산업융합연구 제20권 제10호 pp. 17-24, 2022
ISSN 2635-8875 / e-ISSN 2672-0124
DOI : https://doi.org/10.22678/JIC.2022.20.10.017

안전한 Lora 네트워크를 위한 블록체인(A-PBFT) 기반 인증 기법

김상근*
성결대학교 컴퓨터공학과 교수

Blockchain (A-PBFT) Based Authentication Method for Secure Lora Network

Sang-Geun Kim*
Professor, Dept. of Computer Engineering, SungKyul University

요 약 장거리 무선 표준 LPWAN 표준의 비 대역망 기술인 Lora는 내부 단말 인증 및 무결성 검증에 ABP, OTTA 방식과 AES-128 기반 암호 알고리즘(공유키)을 사용한다. Lora는 최근 펌웨어 변조 취약점과 공유키 방식의 암호 알고리즘 구조상 MITM 공격 등에 방어가 어려운 문제가 존재한다. 본 연구는 Lora 네트워크에 안전성 강화를 위해 블록체인을 합의 알고리즘(PBFT)을 적용한다. GPS 모듈을 활용하여 노드 그룹을 검색하는 방식으로 인증과 PBFT의 블록체인 생성과정을 수행한다. 성능분석 결과, 새로운 Lora 신뢰 네트워크를 구축하고 합의 알고리즘의 지연 시간이 개선했음을 증명하였다. 본 연구는 4차 산업 융합연구로써 향후 Lora 장치의 보안 기술 개선에 도움이 되고자 한다.

키워드 : Lora, 사물인터넷, 장치 인증, 합의 알고리즘, 블록체인

Abstract Lora, a non-band network technology of the long-distance wireless standard LPWAN standard, uses ABP and OTTA methods and AES-128-based encryption algorithm (shared key) for internal terminal authentication and integrity verification. Lora's recent firmware tampering vulnerability and shared-key encryption algorithm structure make it difficult to defend against MITM attacks. In this study, the consensus algorithm(PBFT) is applied to the Lora network to enhance safety. It performs authentication and PBFT block chain creation by searching for node groups using the GPS module. As a result of the performance analysis, we established a new Lora trust network and proved that the latency of the consensus algorithm was improved. This study is a 4th industry convergence study and is intended to help improve the security technology of Lora devices in the future.

Key Words : Lora, IoT(Internet of Things), Authentication, Consensus Algorithm, Block-Chain

1. 서론

행정안전부에서 발표한 2019, 정부사물인터넷 도입 가이드라인에 따르면 '불법 장치 및 접근', '악성코드나 오작동', '센싱 정보 유출' 등 보안 위협의 대응방안으로 VPN(Virtual Private Networks)과 OAuth 2.0(Open Authorization 2.0)의 추가 구현을 권고하고 있다[1]. 기존 Lora 네트워크의 인증기법인 ABP(Activation By Personalization) 방식은 세션 키의 H/W 키 노출 취약성, LoraWan 장치의 암호화 키 및 통신 데이터 노출 등 보안 취약점이 등이 알려졌다[2]. Lora는 ABP 인증 방식보다 안전한 OTTA(Over-The-Air Activation) 인증 방식을 지원하며, 이외 FISYS의 HSM(Hardware Security Module), eWBM의 RoT(Root of Trust), Microchip의 TrustFLEX 등 H/W 보안 기술들이 개발/출시됐다[3,4,5]. 문제는 기존 H/W 보안 모듈을 지원하지 않은 Lora 제품들의 보안 문제, 권고 보안 기술인 VPN과 OAuth 2.0 기술 등 적용/개발의 어려운 문제가 존재한다.

본 연구는 저수준의 Lora 표준 장치 규격을 고려하여, 강력한 보안 수준 제공을 위해 S/W 수준(프로토콜)에서 동작하는 PBFT 블록체인을 활용하여 신뢰 네트워크를

*Corresponding Author : Sang-Geun Kim(sgkim@sungkyul.ac.kr)
Received July 4, 2022 Revised August 4, 2022
Accepted October 20, 2022 Published October 28, 2022

구축한다. Lora 전용 SX1276 모듈을 활용하여 실험 네트워크를 구축하고, 프로토콜 내부에는 GPS 기반으로 동작하는 수정된 A-PBFT 합의 알고리즘을 적용했다. 본 논문의 구성은 다음과 같다. 2장 관련 연구에서 Lora 기술 현황과 연구 비교 분석, 3장은 A-PBFT 합의 알고리즘, 4장은 안전성 및 성능분석, 5장 결론으로 마친다.

2. 관련 연구

2.1 Lora 표준 기술 및 현황 분석

기존 WiFi, Bluetooth 등 근거리 통신 기술은 높은 전송률(Throughput)을 제공하지만, 거리 제한과 전력 소모량이 비교적 많아 개인 또는 홈 네트워크 등 소규모 네트워크에 적합하다. 로라(Lora), 시그폭스(SIGFOX) 등은 저전력 장거리 통신 표준(LPWAN)이다. IoT 환경에서 다중통신이 가능하고, 비 대역 통신대역으로 통신사 없이 네트워크를 구축할 수 있다[6,7]. Fig. 1은 Lora 네트워크의 구조를 나타낸다[8].

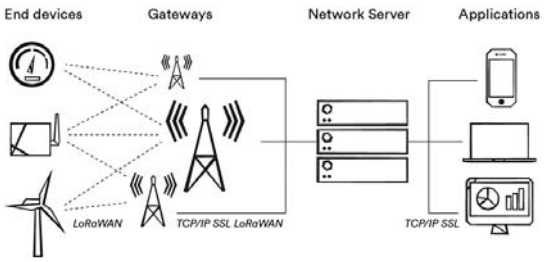

Fig. 1. Lora Network architecture

다수의 Lora 모듈, 게이트웨이(LoraWan), 서버로 구성되는 네트워크 구조이다. Lora 특허를 보유하여 전량 공급하는 Semtech의 SX-127(x) 시리즈 기준으로 1~3 Km 이상(최대 10 Km) 통신이 가능하다. 그러나 처리 성능이 제한적이기 때문에 가정이나 건물의 원격 검침용 등 센서 데이터 수준의 모니터링에 적합하다[9]. 국내 통신 3사 SKT(Lora), LGU+와 KT(NB-IoT)는 사물인터넷 서비스를 위해 전용망을 구축이 완료된 상태이다. Table 1은 국내 시범 서비스 사례를 나타낸다. 통신 3사가 비교적 저렴한 가격에 IoT 서비스를 제공하고 있지만, 아직 낮은 대중성과 해킹 취약점, 표준 플랫폼/보안 규격 부재 등 해결해야 할 문제가 남아있다.

Table 1. Lora service case

Public/Business	Service Name
Korea Expressway Corporation	Smart street light, slope warning system
Osan, Gyeonggi-do	Wearable devices for the elderly and children living alone, Dementia patient management service
Guro-gu, Seoul	Lora-based self-network construction
SKcarrental	Vehicle operation management service
CoXlab Inc	IoT platform iotown
Korea Water Resources Corporation	Smart water supply operation management
PLNetworks	Food safety monitoring system

Fig. 2는 Lora 네트워크의 세션 키 교환과정을 나타낸다[10].

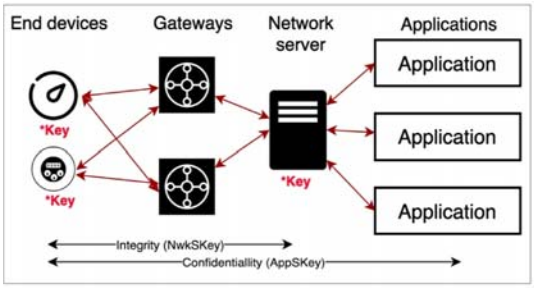

Fig. 2. Lora network security(session)

펌웨어 해킹과 장치 도난 등으로 정보 유출 방지를 위한 보안 기능을 제공한다. 단말 인증 및 데이터 무결성 확보에 네트워크 세션 키, 데이터 보호에 애플리케이션 세션 키를 사용한다. 암호화에는 AES-128 CMAC를 독립적인 보안 계층에 적용하고 있다[11]. 내부 패킷 프레임(포맷 구조, 메시지 복호화, 키 스트림, 카운터블럭)의 모든 정보를 암호화하지 않는다.

Lora 환경의 보안 강화에 가장 큰 문제점은 모듈 자체의 통신 및 처리 성능의 한계이다. 가장 대표적으로 활용되는 PKI나 RSA 알고리즘은 게이트웨이나 서버 노드에서 사용되고, 저수준의 Lora 소형 모듈에는 적합하지 않다[12]. 장치 해킹 방지에 HSM 보안 모듈이 시장에 확대되는 추세이지만, 이외 대응이 어렵다고 알려진 해킹(MITM, Replay, Join) 공격 등에 대한 경량 프로토콜도 개발도 필요하다.

2.2 Lora 보안 연구 비교 분석

Table 2는 3년 이내 학술검색 결과 (‘사물인터넷’, ‘보안’ 키워드)에서 Lora 기반 보안 연구를 비교 분석한 결

과이다[13-24]. 선정된 논문은 설계 및 구현과 실험을 포함한다. 비교 항목은 1. 제안 특징, 2. 알고리즘, 3. 장점, 4. 단점으로 차이점을 비교 분석했다.

Table 2. Lora related work comparison

Name	Description	
Kim, H. G.	1	Generating a shared key using a partial key set
	2	Hash function, XOR
	3	Suitable for low-power IoT devices
	4	Limitations of offline key distribution
Kim, J. H	1	Key duplication authentication
	2	AES-128
	3	Entry and D2D supplementation
	4	Difficulty in defending against devices and MITM attacks
Lee, J. H.	1	Obfuscated with Fcnt header encryption
	2	Random function, XOR
	3	Header plaintext encryption
	4	Difficulty in defending against devices and MITM attacks
Jeon, S. H, Kim, S. K.	1	Blockchain-based smart grid
	2	Hyperledger Fabric
	3	De-neutralization controllable
	4	Inappropriate consensus algorithm
Yu Jiang	1	RFF, Physical layer authentication
	2	RFF feature extraction/validation
	3	Relying on Lora Gateway Nodes
	4	High impact on SNR(accuracy)
Sascha Kaven at el	1	RSSI-based device authentication
	2	RSSI local location
	3	Suitable for low-power IoT devices
	4	Difficulty in defending against devices and MITM attacks
SM Danish at el	1	Multiple authentication
	2	Ethreum(PoS)
	3	Complementing Lora signup
	4	High performance/high power requirements
Jung, T. H.	1	Machine learning-based attack detection
	2	DBSSCAN
	3	Suitable for low-power IoT devices
	4	Difficulty in learning attack patterns
R Sanchez	1	Lora key distribution technique
	2	ECDH
	3	No protocol modification required
	4	Difficulty in defending against devices and MITM attacks
A Anastasiou	1	Update server network security
	2	LSB(self-developed)
	3	Applicable by firmware update
	4	Inappropriate consensus algorithm
Jiayao Gao	1	RSSI-based key generation algorithm
	2	RSSI Dual Channel
	3	Suitable for low-power IoT devices
	4	Difficulty in defending against devices and MITM attacks
V Ribeiro	1	Security key management
	2	Hyperledger Fabric
	3	Decentralized key management
	4	Inappropriate consensus algorithm
Kun-Lin Tsai	1	Generate secure session key
	2	PKC, ECC
	3	Leverage lightweight encryption
	4	High cost to build/develop PKI

국/내외 논문 검토 결과 Lora의 보안 취약점에 대한 다양한 논문들을 확인했으며, 크게 2가지 종류로 분류할 수 있다. 첫째, 제한적인 환경에서 무선 통신 특성과 저수준 연산 알고리즘을 활용하는 최적화 연구이다. 대표적으로 제한적인 환경을 위한 연구는 Yu Jiang의 RSSI 기반 인증, Jiayao Gao의 키 생성 연구가 있다[17,18]. 저수준 연산 알고리즘은 Kim, H. G.의 키 이중화, Lee, J. H.의 Fcnt 헤더 난독화, Kun-Lin Tsai의 ECC 기반 키 생성 연구가 있다[13,14,23] 둘째, 인증 및 무결성 강화를 위한 보안 관련 연구이다. 대표적으로 Jeon, S. H Kim, S. K.의 스마트 그리드와 V Ribeiro의 보안 키 관리 연구가 있다[16,22].

문제점 분석 결과, 첫 번째 연구들은 대부분 MITM 공격 방어가 어려웠고, 두 번째 연구들은 Lora 환경에 적절하지 않은 알고리즘 활용이 문제로 나타났다. 두 가지 특징을 고려했을 때, 문제점의 원인은 첫째 해킹 공격의 다양성에 고려하지 않았고, 둘째는 추가 적용된 기술들이 이론 연구로써 Lora 환경을 고려하지 않았기 때문이다. 환경을 고려하지 않았다는 것은 실제 Lora 장치에서 발생하는 필드 데이터를 제안/실험에서 명확히 분석/검증되지 않았다는 의미이다.

3. A-PBFT 기반 인증 기법

3.1 네트워크 구조 및 개발 요구사항

Fig. 3은 제안하는 네트워크 구조를 나타낸다. 저수준 Lora 모듈을 직접 설치하고, 통신환경을 분석해야 한다. 기본 보안 인증 방식을 사용하지만, 모든 노드를 검증하는 PBFT로 인해 신뢰 네트워크를 구축한다.

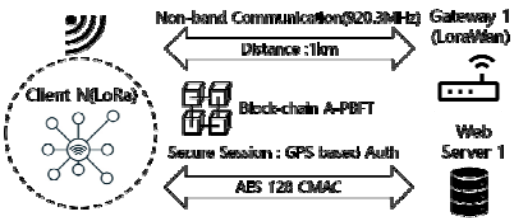

Fig. 3. Proposed network structure

① 네트워크 종류 : Lora 표준 네트워크(비대역)
② 통신 구성 : (Lora)n : 1(Gateway) :1(Server)
③ 네트워크 규모 : 소규모, 1km 이내
④ 프로토콜 스택 : Lora, MQTT

⑤ 블록체인 : Private, A-PBFT(Simple Mode)
⑥ 보안 : AES-128 CMAC, OTTA, GPS 기반 인증

블록체인(합의 알고리즘)의 특성은 다음과 같다.
① 블록생성 : 초기 세션 1회(기존 PBFT)
② 블록갱신 : 위치 이동, 세션 종료
③ 블록검증 : 기본(Normal)/제안(Simple)
④ 간소화모드 : GPS 기반 거리 계산(그룹 탐색)
⑤ 블록크기 : 70~100byte(10~20 트랜잭션)

3.2 A-PBFT 전체 동작 과정

Fig. 4는 A-PBFT 프로토콜 전체 과정을 나타낸다.

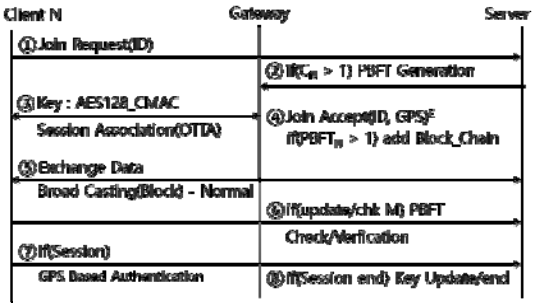

Fig. 4. A-PBFT protocol progress(flow)

① 장치 요청 : 초기 네트워크를 구축할 때 사용자에게 인가된 장치들의 식별자(ID)를 등록한다. 인가되지 않은 장치는 네트워크에 참여할 수 없다.
② 블록체인 생성 : 장치(C)의 초기 블록체인을 생성(초기 1회)을 시작한다. PBFT는 기존 선행 절차로 리더 선택 절차를 진행해야 한다.
③ 세션 생성 : 공유키(AES) 생성하고, 보안 세션을 생성한다. 세션 키가 지속 갱신되는 Lora 표준 모델의 OTTA 모드를 사용한다.
④ 참여 수락 : 장치 식별자(ID)와 GPS 정보를 암호화하여 전송한다. 새로운 블록체인 정보를 생성한다. 이때 서버는 전체 Lora 장치의 위치 정보 테이블을 저장/유지한다.
⑤ 데이터 교환 : 생성된 블록을 브로드캐스팅(Broadcasting)하여 사전 준비 절차(Pre-Prepare)를 시작한다.
⑥ 검증 : 과반수의 블록체인이 정상 검증되면 완료(Commit) 절차를 진행한다.
⑦ 세션 갱신 : 상태 변경 및 종료 시에 발생하는 갱신 과정은, GPS 기반 장치 인증을 수행하여 블록체인 검증을 간소화한다.
⑧ 세션 종료 : 접속 종료, 통신 에러, 세션 만료 등 상태에 따라 세션을 종료하여 자원을 해제한다.

3.3 A-PBFT 내부 동작과정

Fig. 5는 A-PBFT의 내부 동작 과정(기본)을 나타낸다. (기본 선 : 기존 PBFT, 점선 : 제안 A-PBFT)

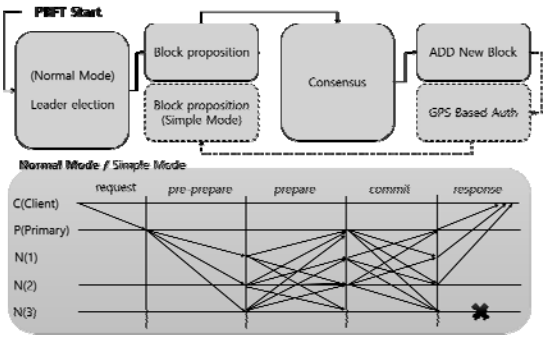

Fig. 5. A-PBFT protocol progress(normal mode)

초기 1회 진행되는 블록체인 합의 절차는 기존 PBFT 합의 알고리즘(Normal)과 같다. 장치(C)에 트랜잭션이 발생하면 리더(Leader)로 선정된 노드(Primary)를 시작으로 사전 준비, 준비, 확정 3가지 절차를 수행한다. PBFT는 노드가 증가할수록 네트워크 통신비용에 부담이 될 수 있기 때문에, A-PBFT는 GPS 기반 노드 그룹 탐색(Simple)으로 기존 합의 알고리즘 절차를 간소화한다.

3.4 GPS 기반 노드 그룹 탐색

Fig. 6은 GPS 기반 그룹 탐색 과정 예를 나타낸다. Lora 장치는 다소 제한적인 환경에서 원거리 모니터링

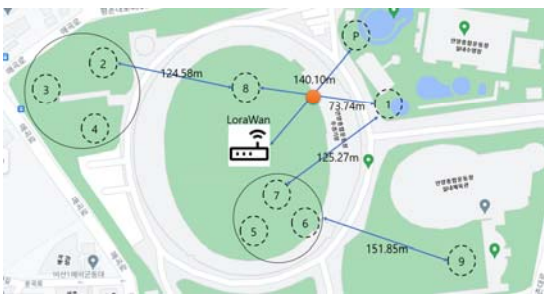

Fig. 6. GPS based group select(sample)

센서 장치 용도로 활용된다. 실제 센서에서 발생하는 데이터를 PBFT 알고리즘의 실시간 처리에 한계가 있다. GPS 기반 거리 인증은 게이트웨이(LoraWan)장치를 기준으로 가장 가까운 Lora 노드를 그룹화하고 블록체인을 검증한다.

Table 3은 서버에 저장된 Lora 장치 10 노드(리더 포함)의 GPS 정보 테이블 예를 나타낸다.

Table 3. Lora GPS table(10 node sample)

Client(N)	GPS	Location
LoraWan	37.40541477277268, 126.94640855421403	Anyang Sports Complex
Leader(P)	37.40630986156779, 126.94752385876681	Primary Node
1	37.4057095729626, 126.94799291208375	Node 1
2	37.40612770553381, 126.9449961825589	Node 2
3	37.40585447065246, 126.94425090895534	Node 3
4	37.40552327552099, 126.94500139426242	Node 4
5	37.40474496119929, 126.94648151806251	Node 5
6	37.4049188406321, 126.94708607567102	Node 6
7	37.40522933861557, 126.94658054042942	Node 7
8	37.405817211273266, 126.94641897762025	Node 8
9	37.40439306111256, 126.94869128035562	Node 9

① 리더 선택 및 위치 계산 : 서버와 근접한 게이트웨이(LoraWan)은 초기 등록된 GPS 정보를 참조하고, 선출된 리더(P)와의 거리(D) 중간 좌표를 계산한다.

② 그룹 탐색 : 중간 좌표(D/2)로부터 가장 가까운 Lora 노드 그룹은 1번, 8번이다. 노드 2개로 합의 알고리즘을 수행할 수 없으므로 추가 노드를 탐색한다. 8번에 근접한 2번, 1번에 근접한 7번 노드가 있다. 둘 중에 거리가 더 가까운 2번 노드를 선택한다.

③ 추가 그룹 탐색 : 현재 선택된 노드는 1, 8, 2번 노드이다. 2번에 근접한 노드 3, 4번을 추가한다. 전체 노드의 5/10개가 선택되어, 블록체인을 검증을 진행한다. PBFT는 배신자 노드 N이 존재할 때 최소 3N+1 노드(4개)가 정상이면 합의 알고리즘을 신뢰한다.

④ 그룹 변경 : 통신 지연 및 장치 문제 등으로 인해 탐색 중간 노드가 유실될 수 있다. 8번과 가까운 2번 노드가 문제가 생긴 경우, 가까운 다른 노드로 그룹을 변경해야 한다. 1번 노드와 가까운 7번 노드 선택하고 탐색해 나간다. 노드의 개수가 전체 노드의 과반수 선택되면 합의 알고리즘을 진행한다.
실제 장치 문제로 인해 Lora 장치의 블록체인 갱신이 어렵다면, 기존 블록체인 갱신을 정지(Lock)하고 오프라인 장치를 점검해야 한다. 본 연구의 블록체인 환경은 거래처럼 빈번하게 수행하지 않기 때문에, 실제 트랜잭션 발생이 지정된 주기(비컨 대기) 시간에 동작한다.

⑤ GPS 저장 및 업데이트 : 초기 네트워크 구축 과정에서 생성된 GPS 정보는 서버에 암호화하여 저장한다. 정상 통신 확인 송수신하는 GPS 정보는 해시값만 교환하여, 무결성만 검사하도록 한다. 실제 GPS 교환 및 업데이트는 오프라인 장치 검침만을 원칙으로 하고, IoT 장비와 서버에서 양방향 고정(Lock)한다. 지속하여 통신을 수행하지 않고, 안전한 상태에서만 이를 통신하고, 업데이트하는 방식을 사용한다.

Fig. 7은 GPS 기반으로 선택된 A-PBFT의 내부 동작 과정(Simple)의 예를 나타낸다. 앞서 선택된 1, 2, 3, 4, 8번(5개)의 노드를 중심으로 블록체인을 검사하였고, 기존 PBFT의 전체 통신량(10 노드 --〉 5 노드)을 간소화 시켰다. (점선 : 5, 6, 7, 9 노드 검사 생략)

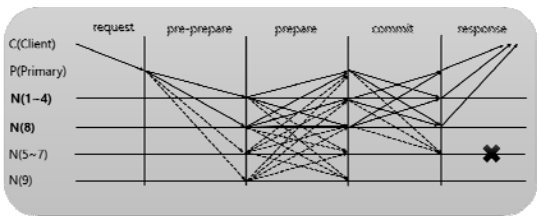

Fig. 7. A-PBFT protocol progress(simple mode)

4. 성능분석

4.1 Lora 네트워크 환경 설정

Lora 장치는 게이트웨이(Lorawan)을 통해 웹 서버와 통신하도록 구현한다. Lora H/W와 S/W 환경 설정은 다음과 같다.

① H/W : Lora RF(SX1276), LoraWan, GPS 수신기, 호환 안테나, 개인 PC(웹 서버)

② S/W : Arduino IDE(Lora, LoraWan), Ubuntu Linux 16.04 LTS(OS), Apache 2(Web)
③ 거리/전송률 : 1km 이내, 약 2~5kb(기본)
④ 장치 통신 방식 : Lora, MQTT
⑤ 작동 주파수 : 920.3(기본) – 923.3MHz(국내)
⑥ 통신 방식 : A 클래스(Sync), B(Data) 클래스

4.2 안전성 분석

게이트웨이(LoraWan)와 서버는 처리 능력과 통신 속도가 Lora 센서 장치와 비교하여 훨씬 준수하다. 정부 사물인터넷 도입 가이드라인[1]에서 권고하는 TLS(Transport Layer Security), PKI(Public Key Infrastructure) 등은 본 연구 대상에서 제외한다. 본 연구의 핵심 안전성 분석 대상은 해킹 문제가 지속하여 알려진 Lora와 Lora Wan 사이(Client와 Gateway) 통신 취약점이다.

① 악의적 노드 공격 : PBFT는 네트워크 내부에 악의적 노드 n개 있을 때, 총 노드 개수가 3n+1개 이상이면 해당 네트워크에서 이루어지는 합의는 신뢰할 수 있다. 소규모 네트워크에서 규모가 작은 노드는 적은 수의 노드만으로 해킹 공격에 성공할 수 있다는 가능성이 있다. 본 연구는 네트워크 초기 구축 시에 저장된 GPS 테이블을 활용하여 탐색 된 그룹의 블록체인을 검사하는 방식을 추가했다. 세션 성립 절차와 세션 유지 단계에서 블록체인 검사 방법을 다르게 사용했다. 공격자는 세션 내부의 선출된 리더 노드, 그룹 탐색 알고리즘, 서버의 GPS 테이블을 모두 알고 변조해야 하는 공격의 어려움을 가진다.

② 인가되지 않은 장치 참여 : 세션을 수립하는 과정에서 암호화된 GPS 정보를 서버에 전송해야 한다. 초기 네트워크 구축 단계에서 이미 저장된 GPS 정보와 다르거나, 확인되지 않은 위치에서 인가 요청은 거부된다. 세션을 해킹하여 실제 내부 암호화키를 공격해도 존재하지 않는 GPS 정보를 미리 입력할 수 없다. 이는 서버 내부 GPS 테이블을 해킹하고, 변조해야 하는 공격의 어려움을 가진다.

③ GPS 재생 공격 : 기본적으로 PBFT 블록체인을 해킹 공격 성공해야 한다. 내부 트랜잭션 정보를 변조, 조작해야 하기 때문이다. 통신에 사용되는 GPS 정보는 실제 위치 정보가 아닌, 암호화된 GPS의 해시(Hash)값이다. 암호화키가 노출되어 얻을 수 있는 GPS 정보는 무결성 검사 용도의 해시값이다. GPS 정보를 업데이트는 신규 장비 추가 또는 제거와 같은 물리적인 환경을 직접 점검하는 과정에서 수행된다.

4.3 성능분석

PBFT 알고리즘은 전체 통신량은 클라이언트를 포함하여 2N ^ 2번 발생한다. 예로 4 노드 64번, 7 노드 196번, 10 노드 400번이다. 10 노드 기준 탐색하는 5개 노드 그룹(1, 2, 3, 4, 8)의 통신량은 1/4 수준(100번)이다. 제안 A-PBFT는 LoraWan 게이트웨이와 가까운 노드 그룹을 탐색하여 통신량을 줄이고, 안정적인 통신 상태를 유지할 수 있다. Table 4와 Fig. 8은 노드 수 증가에 따른 합의 지연(비교)을 나타낸다.

Table 4. A-PBFT delay time(ms)

Node		PBFT	Propose	Total
4	Max	38.24	12.98	51.22
	Avg	35.11	6.99	42.1
	Min	28.45	5.39	33.84
7	Max	142.61	68.74	211.35
	Avg	79.53	13.64	93.17
	Min	69.11	12.38	81.49
10	Max	972.3	469.61	1441.91
	Avg	587.82	244.01	831.83
	Min	295.13	195	390.13

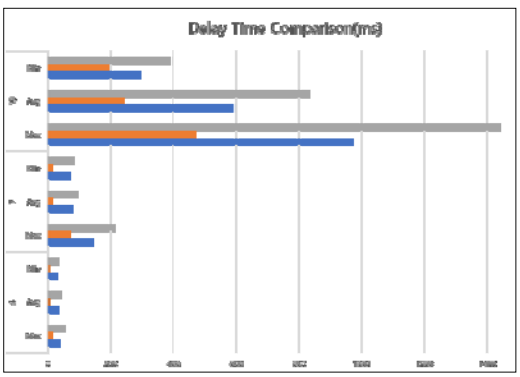

Fig. 8. A-PBFT delay time(ms) – chart

회색 : PBFT, 주황 : A-PBFT, 파랑 : 전체(합산)의 최대, 평균, 최소 지연 시간을 나타낸다. 기존 PBFT는 노드 증가에 따라 지연 시간이 급격하게 증가한다. 전제안 A-PBFT는 간소화 절차로 인해 평균 지연 시간 4 노드 기준 약 82%, 7 노드 기준 약 83%, 10 노드 기준 약 58%로 통신상의 송/수신 브로드캐스팅 오버헤드가 감소하여

성능이 크게 개선된 것으로 분석된다.

5. 결론

본 연구는 IoT 제품 개발을 위한 선행 연구로써, PBFT 알고리즘을 기반으로 신뢰 네트워크를 제공한다. 안전성과 성능분석 결과, 기존 방식과 다른 신뢰 네트워크를 제공하고, GPS 기반 인증으로 노드 인증 과정을 크게 간소화 시킬 수 있다는 것을 증명했다.

앞으로 모든 Lora 모듈에 S/W 형태로 탑재될 수 있도록 하는 기술 개발이 1차 목표이다. 장거리 센서 통신을 위한 Lora 전용 칩셋과 GPS 기반 H/W 모듈 제작하고 펌웨어 프로그래밍 단계에 있다. 현재 시중의 Lora 모듈과 Lorawan 장비, GPS 모듈 및 안테나 등 시세가 모두 개인이 구매할 수 있는 수준이다. 관련 제품이 출시 된다면 기존 통신사의 블록체인 서비스에 가입하지 않고, 저렴한 비용으로 개인 블록체인 네트워크를 구축할 수 있다. 향후 관련 연구로써 실무 환경에 필요한 기능으로 도난 방지, 검침 장비, 안전 감지, 환경 모니터링 센서 등으로 제품 출시를 확대할 계획이다.

REFERENCES

[1] Ministry of the Interior and Safety. (2019. 07. 01.). Guidelines for the introduction of the government IoT. Retrieved from https://www.mois.go.kr/

[2] Gareth Halfacree. (2020. 01. 28.). IOActive Highlights Security Failings in LoraWAN Deployments, Publishes Auditing Framework. Retrieved from https://www.hackster.io/

[3] ETRI. (2018. 07. 10.). Development of LPWAN security technology based on Hardware Security Module for safe IoT devices, Retrieved from https://scienceon.kisti.re.kr/

[4] Kim, S. E. (2017. 08. 10.). Security platform IoT dedicated network solution, LoRa certification, Retrieved from https://www.datanet.co.kr/

[5] Lee, S. M. (2020. 10. 13.). Microchip Introduces Wi-Fi MCU Module to Improve IoT Security, Retrieved from https://www.e4ds.com/

[6] Mah, S.-H., & Kim, B.-S. (2019). Lora Technology Analysis and Lora Use Case Analysis By Country. *The Journal of The Institute of Internet, Broadcasting and Communication*, 19(1), 15-20. DOI : 10.7236/JIIBC.2019.19.1.15

[7] Lee, D. H., Jang, G. H., Lee, C., Lee, Y. S., Lee, C. H., Kim, N. G., & Cho, S. R. (2020). Investigation on Low Power Communication for Power-Efficient Communication. *Journal of Korean Institute of Communications and Information Sciences*, 45(5), 805-812. DOI : 10.7840/kics.2020.45.5.805

[8] Actility, (2019. 07. 01.). The LoraWAN Network Server is the brain and the controller of a LoraWAN network, Retrieved from https://www.actility.com/

[9] Mun, T. H., & Kim, J. H. (2017). SK Telecom IoT dedicated network (Lora & LTE-M) construction and business status. *Information and Communications Magazine*, 34(2), 3-5.

[10] Proxis. (2020. 01. 28.). Articles and Reports IOActive security researchers say LoraWAN networks are vulnerable to cyber-attacks Retrieved from https://www.proxis.ua/

[11] LoRa Alliance, (2017. 07. 01.). lorawan_security_whitepaper, Retrieved from https://lora-alliance.org/

[12] Ann R. Thryft, (2020. 03. 05.). Key management concerns impact LoraWAN IoT device security, Retrieved from https://www.embedded.com/

[13] Kim. H. G. (2018). Research on Authentication and Key Agreement in a wireless sensor network under 1 Kbps communication capability. Kookmin University Graduate School of Financial Information Security Master's Thesis.

[14] Kim., J. H. (2018). Practical security improvement for LoraWAN communication. Yonsei University, Computer Science Ph.D. Thesis.

[15] Lee., J. H. (2018). The Security Vulnerability Analysis and Countermeasure Against Replay-attack in LoraWAN. Ajou University, Graduate School of Computer Science Master's thesis.

[16] Jeon, S. H., Kim, S. G. (2021). A Design of Blockchain-based Lora Multi-hop Network for Smart Grid. *Journal of the Korea Institute of Information and Communication Engineering*, 25(3), 440-448. DOI : 10.6109/jkiice.2021.25.3.440

[17] Yu Jiang, Hua Fu, Aiqun Hu, Wen Sun, (2021). A Lora-Based Lightweight Secure Access Enhancement System, *Security and Communication Networks*, vol. 2021, 16. DOI : 10.1155/2021/3530509

[18] Kaven, S., Bornholdt, L., & Skwarek, V. (2021). Authentication by rssi-position based localization in a Lora lpwan. *In 2020 6th IEEE Congress on Information Science and Technology (CiSt)*, 448-454. DOI : 10.1109/ACCESS.2019.2929212

[19] Danish, S. M., Lestas, M., Asif, W., Qureshi, H. K., & Rajarajan, M. (2019). A lightweight blockchain based two factor authentication mechanism for LoraWAN join procedure. *In 2019 IEEE International Conference on Communications Workshops (ICC Workshops)*. 1-6.
DOI : 10.1109/ICCW.2019.8756673

[20] Jung, H. T., Lee, S. H., & Kim, K. C. (2019). Implement Detecting Network Attack through Machine Learning in LoraWAN Environment. *Journal of Korean Institute of Communications and Information Sciences*, 44(8), 1547-1555.
DOI : 10.7840/kics.2019.44.8.1547

[21] Sanchez-Iborra, R., Sánchez-Gómez, J., Pérez, S., Fernández, P. J., Santa, J., Hernández-Ramos, J. L., & Skarmeta, A. F. (2018). Enhancing Lorawan security through a lightweight and authenticated key management approach. Sensors, 18(6), 1833.
DOI : 10.3390/s18061833

[22] Anastasiou, A., Christodoulou, P., Christodoulou, K., Vassiliou, V., & Zinonos, Z. (2020, May). Iot device firmware update over Lora: The blockchain solution. *In 2020 16th International Conference on Distributed Computing in Sensor Systems* (DCOSS), 404-411. DOI : 10.1109/DCOSS49796.2020.00070

[23] Ribeiro, V., Holanda, R., Ramos, A., & Rodrigues, J. J. (2020). Enhancing key management in LoraWAN with permissioned blockchain. Sensors, 20(11), 3068. DOI : 10.3390/s20113068

[24] Tsai, Kun-Lin & Leu, Fang-Yie & Hung, Li-Ling & Ko, Chia-Yin. (2020). Secure Session Key Generation Method for LoraWAN Servers. IEEE Access. PP. 1-1.
DOI : 10.1109/ACCESS.2020.2978100

김 상 근(Sang-Geun Kim) [정회원]

- 1996년 2월 : 중앙대학교 컴퓨터공학과 (공학박사)
- 1996년 3월~현재 : 성결대학교 컴퓨터공학과 교수
- 2003년~2004년 : Sydney University 방문교수

- 관심분야 : 정보보안, 핀테크, 빅데이터
- E-Mail : sgkim@sungkyul.ac.kr