IoT 상태 정보를 활용한 스마트 팩토리의 이상 데이터 탐지 방법

안정섭*, 조대호**
*성균관대학교 전자전기컴퓨터공학과
**성균관대학교 소프트웨어플랫폼학과
e-mail : *sc4217@skku.edu, **thcho@skku.edu

A Method for False Data Detection Using IoT Status Information in Smart Factory

Jung-Sub Ahn*, Tae-Ho Cho**
*Department of Electrical and Computer Engineering, Sungkyunkwan University
**Department of Software Platform, Sungkyunkwan University

요 약

최근 4차 산업혁명의 등장으로 스마트 팩토리의 핵심 통신 기술인 무선 센서 네트워크에 대한 관심이 높아지고 있다. 무선 센서 네트워크 기반의 사물 인터넷은 배치된 센서 노드들을 통해 정보를 수집하고 이를 이용하여 다양한 서비스를 제공한다. 센서 노드는 개방된 환경에 배치되기 때문에 공격자에 의해 쉽게 탈취되고 훼손당할 수 있다. 이러한 훼손된 노드는 허위 보고서 삽입 공격 등 네트워크 보안 공격으로 악용될 수 있다. 허위 보고서 삽입 공격을 막기 위해 중간 여과 기법을 활용한 다양한 무선 센서 네트워크 보안 기법이 제안되었다. 하지만 기존 중간 여과 보안기법들은 보안성 조절을 위해 보안 경계값을 가지는데 훼손된 노드의 수가 보안 경계값과 같거나 이를 넘어갈 경우 허위보고서를 필터링하지 못한다. 본 논문에서는 사물 인터넷 기기들의 상태 정보를 이용하여 잘못된 이상 값을 추론하여 오작동을 방지하는 방법을 제안한다. 제안 방법에서는 노드에서 생성된 보고서와 이와 연관된 사물 인터넷 기기들의 상태를 이용하여 허위 보고서의 유무를 판단한다. 따라서 제안방법은 사물 인터넷 기기의 상태 값을 이용하여 추론을 하므로 허위 이벤트를 탐지할 수 있다.

1. 서론

스마트 팩토리는 생산 공정에 정보통신기술(Information and Communication Technology; 이하 ICT)을 융합하여 데이터를 기반으로 의사 결정을 통해 최적화된 공정을 도출하는 지능형 생산 공장이다[1]. 스마트 팩토리의 핵심 기술은 사물 인터넷(Internet of Things; 이하 IoT)와 사이버 물리 시스템(Cyber Physical System; 이하 CPS)으로 구성된다[2]. 스마트 팩토리는 산업 기기와 생산의 모든 과정이 네트워크로 연결되기 위하여 기본적으로 무선 통신으로 연결된 무선 센서 네트워크(Wireless Sensor Network; 이하 WSN)를 이용한다[3]. 하지만 WSN의 취약점들로 인해 스마트 팩토리는 다양한 보안 공격에 노출되어있다. 네트워크 보안을 위해 각각의 인증방법이 존재하지만 운영 및 효율성에 한계가 있으므로 두가지 이상의 보안 요소를 결합하여 보안 기능을 강화할 필요가 있다[4-5]. 특히, 배치된 센서 노드들을 훼손시켜 허위 보고서 삽입 공격이 일어날 경우 허위 보고서는 스마트 팩토리의 이상 동작을 한다. 허위 보고서를 탐지하기 위한 중간 여과 방식의 다양한 보안 기법이 제안되었지만 이 보안 기법들은 기본적으로 보안 경계값 이하의 노드 훼손의 경우에만 보안을 제공한다. 보안 경계값보다 훼손된 노드가 클 경우 공격자는 중간 여과와 싱크 노드에서의 보안조차 막지 못하는 허위 보고서를 만들 수 있다. 이러한 문제점을 고려하여 기존과 다른 접근방식을 통해 보안을 강화시킬 필요가 있다.

본 논문에서는 스마트 팩토리에 존재하는 IoT 기기들의 상호 협력을 통해 보안성을 제공하는 방법을 제안한다. 제안 방법에서는 보고서의 값에 따라 이상 데이터를 검사하고 연관된 IoT 기기들의 상태를 통해 허위 보고서의 유무를 추론한다. 추론 결과 허위 보고서로 판단되면 허위 보고서를 제거하여 IoT 기기들의 이상 행위를 방지한다. 또한 추론을 통해 보안 프로토콜에 효율적인 보안 강도를 재설정하여 안전한 공정 시스템을 유지할 수 있다.

본 논문의 구성은 다음과 같다. 2장에서는 관련연구인 무선 센서 네트워크 응용 계층 보안 기술과 스마트 팩토리에 대하여 상세히 설명한다. 3장에서는 제안 기법에 대

하여 소개하고, 마지막으로 4장에서는 결론 및 향후 연구에 관해 서술한다.

2. 관련 연구

2.1 무선 센서 네트워크 응용 계층 보안 기술

WSN은 수많은 센서 노드와 싱크 노드들로 이루어져 있으며 센서 노드들간 무선 통신을 통해 이벤트 보고서를 싱크 노드들로 전달한다. 센서 노드들은 개방된 환경에 배치되어 있어 쉽게 정보를 탈취당할 수 있다. 공격자는 노드들을 훼손하여 무선 네트워크에 허위 보고서를 주입시킬 수 있다. WSN에서 허위보고서를 방어하기 위해 Statistical En-route Filtering (SEF), Cluster-based False Data Filtering Scheme (CFFS), Interleaved Hop-by-hop Authentication (IHA) 등 대칭키를 응용한 다양한 보안기법이 제안되었다. 기존 보안 기법들은 메시지 인증 코드(Message Authentication Code; 이하 MAC)을 이용한 중간 여과 기법을 사용하고 사전에 설정된 보안 경계값을 통해 보고서에 MAC 수를 조절하여 보안 강도를 조절한다. 또한 글로벌 키풀을 사용하여 키 관리를 통해 싱크 노드에서 보고서에 포함된 MAC들을 최종적으로 검증한다. 공격자는 훼손한 노드에서 허위 이벤트를 발생시켜 탐지 불가능한 MAC을 생성할 수 있다. 이러한 이유로 네트워크 응용 보안 기법에서 보안 경계값만큼 센서 노드가 훼손된다면 중간 여과 보안과 싱크노드에서의 보안도 무력화 된다. 그러므로 공격자는 수많은 노드을 훼손시키고 허위 보고서를 주입하므로 이와 연관된 서비스들의 이상 동작을 유발 시킨다. 그러므로 이러한 문제를 해결하기 위해서는 경계값 이상의 센서 노드가 훼손된 경우를 고려한 새로운 보안 방법이 필요하다.

2.2 스마트 팩토리

스마트 팩토리는 ICT와 생산시스템을 융합하여 산업기기와 생산의 모든 과정이 네트워크에 연결되므로 이를 기반으로 실시간 상호작용과 기존의 생산 프로세스를 개선하여 생산 효율성을 높이는 지능형 시스템이다. 스마트 팩토리는 센서 모듈과 유·무선 네트워크로 구성되며 기본적으로 센서 노드들은 이웃 노드 간 협력적 통신을 통해 게이트웨이를 연결하는 WSN으로 구성된다. 특히, 스마트 팩토리는 다양한 센서와 기기들의 데이터를 기반으로 분석하고 의사결정을 하는 데이터 기반의 공장 운영체제이므로 싱크 노드까지 전달된 허위 보고서는 스마트 팩토리의 오작동을 일으킬 수 있다.

3. 제안 기법

3.1 허위 보고서 탐지

제안 기법은 기존 WSN 보안기법에서 보안 경계값만큼 센서 노드가 훼손되었을 경우를 고려하여 새로운 접근 방법을 제시한다. 제안 방법은 보고서들의 내용과 연관 센서 데이터를 이용하여 허위보고서를 탐지한다. 싱크 노드는 센서 노드들의 보고서들을 사전에 설정한 임계치만큼 누적하여 저장하고 이 보고서들을 이용하여 허위보고서를 검증한다. 만약 의심상황으로 갈 경우 3.2에 소개된 기법과 같이 상황 추론을 통해 데이터 업데이트 유무를 결정한다. 그러므로 기존 보안 기법의 한계점인 센서 노드 훼손율에 관계없이 허위 보고서를 탐지할 수 있다.

3.2 상태정보를 활용한 이상 데이터 탐지 기법

싱크 노드에서는 아래의 단계들을 통해 허위 보고서의 유무를 추론한다.

단계 1 : 누적된 보고서들은 사용자가 사전에 설정한 오차범위 임계치를 통해 허위 보고서를 의심하게 된다.

단계 2 : 허위 보고서 의심여부를 받은 보고서는 보고서에 연관된 IoT 기기들의 상황 정보를 요청한다.

단계 3 : 요청된 상황 정보들과 허위 데이터 의심 보고서를 통해 허위 보고서 유무를 추론한다.

단계 4 : 추론 결과 허위 보고서로 판단이 되면 보안 경계값을 재설정하거나 키 재분배를 통해 보안성을 재구성한다.

제안 기법은 위의 단계를 통해 허위 보고서는 IoT 기기까지 전달되지 않고 보안을 유지할 수가 있다.

4. 결론 및 향후 연구

WSN에서 완벽하게 위조된 허위 보고서는 스마트 팩토리의 오작동을 일으킬 수 있다. 본 논문에서는 WSN 기반 IoT 구성을 가지는 스마트 팩토리에서 기존에 존재하는 WSN 보안 프로토콜의 취약점인 보안 경계값 이상 노드가 훼손되었을 때 허위 보고서를 추론하는 방법에 대해 제안한다. 제안 방법은 허위 데이터가 싱크 노드로 저장되는 것을 방지하고 보안 강도를 동적으로 조절할 수 있도록 해준다. 제안 방법은 WSN기반 IoT 시스템 응용 분야들에서 네트워크 보안을 더욱 강화시킬 것으로 기대한다. 우리는 추후 제안 방법의 상황 추론 과정에 퍼지 논리를 적용하여 규칙 기반 시스템을 구성하고 다양한 실험 환경을 만들어 제안 방법의 타당성을 검증할 계획이다.

ACKNOWLEDGEMENT

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

참고문헌

[1] 박상기, and 이명래. "중소기업을 위한 스마트팩토리." (2016).

[2] GTAI, http://www.gtai.de/GTAI/Navigation/EN/Invest/Industries/Smarter-business/smart-solution

[3] 조혜지, 김용균 " 스마트 팩토리 기술 및 산업 동향"

정보통신기술진흥센터 15-25.
[4] 김현진, 김진영, and 백주련. "스마트 팩토리 보안 사고 유형 분석 및 대안 프레임 제시." 한국컴퓨터정보학회 학술발표논문집 26.2 (2018): 161-164.
[5] 이준희, 김신령, and 김영곤. "빅데이터 분석을 활용한 스마트 팩토리 이상탐지 및 보안 강화 시스템에 관한 연구." 한국통신학회 학술대회논문집 (2017): 347-348.