한국컴퓨터정보학회 하계학술대회 논문집 제23권 제2호 (2015. 7)

무선 센서 네트워크의 동적 여과 기법에서 에너지 절약을 위한 효율적인 키 재분배 기법

박동진°, 조대호*
°성균관대학교 소프트웨어플랫폼학과, *성균관대학교 전자전기컴퓨터공학과
e-mail : jin1307e@skku.edu°, thcho@skku.edu*

Efficient Key Re-dissemination Method for Saving Energy in Dynamic Filtering of Wireless Sensor Networks

Dong-Jin Park°, Tae-Ho Cho*
°Dept. of Software platforms, Sungkyunkwan University, *Dept. of Information and Communication Engineering, SungKyunKwan University

● Abstract ●

WSN의 센서 노드는 제한된 자원으로 인해 보안상의 취약성을 가지며 공격자는 쉽게 임의의 데이터를 삽입하는 허위 데이터 주입 공격을 할 수 있다. WSN에서는 이러한 공격이 치명적이기 때문에 허위 데이터를 가능한 빨리 여과해야 한다. 허위 데이터 주입 공격을 탐지하는 기법으로 동적 여과 기법이 제안되었는데 이 기법은 초기 분배된 비밀키에 대한 재분배가 이루어지지 않아 같은 공격에 계속 노출될 경우 불필요한 에너지 소모가 발생한다. 본 논문에서 제안하는 기법은 효율적인 키 재분배를 통해 허위 데이터를 빨리 감지하고 에너지 효율성을 향상시킨다. 전달 노드에서 허위 데이터가 탐지되면 정의된 알람 메시지를 통해 베이스 스테이션에 보고되고 키 재분배를 수행하여 더 효율적으로 허위 데이터를 감지한다. 그러므로 제안 기법은 기존 기법과 비교하였을 때 허위 데이터를 조기에 감지하고 전체 네트워크의 에너지를 절약한다.

키워드: 무선 센서 네트워크(Wireless Sensor Network), 허위 데이터 주입 공격(False Data Injection Attack), 동적 여과 기법(Dynamic En-route Filtering scheme), 키 재분배(Key Re-dissemination)

I. Introduction

무선 센서 네트워크(Wireless Sensor Network; 이하 WSN)는 제한된 자원(연산능력, 메모리, 전력, 단거리 무선 통신 등)을 가진 다수의 소형 센서 노드와 데이터를 수집하는 기지 노드(Base Station; 이하 BS)로 구성된다[1]. 센서 노드는 제한된 자원으로 인해 공격자에게 쉽게 포획 또는 손상되는 보안상의 취약성을 가진다. 이러한 취약성으로 공격자는 쉽게 임의의 데이터를 삽입하는 허위 데이터 주입 공격(false data injection attack)을 할 수 있다. 이 공격의 피해는 잘못된 알람을 일으키고 데이터 전달과정에서 에너지 소모를 일으켜 네트워크 수명을 감소시킨다. 제한된 자원을 갖는 WSN에서는 이러한 공격이 치명적이므로 가능한 한 빨리 공격을 검출하는 것이 중요하다. 이러한 공격을 탐지하는 기법으로 동적 여과 기법(Dynamic En-route Filtering scheme; 이하 DEF)이 제안되었다[2]. DEF는 초기에 분배된 비밀키에 대한 재분배가 이루어지지 않기 때문에 같은 공격에 계속 노출되어 불필요한 에너지 소모가 발생한다. 이를 위해 우리의 제안 기법은 효율적인 키 재분배 방법을 통해 허위 데이터의 빠른 감지와 에너지를 절약하는 방법을 제안한다. 본 논문은 II장에서 기존 기법인 DEF를 소개하고 제안하는 기법의 동기를 언급한다. III장에서는 제안한 기법을 설명하고 마지막으로 IV장에서 본 연구의 기여를 제시한다.

II. Background

1. DEF

DEF는 허위 데이터 주입 공격을 효율적으로 탐지하기 위해 제안된 기법이다. DEF는 3단계 과정을 가진다. 배포 전 단계에서 BS는 해쉬 함수를 사용해 인증키를 생성하는 seed키와 키 풀에서 임의로 선택된 $l+1$개의 비밀키를 각 센서에 분배한다. 배포 후 단계에서 각 노드는 자신의 비밀키로 인증키를 암호화하여 클러스터 헤드(Cluster Head; 이하 CH)에 전송한다. CH는 노드들에게 받은 암호화된 인증키를 취합해 미리 정해진 일정 홉 수만큼 전달한다. 수신한 노드는 메시지의 비밀키 인덱스를 비교하여 자신의 비밀키와 일치하는 것이 있으면 복호화하고 인증키를 저장한다. 여과 단계에서 CH는 취합된 데이터와 인증키를 전달 노드에 전송한다. 수신한 전달 노드는 자신의 인증키로 인증키 메시지와 취합된 데이터를 검증하고 다음

전달노드에 검증 결과를 전달한다.

2. Motivation

기존 기법에서 키 노출을 통해 공격이 발생할 경우 네트워크의 센서들은 키 재분배를 통해 네트워크의 보안성을 향상시켜야 한다. 이때 전체 네트워크를 대상으로 재분배하면 많은 불필요한 에너지 소모가 있다. 따라서 제안 기법은 효율적인 키 재분배를 통해 허위 데이터 주입 공격을 조기에 탐지하고 에너지 소비를 줄이는 방법을 제안한다.

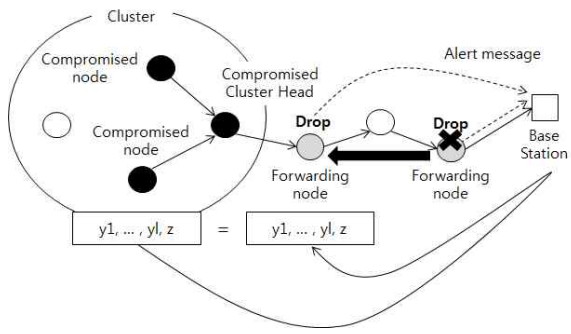
III. The Proposed Scheme

1. Assumptions

BS는 허위 데이터가 전달 노드 상에서 탐지될 때마다 보고 받는다. 보고받는 메시지는 알람 메시지(alert message)로 정의하였고 소스 클러스터 ID, 검증 클러스터 ID, 검증 키 Index를 가진다. 소스 클러스터 ID는 허위 데이터 발생 클러스터를 말하며, 검증 클러스터 ID는 허위 데이터 탐지 클러스터를 말하고 검증 키 Index는 검증한 키의 Index이다. BS는 모든 라우팅 경로를 알고 있다. 키 재분배 시점은 미리 정의된 임계값을 넘었을 때 수행하고, 임계값의 적절한 선택은 향후 연구 과제이다.

2. The Proposed Scheme

Fig 1은 키 재분배를 통한 허위 데이터 탐지를 보여준다. 전달 노드는 허위 데이터를 탐지할 때 알람 메시지를 BS에게 전송한다. BS는 허위 데이터 발생 임계값에 도달하면 키 재분배를 실행한다. BS는 모든 노드의 키를 알고 알람 메시지를 통해 소스 클러스터를 알 수 있으므로 그 클러스터의 비밀키와 동일한 키를 생성한다. BS는 소스 클러스터의 다음 노드에 생성한 키를 전달한다. 배포 후 단계를 통해 공격 발생 클러스터의 인증키들은 다음 홉 전달 노드에서 해당하는 비밀키가 존재하므로 인증키를 저장한다. 소스 클러스터에서 허위 데이터 주입 공격이 발생하면 다음 노드에서 MAC을 검증하여 허위 데이터 유무를 조기 탐지한다.



Detection of false data by key re-dissemination

IV. Conclusions

기존 DEF에서는 10홉 이내에 90% 확률로 허위 데이터를 탐지한다 [2]. 제안 기법은 DEF 탐지 능력을 동일하게 가지며 소스 클러스터와 한 홉 내에서 검증될 확률을 상승시켰다. 따라서 제안한 키 재분배 기법을 통해 기존 기법보다 허위 데이터를 조기 탐지하고 전송되는 홉 수를 줄여 에너지를 절약하였다.

Acknowledgement

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

References

[1] Akyildiz, Ian F., et al. "A survey on sensor networks." Communications magazine, IEEE 40.8 (2002): 102-114.

[2] Yu, Zhen, and Yong Guan. "A dynamic en-route filtering scheme for data reporting in wireless sensor networks." IEEE/ACM Transactions on Networking (ToN) 18.1 (2010): 150-163.