JKIICE Journal of the Korea Institute of Information and Communication Engineering

한국정보통신학회논문지 Vol. 25, No. 3: 440~448, Mar. 2021

스마트 그리드를 위한 블록체인 기반 LoRa 멀티홉 네트워크 설계

전성호[1] · 김승구[2*]

A Design of Blockchain-based LoRa Multi-hop Network for Smart Grid

Seongho Jeon[1] · Seungku Kim[2*]

[1]Graduate Student, Department of Electronic Engineering, Chungbuk National University, Cheongju, 28644 Korea

[2*]Associate Professor, Department of Electronic Engineering, Chungbuk National University, Cheongju, 28644 Korea

요 약

본 논문은 스마트 그리드 환경에 사용되는 네트워크 기술의 문제점을 제시하고, 이를 해결하기 위해 블록체인 기반의 LoRa 멀티홉 네트워크를 제안하고 구현한다. 스마트 그리드는 다양한 환경에 구축되어 운영되기 때문에 인터넷 인프라 구축이 불가능한 경우가 있다. 저자는 Flooding 라우팅 프로토콜을 사용한 멀티홉으로 LoRa 네트워크를 제안한다. 스마트 그리드 환경은 응용에 따라 다양한 전력망 프로토콜을 사용하는 독립적인 네트워크를 구성한다. 이는 네트워크마다 독립적인 인프라를 구축해야 한다는 문제가 있다. 이를 하나의 게이트웨이 장치가 다중 전력망 프로토콜을 지원하여 네트워크 통합이 가능한 방법을 구현한다. 마지막으로 스마트 그리드 환경에서 데이터의 무결성을 보장하기 위해 하이퍼레저 기반의 블록체인을 LoRa 네트워크에 적용하고 물리적으로 분산하여 보안성을 강화하였다. 세 가지 제안사항을 실제 테스트베드에 구축 후 실험을 통해 네트워크가 정상적으로 동작함을 확인하였다.

ABSTRACT

This paper presents problems of network technology in smart grid and implements a blockchain-based LoRa multi-hop network to solve them. Since some smart grid applications are operated in harsh environments, it is difficult to establish communication infrastructure. We propose a LoRa network with multi-hop using the Flooding routing protocol. Smart grid environment composes an independent network using various power grid protocols depending on the application. Since this has a problem that an independent infrastructure must be established for each network, a single gateway device supports multiple power grid protocols to implement a method for network integration. Lastly, the author applied Hyperledger-based blockchain to the LoRa network to ensure the integrity of data in a smart grid environment, and strengthened security by physically distributing it. After constructing the three suggestions on the actual test bed, we confirmed that the network operates normally through experiments.

키워드 : LoRa, 네트워크, 블록체인, 스마트 그리드, 전력망 프로토콜

Keywords : LoRa, Network, Blockchain, Smart grid, Power network protocol

Received 6 January 2021, **Revised** 12 January 2021, **Accepted** 17 January 2021

*** Corresponding Author** Seungku Kim(E-mail:kimsk@cbnu.ac.kr, Tel:+82-43-261-2479)
Associate Professor, Department of Electronic Engineering, Chungbuk National University, Cheongju, 28644 Korea

Open Access http://doi.org/10.6109/jkiice.2021.25.3.440 print ISSN: 2234-4772 online ISSN: 2288-4165

Ⅰ. 서 론

IT 기술이 발전하면서 멀게만 느껴졌던 스마트 그리드(Smart Grid)가 우리의 일상과 가까워지고 있다. 그에 따라 스마트 그리드 분야에 세 가지 이슈가 생기게 되었다. 첫 번째는 스마트 그리드의 통신 반경 문제이다. 낮은 토지비용과 구축의 효율을 위해 상대적으로 인프라가 부족한 지역에 집중된 신재생에너지는 인터넷 통신 인프라 구축에 비용이 많이 소모된다. 따라서 인터넷을 대신하여 인프라 구축이 저렴하고 넓은 범위 통신과 배터리 성능이 좋은 LPWAN(Low Power Wide Area Network)이 주목을 받고 있다. 두 번째는 스마트 그리드의 독립적인 네트워크 인프라 구축문제이다. 다양한 분야의 스마트 그리드에서 전력망 프로토콜이 각자 다르게 사용되고 있다. 이는 하나의 데이터를 각기 다른 전력망 프로토콜과 연결해야 한다는 것을 뜻한다. 세 번째는 스마트 그리드의 데이터 보안 문제이다. 데이터가 해킹 등으로 데이터의 위조나 변조가 일어나게 되면 사용량보다 적거나 많게 신고될 수 있다. 이를 방지하기 위해 데이터의 무결성을 보장하는 보안 방안들이 중요해지고 있다.

본 논문에서는 통신의 경우 기존의 통신 범위보다 원거리 통신이 가능하도록 LPWAN 중 LoRa 네트워크를 멀티홉으로 구성하여 기존의 통신 거리를 확장하는 방안을 제안한다. 멀티홉 네트워크는 패킷 전송 시 송신 노드에서 직접 최종 수신 노드로 전송하는 기존의 방식이 아닌 1개 이상의 중계 노드를 경유하는 전송방식을 뜻한다. 그 결과 각 노드의 통신 거리를 중계 노드 수만큼 더하여 통신 거리를 늘릴 수 있다. 독립적인 네트워크 경우 기존의 파편화된 전력망 네트워크를 통합한 멀티 전력망 게이트웨이를 제안한다. 하나의 데이터를 각 전력망 서버로 연결해주도록 게이트웨이 내에 각 프로토콜에 맞는 클라이언트를 통합 구현하여 서버와 연동한다. 세 번째는 스마트 그리드의 데이터 보안 문제이다. 데이터를 블록체인 네트워크의 원장에 기록하여 데이터의 무결성을 보장하는 방법을 제안한다. 특히 물리적인 공격에도 데이터의 손실을 막기 위해 기존의 서버에 논리적으로 분산화된 블록체인이 아닌 각 게이트웨이를 블록체인 네트워크로 연결하여 물리적으로 분산된 블록체인 네트워크를 제안한다. 이는 해킹으로부터 데이터의 무결성을 보장하고, 물리적인 공격에서도 데이터의 손실을 막을 수 있다.

본 논문에서는 스마트 그리드의 세 가지 이슈를 해결하기 위한 블록체인 기반의 LoRa 멀티홉 네트워크를 제안한다. 2장에서는 관련된 연구들을 서술한다. 4장에서는 관련 연구를 바탕으로 문제점을 지적하고 이를 해결하려는 방안을 서술하여 결과적으로 블록체인 기반의 LoRa 멀티홉 네트워크를 제안하고 설계한다. 5장에서는 제안한 시스템을 바탕으로 테스트베드를 구축하여 네트워크가 정상적으로 형성되는지를 확인한다. 6장에서는 본 네트워크의 결론을 보이며 논문을 끝맺는다.

Ⅱ. 관련 연구

본 장에서는 스마트 그리드의 통신, 전력망 프로토콜, 보안에 관한 관련 연구들을 소개한다.

2.1. LoRa 네트워크

LoRa[1]는 LPWAN의 대표적인 통신 기술인 저전력 광범위 무선 통신 프로토콜이다. CSS 변조 방법과 물리계층의 SF(Spreading Factor) 조절을 통해 최대 20km의 통신 거리를 지원한다. 통신에 사용되는 네 가지 매개변수는 SF, Bandwidth, Coding Rate, TX Power이다. 주파수 대역은 ISM(Inderstrial, Scientific and Medical) 대역에서 사용되며 국내에서는 920~925MHz 대역을 사용한다. 최대 데이터 속도는 5.47kbps로 소량의 데이터를 장시간 동안 통신하는 데 적합하게 설계되었다. 또한, 배터리 수명이 10년 이상이기 때문에 한 번 설치해두면 약 10년간 센서 노드로 사용할 수 있다. 이론상 최대 20km의 통신 거리를 가지고 있는 LoRa지만 실제 실험 결과는 이론에 미치지 못한다.

Mohammad Mohammadi Erbati[2] 등은 실외 및 실내에서의 LoRaWAN의 통신 거리 측정에 관한 연구를 진행하였다. 도시 환경에서 LoRa 게이트웨이의 적용 범위를 측정하였고 실외 시나리오에서 1,850m의 통신 거리를 측정하게 되었다. 이는 기존의 LoRaWAN의 사양에서 도시 상황에서 이론적으로 측정 가능한 2~5km의 통신 범위보다 훨씬 적은 범위의 커버리지이다. 김동훈 등은 국내 스마트 에너지 캠퍼스 테스트베드에서 LoRa 네트워크를 구축할 때 복합 실내 및 실외 환경에서의 LoRa 통신 범위 측정할 때 LoRa PHY에 단순화된 경로

손실 모델을 설정하고 통신 범위 계산과 응용 프로그램 매개변수가 MAC 성능에 미치는 영향 등을 비교하였다[3]. 복합적인 실내 및 실외 환경에서 단순화된 경로 손실 모델로 최대 통신 거리에서 통신 신뢰성을 분석한 최대 범위는 1.34km로 나타났다. LoRa MAC 실험 성능에서 Payload 길이가 길어질수록, 패킷 전송 주기가 짧아질수록 패킷 전달률이 줄어드는 것을 확인했다. 이를 통해 다양한 SF 값으로 신뢰성 있는 최대 통신 범위를 최대 630m~1344m로 계산하였다. 위와 같은 LoRa의 통신 거리와 관련된 연구로 기존의 LoRa 네트워크의 최대 통신 범위가 다양한 환경에 따라 달라질 수 있음을 알 수 있다. 특히 NLOS 환경이 포함된다면 통신 거리는 매우 짧아진다. 이처럼 다양한 스마트 그리드 환경 때문에 LoRa의 통신 범위가 부족할 수 있다. 특히 해안지역 또는 고산지대의 신재생에너지 발전의 경우 단말과 게이트웨이 간의 통신 범위가 LoRa로는 부족할 수 있다. 이를 통해 통신 반경 확장이 필요하고 LoRa의 멀티홉 연구가 필요하다는 점을 알 수 있다.

2.2. 블록체인

블록체인의 사전적 정의는 "거래 정보를 블록 단위로 저장하고 체인 형태로 묶은 분산형 데이터 저장기술"을 말한다. 거래의 변조나 왜곡을 막기 위해 저장된 데이터를 블록 단위로 생성하고 분산하여 저장하기 때문에 데이터의 무결성을 보장할 수 있다. 쉽게 자료를 저장하고 복사할 수 있는 디지털 환경에서는 복사된 자료와 원본 간의 품질 차이가 나지 않는데 이는 누군가가 악의를 가지고 기록을 조작하거나 잘못된 기록을 남겨도 수정된 사본과 원본 간에 차이가 구분되지 않음을 보여준다. 이러한 문제를 해결하기 위해 블록체인은 국립표준기술연구소에 의해 공표된 표준 해시 알고리즘인 SHA-256 기반의 해시 함수를 암호로 사용한다. 해시 함수란 다양한 길이를 가진 데이터를 고정된 길이를 가진 데이터로 매핑하는 알고리즘으로 각각의 데이터를 텍스트로 표시할 경우 그 길이가 다를 수 있지만 해시 함수로 변환하면 항상 일정한 길이의 해시값이 나오게 된다. 이러한 해시 연산 과정을 거쳐 하나의 거래가 하나의 해시값에 대응하는 1대1 구조를 이루게 된다. 블록체인에는 크게 세 가지의 이점이 존재한다. 먼저 네트워크 참여자들이 직접 거래할 수 있는 P2P(Peer to peer) 방식이기 때문에 데이터의 탈중앙화 가능하다는 점이다. 다음은 원장에 기록된 거래는 변경 및 조작이 불가능하다는 점에서 데이터 무결성을 보장할 수 있다. 마지막으로 다수의 노드가 같은 블록을 분산 저장하고 있으므로 외부 공격에 안전하다.

Victor Ribeiro 등은 LoRaWAN 네트워크의 키 관리를 위한 블록체인 기반의 안전한 분산 스토리지 기능을 제안하였다[4]. 암호화 키는 Join Server에서 관리하지만 동일한 서버에 구현한 프라이빗 블록체인 인프라에 저장된다. 스마트 계약을 통해 LoRaWAN 환경에서의 키 관리를 블록체인 네트워크에서 담당하며 최종 장치의 인증 및 통신에 사용되는 보안 키의 가용성을 보장하는 안전한 분산 스토리지를 구성했다. Zakaria Abou El Houda 등은 안전한 스마트 그리드를 위해 AMI(Advanced Metering Infrastructure) 아키텍처에서 블록체인 기반의 접근 제어 방식을 제안하였다[5]. 기존의 접근 제어 방식은 홈 네트워크 내부에서 악성코드를 원격으로 실행시켰을 때 외부에서 스마트 미터로 직접 접근이 가능해지므로 DDoS (Distributed Denial of Service) 공격이 가능해짐을 지적하고 이를 블록체인을 활용하여 스마트 계약을 사용한 접근 제어로 관리하여 인증된 주체들만 리소스에 접근할 수 있게 구현했다. 보안에 관련한 블록체인 연구를 통해 스마트 계약과 분산 네트워크로 보안성을 높일 수 있음을 보았다. 하지만 기존의 연구들은 하나의 서버에 논리적으로 분산된 블록체인 네트워크를 구성하여 이를 구현했다. 이는 서버에 물리적인 공격이 가해졌을 때 기존에 구현해둔 블록체인 네트워크는 물론 관련 데이터의 손실도 가져올 수 있다. 이를 통해 물리적으로 분산된 블록체인 네트워크의 필요하다는 점을 알 수 있다.

Ⅲ. 제안하는 시스템

본 장에서는 스마트 그리드 환경에서 새로운 블록체인 기반 LoRa 멀티홉 네트워크를 제안한다.

3.1. LoRa 멀티홉 네트워크

본 논문에서는 메쉬 토폴로지 네트워크를 Flooding 라우팅 방식을 사용하여 구현하였다. Flooding은 특정 노드에서 수신한 패킷을 해당 노드의 통신 반경 내에 있는 모든 노드에 전달하는 방식으로 동작한다. 중계 노드

가 그와 접하는 노드의 통신 반경 내에 존재한다면 Flooding 라우팅을 통해 멀티홉으로 출발 노드와 도착 노드 간의 통신이 가능해진다. 이는 기존 NLOS 환경에서의 LoRa의 통신 범위를 확장할 수 있음을 보여준다. 하지만 기존 LoRa의 데이터 링크 계층에서 사용하는 Pure Aloha 매체 접근 방식은 노드가 전송할 패킷이 있으면 언제든지 전송하는 프로토콜이기 때문에 멀티홉 네트워크의 라우팅 과정 중에서 동시 전송 충돌에 의한 순환중복검사(Cyclic Redundancy Check) 오류가 일어날 수 있다. 순환중복검사 오류는 데이터 전송 시 순환중복검사를 사용하여 대기 순서표를 삽입하는데 이 순서대로 데이터가 들어오지 않을 때 발생하는 오류이다. 이를 줄이기 위해 LoRa 매체 접근 방식을 CSMA/CA 방식으로 구현하였다. CSMA/CA는 채널의 유휴상태를 판단하기 위해 채널의 에너지값을 확인한다. 에너지값이 정해진 임계값보다 크다면 다른 패킷이 채널을 점유하고 있다고 판단하고, 작다면 채널이 유휴상태라고 판단하고 패킷을 전송하게 된다. 이처럼 채널의 사용 여부를 판단하는 알고리즘을 통해 패킷 간의 충돌을 피할 수 있고 순환중복검사 오류를 줄일 수 있으며 추가로 처리량이 증가하고 데이터 손실이 적어지게 되는 이점이 있다.

3.2. 멀티 전력망 게이트웨이 구현

본 논문에서 사용한 프로토콜은 전력설비 감시, 계측, 제어, 보호를 위한 통신 프로토콜인 IEC61850과 전력에너지 분야 사물인터넷 규격인 e-IoT 서비스 제공을 위한 공통 플랫폼인 oneM2M을 사용한다. IEC61850은 전력 유틸리티 자동화를 위한 통신 네트워크와 시스템에 관한 표준으로 통신 프로토콜에 관한 내용을 포함해 애플리케이션에 초점을 맞춘 아키텍처를 정의하고 있다[6]. oneM2M은 공통 플랫폼을 글로벌 표준으로 제정하여 사물인터넷 시장을 확대하는 표준 플랫폼으로 스마트홈과 같은 로컬 디바이스로 구성된 서비스뿐만 아니라 클라우드 기반의 서비스를 제공할 수 있다[7].

이렇게 두 가지 전력망 프로토콜을 적용한 게이트웨이를 LoRa 모듈을 연결한 라즈베리 파이에 구현한다. 먼저 IEC61850은 모든 장비와의 연결을 위해 세부 규칙까지 규격을 정해야 하므로 장비 내에 포함하여 솔루션으로 제공하는 경우가 대부분이다. 이를 개발하기 위해 오픈소스로 제공하는 libIEC61850을 이용하여 구현했다[8]. IEC61850은 프로토콜의 목적 자체가 다양한 형태의 디바이스와 통신할 수 있게 하는 것이 목표이므로 전달하고자 하는 데이터의 자료형(int, float, char 등)을 서버와 클라이언트 모두 맞춰주어야 한다. 게이트웨이 내에 IEC61850 클라이언트를 구현하여 모니터링 서버로 송신할 수 있도록 구현하였다. oneM2M은 오픈소스로 제공하는 Mobius 플랫폼을 사용했다. Mobius는 IoT 디바이스 정보를 관리하고 접근 제어, 인증, 사용자 관리, 복수의 IoT 서비스 조합을 제공하는 애플리케이션을 통한 서비스 플랫폼이다[9]. 게이트웨이 내의 클라이언트는 Mobius 플랫폼 내의 게이트웨이인 nCube Thyme을 사용하였다. nCube는 TAS(Thing Adaptation Software)라는 실제 사물을 디바이스로 연결하기 위한 소프트웨어를 통해 데이터를 획득할 센서를 디바이스에 연결하기 위한 소프트웨어로 센서와 nCube Thyme 간의 연결통로를 만드는 역할을 한다. 그 후 데이터를 Mobius 서버로 전송하는 방식으로 동작한다[10]. 이를 위해 데이터를 TAS에서 병렬적으로 처리 가능한 TAS 메시지로 구성이 필요하다.

게이트웨이의 위의 두 가지 클라이언트에 LoRa 통신으로부터 전송받은 데이터를 전달하는 방법으로 게이트웨이 내부의 LoRa 컨트롤러와 두 개의 클라이언트 간의 프로세스 간 통신을 사용하였다. LoRa 컨트롤러와 IEC61850 클라이언트는 동일한 C++ 언어 프로그램이므로 데이터 공유 방식을 사용하였다. LoRa 컨트롤러와 oneM2M 클라이언트는 Mobius가 Javascript 기반의 node.js로 구현되어 있어서 이종 언어 간의 통신을 위해 메시지 교환 방식인 Unix domain socket을 사용하였다. 그러므로 LoRa 컨트롤러에서 데이터를 데이터 공유 방식과 Socket 통신방식을 모두 사용하도록 구현하였고 각각 클라이언트에서 데이터를 정상적으로 받아오도록 프로그래밍하였다.

3.3. 물리적으로 분산된 블록체인 네트워크

물리적으로 분산된 블록체인 네트워크는 기존의 서버 내에 논리적으로 분산화한 블록체인 네트워크와 달리 물리적인 탈중앙화를 이룬다는 이점이 있다. 물리적인 탈중앙화는 각 블록체인 노드가 개별적으로 분산원장을 가지고 있다는 뜻이고 물리적인 공격에 있어서 데이터의 손상을 방지하고 무결성을 보일 수 있다. 물리적으로 분산된 블록체인 네트워크는 LoRa 게이트웨이에 구현한다.

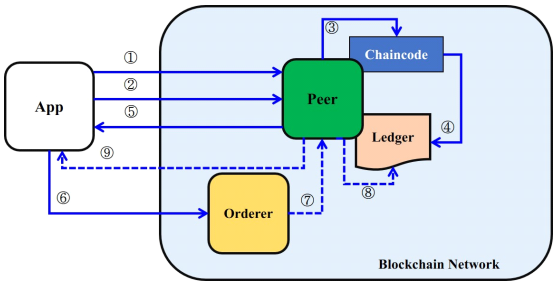


Fig. 1 Hyperledger Fabric Network Transaction Process

블록체인 플랫폼은 하이퍼레저 패브릭(Hyperledger Fabric)을 사용한다. 하이퍼레저 패브릭은 IBM에서 개발한 허가형 프라이빗 블록체인으로 그림 1과 같이 클라이언트(Client), 피어(Peer), 오더러(Orderer) 이렇게 세 가지 구조로 볼 수 있다[11]. 클라이언트는 블록체인 네트워크와 통신을 할 수 있도록 해주는 애플리케이션 노드이다. 거래 요청이 들어오면 피어 노드에 트랜잭션(Transaction, 거래)을 생성해서 엔도저(Endorser, 보증) 피어에 보내는 일을 한다. 이후 거래에 대한 응답(Response)이 들어오면 해당 거래에 대한 제안(Proposal)을 오더러에 보내게 된다. 피어는 하이퍼레저 패브릭에 가장 기본이 되는 노드로 거래 원장(Ledger)과 체인코드(Chaincode)를 가지고 있다. 클라이언트로부터 받은 트랜잭션을 검증하고 응답하여 오더러가 합의 과정 하도록 하여 합의가 된 트랜잭션에 대해서는 원장에 기록하여 갱신한다. 엔도저 피어는 체인코드가 설치된 피어로 트랜잭션 제안을 받아 체인코드로 시뮬레이션을 한 후 거래가 온전한지 확인한다. 앵커(Anchor) 피어는 같은 채널의 피어를 연결해주는 노드이며 트랜잭션을 다른 피어들에 전달한다. 커미터(Committer) 피어는 오더러가 생성한 블록을 전달받아 체인에 연결하는 피어이며 블록의 검증이 유효한 경우 원장을 업데이트 하는 피어이다. 오더러는 트랜잭션에 대한 합의 알고리즘에 따라 블록을 생성하는 역할을 한다. 합의 알고리즘의 종류는 Solo, Kafka, Zookeeper 등이 있으며 각 알고리즘에 따라 트랜잭션의 순서를 정렬한다.

블록체인 네트워크 구성을 위해 라즈베리 파이에 구현한 통합 프로토콜 게이트웨이에 하이퍼레저 패브릭을 설치한다. 하지만 라즈베리 파이는 하이퍼레저 패브릭이 지원하지 않는 ARM 아키텍처를 기반이기 때문에 라즈베리 파이에서 동작할 수 있게 컨테이너 기반의 오픈소스 가상화 플랫폼인 도커(Docker)를 사용하여 설치한다. 먼저 기존의 하이퍼레저 패브릭 코드를 수정하여 ARM 아키텍처에서 동작할 수 있게끔 설계한다. 수정한 파일과 설정값들을 컨테이너로 저장하여 도커 이미지로 관리한다. OS와 격리된 구조로 서비스를 구동하기 때문에 라즈베리 파이에서 사용이 가능하다. 물리적인 탈중앙화를 이루는 분산 블록체인 네트워크는 각 피어를 게이트웨이에 각각 생성하고 이를 인터넷으로 묶어서 구현한다. 오더러는 1번 게이트웨이에 구성하여 블록생성을 관장하고 나머지 게이트웨이에는 하나의 피어를 구성하여 애플리케이션으로부터 블록체인 네트워크 접근 요청에 따라 트랜잭션을 과정을 거치게 한다. 클라이언트 애플리케이션은 node.js로 구현하였으며 LoRa 패킷으로부터 데이터를 전달 받기 위해 메시지 전달 방식인 Unix domain socket으로 구현했다. 전달받은 데이터는 트랜잭션 과정을 거쳐 각 피어의 원장에 분산되어 기록된다.

본 논문에서 제안하는 스마트 그리드를 위한 블록체인 기반 LoRa 멀티홉 네트워크의 전체 구조는 그림 2와 같다.

Ⅳ. 성능 평가

본 장에서는 앞서 제안한 시스템을 구현하여 실제 환경에서 테스트베드를 구축하여 실험한다. 4.1절은 실험 환경에 관해 설명하고 4.2절에서 성능 평가를 통해 네트워크가 정상적으로 작동하는지 확인한다.

4.1. 실험 환경

LoRa를 멀티홉 네트워크로 구현하기 위해 프로그래밍에 용이한 라즈베리 파이 3 B+에 Libelium의 Cooking hacks 쉴드와 Semtech의 LoRa 네트워크 칩인 SX1272을 연결해 LoRa 센서 노드 및 게이트웨이로 사용하였다[12]. LoRa 주파수 대역은 국내에서 사용 가능한 ISM 대역인 920MHz 주파수 채널에서 실험하였다. 충북대학교 내에서 멀티홉 네트워크를 구성하기 위해 전송범위를 줄여서 실험하였고 LoRa의 매개변수는 SF 8, Bandwidth 500kHz, Coding Rate 4/5, Tx power 5.012mW를 사용하였다. LoRa의 데이터 링크 계층의 MAC 프로토콜은 CSMA/CA를 사용하고 네트워크 계

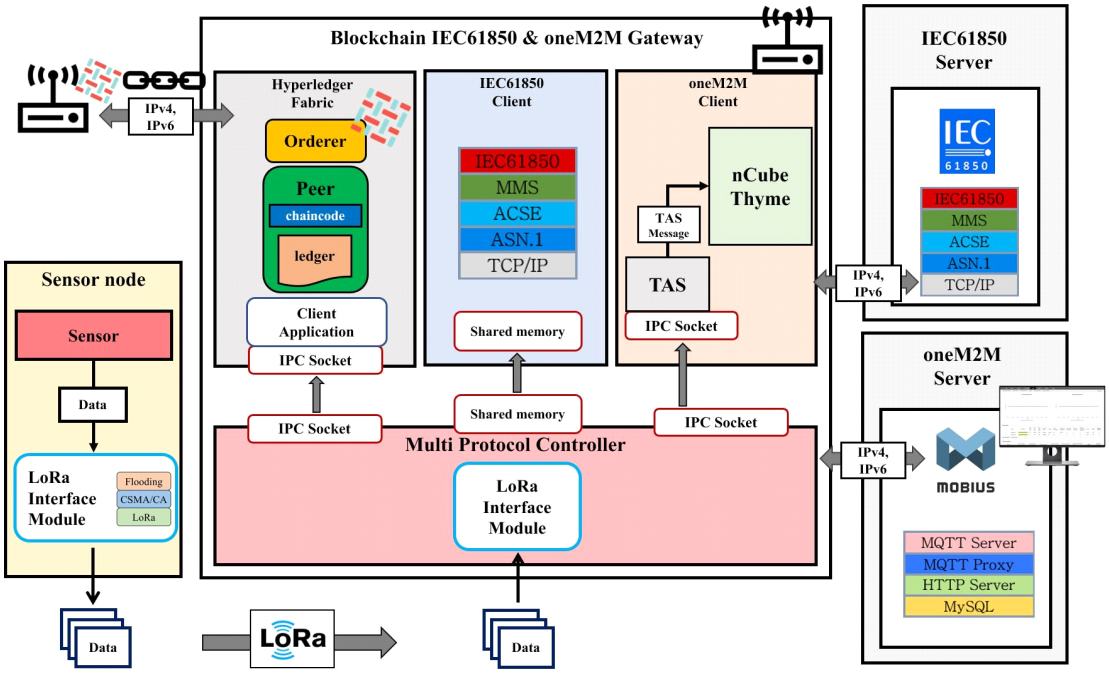


Fig. 2 Blockchain-based LoRa multi-hop network architecture

층의 라우팅 프로토콜은 Flooding을 사용하였다. 사용 OS는 블록체인 플랫폼인 하이퍼레저 패브릭의 사양을 맞추기 위해 Raspberry Pi OS 64bit를 사용하였다.

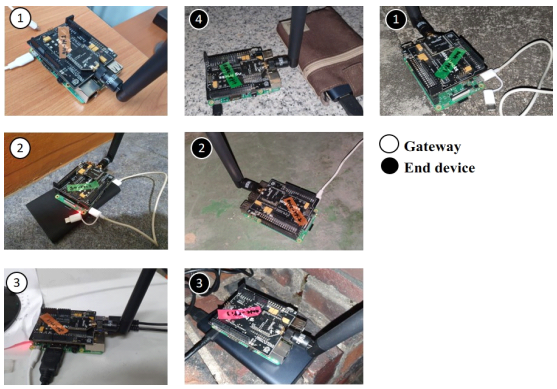


Fig. 3 Photos of gateway/sensor nodes placed on the campus of Chungbuk National University

게이트웨이는 3장에서 구현한 시스템을 사용하였다. 블록체인 플랫폼은 하이퍼레저 패브릭 1.4를 Docker 이미지로 구현하여 ARM 환경에서 동작하게 하였다.

실험은 충청북도 청주시 충북대학교 내에 구축한 테스트베드에서 진행하였다. 그림 3과 같이 3개의 게이트웨이와 4개의 센서 노드를 사용하여 네트워크를 구축하였다. 게이트웨이 1~3은 물리적으로 분산된 블록체인 네트워크를 구성하기 위해 인터넷에 연결하였다. 센서 노드 1, 4는 멀티홉 확인을 위해 2홉으로 구성하였고 나머지는 1홉으로 구성하였다.

4.2. 실험 결과

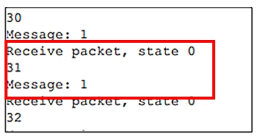
실험은 멀티홉 네트워크의 성능평가, 물리적 공격 후 블록체인 네트워크 확인, 테스트베드 내에서 네트워크 확인까지 총 세 가지를 확인한다. 먼저 1홉으로 구성한 LoRa 네트워크와 2홉으로 구성한 LoRa 멀티홉 네트워크의 성능을 비교한다. 표 1의 Latency는 1홉의 네트워크 지연시간과 2홉의 네트워크 지연시간을 비교한 결과이다.

Table. 1 LoRa Multi-hop Performance Evaluation

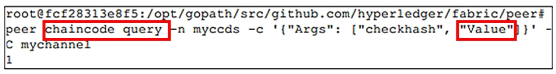
	Latency (ms)	Packet Loss Rate (%)
1-hop	37	124
2-hop	100	98

먼저 1홉으로 구성한 LoRa 네트워크와 2홉으로 구성한 LoRa 멀티홉 네트워크의 성능을 비교한다. 표 1의 Latency는 1홉의 네트워크 지연시간과 2홉의 네트워크 지연시간을 비교한 결과이다. 2홉 네트워크의 지연시간이 1홉 네트워크의 지연시간보다 87ms 긴 것을 알 수 있다. 2홉은 멀티홉 구성으로 센서 노드와 게이트웨이 사이에 중간 노드를 거치기 때문에 1홉보다 지연시간이 더 걸리게 된다. 하지만 실시간으로 데이터를 확인하지 않고 일정한 시간 간격으로 계측 데이터를 전송하는 스마트 그리드 네트워크의 특성상 위와 같은 지연시간은 네트워크에 크게 영향을 미치지 않는다. 표 1의 Packet Loss Rate는 각 센서 노드에서 100개의 패킷을 보냈을 때 1홉 네트워크의 에러율과 2홉 네트워크의 패킷 손실률을 비교한 결과이다. 1-hop에서는 100개 모두 정상적으로 받았지만 2-hop에서는 2개를 놓친 것을 알 수 있다.

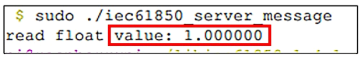
다음은 구축한 테스트베드에서 센서 노드와 게이트웨이 간의 LoRa 네트워크를 확인한다. 게이트웨이에서 수신한 패킷이 블록체인 네트워크에서 분산되어 저장되는지 확인하고 IEC61850과 oneM2M 프로토콜을 통해 서버로 전송되는지 확인한다. 먼저 각 센서 노드에서 LoRa로 패킷을 송신한다. 1홉으로 구성한 네트워크에서는 게이트웨이에서 바로 수신하고, 2홉으로 구성한 네트워크에서는 중간 노드의 Flooding 라우팅을 통해 게이트웨이에서 수신한다. 3개의 게이트웨이 모두 그림 4의 (a)와 같이 게이트웨이에서 센서 노드로부터 패킷이 정상적으로 수신됨을 확인하였다. 패킷이 수신되면 패킷 내의 데이터를 먼저 블록체인 네트워크의 체인코드와 연동되는 애플리케이션과 Socket 통신하여 데이터를 전달하게 된다. 그 후 애플리케이션에서 체인코드와



(a) Receive Packets from Gateway



(b) Check Value on Blockchain ledger

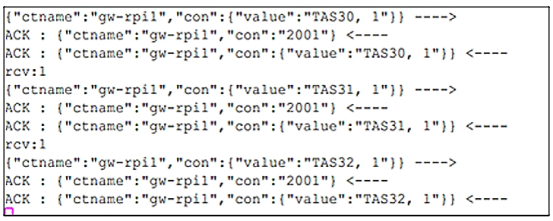


(c) Checking data on IEC 61850 servers

Fig. 4 Check received packets with the Blockchain ledger and IEC61850 server

트랜잭션 과정을 거치게 되고 결과적으로 invoke 함수를 통해 원장에 기록되었다. 각 게이트웨이에서 그림 4의 (b)처럼 query 함수를 통해서 값을 확인할 수 있음을 확인하였다.

또한, 패킷 내 데이터를 IEC61850 클라이언트와 메모리 공유 방식으로 데이터를 전달하여 전력망 프로토콜로 통신을 확인하였다. 그림 4의 (c)와 같이 IEC61850 서버에서 데이터가 정상적으로 서버에 출력됨을 확인하였다.



(a) Transform incoming data into TAS Message

(b) Send to Mobius Server

Fig. 5 Send received packets to Mobius

다음은 패킷 내 데이터를 oneM2M 클라이언트로 보내어 서버로 전송하는 과정을 확인한다. 패킷 데이터와 Socket 통신으로 oneM2M 클라이언트로 전송된 데이터는 TAS에서 TAS 메시지로 변환하는 과정을 거친다. TAS 메시지는 데이터를 병렬적으로 처리하여 그림 5의 (a)처럼 JSON 형식의 데이터로 변환하여 nCube Thyme에 전송하게 된다. TAS 메시지는 ctname과 con으로 구성되는데 ctname은 게이트웨이의 이름을 의미하고 con은 실제 데이터값을 나타낸다. 데이터 전송이 성공했다면 nCube Thyme이 TAS에게 ACK (acknowledgement code)를 보내 정상적으로 수신됨을 알리고 nCube Thyme은 TCP/IP 모듈을 이용하여 Mobius 서버로 메시지를 그림 5의 (b)처럼 전송한다. 마지막으로 Mobius 서버에 전송받은 데이터는 리소스 모니터링 웹서버에서 게이트웨이별로 확인할 수 있다. 이를 통해 제안한 네트워크가 테스트베드에서 정상적으로 동작함을 확인하였다.

마지막으로 네트워크 동작 중 블록체인 네트워크를 형성한 게이트웨이에 물리적인 공격 발생 시에도 타 게이트웨이에서 분산원장으로 데이터가 유지되는지 확인한다. 실험은 1번 게이트웨이가 물리적인 공격으로 전원이 꺼짐을 가정한다. 그림 6과 같이 1번 게이트웨이에서 수신했던 데이터가 3번 게이트웨이의 원장에서 정상적으로 남아있어 물리적으로 분산화된 블록체인이 물리적 공격에 우수함을 알 수 있다.

```
root@peer0:/opt/gopath/src/github.com/hyperledger/fabric/peer# peer chaincode query -n myccds -c '{"Args": ["checkhash", "Value"]}' -C mychannel
gw1: 12
```

(a) Data available from the ledger on Gateway 1

```
root@peer2:/opt/gopath/src/github.com/hyperledger/fabric/peer# peer chaincode query -C mychannel -n myccds -c '{"Args":["checkhash","Value"]}'
gw1: 12
```

(b) Data available from the ledger of gateway 2 after power off gateway 1

Fig. 6 Decentralized blockchain ledger safe from physical attacks

V. 결 론

본 논문에서는 다양한 스마트 그리드 환경에 적용 가능한 블록체인 기반의 LoRa 멀티홉 네트워크를 제안하였다. 기존 스타 토폴로지의 LoRa 네트워크는 인프라 구축이 어려운 격오지에 위치한 스마트 그리드 환경에서 통신 거리가 부족할 수 있으므로 LoRa 네트워크를 멀티홉으로 구현하도록 메쉬 토폴로지의 Flooding 라우팅 알고리즘을 사용하여 통신 거리를 확장하였다. 이렇게 받은 데이터는 다양한 전력망 프로토콜을 따라 각각 구현된 게이트웨이로 보내지는 기존의 방식에서 게이트웨이를 통한 멀티 프로토콜로 구현하여 하나의 게이트웨이에서 각 서버로 보내는 방식으로 네트워크를 설계하였다. 다양한 전력망 프로토콜 중 IEC61850과 oneM2M을 사용하였고 각 클라이언트를 라즈베리 파이 게이트웨이 통합하여 IEC61850 서버와 oneM2M 플랫폼인 모비우스 서버로 연동되도록 구현하였다. 또한, 게이트웨이 해킹으로 데이터의 변조가 가능하므로 데이터 무결성을 보장하기 위해 블록체인 네트워크를 구성하여 블록 내의 원장에 기록하여 관리하였다. 기존의 서버에 구현되어 논리적으로 분산된 블록체인 네트워크는 물리적인 공격에 취약하다는 점을 지적하고 이를 개선하기 위해 물리적으로 분산화한 게이트웨이를 제안하여 물리적인 공격에도 데이터의 안전을 보장할 수 있도록 구현하였다. 구현한 네트워크로 테스트베드를 구축하여 정상적으로 네트워크가 동작함을 확인했다. 블록체인 기반의 LoRa 멀티홉 네트워크는 다양한 스마트 그리드 환경에 적용할 수 있고 데이터의 무결성을 보장하기 때문에 넓은 범위의 통신이 필요한 전력 네트워크를 구성할 때 유용하게 사용이 가능할 것으로 기대한다.

ACKNOWLEDGEMENT

This work was supported by the National Research Foundation of Korea(NRF) grant funded by the Korea government(MSIP) (No. 2019R1 F1A1061970).

REFERENCES

[1] LoRa Alliance. LoRaWAN Specification v1.1 [Internet]. Available: https://lora-alliance.org/resource-hub/lorawanr-specification-v11.

[2] M. M. Erbati, G. Schiele, and G. Batke, “Analysis of LoRaWAN technology in an Outdoor and an Indoor Scenario in Duisburg-Germany,” *2018 3rd International Conference on Computer and Communication Systems*, Nagoya, pp. 273-277, 2018.

[3] D. H. Kim, E. K. Lee, and J. H. Kim, “Experiencing LoRa Network Establishment on a Smart Energy Campus Testbed,” *Sustainability*, vol. 11, no. 7, pp. 1917, 2019. DOI: https://doi.org/10.3390/su11071917.

[4] V. Ribeiro, R. Holanda, A. Ramos, and J. J. P. C. Rodrigues, “Enhancing Key Management in LoRaWAN with Permissioned Blockchain,” *Sensors*, vol. 20, no. 11, pp. 3068, 2020. DOI: https://doi.org/10.3390/s20113068.

[5] Z. A. E. Houda, A. Hafid, and L. Khoukhi, “Blockchain Meets AMI: Towards Secure Advanced Metering Infrastructures,” *ICC 2020 - 2020 IEEE International Conference on Communications (ICC)*, Dublin, Ireland, pp. 1-6, 2020.

[6] IEC61850-7 Communication networks and systems for power utility automation – Part 7-3: Basic communication structure for substation and feeder equipment – Common data classes Edition [Internet]. Available:

https://joinup.ec.europa.eu/collection/ict-standards-procurement/solution/iec-61850-7-32010-communication-networks-and-systems-power-utility-automation-part-7-3-basic.
[7] oneM2M. oneM2M Release 2 Technical Specifications [Internet]. Available: https://www.onem2m.org/technical/published-drafts/release-2.
[8] libIEC61850. libIEC61850 open source libraries for IEC 61850 [Internet]. Available: http://libiec61850.com/libiec61850.
[9] Mobius. Installation Guide Mobius_v2 [Internet]. Available: https://github.com/IoTKETI/Mobius/wiki.
[10] Mobius. User guide nCube Thyme for node.js v2 [Internet]. Available: https://github.com/IoTKETI/nCube-Thyme-Nodejs/wiki.
[11] E. Androulaki, A. Barger, V. Bortnikov, C. Cachin, K. Christidis, A. D. Caro, D. Enyeart, C. Ferris, G. Laventman, Y. Manevich, S. Muralidharan, C. Murthy, B. Nguyen, M. Sethi, G. Singh, K. Smith, A. Sorniotti, C. Stathakopoulou, M. Vukolić, S. W. Cocco, and J. Yellick, “Hyperledger fabric: a distributed operating system for permissioned blockchains,” in *Proceedings of the Thirteenth EuroSys Conference*, New York: NY, pp. 1-15, 2018.
[12] Semtech, SX1272/3 Datasheet [Internet]. Available: https://www.semtech.com/products/wireless-rf/lora-transceivers/sx1272.

전성호(Seongho Jeon)

2019년 2월: 충북대학교 전자공학부 공학사
2019년 3월 ~ 현재: 충북대학교 전자공학전공 석사과정
※관심분야 : LPWAN, LoRa, Blockchain

김승구(Seungku kim)

2007년 2월: 고려대학교 전기전자전파공학부 공학사
2010년 2월: 고려대학교 전자컴퓨터공학과 공학석사
2013년 8월: 고려대학교 전자컴퓨터공학과 공학박사
2013년 9월~2015년 8월: 삼성전자 소프트웨어센터 책임연구원
2015년 9월~현재: 충북대학교 전자공학부 부교수
※관심분야 : WSN, WBAN, VANET, Bluetooth