IoT 환경에서 측정 데이터를 이용한 허위 보고서 탐지 방법

강예림*, 조대호**
*성균관대학교 전자전기컴퓨터공학과
**성균관대학교 소프트웨어플랫폼학과
e-mail : *missye7322@skku.edu, **thcho@skku.edu

Measured Data Based a False Report Filtering Method in IoT Environment

Ye-Lim Kang*, Tae-Ho Cho**
*Department of Electrical and Computer Engineering, Sungkyunkwan University
**Department of Software Platform, Sungkyunkwan University

요 약

무선 센서 네트워크 기반 사물인터넷 환경은 산업, 의료 등 다양한 분야에 응용된다. 개방된 공간에 센서 노드가 배치되며 무선 통신을 이용하기 때문에 쉽게 훼손되며, 이를 통해 공격자로부터 허위 보고서 주입 공격이 발생할 수 있다. 악의적으로 생성된 허위 보고서가 기지국으로 전송되면 센서 노드의 불필요한 에너지가 소모되며 사물인터넷 장치에서는 이상 동작을 실행하는 것이 가능하다. 무선 센서 네트워크의 보안 프로토콜 중 하나인 Interleaved Hop-by-hop Authentication은 훼손된 센서 노드의 개수가 보안 경계값을 초과할 경우 허위 보고서 주입 공격을 방어할 수 없다. 본 제안기법에서는 센서 노드와 사물인터넷 장치에서 측정된 데이터를 이용한 허위 보고서 탐지 방법을 제안한다. 제안 기법은 각각 측정된 데이터를 이용하여 허위 보고서의 정확한 탐지가 가능하며 사물인터넷 장치의 이상 동작 실행을 방지할 수 있어 보안성이 강화될 것을 기대한다.

1. 서론

무선 센서 네트워크(Wireless Sensor Network; 이하 WSN)에서는 수많은 센서 노드가 배치되어 저비용으로 의료, 국방, 가정과 같은 다양한 분야에서 응용된다[1]. 사물인터넷(Internet of Things; 이하 IoT)은 모든 사물이 상호 연결되어 의사 결정을 하는 시스템이다. WSN 기반의 IoT 환경에서 센서 노드가 이벤트를 탐지하면 기지국(Base Station; 이하 BS)으로 데이터를 전달한다. IoT 장치는 Message Queue Telemetry Transport (MQTT) 프로토콜을 사용하여 데이터를 전달받아 적절한 동작을 실행한다[2]. MQTT는 장치 간의 통신을 위해 TCP/IP 위에서 동작하는 발행과 구독 기반의 프로토콜이다. WSN은 개방된 공간에 배치되어 무선 통신을 이용하기 때문에 공격자가 센서 노드를 훼손시켜 허위 보고서를 작성하는 것이 가능하다[3]. 허위 보고서가 전송되면 센서 노드의 불필요한 에너지가 소모되고 IoT 장치는 이상 동작을 실행한다. 훼손된 센서 노드의 개수가 보안 경계값(Security Threshold; 이하 T)을 초과하면 전송된 허위 보고서는 IoT 장치의 이상 동작 실행을 유발한다. WSN 보안 프로토콜인 Interleaved Hop-by-hop Authentication (IHA)는 이러한 허위 보고서 주입 공격을 방어하는 것이 불가능하다[4]. 따라서 본 논문에서는 BS가 측정 데이터를 이용하여 허위 보고서를 탐지하며 IoT 장치의 이상 동작 실행을 방지한다.

본 논문의 구성은 다음과 같다. 본 논문의 2장에서는 허위 보고서 주입 공격, MQTT, IHA의 동작 원리에 관해서 설명한다. 3장에서는 제안 기법에 대하여 설명하며 마지막으로 4장에서 결론을 내린다.

2. 관련 기술

2.1 허위 보고서 주입 공격

허위 보고서 주입 공격은 공격자가 센서 노드를 훼손시켜 네트워크에 허위 보고서를 주입하는 공격이다. 공격자는 센서 노드를 훼손시켜 키 정보를 획득한다. 공격자는 획득한 키 정보를 이용하여 발생하지 않은 이벤트에 대한 허위 보고서를 작성한다. 허위 보고서가 BS로 전송되면 센서 노드의 불필요한 에너지가 소모되어 네트워크의 에너지 효율성이 감소한다. BS를 통해 허위 보고서를 수신한 IoT 장치는 이상 동작을 실행한다.

2.2 Message Queue Telemetry Transport

MQTT는 발행, 구독을 기반으로 하는 통신 프로토콜이

다. MQTT는 TCP/IP 위에서 동작하며 임베디드 장치 및 애플리케이션을 네트워크와 연결하는 것을 목표로 한다. MQTT는 자원이 제한적인 장치에 적합하며 발행자와 구독자, 브로커로 구성된다. 브로커는 클라이언트 사이에 데이터의 교환과 저장을 담당하는 서버 역할을 하며 Topic을 생성한다. Topic은 데이터들이 전달되는 채널 이름을 의미한다. 브로커에는 다양한 데이터들이 전달된다. 이러한 데이터들을 주제별로 분류하기 위해서 브로커는 Topic이라는 채널을 생성한다. 특정 Topic의 데이터를 수신하기 위해서 구독자는 Topic을 구독한다. 브로커를 통해 데이터는 Topic의 모든 구독자에게 전송된다. 발행자는 Topic에 데이터를 갱신한다.

2.3 Interleaved Hop-by-hop Authentication

IHA는 센서 노드와 BS가 허위 보고서를 탐지하는 WSN 보안 프로토콜이다. 이벤트를 탐지한 센서 노드는 메시지 인증 코드(Message Authentication Code; 이하 MAC)를 포함한 보고서를 생성하여 BS로 전송한다. 보고서를 BS로 전달하는 과정에서 센서 노드는 보고서의 허위 여부를 판별하는 검증 과정을 거치게 된다. 첫 번째로 보고서를 수신한 센서 노드는 보고서 내의 MAC의 개수를 확인한다. 두 번째로 센서 노드는 하위 연합 노드와 공유하고 있는 페어와이즈 키(Pairwise Key)를 이용하여 MAC을 생성한다. 세 번째로 센서 노드는 보고서 내의 MAC 리스트에 있는 마지막 MAC과 일치하는지를 확인한다. 검증에 성공하면 센서 노드는 MAC 리스트에 있는 마지막 MAC을 제거한다. 네 번째로 센서 노드는 상위 연합 노드와 공유하고 있는 페어와이즈 키를 이용하여 MAC을 생성한 후에 MAC 리스트의 맨 앞에 추가하여 보고서를 BS로 전송한다. 마지막으로 BS에서는 MAC을 검증하여 보고서의 허위 여부를 결정한다. 정상적으로 검증이 될 경우 BS는 사용자에게 보고서를 전달한다.

3. 제안 기법

3.1 동기

훼손된 센서 노드의 개수가 T를 초과하면 IHA는 허위 보고서 탐지 기능을 상실한다는 취약점이 존재한다. 이러한 취약점을 가진 보고서는 BS를 통해 IoT 장치로 전달되며 IoT 장치는 이상 동작을 실행한다. 따라서 IoT 장치가 올바른 동작을 수행하기 위해 보고서의 허위 여부를 판별하는 것이 중요하다.

3.2 가정

센서 노드에서 BS까지 보고서가 전송되는 동안 패킷 손실은 발생하지 않는다. IoT 장치와 BS는 강도 높은 보안 프로토콜을 사용하기 때문에 훼손되지 않는다.

3.3 동작과정

이벤트가 발생하면 센서 노드와 IoT 장치는 동시에 같은 이벤트 탐지가 가능하다. BS에서는 센서 노드의 이벤트 보고서, IoT 장치의 이벤트 보고서를 수신한다. BS는 각각의 측정 데이터를 기반으로 보고서의 허위 여부를 판별한다. 정상적으로 2개의 보고서를 수신하면 BS는 각각의 측정 데이터값을 비교한다. 비교한 측정 데이터값이 같다면 BS는 수신한 보고서가 정상 보고서라고 판단한다. 허위 보고서만 도달했을 경우 BS는 보고서를 폐기하며 IoT 장치에 전달하지 않는다.

4. 결론

훼손된 센서 노드의 개수가 T를 초과한다면 IHA에서는 허위 보고서 탐지 기능이 동작하지 않는다. 따라서 IoT 장치가 이상 동작을 실행하는 것을 방지하지 못한다는 취약점을 가지고 있다. 본 논문에서는 IoT 환경에 센서 노드와 IoT 장치가 배치되고 BS는 2개의 이벤트 보고서를 수신한 후 측정 데이터를 이용하여 허위 보고서를 탐지하는 방법을 제안하였다. 측정 데이터를 기반으로 보고서의 허위 여부를 판별하기 때문에 IoT 장치에서의 이상 동작 실행 방지가 가능하며 보안성이 강화되는 것을 기대한다.

ACKNOWLEDGEMENT

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

참고문헌

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

[2] Al-Fuqaha, Ala, et al. "Internet of things: A survey on enabling technologies, protocols, and applications." IEEE communications surveys & tutorials 17.4 (2015): 2347-2376.

[3] Wang, Yong, Garhan Attebury, and Byrav Ramamurthy. "A survey of security issues in wireless sensor networks." (2006).

[4] ZHU, Sencun, et al. An interleaved hop-by-hop authentication scheme for filtering of injected false data in sensor networks. In: Security and privacy, 2004. Proceedings. 2004 IEEE symposium on. IEEE, 2004. p. 259-271.