산업융합연구 제20권 제6호 pp. 37-45, 2022
ISSN 2635-8875 / e-ISSN 2672-0124
DOI : https://doi.org/10.22678/JIC.2022.20.6.037

IoT 환경에서 신뢰 네트워크 구축을 위한 블록체인 기반의 경량 합의 알고리즘(L-PBFT)

박중오
성결대학교 파이데이아학부 조교수

Blockchain-based lightweight consensus algorithm (L-PBFT) for building trust networks in IoT environment

Jung-Oh Park
Assistant Professor, Division of Paideia, Sungkyul University

요 약 사물인터넷(IoT)의 발달과 함께 관련 네트워크 인프라는 외부 해킹과 같은 위협을 보호할 수 있는 새로운 기술이 요구되고 있다. 본 연구는 블록체인 합의 알고리즘을 기반으로 IoT 네트워크를 보호할 수 있는 L-PBFT 합의 알고리즘을 제안한다. 소규모 네트워크에 적합한 블록체인(Private) 모델을 설계하고, 초소형/저전력 IoT 장치를 대상으로 처리 성능을 테스트하고 안정성을 검증했다. 성능 분석 결과 L-PBFT는 노드 수가 적어도 합의 알고리즘의 동작(최소 14%, 최대 29%)을 준수하고, 기존 보안 프로토콜과 다른 신뢰 네트워크(보안 채널 분리)를 구축함을 증명하였다. 본 연구는 4차 산업 융합연구로써 향후 IoT 장치 보안 제품 개발에 도움이 되는 기반 기술이 될 것이다.

키워드 : 블록체인, IoT, PBFT, 보안, 합의 알고리즘

Abstract With the development of the Internet of Things (IoT), related network infrastructures require new technologies to protect against threats such as external hacking. This study proposes an L-PBFT consensus algorithm that can protect IoT networks based on a blockchain consensus algorithm. We designed a blockchain (private) model suitable for small networks, tested processing performance for ultra-small/low-power IoT devices, and verified stability. As a result of performance analysis, L-PBFT proved that at least the number of nodes complies with the operation of the consensus algorithm(minimum 14%, maximum 29%) and establishes a trust network(separation of secure channels) different from existing security protocols. This study is a 4th industry convergence research and will be a foundation technology that will help develop IoT device security products in the future.

Key Words : Block-Chain, IoT, PBFT, Security, Consensus Algorithm

1. 서론

모빌리티 리포트(Ericsson Mobility)는 세계 IoT 연결이 2020년 126억 개에서 2025년 269억 개로 약 2.1배 증가한다고 예상했고, 팔로알토 네트웍스(Palo Alto Networks)는 2021년 IoT 연결 중에 80%는 비업무용으로 기업망에 연결되는 사례가 증가했다고 조사됐다[1,2]. IoT 장치들의 연결과 종류가 급격하게 증가함에 따라 민감 데이터 보안에 대한 중요성이 점차 높아지고 있다. 사례에는 에이서스(ASUS) 업데이트 서버, N 번 방 IP카메라, IoT 펌웨어(firmware) 해킹 등 지속하여 보안 사고가 증가하여 이에 대한 해결책이 될 새로운 기술 개발이 요구되고 있다[3-5].

본 연구는 소규모 네트워크 환경을 중심으로 IoT 표준 프로토콜을 분석하고 경량화된 블록체인 L-PBFT

*Corresponding Author : Jung-Oh Park(pjo21@naver.com)
Received April 14, 2022 Revised May 20, 2022
Accepted June 20, 2022 Published June 28, 2022

합의 알고리즘을 제안한다. 자체 배터리를 사용하는 초소형/초저전력 IoT 장치를 고려하여 블록체인 기반 신뢰 네트워크를 구축하였고, 성능 개선을 위해 내부 프로토콜을 동작을 수정했다. 본 논문의 구성은 다음과 같다. 2장 관련 연구에서 기존 IoT-블록체인 기술 현황과 관련 연구 비교분석, 3장은 L-PBFT 합의 알고리즘, 4장은 안전성 및 성능 분석, 5장 결론으로 마친다.

2. 선행연구

2.1 IoT 및 블록체인 현황과 기술 분석

가트너(Gartner)에 의하면 IoT 관련 기업의 3/4이 블록체인을 도입했거나 2020년 말까지 도입할 예정이며, 블록체인 도입 기업 86%가 두 핵심기술을 함께 개발한다고 발표했다[6]. 대표적인 블록체인 IoT 융합기술로써 IoTA 재단 'tangle', 리눅스 재단의 'HyperLedger', IOTchain의 'IoT Chain', Waltonchain Technology의 'Walton Chain' 등이 있다[7]. 국내는 표준화 초기 단계로 IoT 장치를 위한 Lightweight 블록체인 표준개발(과제)이 최근 수행되었다[8]. Table 1과 같이 2020년 국내 블록체인 시범사업 사례를 살펴보면 공공기관과 지자체를 중심으로 전 분야의 데이터 관리 플랫폼을 구축하는 진입 단계이다[9].

핵심 기능은 서버 탈중앙화로 인한 부하분산과 신뢰 네트워크를 기반으로 각 지자체/기관의 중요 데이터 변조 등을 방지하는 것이다. IoT 환경과 관계가 높은 분야는 유통/교통/식품/운송 분야이다. 실제 현장에서 IoT 장치로부터 수집된 정보를 블록체인으로 저장/공유하여 정보의 조작을 방지하고 추적하는 데 유용하다[10].

IoT 환경은 블록체인 기술 적용에 앞서 해결해야 할 다양한 문제점이 존재한다.

주요 문제는 프로토콜 스택 호환성, 전송방식에 따른 저장/처리 성능 문제 등이 있다. Table 2는 블록체인 방식(Public과 Private)을 나타낸다[11].

Table 1. 2020 Block-chain pilot Project

Field	Institutions	Project Title
Safety	National Police Agency	Digital evidence management platform
Farming	Rural Development Administration	Open field crop production distribution management platform
Social safety net	Ministry of Health and Welfare	Platform for managing the overlapping welfare
Food safety	Ministry of Food and Drug Safety	Food safety data platform
Medical	Gangwon-do	Integrated management platform for chronic diseases in Gangwon-do
Authentication	Gyeongsangnam-do	Local public service platform based on distributed identification(DID)
Transportation	Sejong Special Self-Governing City	Trust platform for autonomous vehicles
Environment	Busan	Water supply smart water quality management system

Table 2. Block-chain method and features

	Public	Private
Accessibility	Y	N(permission required)
Speed	Slow	Fast
Identity	Anonymous	Authorized
Fees	Y(Required)	N
Hardfork	Y	N
Decentralization	High	Low
Rule change	Hard	Easy
Security	High	Vulnerable
Subject	All users	Central
Algorithm	PoW, PoS, DPoS	BFT

소규모 IoT 네트워크를 고려했을 때, Private 방식의 빠른 BFT 계열 합의 알고리즘이 적절하다. Yue Hao, Meshcheryakov, Seyed Mojtabasms의 블록체인 성능 및 비교분석에 따르면 BFT 계열의 PBFT 합의 알고리즘의 대기시간 및 처리량, 에너지 효율성 등 다양한 측면에서 성능이 뛰어남을 검증했다[12-14].

Fig. 1은 PBFT의 전체 동작 과정을 나타낸다[15].

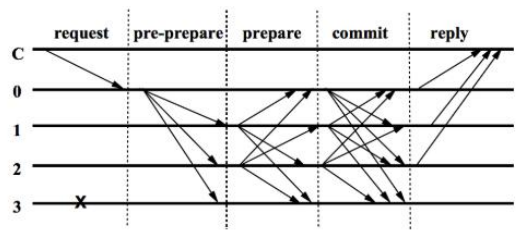

Fig. 1. PBFT-based consensus algorithm

PBFT는 리더(Leader)선출 이후, 요청(request)을 모든 장비에 전파하고 2/3의 검증이 성공하면 블록을 업데이트한다. 이외 브로드 캐스팅 과정을 통해 높은 확률로 이상 노드를 제거한다. 블록체인 네트워크 구축과 함께 소규모 네트워크를 위한 전용 통신 프로토콜이 요구된다. IoT 통신에는 MQTT(Message Queue Telemetry Transport)와 CoAP(Constrained Application Protocol)가 있다[16]. Table 3은 MQTT와 CoAP를 지원하는 무선 통신 표준 규격을 나타낸다[17].

Table 3. Standard wireless Communication type

Short distance		
Bluetooth		802.15.1, 1Mbps, Low power
Z-Wave		802.15.4, 9.6~40kbps, Low power
WiFi		802.11.x, 1-72Mbps, High
Zigbee		802.15.4, 250kbps, Ultra low power
Long distance		
NB-IoT	LTE	27kbps~5Mbps, Low power
Cat-0(1)		1Mbps~5Mbps, High
Cat-M1		300kbps, relatively High
Sigfox, Lora	Unlicensed band	100bps~5.4kbps, Ultra low power

단거리 프로토콜의 경우 높은 전송률의 장점이 있지만 블록체인 네트워크 구축의 폭(예 : Wifi 802.11ah 기준 최대 1km)이 유연하지 않고 전력 소모량이 많다. 제안 프로토콜 구현에는 비면허 대역 광역 IoT 기술 표준(LPWAN)의 Lora 프로토콜을 선택했다. 프로토콜 적용 요구사항으로 소형 HW, 낮은 비용, 초저전력, 통신 거리(1km 이상), 단순 네트워크 등 조건을 만족한다. Fig. 2와 같이 Lora 프로토콜은 IoT 장비와 게이트웨이 사이의 통신, 게이트웨이와 서버 사이는 기존 이더넷이나 Wifi 표준 규격으로 통신을 사용한다[18].

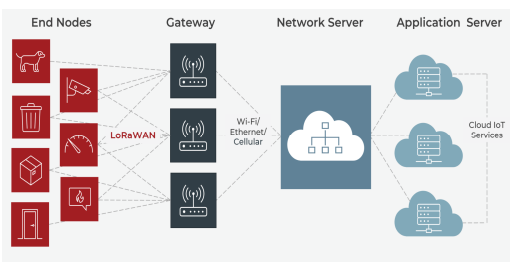

Fig. 2. Lora Network Architecture

2.2 블록체인 기반 IoT 연구 비교분석

Table 4는 3년 이내 학술검색 결과 ('사물인터넷', 'IoT', 'PBFT' 키워드)에서 블록체인 응용과 관련된 대표 연구를 비교 분석한 결과이다[19-35]. 세부 내용으로 구현, 테스트를 모두 포함하는 논문을 선정했다. 비교 항목은 1. 제안 특징, 2. 네트워크 규모/프로토콜, 3. 통신 거리/전력 소모, 4. 합의 알고리즘 및 기타 등으로 차이점을 비교 분석했다.

Table 4. Related Work Comparison

Name	Description	
Gee, S, Y. et el	1	Transaction time synchronization, integrity
	2	Small (Private Network), Wired (Ethernet)
	3	Not required, very high (PKI)
	4	Consensus Algorithm Improper
Jung, Y. S. and Kim, Y. T.	1	Multiple hash chains, integrity
	2	Small (IoT), unverifiable
	3	Unverifiable, very high (PKI)
	4	Unverifiable, very high (PKI)
Kim, M. H., Kim, Y. M.	1	EOSIO-based blockchain management system
	2	Small (IoT), unverifiable
	3	Less than 10 meters, very high (PKI)
	4	Performance Limitations of DPoS Consensus Algorithm
Kim, S. H., Kim, Y. G.	1	Hyperledger blockchain-based authentication
	2	Unverifiable, MQTT
	3	Unverifiable, high (RSA)
	4	Gate-server concentration, lack of performance analysis
Park, H. et el	1	Token-based multi-authentication system
	2	Small (IoT), unverifiable
	3	Unverifiable, Unverifiable
	4	Consensus Algorithm Unverifiable
Kim, H. G., Jung, S. H.	1	OTP-based device authentication system
	2	Small (IoT), unverifiable
	3	Home, low power
	4	Consensus Algorithm Improper
Nam, K. H.	1	Blockchain-based MES management system
	2	small/large, GRpc(Chain-code)
	3	Within several kilometers (smart factory), low to high power
	4	Hyperledger, Focus on access control function, lack of management function

Kim, J. H. et el	1	Grouped node-based authentication system
	2	Small (IoT), unverifiable
	3	Home, High (RSA)
	4	PBFT, Unable to check performance analysis
L Lao et el	1	Location-based blockchain applications
	2	Small/large scale (mobility), unverifiable
	3	Unverifiable, high
	4	PBFT, Lack of field data reliability
Jelena Mišić et el	1	Optimizing the Multiple Entry PBFT Algorithm
	2	Small/Large, Wifi or Cellular
	3	Medium/Long Distance, High (Transmission speed: 2mb)
	4	PBFT, Insufficient number of experimental nodes
T Kim, J Noh, S Cho	1	Blockchain Compression Algorithm
	2	Small (IoT), unverifiable
	3	Unverifiable, low
	4	PBFT, Suitable for lightweight IoT equipment
D Na, S Park	1	Decentralized Lightweight Blockchain
	2	Small/medium scale, wireless (Wifi)
	3	Unverifiable, very high (PKI)
	4	PBFT, Not suitable for lightweight IoT equipment
Wenyu Li et el	1	Multi-layer PBFT optimization
	2	Small/medium scale (IoT), unverifiable
	3	unverifiable, unverifiable
	4	PBFT, Lack of reliability in the experimental environment
J Thakker, Y Park	1	Threshold-based PBFT optimization
	2	Small/medium scale (local), wired (Ethernet)
	3	Unverifiable, very high (large number of nodes)
	4	PBFT, Absence of experimentation in IoT devices
VB Mišić et el	1	Voting-based PBFT optimization
	2	Medium (local), wired (Ethernet)
	3	2km, relatively high
	4	PBFT, Absence of experimentation in IoT devices
Min, Y. A.	1	Reliability-based PBFT optimization
	2	unverifiable, unverifiable
	3	unverifiable, unverifiable
	4	PBFT, Absence of experimentation in IoT devices
Shitang Yu et el	1	Mapping (votes/weights) based PBFT optimization
	2	Small (IoT), unverifiable
	3	unverifiable, unverifiable
	4	PBFT, lack of experimentation in IoT devices

분석 결과, 연구 유형은 크게 보안 인증과 성능 최적화로 분류된다. 소규모, 무선/전용 프로토콜, 근거리/초저전력 등 조건을 만족하는 최적화 연구는 Kim, T의 압축 알고리즘과 Li, W.의 다계층 블록구조 연구 등이 있다[29,31]. 문제는 연구에 활용된 IoT 장치의 표준 프로토콜과 HW 모듈 규격 명세가 명확하지 않다. 실제 필드 데이터 분석이 아닌 이론 연구(수식 검증, 로컬 시뮬레이션)이기 때문이다.

인증 연구는 대표적으로 Gee, S, Y.와 Kim, S. H.의 무결성 및 인증 강화 연구 등이 있다[19,22]. 문제는 센서 수준의 IoT 장치는 PKI나 RSA 알고리즘의 구현이 어렵고, 높은 처리 및 통신으로 인한 전력 소모량이 매우 높다. 무거운 알고리즘 선택은 블록체인 최적화에 앞서 전체 성능 효율성을 저하하는 주요 원인이 될 수 있다. 이외 Public 및 Private 블록체인 구분이 명확하지 않거나, 적절하지 않은 합의 알고리즘 선택 등 이론 연구로써 실험 방법 및 환경이 적합하지 않음을 확인했다.

본 연구는 구현/개발 단계에서 IoT 장치 실험을 위해 다음과 같은 항목을 준수했다. 첫째, 논리 네트워크의 구조와 무선 저전력 IoT 장치 규격을 명확히 정의했다. 두 번째, 물리 네트워크를 구축(노드, 게이트웨이, 서버 등)했다. 셋째, 기존 정상적인 양방향 통신과 제안 프로토콜을 직접 코딩했다. 넷째, 합의 알고리즘의 지연 시간 및 블록 크기 변화 등 성능을 비교분석 했다.

3. L-PBFT 합의 알고리즘

3.1 네트워크 구조 및 IoT 장치 규격

Fig. 3은 제안 네트워크 구조를 나타낸다. Lora 네트워크는 무선 비대역 통신망 920.3MHz 대역을 사용하는 n:1:1로 구성한다. Private 블록체인 방식으로 개인 또는 회사 소규모 네트워크에서 구축하는 경우, 인가된 장치를 제어하는 주체가 필요하다. 1~3km 이내 거리에서 동작하며, 다중 노드 제어에 사용자의 스마트폰을 활용한다. 다음은 본 연구에서 사용된 Lora 네트워크 전체 구조를 나타낸다.

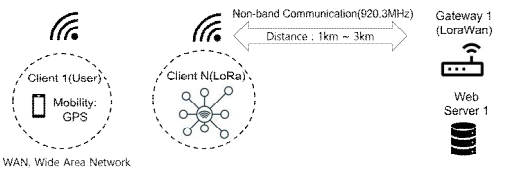

Fig. 3. Proposed Lora Network Architecture

① 프로세서 : 2 * Tensilica LX6 1 * ULPThe
② 칩셋 : ESP32(SX1276)
③ 플래시 / 거리 : 64 bit / 1km ~ 3km
④ 게이트웨이 : LoraWan(single channel)
⑤ 용량 / UDP 전송률 : 8 Mbyte / 135 Mbps
⑥ 기타 지원 : BLE, Wifi(802.11 b/g/n/e/i)
⑦ 개발 환경 : Espressif SDK, Arduino, MircoPython, NodeMCU

Lora 네트워크의 노드를 구성하기 위한 SX1276 모듈 총 10개, SX1276-Lorawan(겸용) 1개를 네트워크 구축에 활용했다. 이외 사용자 스마트폰은 안드로이드 9.0(GalaxyTab-A), 노트북(MSI-GE62)에서 데이터 통신 연계를 위해 아파치 웹 서버를 사용하여 구축했다.

3.2 L-PBFT 합의 알고리즘 전체 과정

Fig. 4는 제안 L-PBFT의 전체 동작 과정을 나타낸다. 초기 네트워크 구축 단계에서 IoT 장치 그룹과 Lorawan, 서버 등은 모두 사용자가 신뢰할 수 있는 인가받은 장치라고 가정한다. 블록체인 생성 이전단계에서 AES-128 표준 암호(CBC 운영 모드) 방식으로 공유키를 생성하고 보안 세션을 생성한다.

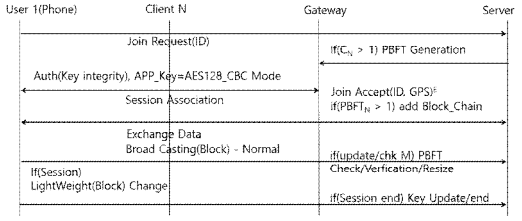

Fig. 4. Operation Process of L-PBFT(Diagram)

세션 성립 이후 기존 PBFT 합의 알고리즘을 반드시 1회 수행한다. 이후 세션이 유지되는 동안 사용자의 스마트폰 요청에 따라 경량 모드(제안)로 전환한다. 이외 통신 문제 및 접속 종료 상태에 따라 세션을 종료한다. 기존 방식과의 차이점은 IoT 장치 노드 이외에 사용자 스마트폰 노드가 참여한다. 역할은 전체 노드에서 발생하는 블록 생성 및 처리 과정 상태를 지속하여 확인한다.

3.3 L-PBFT 내부 동작과정

Fig. 5는 L-PBFT의 두 가지 합의 알고리즘의 동작 과정을 나타낸다. 초기 1회 세션 생성은 기존 PBFT 합의 알고리즘의 동작(NORMAL) 과정과 같다. 브로드캐스팅(broadcasting)된 블록들을 모두 전송하고, 2/3 이상(정상)의 블록 해시값을 검증한다. 배신자 노드가 n개 있을 때, 총 노드 개수가 3n+1개 이상이면 합의 결과를 신뢰할 수 있다.

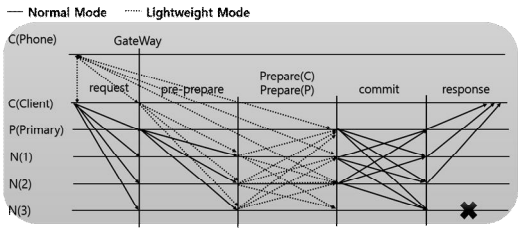

Fig. 5. Operation Process of L-PBFT(Flow)

합의 알고리즘을 1회 완료 이후 경량 모드(제안)로 전환하게 되는데, 기존 PBFT에서 변경된 점은 미리 사용자의 스마트폰을 리더 노드로 변경하고, 합의 절차를 진행한다는 차이점이 있다. PBFT는 초기 과정에서 리더를 선택하는 과정이 필수이다. 본 연구는 사용자의 스마트폰을 안전한 노드로 가정하고, 리더로 선정하여 Prepare(사준 준비) 절차까지 수행한다. 사전 준비된 메시지 수가 전체 노드의 2/3 이상이면 각 노드는 Prepare(P) 상태로 전환 후 대기한다. 이때, 다음 선정될 리더 정보를 스마트폰에서 미리 지정한다. 노드 갱신으로 인한 새로운 합의 알고리즘이 시작되면, 앞서 지정된 리더 노드를 선정한다. 스마트폰을 통해 Commit(확정)을 보내고, 블록체인을 검증/저장한다. 스마트폰을 활용하는 장점/단점은 다음과 같다.

① 처리 분산 : 기존 PBFT 동작의 네트워크 오버헤드를 분산시킨다. 리더 노드 선택과 함께 미리 사전 준비단계를 수행 준비한다. IoT 노드에서 실제 합의 알고리즘은 Commit(확정) 절차만 수행하게 된다.

② 리더 노드 이중화 : 기존 PBFT는 리더 노드가 악의적인 노드가 선택될 때 크게 취약해지는 문제가 있다. 리더 노드의 통신 채널을 분산시키는 방법은 감지 및 복구로 인한 성능 저하 문제를 해결할 수 있다.

③ 외부 통신 활용 : 스마트폰은 셀룰러 망(Cellular Networks)을 통해 직접 서버와 통신하여 안정적인 통신 상태를 제공한다. 또한, IoT 노드와 다른 통신 세션(보안)을 사용하여 통신 채널을 분리한다.

④ 모니터링 : 기존 PBFT는 통신 장애나 부정확한 모니터링으로 인해 합의 처리량이 크게 떨어지는 문제가 있다. 스마트폰의 상태 제어를 통해 합의 알고리즘 처리 중간 단계에서 이를 제어할 수 있다.

⑤ 구현의 어려움 : 리더 이중화 및 게이트웨이 통신, 서버와 스마트폰 통신 추가로 인해 프로토콜 개발 과정이 훨씬 복잡해진다.

⑥ 경량화 모드의 한계 : 기존 PBFT의 최적화에는 한계가 있다. 소규모 네트워크 환경에서 Private 블록체인 방식에 적합하다. Public 블록체인 방식으로 전환하는데 성능 및 보안 문제 때문에 모델 자체를 변경하거나, 새로운 합의 알고리즘을 개발해야 한다.

4. 성능 분석

4.1 블록체인 및 통신 환경 설정

성능 분석에 실제 악의적인 노드와 전파 지연으로 인한 통신 지연 시간은 제외하고 분석했다. 안전성 및 성능 분석을 위한 파라미터 설정은 다음과 같다.

① 블록 생성 : 세션 시작 1회, 세션 유지(경량 모드)
② 시간 주기 : 유지 : 3,600초, 경량 : 480초
③ 트랜잭션 : 10~20 트랜잭션
④ 블록 크기 : 78~100바이트
⑤ 노드 구성 : 4 노드, 7 노드, 10 노드
⑥ 내부 통신 방식 : B 클래스(비콘)
⑦ 보안 인증 : OTTA(Over-The-Air-Activation)

확산계수(SF : Spreading Factor) 수신감도 최적화를 위해서 블록체인 갱신 주기를 SF7(1km 이내), 1시간(3,600초)으로 설정했다. 배터리를 사용하는 소형 장치를 고려하여 B 클래스 방식(비컨 주기 128초), 보안 인증에 세션마다 공유키를 갱신하는 OTTA 방식을 사용한다. 실험 환경은 건물의 방해(전파 간섭)가 적은 열린 공간에서 실험을 수행했다. LoraWan 장치 성능이 제한적인 싱글 채널 지원 모델이기 때문에 전체 Lora 내부 모듈의 요청/응답 통신 지연 시간을 3,000ms 추가 설정했다.

4.2 안전성 분석

PBFT의 합의 알고리즘은 기본적으로 악의적인 노드가 n개 있을 때, 전체 노드 개수가 3n+1개 이상 검증되면 합의는 신뢰할 수 있다. 프로토콜 절차 수행에서 내부 중요 파라미터는 통신 암호화를 수행하는 공유키 등이다.

① 합의 알고리즘 취약성(보완) : 기존 PBFT의 근본적인 안전성 문제는 악의적인 노드가 참여할 수 있다는 것이다. PBFT 합의 초기 절차에서 선택되는 리더 노드의 악의적인 공격 참여가 가장 문제가 크다. 본 연구는 기존 PBFT 과정을 스마트폰을 노드에 참여시키고 리더 노드의 역할(사전준비, 확정)을 분리하여 통신 채널을 이중화한다.

② 세션 키 취약성 : Lora는 기본 AES-128 암호 공유키 방식을 사용한다. 사전 준비 절차의 사용자 스마트폰은 LTE 기준 상호인증 알고리즘(EPS-AKA)으로 생성된 보안 세션을 사용한다. Lora의 공유키가 노출되어도, 공격자는 다른 보안 채널(스마트폰 - 서버)에서의 사전 준비단계 메시지를 분석하여 유추해야 하므로 분석 복잡도가 훨씬 높다.

③ 비정상 장치 참여 가능성 : 본 연구의 주요 목적은 처리 오버헤드(overhead)를 분산시키는 것이다. 현재 상용화되어 활용되는 PBFT 알고리즘 악의적 노드 개수 문제까지는 해결책을 제시하지 않는다. 이는 현재 대표적인 PBFT 기반의 RBFT, Tendermint, Hyperledger 등 합의 알고리즘도 점차 해결해 나가야 할 문제이다.

4.3 성능 분석

기존 PBFT와 제안 합의 알고리즘의 합의 지연, 블록체인 크기를 측정하였다. Fig. 6은 합의 과정 이후 각 노드의 전체 블록체인 크기의 변화를 나타낸다. 기본 노드에서 식별 및 센서 데이터는 임의의 10~20 트랜잭션, 최대 100바이트 정도 용량의 블록을 생성했다. 노드 개수에 따른 세션 성립 횟수는 전체 2N ^ 2이다. 4 노드 = 64번, 10 노드 = 400번이다. 기본 합의 알고리즘 동작이 같으므로 블록 생성의 크기는 기존 PBFT 알고리즘과 큰 차이가 없다.

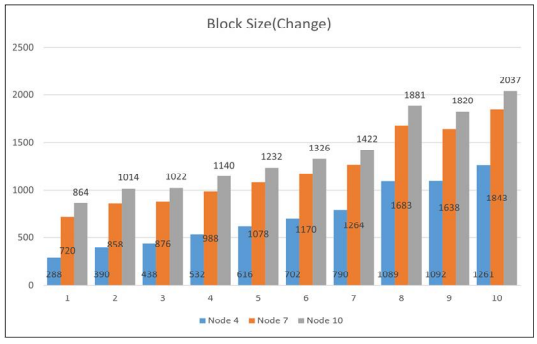

Fig. 6. Block-chain size of a node(Change)

Table 5는 노드 수 증가에 따른 평균 합의 지연을 나타낸다. 지연 시간은 요청(Request) 시간에서 마지막 응답(response) 시간의 간격이다. Fig. 7은 노드 수 증가에 따른 평균 합의 지연(ms : 밀리초)을 나타낸다.

Table 5. Delay Time Comparison(ms)

Node		PBFT	Propose	%	Total
4	Max	38.24	12.98	33	51.22
	Avg	35.11	6.99	19	42.10
	Min	28.45	5.39	18	33.84
7	Max	142.61	68.74	48	211.35
	Avg	79.53	13.64	17	93.17
	Min	69.11	12.38	17	81.49
10	Max	972.30	469.61	48	1441.91
	Avg	587.82	244.01	29	831.83
	Min	295.13	195	66	390.13

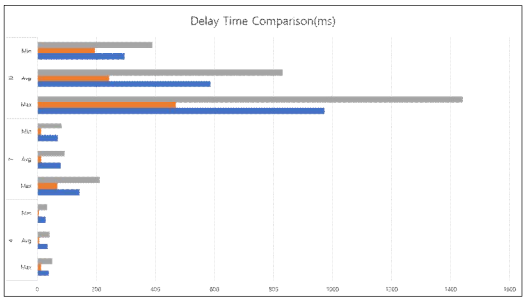

Fig. 7. Delay Time Comparison(ms) - Chart

성능 효율성은 최저 4 노드 평균 19%, 최대 10 노드 평균 29%가 증가했다. 최저/최대 노드를 비교했을 때, 요청의 횟수(약 6배)가 큰 차이가 있음에도, 오히려 다수 노드에서 평균 성능이 개선의 비중이 증가했다. 10 노드 이내 소규모 Lora 네트워크는 성능 저하가 크지 않음을 알 수 있다. 요청 증가에 따른 성능 감소 문제를 처리 및 통신 성능이 준수한, 스마트폰의 사전 준비 절차를 미리 수행함으로써 해결했다.

5. 결론

PBFT는 Iot 환경에서 해결해야 할 기술적인 문제들이 아직 많이 남아있다. 노드들이 분산된 블록을 공유하기 위하여 첫 블록부터 마지막 블록 생성까지 전체 블록 정보를 통신해야 한다. L-PBFT에서 이를 사전 준비 단계로 최적화했지만, 10 노드 이내의 소규모 네트워크 범위 내 적절한 기술이다. 이외 악의적인 노드가 1/3 이상일 때 안전성 문제를 개선할 기술이 필요하다.

본 연구는 기존 PBFT의 리더 역할과 통신 채널을 분리하여 안전성을 보완하고, 검증단계에서 기존 PBFT와 비교하여 동일 블록 처리에서 높은 성능 효율성을 확인하였다. 향후 연구로는 첫째, Lora 이외 고성능 IoT 장비(Wifi 또는 LTE 모듈), 고가 다채널 LoraWan 장비, 고성능 전용 안테나 등을 활용하여 네트워크의 규모를 확장할 계획이다. 둘째, 다양한 분야에서 블루투스나 이더넷 표준 통신을 수행하고 있는 점을 고려하여, 안전한 Lora 네트워크를 연계하는 방안을 새롭게 설계할 계획이다.

REFERENCES

[1] Ericsson. (2020). Ericsson Mobility Report. Retrieved from https://www.ericsson.com

[2] Palo Alto Networks. (2021). The Connected Enterprise: IoT Security Report 2021. Retrieved from https://www.paloaltonetworks.com/

[3] D. W. Kim. (2020). Trends in Supply-Chain Security Technologies. *Electronics and Telecommunications Trends, 35(4),* 149-157. DOI : 10.22648/ETRI.2020.J.350413

[4] E. Lee, J. Moon, C. Han & I. G. Lee. (2021). Blockchain Network Security Threat Detection Technology Trend Analysis. *Korea Institute of Information Security and Cryptology, 31(3),* 61-71.

[5] Y. J. Kim, J. H. Kim & S. J. Kim. (2021). A Study on Systematic Firmware Security Analysis Method for IoT Devices. *Journal of The Korea Institute of Information Security and Cryptology, 31(1),* 31-49. DOI : 10.13089/JKIISC.2021.31.1.31

[6] Gartner. (2021). Gartner Survey Reveals Blockchain Adoption Combined With IoT Adoption Is Booming in the U.S. Retrieved from https://www.gartner.com

[7] E. K. Hong, S. J. Lee & S. H. Seo. (2018). Blockchain Technology Trends for the Internet of Things. *Journal of The Korea Institute of Information Security and Cryptology, 28(3),* 38-46.

[8] J. S. Park. (2021). *Standard Development of Lightweight Blockchain for IoT devices.* Electronics and Telecommunications Research Institute.

[9] K. H. Kuk. (2020). *Blockchain core technology and application examples by domestic and foreign industries.* Retrieved from : https://www.iitp.kr/

[10] ETRI WebZine. (2020). What innovations will blockchain bring?. Retrieved from : https://www.etri.re.kr/

[11] Eugene Tarasenko. (2021). Private Blockchain vs Traditional Centralized Database. Retrieved from : https://merehead.com/

[12] Y. Hao, Y. Li, X. Dong, L. Fang & P. Chen. (2018). Performance Analysis of Consensus Algorithm in Private Blockchain, *IEEE Intelligent Vehicles Symposium (IV),* 280-285. DOI : 10.1109/IVS.2018.8500557

[13] Y. Meshcheryakov, A. Melman, O. Evsutin, V. Morozov & Y. Koucheryavy. (2021). On performance of PBFT blockchain consensus algorithm for IoT-applications with constrained devices. *IEEE Access, 9,* 80559-80570. DOI : 10.1109/ACCESS.2021.3085405

[14] S. M. H. Bamakan, A. Motavali & A. B. Bondarti. (2020). A survey of blockchain consensus algorithms performance evaluation criteria. *Expert Systems with Applications, 154(10),* 113385. DOI : 10.1016/j.eswa.2020.113385

[15] Aston. (2020). Consensus Algorithm — PBFT (Practical Byzantine Fault Tolerance). Retrieved from : https://medium.com/

[16] D. Seo & D. Lee. (2019). Lightweight Protocol for Low Power and Reliability Improvement Based on CoAP in the Internet of Things(IoT) Environment. *Journal of Korea Society of Digital Industry and Information Management, 15(1),* 21-28. DOI : 10.17662/KSDIM.2019.15.1.021

[17] Ministry of Public Administration and Security. (2019). *Guidelines for the introduction of the government IoT.* Retrieved from : https://www.mois.go.kr/

[18] Cardinal Peak. (2022). *Everything you need to know about LORA and how to set up your LORA gateway to view IoT device data.* Retrieved from: https://www.cardinalpeak.com/

[19] S. Y. Ji, S. E. Kim, E. J. Yun & D. Y. Seo. (2018). Time Synchronization between IoT Devices in a Private Network using Block-Chain. *Journal of The Institute of Internet, Broadcasting and Communication, 18(5),* 161-169. DOI : 10.7236/JIIBC.2018.18.5.161

[20] Y. S. Jung & Y. T. Kim. (2021). Multi-blockchain model ensures scalability and reliability based on intelligent Internet of Things. *Journal of Convergence for Information Technology, 11(3),* 140-146. DOI : 10.22156/CS4SMB.2021.11.03.140

[21] M. H. Kim & Y. M. Kim. (2019). Implementing Blockchain Based Secure IoT Device Management System. *Journal of Korean Electrical and Electronics Engineers, 23(4),* 1343-1352. DOI : 10.7471/ikeee.2019.23.4.1343

[22] S. H. Kim & Y. G. Kim. (2019). A Study on Light Weight Authentication Method of Distributed Cluster-based IoT Devices. *Journal of The Institute of Internet, Broadcasting and Communication, 19(2),* 103-109. DOI : 10.7236/JIIBC.2019.19.2.103

[23] H. Park, M. S. Kim & J. H. Seo. (2019). IoT Multi-Phase Authentication System Using Token Based Blockchain. *KIPS Transactions on Computer and Communication Systems, 8(6),* 139-150. DOI : 10.3745/KTCCS.2019.8.6.139

[24] H. G. Kim & S. H. Jung. (2020). IoT Authentication System Using Blockchain and TOTP. *Journal of The Korea Society of Computer and Information, 25(2),* 113-122. DOI : 10.9708/jksci.2020.25.02.113

[25] K. H. Nam. (2021). Implementation of Intelligent IoT MES Platform based on Hyperledger Fabric. *Journal of Korean Institute of Information Technology, 19(11),* 133-142. DOI : 10.14801/jkiit.2021.19.11.133

[26] J. H. Kim, J. W. Heo & M. S. Jun. (2019). Design of Device Authentication Protocol Based on C-PBFT in a Smart Home Environment. *Journal of Korea Academia-Industrial cooperation Society, 20(5),* 550-558. DOI : 10.5762/KAIS.2019.20.5.550

[27] L. Lao, X. Dai, B. Xiao & S. Guo. (2020). G-PBFT: a location-based and scalable consensus protocol for IoT-Blockchain applications. *In 2020 IEEE International Parallel and Distributed Processing Symposium (IPDPS),* 664-673. DOI : 10.1109/IPDPS47924.2020.00074

[28] J. Mišić, V. B. Mišić, X. Chang & H. Qushtom. (2020). Multiple entry point PBFT for IoT systems. *In GLOBECOM 2020-2020 IEEE Global Communications Conference,* 1-6. DOI : 10.1109/GLOBECOM42002.2020.9322641

[29] T. Kim, J. Noh & S. Cho, (2019). SCC: storage compression consensus for blockchain in lightweight IoT network. *In 2019 IEEE International Conference on Consumer Electronics (ICCE),* 1-4. DOI : 10.1109/ICCE.2019.8662032

[30] D. Na & S. Park. (2021). Fusion Chain: A Decentralized Lightweight Blockchain for IoT Security and Privacy. *Electronics 2021, 10(4),* 391. DOI : 10.3390/electronics10040391

[31] W. Li, C. Feng, L. Zhang, H. Xu, B. Cao & M. A. Imran. (2020). A scalable multi-layer PBFT

consensus for blockchain. *IEEE Transactions on Parallel and Distributed Systems, 32(5),* 1146-1160. DOI : 10.1109/TPDS.2020.3042392

[32] J. Thakker & Y. Park. (2020). Resilient and Efficient Blockchain Consensus Protocol for Internet-of-Things. *In 2020 IEEE International Conference on Consumer Electronics (ICCE),* 1-6. DOI : 10.1109/ICCE46568.2020.9043061

[33] V. B. Mišić, J. Mišić & X. Chang. (2021). The Impact of Vote Counting Policy on the Performance of PBFT. *In 2021 IEEE Canadian Conference on Electrical and Computer Engineering (CCECE),* 1-6. DOI : 10.1109/CCECE53047.2021.9569079

[34] Y. A. Min. (2021). The Modification of pBFT Algorithm to Increase Network Operations Efficiency in Private Blockchains. *Applied Sciences, 11(14),* 6313. DOI : 10.3390/app11146313

[35] S. Yu, K. Lv, Z. Shao, Y. Guo, J. Zou & B. Zhang. (2018). A high performance blockchain platform for intelligent devices. *In 2018 1st IEEE international conference on hot information-centric networking (HotICN),* 260-261. DOI : 10.1109/HOTICN.2018.8606017

박 중 오(Jung-Oh Park) [정회원]

· 2000년 7월 : 성결대학교 컴퓨터공학과 졸업
· 2003년 3월 : 명지대학교 전자계산교육 석사
· 2011년 8월 : 숭실대학교 컴퓨터공학 박사
· 2016년 3월~현재 : 성결대학교 조교수
· 관심분야 : PKI, Network security, 암호학
· E-Mail : pjo21@naver.com