M$로부터 의사 난수 생성기(PRF) $F_K(N)$를 이용하여 파생된다. 이때 $F_K(N)$에 어떤 매개변수가 사용되느냐에 따라 파생되는 키가 달라지는데 크게 두 분류로 나눌 수 있다. 첫 분류는 초기 노드 설치 전 각 노드에게 할당되는 $K_M$과 난수 X, 그리고 자신의 ID를 통해 표 3과 같이 생성

| 키 명칭 | 표기 | 생성식 |
|---|---|---|
| master key | $K_M$ | |
| Sensor node master key | $K_{M_i}$ | $F_{K_M}(i) = K_{M_i}$ |
| Cluster Head master key | $K_{M_j}$ | $F_{K_M}(j) = K_{M_j}$ |
| 임시 MAC key | $K_{M_X}$ | $F_{K_M}(X) = K_{M_X}$ |

표 3 계층적 Master Key

되는 계층적 개인 마스터 키와 임시 MAC 키가 되겠다.

두 번째 분류는 베이스 스테이션으로부터 전송된 난수

| 통신 모델 | 암호화 키 | MAC key |
|---|---|---|
| B to all node (broadcasting key) | $F_{K_M}(N_B+1) = K_B$ | $F_{K_M}(N_B+2) = K_{MAC_B}$ |
| B to S (1:1) | $F_{K_{M_i}}(N_B) = K_{BS_i}$ | $F_{K_{M_i}}(N_B+1) = K_{MAC_{BS_i}}$ |
| B to C (1:1) | $F_{K_{M_j}}(N_B) = K_{BC_j}$ | $F_{K_{M_j}}(N_B+1) = K_{MAC_{BC_j}}$ |
| C to S (1:1) | $F_{K_{M_i}}(N_{B_j}) = K_{C_jS_i}$ | $F_{K_{M_i}}(N_{B_j}+1) = K_{MAC_{C_jS_i}}$ |
| C to all S (cluster key) | $F_{K_M}(N_{B_j}) = K_{C_jS}$ | $F_{K_M}(N_{B_j}+1) = K_{MAC_{C_jS}}$ |
| C to C (1:1) (session key) | $K_{C_iC_j}$ | $K_{MAC_{C_iC_j}}$ |
| C to all C (cluster group key) | $F_{K_M}(N_B+3) = K_{CG}$ | $F_{K_M}(N_B+4) = K_{MAC_{CG}}$ |
| S to S(1:1) (session key) | $K_{S_iS_j}$ | $K_{MAC_{S_iS_j}}$ |

표 4 통신 모델에 따른 key 와 MAC key

를 통해 생성되는 키들이다. 각 노드에게는 $N_B$, $N_{B_j}$가 전송된다. $N_B$는 모든 노드에게 똑같이 전송되는 난수이며 $N_{B_j}$클러스터 단위로 전송된 난수이다. 이렇게 계층적으로 전송된 난수는 각 노드가 가지고 있는 $K_M$과 개인 마스터 키, $F_K(N)$의 조합으로 표4와 같이 각 통신 모델에 사용될 키와 MAC키를 생성한다.

### 5. 제안 Protocol

전체 프로토콜은 초기 수립 과정, 세션 수립, 노드 추가, 삭제, 키 갱신으로 구성되어 있으나 본 논문에서는 초기 수립 과정만을 논하겠다.

프로토콜에서 이루어지는 키생성 방법은 표4 를 참조한다. 센서 노드 설치 전 센서 노드와 클러스터 헤드는 마스터 키 $K_M$ 을 미리 저장한 후 각자 자신의 마스터 키 $K_{M_i}$, $K_{M_j}$와 임시 MAC 키 $K_{M_X}$를 생성한다.(표 3참조) 다음은 센서 노드가 설치되고 클러스터 헤드가 배치된 후 프로토콜 과정이다.

#### 5.1 초기 수립 과정

[Step 1]. bootstrapping 과정[2][3] 으로써 초기 설치된 모든 센서 노드들은 자신의 위치를 브로드케스팅을 통해 인접 클러스터 헤드에게 알린다.

S -> C : $ID_i\#\|E(K_{M_i}, N_i)\|MAC(K_{M_X}, ID_i\#\|N_i)$

[Step 2]. Clustering[2][3]과정으로써 각 클러스터 헤드는 Step 1을 통해 수집된 센서 노드의 위치를 바탕으로 다른 클러스터 헤드와 조율하여 최소 통신비용 위주로 클러스터링한다.

[Step 3]. 클러스터 헤드는 수집된 센서 노드의 ID를 통해 각 센서 노드의 마스터 키의 집합 $\{K_{M_i}\}$을 생성, 센서 노드로부터 수신된 메시지를 복호화하고 MAC을 인증한다.

[Step 4]. 클러스터 헤드는 수집된 센서 노드의 ID가 유효한 ID인지 확인하기 위해 베이스 스테이션에게 보낸다.

C -> B :

$ID_j\#\|E(K_{M_j}, \{ID_i\#\}\|N_j)\|MAC(K_{M_X}, ID_j\#\|\{ID_i\#\}\|N_j)$

[Step 5]. 베이스 스테이션은 클러스터로부터 받은 센서 노드의 ID를 확인한다.

[Step 6]. 센서 노드, 클러스터 헤드 모두에게 보내질 난수 $N_B$ 와 각 클러스터 마다 다르게 보내질 난수 집합{ $N_{B_i}$}을 생성하여 각각을 각 클러스터 헤드에게 보낸다.

B -> $C_i$ :

$E(K_{M_i}, N_B \| N_{B_i}) \| MAC(K_{M_x}, N_i \| N_B \| N_{B_i})$

[Step 7]. 각 클러스터 헤드는 수신한 난수 $N_B$ 와 $N_{B_i}$ 를 통해 통신에 필요한 키들을 생성한다.

[Step 8]. 각 클러스터 헤드는 자신의 클러스터에 존재하는 모든 센서 노드에게 난수 $N_B, N_{B_i}$ 를 전송한다.

C -> S :

$ID_i \# \| E(K_M, ID_i \# \| N_B \| N_{B_i}) \| MAC(K_{M_x}, ID_i \# \| N_B \| N_{B_i})$

[Step 9]. 각 센서 노드는 수신한 난수 $N_B, N_{B_i}$ 를 통해 통신에 필요한 키들을 생성한다.

[Step 10]. 모든 노드들은 키 생성을 끝내고 키 생성에 사용되었던 정보인 개인 마스터 키와 수신한 난수를 완전히 삭제한다.

## 6. 비교 분석

본 논문에서 제시한 키 관리 프로토콜은 각 센서 노드와 클러스터 헤드가 계층적인 마스터 키와 동일한 의사 난수 생성기를 소유한 상태에서 베이스 스테이션으로부터 분배받은 계층적인 난수와의 조합으로 통신에 필요한 임의의 키를 생성할 수 있도록 하였다. 이는 아무리 많은 센서 노드가 물리적인 위험으로 인한 키에 대한 정보가 유출 되었다 하여도 계층적인 난수를 모를 경우 센서 네트워크 전체에 피해가 가지 않으며, 센서 노드의 폐기, 키 갱신을 통해 복원될 수 있다. 이는 기존 논문의 확률적인 키 분배 방법과 랜덤 키 사전 분배 방법에서 여러 센서 노드가 물리적인 위험으로 인한 키 정보 유출이 네트워크를 위험에 노출 시키는 것과는 비교될 수 있다. 또한 다음과 같은 추가적인 이점을 가지고 있다.

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

본 논문과 동일한 네트워크 모델을 적용한 G. Jolly의 논문[4]과 비교하면 다음과 주제로 논할 수 있다.

- 에너지 효율

본 논문은 다양한 통신 모델을 지원할 수 있도록 최대한 많은 키를 생성하도록 프로토콜을 설계하였다. 이는 키를 생성하기 위한 계산적 부담을 준다.

또한 키 수립에 필요한 통신 횟수는 비슷하지만 MAC을 사용하여 인증을 제공해 주었다. 이는 패킷길이의 증가로 통신 부담을 주었다.

하지만 이런 단점은 키의 다양성과 보안성을 강조함으로써 발생한 문제라 할 수 있다. 본 논문에서 제시하고 있는 키들은 각각 독립적으로 생성된다는 점에서 얼마든지 축소할 수 있으며 그로인해 에너지 효율성도 증가할 것이다.

- 보안성

본 논문은 키의 생성에서 직접적인 키의 이동 없이 임의로 생성되고 있다. 이는 G. Jolly[4]의 비해 키에 대한 비밀성이 유지된다.

## 7. 결론

본 논문에선 키 생성 방법에 있어 보안성과 다양성, 융통성을 강조하였다. 또한 센서 노드의 에너지 소비 중 통신의 의한 소비가 80% 이상을 차지하다는 점을 감안하여[4] 키 수립에 필요한 통신은 G. Jolly의 논문[4]을 바탕으로 설계하였다. 이는 최소한의 통신 회수로 에너지 효율을 제공해준다.

향후 과제로는 통신 모델을 축소, 확대한 프로토콜 개발과 다른 네트워크 모델로 쉽게 변형 할 수 있는 방법들에 대한 체계적인 연구가 필요하며, 실제 시뮬레이션을 통한 성능 평가가 필요하다.

## 8.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.