EDDK 기반 WSN에서 그리드 라우팅을 이용한 에너지 효율 향상 기법

정원진*, 조대호**
*성균관대학교 전자전기컴퓨터공학과
**성균관대학교 소프트웨어플랫폼학과
e-mail: *wonjin12@skku.edu, **thcho@skku.edu

Energy Efficiency Improvement Method Using Grid Routing in EDDK-based WSNs

Won-Jin Chung*, Tae-Ho Cho**
*Department of Electrical and Computer Engineering, Sungkyunkwan University
**Department of Software Platform, Sungkyunkwan University

요 약

무선 센서 네트워크는 다양한 환경에 배치된 센서 노드를 통해 수집된 이벤트 데이터를 활용하기 위해 구성된다. 무선 센서 네트워크에서 사용하는 센서 노드는 에너지가 제한적이고 공격자에 의해 훼손되기 쉽다. 따라서 무선 센서 네트워크에서는 에너지 효율과 보안이 핵심 요구사항이며 이를 해결하기 위해 다양한 기법이 제안되었다. Energy-efficient Distributed Deterministic Key management scheme (EDDK)는 분산된 페어와이즈 키를 사용하는 보안 기법이다. 하지만 센서 노드의 에너지는 키 업데이트가 빈번하게 발생하는 환경에서 빠르게 감소한다. 본 논문에서는 로컬 클러스터 키를 제거하여 키 업데이트 수를 줄이고, 그리드 라우팅 기법을 이용하여 마스터 노드가 해당 센서 노드에 라우팅 제어 메시지를 전달함으로써 보안성이 유지되며 에너지 효율이 향상된다.

1. 서론

무선 센서 네트워크(Wireless Sensor Networks; 이하 WSN)는 다양한 환경에서 소리, 온도, 진동 등 각종 센서를 이용하여 사용자가 원하는 이벤트를 탐지하고 정보를 수집하는 센서 노드와 수집된 정보를 분석하는 기지국(Base Station; 이하 BS)으로 이루어져 있다. WSN은 넓은 지역의 환경을 모니터링하며, 이벤트를 감지하면 이벤트 알림 패킷을 생성하여 센서 노드 간의 무선통신으로 BS로 전송한다. WSN는 정보를 다양하게 수집하여 전장, 재난 감지 모니터링 등 다양한 분야에 활용될 수 있다[1]. 하지만 센서 노드는 배터리, 통신 거리, 메모리, 컴퓨팅 파워에서 제한된 성능을 가진다. 센서 노드는 배터리로 동작하며, 한번 배치된 센서 노드는 재충전이 어렵기 때문에 센서 노드의 에너지 관리는 중요한 요소이다. 센서 노드는 ZigBee와 같은 무선 통신을 사용하여 통신 거리에 한계가 존재한다. 이벤트를 탐지한 센서 노드가 BS로 패킷을 전송하기 다수의 센서 노드가 통신에 참여한다. 센서 노드의 크기는 소형이기 때문에 작은 크기의 메모리 카드가 사용된다. 따라서 센서 노드의 메모리에 많은 데이터를 저장할 수 없으며 라우팅 정보와 같은 필수적인 정보들만 저장되어 사용한다. 또한 센서 노드는 외부 환경에 배치되어 무선 통신을 하기 때문에 물리적 공격, 재밍 공격과 같은 외부자 공격에 취약하다. 공격자는 훼손된 노드의 정보를 이용하여 센서 노드의 에너지를 소비하는 공격, 잘못된 정보 전달 등 다양한 내부자 공격을 시도할 수 있다. 그러므로 센서 노드의 중요 정보를 보호하는 것이 매우 중요하며 이를 위해 다양한 보안 기법이 연구되었다. X.Zhang에 의해 제안된 Energy-efficient Distributed Deterministic Key management scheme (EDDK)는 페어와이즈(Pairwise) 키와 로컬 클러스터(Local Cluster) 키 설정 및 유지 관리에 중점을 둔 기법이다[2]. EDDK는 키 업데이트, 시퀀스 번호, 메시지 인증 코드를 사용하여 재전송 공격, 메시지 위변조 같은 네트워크에서 발생되는 전반적인 공격을 탐지한다. 하지만 네트워크 통신량이 많은 환경에서는 빈번한 키 업데이트로 센서 노드의 잔여 에너지가 빠르게 감소한다. 본 논문에서는 로컬 클러스터 키를 제거하고 그리드 라우팅을 이용하여 에너지 효율이 향상된다. 본 논문의 구성은 다음과 같다. 2장에서는 EDDK에 대해 설명한다. 3장에서는 제안기법에 관해 설명하고, 마지막 4장에서는 결론 및 향후 계획을 제시한다.

2. 에너지 효율적인 분산 키 관리 기법(EDDK)

EDDK는 페어와이즈 키, 로컬 클러스터 키, 공개키 및 개인키를 사용하는 기법이다. 센서 노드는 의사 난수 함수

(Pseudo-random Function) 와 초기키(Initial Key) 를 저장하고 센서 필드에 배포된다. 이후 의사 난수 함수와 초기키를 이용하여 노드의 개별키(Individual key)를 계산한다. EDDK는 보안을 향상하기 위해 각 노드의 개별키를 사용하여 페어와이즈 키와 메시지 인증 코드 키를 도출한다. 이후 센서 노드는 이웃 노드와 페어와이즈 키를 설정한다. 페어와이즈 키를 생성 과정에서 키를 분산시키기 위해 센서 노드에서 생성된 난수를 포함한다. 페어와이즈 키 설정이 완료된 시점에서 의사 난수 함수와 초기키를 삭제한다. WSN에 배치된 센서 노드의 초기 키설정이 완료된 이후 공격자는 센서 노드를 훼손시켜 해당 센서 노드의 중요 정보를 탈취해도 다른 센서 노드의 키 정보를 계산할 수 없다. 로컬 클러스터 키는 하나의 센서 노드가 모든 이웃 노드와 키 정보를 공유하고 정기적으로 업데이트되는 키로써, 라우팅 제어 메시지 등 센서 노드의 로컬 브로드캐스트 메시지를 보호하는 키이다. 페어와이즈 키와 로컬 클러스터 키는 각각의 시퀀스 번호를 가지며, 시퀀스 번호는 키 수명 역할을 한다. 시퀀스 번호가 미리 정의된 값을 초과할 시에는 키 업데이트를 수행하고, 시퀀스 번호를 1로 초기화한다. EDDK에서 사용되는 공개키와 개인키는 새로운 센서 노드를 추가할 때 사용된다.

3. 제안기법

3.1 동기

EDDK에서 페어와이즈 키와 로컬 클러스터 키는 주기적으로 키 업데이트를 한다. 외부자 공격으로 센서 노드가 자주 훼손되는 환경이나 다수의 이벤트 발생으로 네트워크 통신량이 많은 환경에서 페어와이즈 키와 로컬 클러스터 키 업데이트 주기가 짧아진다. 이는 센서 노드의 잔여 에너지를 빠르게 감소시키며 잔여 에너지가 적은 센서 노드의 에너지 고갈을 초래한다.

3.2 가정

센서 노드는 랜덤하게 배치되고 그리드에는 최소 하나의 센서 노드가 존재한다. 마스터 노드는 그리드에서 BS의 거리가 가장 가까운 센서 노드가 선정 된다. BS는 공격받지 않으며, 센서 노드 잔여 에너지를 파악할 수 있다.

3.2 가정

본 논문의 제안기법은 EDDK에서 사용되는 로컬 클러스터 키를 제거하여 키 업데이트에 대한 에너지 소모를 줄인다. 또한 그리드 라우팅 기법을 사용하여 마스터 노드를 선정함으로써 라우팅 제어 정보를 효율적으로 전송한다[3]. 로컬 클러스터 키로 암호화하여 이웃 노드에 전달했던 라우팅 제어 메시지를 마스터 노드가 해당 그리드에 포함된 센서 노드에 페어와이즈 키로 메시지를 암호화하여 전달함으로써 기존 기법보다 보안성을 유지하면서 에너지 효율이 향상된다.

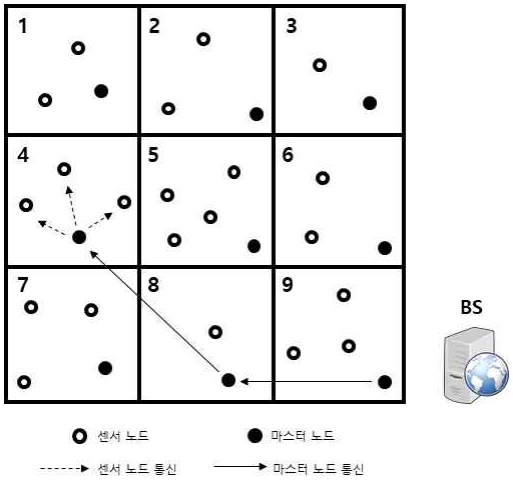

그림 1. 라우팅 제어 메시지 전달

그림 1은 라우팅 제어 메시지가 해당 마스터 노드로 브로드캐스팅되어 그리드에 포함된 센서 노드에 전달되는 과정을 보여준다. 실험 결과 60% 확률로 공격이 발생하는 환경에서 1000번의 이벤트가 발생할 경우 센서 노드의 에너지 효율이 기존기법 보다 약 7.8097% 향상된다.

4. 결론 및 향후 계획

본 논문에서는 EDDK에서 키 업데이트에 소비되는 에너지를 줄이기 위해 로컬 클러스터 키를 제거하고 그리드 라우팅을 이용하여 마스터 노드를 선정한다. 마스터 노드는 페어와이즈 키를 이용하여 각 센서 노드에 라우팅 제어 메시지를 전달한다. 향후 EDDK에서 페어와이즈 키의 시퀀스 번호로부터 발생하는 공격에 대한 탐지 기법을 연구를 진행할 계획이다.

ACKNOWLEDGEMENT

이 논문은 2019년도 정부(교육부)의 재원으로 한국연구재단의 지원을 받아 수행된 기초연구사업임(No. NRF-2018R1D1A1B07048961)

참고문헌

[1] I.F.Akyildiz, et al. "Wireless sensor networks: a survey." Computer networks vol. 38, no. 4, pp. 393-422, 2002

[2] X.Zhang, J.He, and Q.Wei. "EDDK: Energy-efficient distributed deterministic key management for wireless sensor networks." EURASIP Journal on Wireless Communications and Networking 2011, no. 12, 2011.

[3] O.Banimelhem and S.Khasawneh. "GMCAR: Grid-based multipath with congestion avoidance routing protocol in wireless sensor networks." Ad Hoc Networks, vol. 10, no. 7, pp. 1346-1361, 2012