센서 네트워크 기반의 확률적 투표 여과 기법에서 에너지 향상을 위한 인증 키 분배 기법

남수만°, 조대호*
°*성균관대학교 정보통신대학
e-mail:{sm38good, thcho}@skku.edu°*

Authentication Key Distribution Method for Improving Energy Efficiency in Probabilistic Voting-based Filtering Scheme based Sensor Networks

Su-Man Nam°, Tae Ho Cho*
°*College of Information and Communication Engineering, Sungkyunkwan University

● 요 약 ●

센서 네트워크에서 센서는 제한적인 자원 때문에 다양한 공격으로부터 취약하다. 이러한 공격 중 하나인 허위 보고서 삽입 공격은 불필요한 에너지 소모와 허위 알람을 유발한다. 이 공격의 피해를 줄이기 위한 확률적 투표 여과 기법은 검증 노드를 통해 보고서의 맥들을 검증한다. 그러나 허위 보고서가 검증 노드까지 도달하는 데 불필요한 에너지가 소비된다. 본 논문에서, 우리의 제안 기법은 소스의 다음 노드에 키를 배포하여 허위 보고서 삽입 공격을 효율적으로 감지한다. 따라서 제안 기법은 기존 기법보다 에너지 효율성 향상을 기대할 수 있다.

키워드: 무선 센서 네트워크(wireless sensor network), 확률적 투표 여과 기법(probabilistic voting-based filtering scheme), 인증 키 분배(authentication key distribution)

I. 서 론

무선 센서 네트워크(wireless sensor networks)는 센서로부터 감지한 센싱 값을 무선 통신을 통해 베이스 스테이션에 전달하고, 데이터를 분석하여, 사용자에게 정보를 제공한다. 이러한 센서들은 제한적인 하드웨어 자원으로 운영되기 때문에 공격에 취약하다.

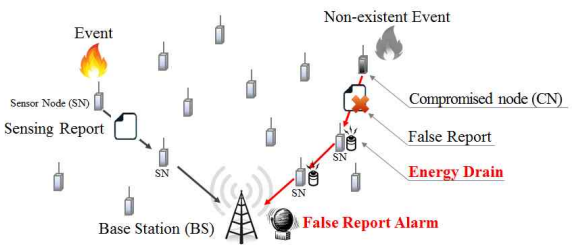

그림 277. 허위 보고서 삽입 공격
Fig. 1. False report injection attacks

센서 네트워크의 응용 계층에서 발생하기 쉬운 허위 보고서 삽입 공격은 그림 1처럼 이벤트 발생 없이 훼손된 노드를 통해 허위 보고서가 주입된다. 주입된 허위 보고서는 다중 홉을 통해 싱크 노드까지 전달하므로 중계 노드에서 불필요한 에너지 소모와 싱크 노드에서 허위 보고서 알람이 발생한다. 이러한 공격을 감지하기 위해 PVFS (Probabilistic Voting-based Filtering Scheme; 이하 PVFS)는 선택된 검증 노드에서 맥을 검증하여 허위 보고서를 감지한다. PVFS는 센서 노드들을 클러스터 단위로 나누고, 그 클러스터에는 클러스터 헤드(Cluster Head; 이하 CH)와 멤버 노드(Member Node; 이하 MN)으로 구성된다. 이 기법은 이벤트가 발생하였을 때 멤버 노드로부터 맥을 수집하고, 수집한 내용을 보고서에 생성하고 전달한다. 전달되는 보고서는 초기 단계에서 정의된 검증 CH를 통해 검증된다. 이러한 PVFS는 맥을 통해 허위 보고서를 검증하지만, 허위 보고서가 네트워크가 주입될 때 불필요한 에너지 소모가 있다. 본 논문에서, 우리의 제안 기법은 소스 CH의 키를 다음 CH에 미리 전달함으로 다음 노드에서 허위 보고서를 즉시 탐지한다. 그러하여 제안 기법은 기존 기법과 비교하였을 때 허위 보고서의 전송을 바로 차단하여 노드의 에너지를 향상하게 시킬 수 있다. 본 논문은 2장에서 기존 기법을 소개하고, 3장에서 제안 기법을 소개한 다음 4장에서 결론을 논한다.

II. PVFS

PVFS는 보고서에 첨부된 허위 맥의 임계 값(Tf)을 통해 허위 보고서 삽입 공격을 감지하기 위해 제안되었다. 이 기법은 키 초기화

및 할당, 보고서 전송, 그리고 여과 단계로 운영된다. 키 초기화 및 할당 단계에서 모든 노드(CH, 멤버 노드)는 싱크로부터 한 키를 할당받고 클러스터 기반으로 배치된다. 그리고 각 CH는 BS로부터 거리를 기반으로 확률적으로 검증 CH를 선택하고, 그 검증 CH에 각 클러스터의 한 키를 전달한다. 보고서 전송 단계는 한 클러스터에서 이벤트가 감지될 때, 그 클러스터의 CH는 멤버 노드로부터 맥을 받고, 한 보고서를 생성한 다음, 다음 노드에 전달한다. 여과 단계는 중계 CH들이 보고서를 받을 때 자신이 받은 키를 통해 그 보고서를 검증한다. 이때 그 보고서의 감지된 허위 맥의 수가 임계 값 이상이라면, 허위 보고서 삽입 공격으로 판별된다.

III. 본 론

1 동기

센서 네트워크에서 높은 보안과 함께 효율적인 에너지 운영은 중요한 이슈이다. 기존 기법에서는 허위 보고서를 검증 노드에서 여과될 때까지 통신을 통한 불필요한 에너지가 소모된다. 그러므로 제안 기법에서는 소스의 다음 CH에 정상 키를 전달하여 빠른 허위 맥을 검증하고, 네트워크의 에너지를 절약한다.

2 제안 기법

응용 계층에서 발생하는 허위 보고서 삽입 공격은 전체 네트워크의 수명을 단축한다. 제안 기법은 허위 보고서 삽입 공격을 효과적으로 감지하기 위해 다음 노드에게 키 전달을 통해 빠르게 허위 맥을 검증한다. 제안 기법은 허위 보고서를 효과적으로 감지하기 위해 키 초기화 및 할당 단계에서 키 전달을 통해 빠르게 허위 맥을 검증한다.

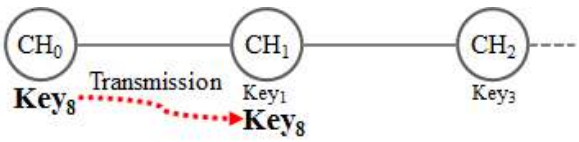

그림 278. 다음 노드에 키 전달
Fig. 2. Key transmission to next node

그림1은 초기 단계에 두 CH 사이에서 키 전달을 보여준다. CH0은 Key8을 미리 할당받고, 그 키를 다음 노드 CH1에 전달한다. CH1은 CH0로부터 받은 키를 통해 CH0에서 만들어진 맥을 검증할 수 있다.

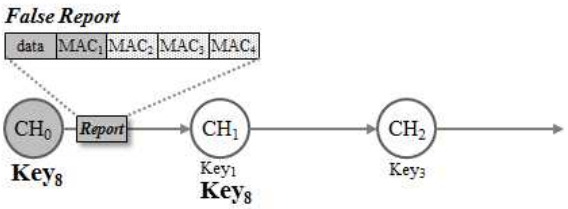

그림 279. 보고서 인증
Fig. 3. Report verification

그림 2는 CH0로부터 허위 보고서가 발생하여 CH1에서 감지되는 과정을 보여준다. CH0은 초기 단계에 훼손되었고, 훼손된 노드는 이벤트 발생 없이 허위 데이터, 허위 맥, 그리고 저장된 맥을 통해 허위 보고서를 생성할 수 있다. 그 허위 보고서는 CH0를 통해 네트워크에 삽입된다. 삽입된 허위 보고서는 CH1에서 Key8를 통해 그 보고서를 검증한다. CH1에서 감지된 허위 보고서는 여가 된다. 그러므로 제안 기법은 이러한 방법을 통해 소스 노드의 다음 노드에서 효율적으로 허위 보고서를 감지할 수 있다.

IV. 결 론

제안 기법은 기존 기법보다 인증 키를 사전에 분배함으로써 허위 보고서의 빠른 여과를 통해 에너지 효율성을 향상한다.

Acknowledgment

이 논문은 2013년도 정부(교육과학기술부)의 재원으로 한국연구재단의 지원을 받아 수행된 기초연구사업임
(No. 2013R1A2A2A01013971).

참고문헌

[1] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam and E. Cayirci, "A survey on sensor networks," Communications Magazine, IEEE, vol. 40, pp. 102-114, Aug. 2002. "

[2] F. Li, A. Srinivasan and J. Wu, "PVFS: A Probabilistic Voting-based Filtering Scheme in Wireless Sensor Networks," International Journal of Security and Network, vol. 3, pp. 173-182, 2008.