Journal of Convergence for Information Technology
Vol. 12. No. 4, pp. 1-8, 2022
e-ISSN 2586-4440
DOI : https://doi.org/10.22156/CS4SMB.2022.12.04.001

Lora 환경에서 블록체인 기반 도난방지 프로토콜 설계 및 구현

박중오
성결대학교 파이데이아학부 조교수

Design and implementation of blockchain-based anti-theft protocol in Lora environment

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

요 약 통신인프라의 발달 등 1인 보유 네트워크 장비 개수가 점차 늘고 있다. 스마트폰과 같은 범용적인 장비들은 S/W 구현으로 도난/분실 방지 기능을 구현할 수 있다. 그러나, 이외 소형 장비들은 표준 통신 기술 규격이나 H/W 한계로 인한 장거리 통신 문제, 기능 부재(인증 및 보안성) 등 실용성이 부족하다. 본 연구는 LPWA 표준 환경의 Lora 통신 프로토콜과 블록체인 기술을 결합한다. 도난 방지 및 보안 기능을 프로토콜에 추가하고, 블록체인 네트워크 구축을 위해 PBFT 합의 알고리즘을 적용했다. 테스트 결과, 안전성(인증 및 신뢰 네트워크)과 성능(블록체인 처리 성능)의 효율성을 확인했다. 본 연구는 4차 산업 융합연구로써 향후 휴대용 또는 소형 장치 도난 방지 제품 개발에 이바지하고자 한다.

주제어 : 블록체인, LPWA, 도난방지, Lora, PBFT

Abstract With the development of communication infrastructure, the number of network equipment owned by one person is gradually increasing. General-purpose devices such as smartphones can implement theft/loss prevention function by implementing S/W. However, other small devices lack practicality such as long-distance communication problems due to standard communication technology specifications or H/W limitations, and lack of functions(authentication and security). This study combines the Lora communication protocol in the LPWA standard environment and the blockchain technology. Anti-theft and security functions were added to the protocol, and the PBFT consensus algorithm was applied to build a blockchain network. As a result of the test, the effectiveness of safety(authentication and trust network) and performance(blockchain processing performance) were confirmed. This study aims to contribute to the future development of portable or small device anti-theft products as a 4th industrial convergence research.

Key Words : Block-chain, LPWA(Low Power Wide Area), Anti-theft, Lora, PBFT

1. 서론

시스코 비주얼 네트워킹 인덱스(Visual Networking Index, VNI)보고서에 따르면, 2023년까지 WiFi 통신 연결 비중이 45%에서 저전력 광대역(LPWA) 기술을 통해 5G로 연결되고, 전 세계 1인당 개인 기기 보유 개수가 크게 증가한다고 예측했다[1]. 스마트폰, 노트북, 태블릿, 스마트 워치 등 대부분 장비가 WiFi와 블루투스 등 프로토콜을 지원하고, 이외 소형 IoT 장치들을 연동 등 새로운 서비스(M2M 연결)를 제공하는 실정이다[2]. 기존 WiFi와 블루투스 및 광대역 통신망을 사용할 수 없는 소형 IoT 센서 장비는 통신 거리 한계와 배

*Corresponding Author : Jung-Oh Park(pjo21@naver.com)
Received January 20, 2022
Revised March 7, 2022
Accepted April 20, 2022
Published April 28, 2022

터리 효율이 떨어지는 문제점이 존재한다. 또한 장거리 통신으로 인한 새로운 보안 문제를 해결해야 한다.

본 연구는 도난 방지 기능을 중심으로 최근 업데이트된 저전력 광대역(LPWA) 표준과 신뢰 네트워크 구축을 위한 블록체인 기술을 결합한다. 국내 환경에 적절하다고 분석된 Lora 통신 프로토콜 및 호환 H/W 모듈 등을 활용하고 구현했다. 본 논문의 구성은 다음과 같다. 2장 관련 연구 및 기존 연구 비교분석, 3장은 제안하는 프로토콜 모델, 4장은 구현 및 테스트와 성능 분석, 5장 결론으로 마친다.

2. 관련 연구

2.1 LPWA(Low Power Wide Area)

IoT 산업계 표준 LwM2M(Lightweight M2M) 국제 표준은 저전력, 암호화 등 에너지 최적화와 보안성을 인증받은 기술이다. Fig 1과 같이 M2M을 위한 프로토콜 계층으로 Rest 기반의 CoAP 프로토콜과 다양한 장치에서 UDP 통신으로 초기 로딩, 클라이언트 등록, 자원 감시/제어, 정보 업데이트 등을 지원한다[3].

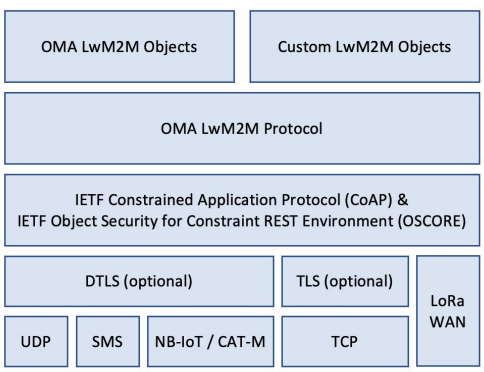

Fig. 1. LWM2M Structure and Protocol

LwM2M은 초기 버전 이후 표준 프로토콜 개선과 함께 LoRa 호환 모듈의 가격 평준화와 저전력 문제가 크게 개선된 후 단일 통신환경에서 지능형 공장, 스마트 물류 등 기술 활용의 범위와 규모(기존 WiFi나 블루투스의 전송 거리)가 크게 확장되었다. 920MHz 비 면허 대역에 약 1Km ~최대 10km 거리와 약 50 Kb 바이트 이하 전송 규격의 네트워크를 구축할 수 있다. Fig 2와 같이 국내는 KT와 SKT 통신사를 중심으로 상용화 중이며, LPWAN 셀룰러 기반 LTE-M과 IoT 저용량 데이터용 NB-IoT가 구축되어있다[4,5].

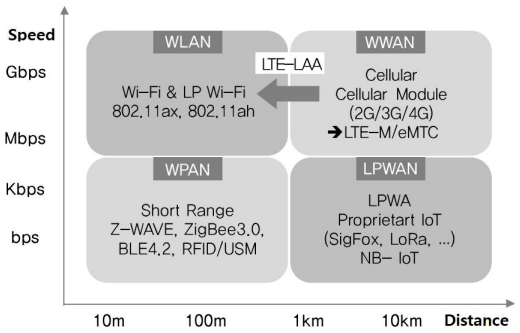

Fig. 2. LPWAN Standard transfer rate Comparison

SigFox, LoRa는 저전력 장거리, 비면허 대역으로 통신사 없이 네트워크를 구축/활용할 수 있는 특징이 있다. 또한, 실제 필요한 H/W 통신 모듈 시세가 아마존 기준 3~10달러 가격으로 형성되어 있어 실제 구축 비용의 부담이 적다. Fig 3은 LoRa 네트워크 구조의 통신 구성을 나타낸다[6].

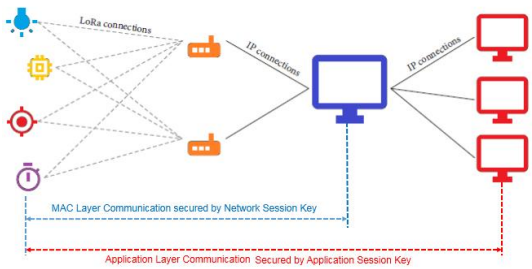

Fig. 3. LoRa Network Aritecture

기존에 LoRa 프로토콜은 센서 장치들을 활용하여 가스/수도/AMI 등 저전력 및 규모와 통신이 적은 모니터링 용도로 사용되고 있다. 하나 이상의 서버와 게이트웨이로 구성되며, 내부 암호화 통신에 공유키 방식의 AES(Advanced Encryption Standard) 암호 표준을 지원한다. 대규모 네트워크에는 적합하지 않으며, 기존 WiFi나 블루투스 네트워크 환경과 연동하는 것이 일반적이다[7]. 문제는 최근(LoRawan 1.1 버전 기준) 약한 키 관리, 취약한 암호화, 취약한 인증 등 해킹에 대한 취약점이 존재하고, 장치 내부 해킹에 대한 취약점도 알려져 있다[8,9]. 분석 결과, 도난 방지 및 보안 기능 구현을 위해 프로토콜의 추가/수정이 필요하다고 분석된다.

2.2 Blockchain

블록체인 기술은 2008년 '나카모토 사토시'에 의하여 알려졌으며, 중개 기관이 없는 거래와 거래자 사이에 신뢰성을 보장한다[10]. 초기 트랜잭션 처리와 에너지 낭비 문제를 해결하기 위해 다양한 변화를 겪어왔고, 다양한 합의 프로토콜이 개선됐다. 핵심은 가장 긴 체인을 선택하여 해시함수를 찾는 과정이다. Fig 4와 같이 블록체인의 종류와 내부 합의 알고리즘 규격에 따라 처리 난이도(성능)에 큰 차이가 있다[11]. 퍼블릭 블록체인 방식은 통신 노드가 공개되어 누구나 참여할 수 있지만, 확장성의 한계와 속도 저하 문제가 있다.

Property	*Public blockchain*	*Consortium blockchain*	*Private blockchain*
Consensus determination	All miners	Selected set of nodes	One organisation
Read permission	Public	Could be public or restricted	Could be public or restricted
Immutability	Nearly impossible to tamper	Could be tampered	Could be tampered
Efficiency	Low	High	High
Centralised	No	Partial	Yes
Consensus process	Permissionless	Permissioned	Permissioned

Fig. 4. Comparisons – Public blockchain, Consortium blockchain and Private blockchain

프라이빗 블록체인 방식은 하나의 주체가 내부 노드를 관리하며, 트랜잭션 속도가 빠른 장점이 있다. 두 블록체인 종류에는 대표적인 합의 알고리즘으로 작업증명(PoW), 지분증명(PoS), 위임형 지분증명(dPoS), 비잔틴 장애 감내(BFT) 등이 존재한다. Fig 5는 각 합의 알고리즘의 특징을 나타낸다[12].

Property	*PoW*	*PoS*	*PBFT*	*DPOS*
Node identity management	Open	Open	Permissioned	Open
Energy saving	No	Partial	Yes	Partial
Tolerated power of adversary	< 25% computing power	< 51% stake	< 33.3% faulty replicas	< 51% validators
Example	Bitcoin	Peercoin	Hyperledger Fabric	Bitshares

Fig. 5. Comparisons – Blockchain Consensus Algorithms

PoW, PoS, dPoS와 PBFT는 블록체인 유형이 다르다. 초기 PoW는 처리 속도(느림)에 따른 에너지 소모와 51% 공격 등 문제가 존재했다. 이후 개선된 POS가 개발되었지만, 여전히 처리 속도에는 한계가 있다고 알려졌다[13]. dPoS와 PBFT는 확장성 문제를 해결하고, 속도를 개선한 공통점을 가지지만, 퍼블릭/프라이빗 블록체인으로 네트워크 환경이 다르다.

본 연구의 제안 모델은 소규모 네트워크(노드의 수가 제한적), 소유자 주체(개인)가 존재, 높은 성능을 고려하여 PBFT(Practical Byzantine Fault Tolerance) 합의 알고리즘을 선택했다. Fig 6은 PBFT의 합의 과정을 나타낸다[14].

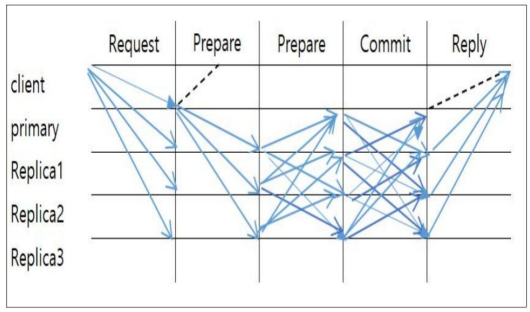

Fig. 6. PBFT Algorithm Process

블록체인 생성/검증에 모든 노드는 Prepare 과정에서 선출된 Replica를 리더로 선출하고 이를 모든 노드에 전달한다. Commit 과정에서 요청된 노드 수가 전체 노드 수의 2/3 이상일 경우 블록을 검증한 후, 검증 결과를 다른 노드에 알려준다[15]. 블록체인 네트워크 구축/운영으로 인한 실제 성능 저하 문제 부분을 해결해야 할 것으로 분석된다.

2.3 도난/분실 관련 연구 비교분석

Table 1은 5년 이내 학술검색(국내) 결과 ('도난', '분실' 키워드)에서 IoT와 블록체인 관련된 대표 연구를 비교 분석한 결과이다[16-21]. 관련 연구가 부족하여 도난당한 상황과 비슷한 유형의 분실, 장치에서 모든 사물을 대상으로 검색 범위를 확대했다. 이외 세부 내용에 설계, 구현, 테스트를 모두 포함하는 논문을 선정했다. 비교분석 항목의 의미는 순서대로 다음과 같다.

1) 표준 통신 프로토콜, 2) 신뢰 네트워크, 3) 전력 소모량, 4) 도난/분실 추적, 5) 보안 기능, 6) 기타 등으로 차이점을 비교 분석했다.

통신이 기반이 되는 모든 장치 연구/개발은 기본적으로 통신 표준 프로토콜을 준수해야 한다. 논문 분석 결과, 통신 프로토콜은 존재하지만 표준 규격을 준수하는지 내용이 명확하지 않고, 인증 및 추적 등 보안 기능을 대부분 고려하지 않은 것으로 분석된다. 일부 블록체인 기반 관리 시스템 연구가 있지만, 소규모 네트워크에 적합하지 않은 블록체인을 사용한다. 이외 대부분 장치의 비용 문제와 소형화 및 거리 제한 등 실용성이 다소 부족한 것으로 분석된다.

Table 1. Related work Comparison

Name	Problem					
	1	2	3	4	5	6
Han, M. S, Lee, W. S	X	X	a little high	X	X	Small Impossible
Son, Y. B, Kim, Y. H	X	○	Unverifiable	X	X	No wireless
Ko, J. H. at el.	○	X	○	○	X	price high
Kwak, H. Y, Chang, J. W., Hu, J. S.	○	X	○	○	X	price high
Jang, W. C., Lee, M. H.	○	X	○	X	X	distance limit
Kim, M. S., Joo, J. H., Park, G. D.	○	X	○	○	X	distance limit

3. 블록체인 기반 LoRa 프로토콜

3.1 도난 방지 모델 설계 고려사항

통신 모델을 설계하는데 네트워크의 규모, 소유자의 존재, 블록의 생성 주기, 중앙화 여부 등 항목을 고려해야 한다. 본 연구가 제안하는 도난 방지 모델(네트워크 중심)의 특성을 파악하면 다음과 같다.

① 네트워크 종류 : LoRa 표준(비대역/셀룰러 X)
② 통신 구성 : n:1:1(다중 노드, 게이트웨이, 서버)
③ 네트워크 규모 : 최소 4 노드, 7 노드, 10 노드
④ S/W 구현 : Arduino(C++), Python

본 연구가 제안하는 도난 방지 모델(합의 알고리즘 중심)의 특성을 파악하면 다음과 같다.

① 실시간성 : 초기 블록 생성 이후 변동 적음
② 블록 생성 요구사항 : 검증된 블록, 협력 생성방식
③ 포크 발생/처리 성능 : 없음/제한적임
④ 블록 검증 : 기본(전체)/간소화 모드
⑤ 블록 제거 : 한계 용량이면 이전 노드 제거
⑥ S/W 구현 : 블록체인 PBFT(C++)

본 연구가 제안하는 도난 방지 모델(위치 확인/추적)의 특성을 파악하면 다음과 같다.

① 위치 추적 정보 : IP(지역), GPS(세부)
② 위치 확인 : 초기 세션 1회(필수)
③ 확인 주기 : GPS 갱신(5초) 도난/분실(3초)
④ 도난/분실 : 1차(지역), 2차(10m)
⑤ 블록 검증 : 도난 이후 블록 검증 간소화
⑥ 세션 갱신 : 5분(300초)
⑦ 세션 종료 : 30분(1800초), 전원(배터리 교체), 추적모드 종료, 모듈 메모리 공간 부족
⑧ S/W 구현 : Arduino(C++), Python

3.2 전체 통신 과정

Fig. 6은 LoRa 기반 PBFT 프로토콜 흐름을 나타낸다.

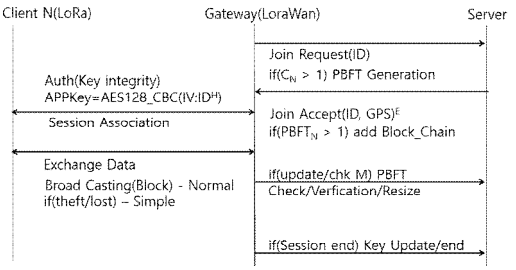

Fig. 6. LoRa-based PBFT Protocol flow

초기 요청에 장치 식별자(ID)를 생성하고, PBFT 블록체인 생성 이후 일반 모드(Normal)로 동작(최초 1회)한다. 기존 프로토콜과 다른 점은 공유키(AppKey)를 생성하는 블록 ID 해시값(선출된 리더) 16바이트를 초기 벡터(IV)로 사용했다. 안전한 세션 성립 이후에는 공유키로 암호화된 ID, GPS 정보를 전송한다.

3.3 프로토콜 - 블록체인 생성 및 검증

Fig 7은 기본 모드와 간편 모드의 수정된 PBFT 블록체인 생성/검증 과정을 나타낸다. (기존 BPFT = 검정 윤곽선, 수정/추가 = 점선 윤곽선)

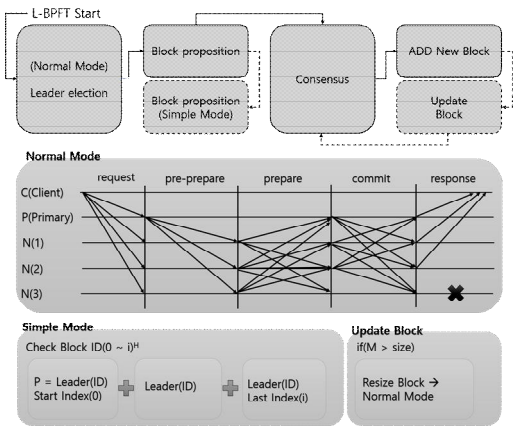

Fig. 7. PBFT(Normal, Simeple) Protocol flow

기본 모드(Normal Mode)에서 PBFT의 브로드 캐스팅(Broad Casting) 및 업데이트(Update)하는 과정은 기존 합의 알고리즘 과정과 같다. 리더선출 이후, 블록을 취합하여, 응답받은 노드가 전체 노드에서 과반수 이상이면 검증하고 블록을 추가한다.

도난/분실로 간편(Simple) 모드가 동작하는 경우, 블록 ID의 해시값을 검사하여 기존 블록체인 검증 과정을 간소화한다. 블록 ID 해시값은 세션마다 생성된다. 예로 세션 갱신이 3회 = 해시 블록 ID 목록(0, 1, 2)는 총 3개의 ID 값을 연속 검사한다. 이외 블록 갱신 단계에서 장치(n)의 PBFT 내부 메모리(M)의 저장공간이 부족한 경우 이전 블록의 크기를 재조정(Resize)하고 전체 블록을 갱신한다.

3.4 프로토콜 - 도난 및 추적

Fig 8은 도난/분실 단계에서 GPS 이동 추적 기능을 나타낸다.

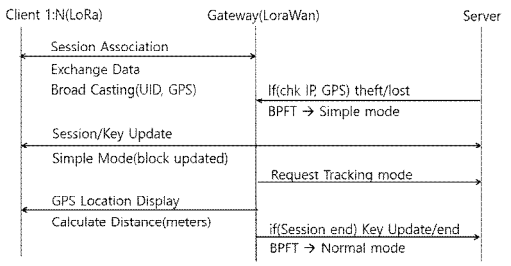

Fig. 8. GPS Tracking Protocol flow

기본적으로 세션이 성립된 이후 장치 ID와 GPS를 브로드 캐스팅한다. 도난/분실을 판단하는 기준은 IP 주소와 GPS 지역 정보(도시, 주)가 일치하는지, GPS 거리(미터 단위)를 계산하여 판단한다. 예로 도난/분실이 발생하면 간편 모드로 전환되고, GPS를 추적하게 된다. 세션 또는 추적모드가 종료되면 다시 기본 모드로 전환하고 새로운 세션을 시작한다.

4. 통신 모듈 구현 및 테스트

4.1 구현 환경 설정

LoRa 장치는 LoRaWAN을 통해 서버와 통신한다. 본 연구에서 사용한 LoRa 하드웨어 모듈 규격과 설정은 다음과 같다. (LoRa RF로 LoraWAN 사용)

① H/W : LoRa RF(SX1276), GPS(NEO-6M), 호환 안테나, 개인 PC(아파치 웹 서버)
② 거리/전송률 : 최대 3km, 약 2~5kb(기본)
③ 작동 주파수 : 920.3(기본) - 923.3MHz(국내)
④ 최대 저장 용량 : 8MB (64M-Bits) 플래시

실험 환경은 정상적인 양방향 통신에서 블록체인 처리 안전성과 성능을 분석한다. 통신 중에 메시지 전달 실패 및 중복으로 인한 전파 지연 시간은 제외한다.

4.2 안전성 분석

PBFT의 합의 과정에서 총 노드 N에 대하여 악의적 노드가 존재할 수 있다. 배신자 노드가 n개 있을 때, 총 노드 개수가 3n+1개 이상이면 해당 네트워크에서 이루어지는 합의는 신뢰할 수 있다. 노드 신뢰성 검증에 최소 4개 노드가 필요한 이유이다. 본 제안 모델에서 주요 보호 파라미터는 공유키, 블록 식별 ID, 장치 식별 UID, GPS 정보이다.

① 공유키 안전성 : 해킹 공격에 대한 위협은 센서 노드에 있는 iot 장비가 가장 취약하다. 공유키 유추를 방지하기 위해 블록 ID 해시값을 IV(AES-128)로 사용했다. 세션이 갱신되면 블록 및 키가 갱신되고, 생성된 블록의 ID 목록을 저장한다. 화이트 리스트 기법으로, 공유키의 IV 파라미터를 유추하는데 웹 서버 또는 합의 알고리즘 양방향 해킹해야 하는 어려움을 가진다.

② 비정상 장치 참여 : GPS 추적에 세션 ID와는 다른 추적 전용 UID를 활용한다. 장치 ID를 확인하고 블록 ID를 유추하는데 웹 서버 해킹과 동시에 세션 갱신 이전에 지속 갱신되는 블록의 과반수를 공격해야 한다. 이는 키 안전성과 같이 PBFT 합의 알고리즘 자체를 해킹해야 하는 어려움이다.

③ GPS 변조 가능성 : 실시간으로 암호화된 GPS 정보를 확인하는데, 공유키 유추와 장치 ID의 목록을 보유한 서버를 해킹 성공해야 한다. 프로토콜 과정에서 GPS 정보는 항상 블록 검증 단계 이후에 수행된다. 이는 앞서 합의 알고리즘과 서버를 둘 다 해킹해야 하는 어려움을 가진다.

4.3 성능 분석

Fig. 9는 두 노드(분실 : 사용자) 그룹의 GPS 정보를 나타낸다.

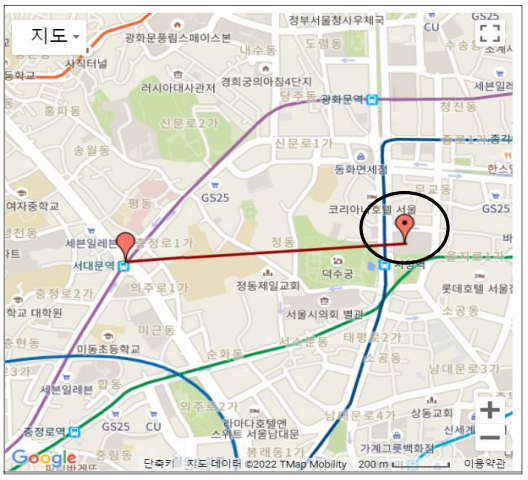

Fig. 9. Location Information(Test Node)

분실된 노드(n)의 위치는 서대문(GPS : 37.56582, 126.96664), 사용자 그룹 n의 위치는 서울시청(GPS : 37.56647, 126.97798)이다. 실제 통신 거리(미터)는 약 1.002m이다. 기존 PBFT(기본 모드)와 수정된 합의 알고리즘(간편 모드 : 분실/도난)의 지연 시간을 측정하였다. Table 2는 노드 수 증가에 따른 평균 합의 최대/평균/최소 지연 시간(ms)을 나타낸다. 지연 시간은 ID 요청 시간에서 마지막 Response 시간의 간격을 의미한다. (10회 반복 측정)

Table 2. Delay Time Comparison(ms) - 1 Session

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

다양한 시간 지연 결과를 분석하기 위해 전체(10회) 중 5라운드까지 기본 모드 수행, 6라운드에 간편 모드를 수행하고 9라운드에서 용량 한계로 인한 블록 크기 재조정을 수행하고, 10라운드에서 다시 기본 모드로 전환 후 세션을 종료했다. 기존 PBFT 알고리즘은 네트워크 노드 수 증가(통신량 $2n^{\wedge 2}$)하면 높은 네트워크 성능이 요구된다. 통신량을 비교하면 4 노드(64회), 7 노드(196회), 10 노드(400회)로 10 노드 이상부터 급격하게 처리량이 증가한다.

세션 성립 및 갱신 단계에서 합의 알고리즘은 최소 2번 수행된다. 시험 결과 10 노드 기준 PBFT의 전체 지연 시간은 587.82ms * 2 = 약 1175ms이다. 제안 프로토콜은 도난/분실 모드로 진입한 후 1075.84ms (587.82 + 488.02ms)로 평균 지연 시간이 99.16ms 개선(9.1%)됐음을 확인했다. 이외 최소(66%), 최대(48%) 효율이 크게 개선됨을 확인했다.

Fig. 10은 노드 수 증가에 따른 평균 합의 최대/평균/최소 지연 시간(ms) - 차트를 나타낸다. 노드 수가 증가함에 따라 지연 시간(0.03초~1초 이상)이 급격하게 증가하는 것을 볼 수 있다.

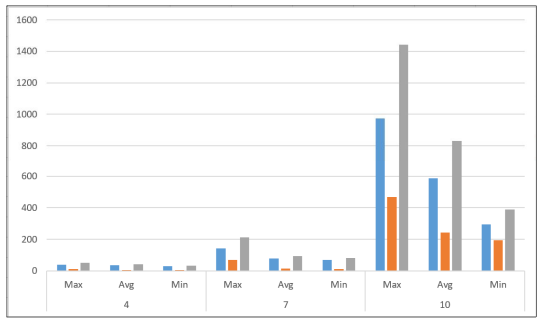

Fig. 10. Delay Time Comparison(ms) - chart

Lora 표준 단말 모드는 기본 1초 이상 지연(Sleep mode) 시간을 가진다. 이외 하드웨어 모듈의 제한적 성능 때문에 정상 통신에 지연 설정이 5초(5000ms) 이상 필요했다. 실험 결과 시간(0.03초~1.6) 범위보다 정상 통신의 지연 시간 비중이 훨씬 높다. 지연의 수준이 다소 적다는 것을 알 수 있다. 주요 지연의 원인은 Lora 장치 테스트 지역(주요 도심권)의 주파수 간섭 등에 의한 음용 지역 발생 문제이다. Table 3은 기존 블록체인 합의 알고리즘과 제안 프로토콜을 다양한 각도로 정성 비교한 결과이다.

Table 3. Block-Chain Algorithm Comparison(Result)

	PUBLIC	PBFT	Proposed
Node	none specified	Authorization required	Authorization required
Time	Slow	Fast	Fast (improved)
Security	High	relatively vulnerable	relatively vulnerable (improved)
Power Consumption	High	Low	Low
Authentication	Implementation required	Implementation required	Implementation required(added)
Centralization	Impossible	Possible	Possible

기존 블록체인 합의 알고리즘들을 비교했을 때, 적절한 환경에서 성능 부분과 안전성 부분을 개선하고, 보완하였다. Lora 하드웨어 모듈의 전력 수준과 내부 통신 성능에 따라 크게 영향을 받았는데, 이는 프로토콜 최적화 이외의 문제로 물리적인 송/수신기, 안테나 및 증폭기 등을 적용하여 전송률과 지연 시간을 개선해야 할 것으로 분석된다.

5. 결론

본 연구는 도난/분실 기능을 중심으로 Lora 통신 환경에 적절한 PBFT 합의 알고리즘을 적용하였다. 장거리 통신이 가능하지만, 저전력, 소규모 네트워크를 고려하여 추적 및 보안 인증 기능을 추가 했다. 또한, 내부 합의 알고리즘 검사를 간소화하여 처리 성능을 최적화 했다. 실제 도난 방지 장치 모듈로써 활용되는 경우 배터리가 부착된 소형 하드웨어 모듈에 적용할 수 있다. 자전거, 오토바이, 자동차, 노트북, PC, 핸드폰 등 분실이 가능한 장치/장비에 장착하여 사용할 수 있다. 배터리 및 GPS와 Lora 통신 모듈을 탑재하는 경우 개당 10달러 이내 가격대로 제품화를 고려할 수 있다.

본 연구는 PBFT 블록체인 네트워크의 최소 노드 구축에 필요한 장치 개수를 4개(최대 10개)로 설정했다. 도난 방지를 위해 저가형 HW 모듈을 설치하여 다수 활용할 수 있는 환경은 홈 네트워크 환경이 적절하다. 본 연구는 향후 소규모 네트워크에서 도난 방지를 위한 Iot 장비 세트 제품 개발에 이바지하고자 한다.

REFERENCES

[1] CISCO. (n. d.). *Cisco Annual Internet Report (2018-2023) White Paper* (Online). https://www.cisco.com/

[2] J. E. Lee, J. H. Kim, S. M. Jeong & J. S. Song. (2018). oneM2M Global Internet of Things(IoT) Standard Trend. *The Magazine of Kiice, 19(1),* 31-43.

[3] Stafan Vaillant. (n. d.). *Lightweight M2M(LWM2M).* DEFINITION OF LIGHTWEIGHT M2M (LWM2M) (Online). https://techradar.softwareag.com

[4] S. Y. Kim, S. K. Park & H. D. Choi. (2016). Wide Range IoT Technology and Standardization based on LPWA. *Electronics and telecommunications trends, 31(2),* 95-106.
DOI : 10.22648/ETRI.2016.J.310210

[5] J. H. Kim, W. J. Park & S. H. Park. (2020). LoRa LPWAN-based Wireless Measurement Sensor Installation and Maintenance Plan. *Journal of the Computational Structural Engineering Institute of Korea, 33(1),* 55-61.
DOI : 10.7734/COSEIK.2020.33.1.55

[6] Lora-alliance Resource-Hub. (n. d.). *(Long Ra3nge) Network and Protocol Architecture & Frame Structure* (Online). https://www.techplayon.com/

[7] S.-H. Mah & B.-S. Kim. (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

[8] H. Noura, T. Hatoum, O. Salman, J. P. Yaacoub & A. Chehab. (2020). LoRaWAN security survey: Issues, threats and possible mitigation techniques. *Internet of Things, 12,* 100303.
DOI : 10.1016/j.iot.2020.100303

[9] I. Butun, N. Pereira & M. Gidlund. (2019). Security risk analysis of LoRaWAN and future directions. *Future Internet, 11(1),* 3.
DOI : 10.3390/fi11010003

[10] D. Y. Lee et al. (2017). Blockchain core

technology and domestic and international trends. *Communications of the Korean Institute of Information Scientists and Engineers, 35(6),* 22-28.

[11] Z. Zheng. (n. d.). *Blockchain challenges and opportunities: A survey* (Online). https://www.researchgate.net/

[12] S. G. Kim. (2020). *Blockchain core technology and domestic and international trends.* IITP, Weekly technology trend- ICT new technology. 1965, 13-25.

[13] J. S. Park et al. (2018). Past, Present and Future of Blockchain Technology, *Electronics and Telecommunications Trends. 33(6),* 139-153. DOI : 10.22648/ETRI.2018.J.330614

[14] Y. A. Min. (2020). A Study on PBFT Modification for Efficient Consensus. *Journal of Information Technology and Applied Engineering, 25(4),* 47-53. DOI : 10.22733/JITAE.2020.10.01.005

[15] D. G. Kim, J. Y. Choi. K. Y. Kim & J. T. Oh. (2018). Performance Improvement of Distributed Consensus Algorithms for Blockchain through Suggestion and Analysis of Assessment Items, *Society of Korea Industrial and Systems Engineering, 41(4),* 179-188. DOI : 10.11627/jkise.2018.41.4.179

[16] M. S. Han & Lee, W. S. (2019). Design of IOT-based Anti-Theft System with Remote Control. *Journal of Knowledge Information Technology and Systems, 14(6),* 655-663. DOI : 10.34163/jkits.2019.14.6.008

[17] Y. B. Son & Y. H. Kim. (2019). Design of Management System for Registering Agricultural Machine Using Blockchain. *The Journal of the Korea Contents Association, 19(12),* 18-27. DOI : 10.5392/JKCA.2019.19.12.018

[18] J. H. Ko. at el (2017). Implementation of GPS-based Wireless Loss Prevention System using the LoRa Module. *Journal of Digital Contents Society, 18(4),* 761-768. DOI : 10.9728/dcs.2017.18.4.761

[19] H. Y. Kwak, J. W. Chang & J. S. Hu. (2019). The Design and Implementation of Dog Loss Prevention Device Combining Wireless Communication and GPS Technology. *Journal of The Korea Society of Computer and Information, 24(2),* 103-109. DOI : 10.9708/jksci.2019.24.02.103

[20] W. C. Jang & M. E. Lee. (2017). Development of LPWA based Bus Entry Notification Systems for Smartphone Loss Prevention at Bus Stop Charging Stand. *Journal of Advanced Navigation Technology, 21(6),* 620-625. DOI : 10.12673/JANT.2017.21.6.620

[21] M. S. Kim, J. H. Joo & G. D. Park. (2017). Development of the Smart Belt System for Preventing Loss of Items using Beacon. *Journal of the Korea Society of Computer and Information, 22(8),* 9-14. DOI : 10.9708/JKSCI.2017.22.08.009

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, Cryptography
· E-Mail : pjo21@naver.com