

산업용 IoT를 위한 BLE 기반 경량 MOM의 보안성 향상 기법

차중혁¹, 이재민², 김동성*

국립금오공과대학교 IT융복합공학과

{jh.cha¹, ljmpaul², dskim*}@kumoh.ac.kr

Security Enhancement Scheme of BLE-based Lightweight MOM for Industrial IoT

Joong-Hyuck Cha¹, Jae Min Lee², Dong Seong Kim*

Kumoh National Institute of Technology

Dept. of IT Convergence Eng.

요약

본 논문은 산업용 IoT 환경에서 BLE(Bluetooth low energy) 기반 경량 MOM(Message-oriented middleware)의 보안성 향상 기법을 제안한다. 산업용 IoT는 산업 공정 제어에 필요한 소형 센서, PLC, 모니터링 기기 등을 기반으로 저지연, 고신뢰 유무선 네트워크를 구축하고 있다. 특히, D2D(Device to device) 무선 통신에 Bluetooth, WiFi Direct가 대표적으로 활용되고 있으며, 이러한 기술들은 엣지 컴퓨팅 및 태스크 오프로딩 기술과 아울러 성장하고 있다. 그러나 Connection-oriented 기반의 D2D 통신은 IIoT의 이기종 기기 및 응용의 유동성 등 동적인 네트워크 구성에 적합하지 않다. 이에 BLE 기반 Message-oriented Middleware(MOM)의 연구를 통해 동적인 네트워크 구성을 도모하였으나, 산업용 IoT와 같이 보안이 요구되는 환경에서는 적용에 제한적이다. 본 논문에서는 이러한 BLE 기반 MOM의 보안성 향상을 위해 엣지 컴퓨팅 환경에서 노드 인증 기법을 제안한다.

I. 서론

산업용 IoT는 산업 공정 제어의 자동화를 목적으로 센서, RFID 등과 기존 산업환경을 다양한 유무선 통신 매체를 기반으로 결합하여 성장하고 있다[1][2]. 무선 통신 기술은 유선 통신 기술을 주축으로 저비용과 높은 유연성을 확보하여 D2D(Device to Device) 형태로 구성된다[3]. D2D 통신을 위한 대표적인 무선 통신 기술들은 Bluetooth, WiFi Direct가 있으며 엣지 컴퓨팅 및 태스크 오프로딩 기술에 활용되고 있다[4].

Bluetooth, WiFi Direct와 같은 무선 통신 기술들은 사용자의 Pairing, Connection과 같은 절차만으로 데이터 교환이 가능하므로 일반적인 유선 통신 기술들보다 저비용과 높은 유연성을 확보할 수 있다. 이에 산업용 IoT 환경에서 무선 통신 기술로 Bluetooth, WiFi Direct 등을 적용하는 연구가 진행되고 있다. 그러나 이러한 사용자 기반의 Connection-oriented 특성은 동적인 네트워크 구성에 한계가 있어, BLE(Bluetooth low energy) 기반의 MOM(Message-oriented middleware)이 연구되었다[5]. 해당 연구는 BLE 프로토콜의 Advertising 패킷을 활용하여 Topic 중심의 발간/구독 기반 데이터 교환을 이루어 네트워크 유동성을 확보하였다. 그러나 인증되지 않은 노드의 참여가 가능한 구조를 가지기 때문에 산업용 IoT와 같이 보안이 요구되는 환경에서 적합하지 않다.

본 논문에서는 산업용 IoT의 엣지 컴퓨팅 환경에서 BLE 기반 경량 MOM의 보안성 향상을 위해 네트워크 참여자 인증 기법을 제안한다. 제안하는 인증 기법은 OTP(One-time password)의 시간 동기화 방식을 활용하여 엣지 서버에서 엣지 기기들을 인증 및 관리하여 보안성을 확보할 수 있게 한다.

II. BLE 기반 Message-oriented Middleware 분석

그림 1은 BLE의 기본 데이터 패킷 구조와 Peripheral(Slave)-Central(Master) 간의 데이터 교환 절차를 보여준다. BLE 데이터 패킷은 Preamble, Access Address, PDU(Protocol Data Unit), CRC(Cyclic Redundancy Check)로 구성된다. 이 중 PDU는 BLE의 Advertising/Pairing/Connection 단계에 맞춰 활용된다. Advertising 단계에서 장치 간의 연결을 위해 정보를 교환하고, Pairing 단계에서 서로를 인증한 뒤 연결돼 데이터를 송수신한다. 기존 BLE 기반 MOM은 소형 이기종 센서 노드들의 네트워크 유동성 확보를 위해 Pairing 과정을 거치지 않고, Advertising 단계에서 데이터를 교환하고자 하였다. 해당 연구는 Broadcasting 기반으로 송수신하여 각 노드를 인증하는 Pairing 단계를 거치지 않아 인증되지 않은 노드의 참여가 가능하여 보안에 취약하다는 문제점이 있다. 이에 본 논문에서는 산업용 IoT 환경의 보안성 및 네트워크 유동성 확보를 위해 BLE 기반 경량 MOM에 네트워크 참여자 인증 기법을 적용하고자 한다.

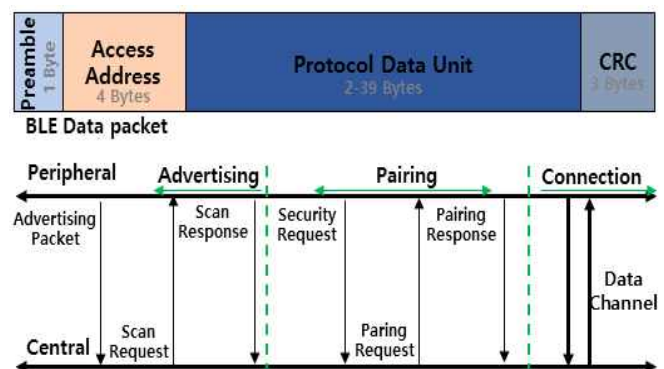


그림 1. BLE의 데이터 패킷 구조 및 교환 절차

III. BLE 기반 경량 MOM의 보안성 향상 기법

그림 2는 본 논문에서 제안하는 BLE 기반 경량 MOM의 보안성 향상을 위한 프레임워크를 보여준다. 제안하는 프레임워크는 산업용 IoT의 엣지 컴퓨팅 플랫폼을 기반으로, 엣지, 엣지 서버, 클라우드를 구성하고 각각의 역할을 서술하였다. 먼저, 각 엣지는 UUID(Universally unique identifier), 시리얼 넘버를 장비설치 과정에서 부여받고 이는 클라우드에 등록하여 연동한다. 그리고 클라우드는 엣지 서버의 도메인 정보를 저장하고 관리하고, 엣지 서버는 자신의 도메인 내의 엣지들의 UUID 및 시리얼 넘버를 클라우드로부터 받아 저장한다. 이때 도메인은 네트워크의 안정성을 위해 BLE 기반 MOM이 엣지 서버가 하나의 도메인을 구성하게 한다. 그리고 엣지 서버는 UUID로 엣지를 식별하고, 시리얼 넘버를 활용하여 OTP를 생성하여 엣지를 인증하고 관리한다.

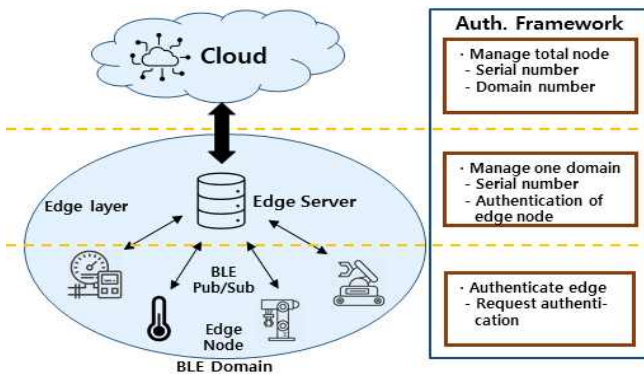


그림 2. BLE 기반 경량 MOM의 보안성 향상을 위한 프레임워크

그림 3은 BLE 기반 경량 MOM의 엣지 인증을 위한 시퀀스 다이어그램을 보여준다. 제안하는 인증 기법은 BLE 기반 경량 MOM의 Simple Discovery 과정[5]에서 엣지의 인증을 이루게 된다. 먼저, 엣지와 클라우드에서 저장되는 시리얼 넘버와 UUID는 장비설치 단계에서 로컬로 저장하게 된다. 이는 BLE Advertising 단계의 특성상 UUID는 공유되기 때문에 시리얼 넘버를 추가하여 OTP 생성을 통해 보안성 향상을 하기 위함이다. 이후 클라우드는 엣지 서버에 시리얼 넘버와 UUID를 공유하고 엣지 서버는 이를 저장 및 관리한다. 그리고 엣지의 네트워크 참여를 위해 엣지는 OTP와 함께 엣지 서버에게 인증 요청을 한다. 엣지 서버는 저장된 UUID를 활용해 식별하고, 시리얼 넘버로 OTP 생성하여 비교 검증하여 인증한다. 그리고 주기적으로 클라우드, 엣지 서버, 엣지의 시간을 동기화한다.

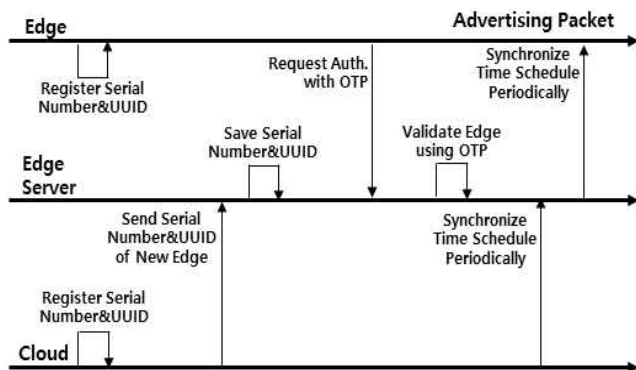


그림 3. BLE 기반 경량 MOM의 인증을 위한 시퀀스 다이어그램

그림 4는 제안하는 보안성 향상 기법을 적용한 BLE 기반 경량 MOM을 엣지 노드들과 엣지 서버를 구현한 결과를 보여준다. 엣지 노드들은 비접촉, 접촉식 체온계를 각각 Adafruit Mini, Arduino를 활용하여 시제품으

로 구현하였다. 엣지 서버는 일반적인 사무용 컴퓨터에 블루투스 4.0 동글을 활용하여 구성하였다. 그리고 클라우드는 Firebase를 활용하여 테스트를 진행하였으며 엣지들은 “Temp”를 Topic으로 등록하고 제안하는 시퀀스 다이어그램과 비교하고 검증이 이루어지는지를 확인하였으며 정상작동함을 보였다.

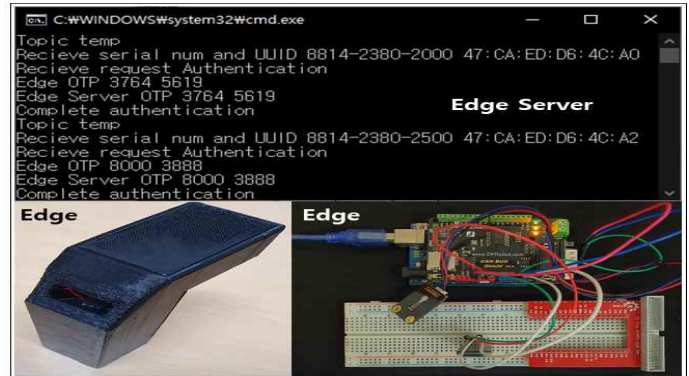


그림 4. 제안하는 보안성 향상 기법을 적용한 BLE 기반 경량 MOM

III. 결론 및 향후 연구

본 논문에서는 산업용 IoT 환경을 위해 BLE 기반의 MOM의 보안성 향상 기법을 제안하고 구현하였다. 보안성 향상 기법은 엣지 컴퓨팅 플랫폼을 활용한 프레임워크와 인증 절차로 이루어지며, 클라우드 서비스를 구성하여 타 서비스와 연동이 가능하게 하였다.

향후에는 대규모 산업용 IoT 환경을 위한 네트워크 설계 기법, Advertising 패킷의 실시간성 향상을 위한 스케줄링 기법 등 BLE 기반 MOM의 확장성과 최적화 관련 연구를 진행하고자 한다.

ACKNOWLEDGMENT

본 연구는 과학기술정보통신부 및 정보통신기획평가원의 Grand ICT연구센터지원사업(IITP-2020-2020-0-01612)과 2009년도 정부(교육과학기술부)의 재원으로 한국연구재단의 대학중점연구소 지원사업(2018R1A6A1A03024003)으로 수행된 연구결과임.

참고 문헌

- [1] D.-S. Kim and H. D. Tran, “Industrial Sensors and Controls in Communication Networks - From Wired Technologies to Cloud Computing and the Internet of Things,” Springer, 2018.
- [2] J. Sengupta, S. Ruj, and S. Bitra, “A Comprehensive Survey on Attacks, Security Issues and Blockchain Solutions for IoT and IIoT,” Journal of Network and Computer Applications, Vol. 149, Jan. 2020.
- [3] M. Rusyady, S. Bhardwaj, and D.-S. Kim, “Toward Reliable Fog Computing Architecture for Industrial Internet of Things,” Preprints 2019, 2019030096 (doi: 10.20944/preprints201903.0096.v1).
- [4] F. Li, Z. Guo, B. Liang, X. Yi, X. Wang, W. Li, and Y. Wang, “A measurement study on device-to-device communication technologies for IIoT,” Computer Networks, Vol. 192, June 2021.
- [5] J. H. Cha, J. M. Lee, and D. S. Kim, “BLE-based lightweight message-oriented middleware in Wireless Sensor Network,” 2021 Winter Conference on KICS, Yong Pyeong Resort, Pyeongchang, Korea, Feb. 3-5, 2021.