논문 22-47-06-02 The Journal of Korean Institute of Communications and Information Sciences '22-06 Vol.47 No.06
https://doi.org/10.7840/kics.2022.47.6.809

함정 전투 시스템의 신뢰성 및 보안성 향상을 위한 블록체인 기반의 데이터 공유 기법

이 종 우◆, 김 형 진*, 이 재 민**, 전 태 수***, 김 동 성°

Blockchain-Based Data Sharing Scheme to Enhance Reliability and Security for Naval Combat Systems

Jong-Woo Lee◆, Hyeong-Jin Kim*, Jae-Min Lee**, Tae-Soo Jun***, Dong-Seong Kim°

요 약

본 논문은 함정 전투 시스템의 신뢰성 및 보안성 향상을 위해 블록체인 기반의 데이터 공유기법(B-DSS, Blockchain-based Data Sharing Scheme)을 제안한다. 제안하는 기법은 공유하는 데이터를 합의 알고리즘 과정을 통해 블록체인에 저장한다. 저장한 데이터의 현재 블록 해시값과 이전 블록 해시값을 비교하여 기존에 저장된 데이터의 변동에 대한 유무를 확인할 수 있다. 또한, B-DSS의 유효성 검토 알고리즘을 통해 블록체인 적용으로 발생할 수 있는 지연을 개선하였다. 모의시험을 통해 B-DSS가 기존 블록체인에 적용된 합의 알고리즘 방식 대비, 데이터 공유 소요 시간을 감소시켜 실시간성 확보를 통해 사용성이 개선됨을 보였다. 또한, 함정 내부의 데이터를 블록체인에 분산 저장하여 기존 데이터 공유 방식 대비, 데이터 무결성 및 변경 추적을 통해 신뢰성 및 보안성 향상을 기대할 수 있음을 보였다.

Key Words : Blockchain, Data Distribution Service, Data Sharing Scheme, Naval Combat System

ABSTRACT

This paper proposes a Blockchain-based Data Sharing Scheme (B-DSS) to improve the reliability and security of a naval combat system. The proposed scheme stores the shared data in the blockchain through the consensus algorithm process. By comparing the current block hash value and the previous block hash value of the stored data, it is possible to check whether there is a change in the existing stored data. In addition, the delay that may occur due to the application of the blockchain was improved through the validation algorithm of B-DSS. Through simulation tests, it was shown that B-DSS improved usability by securing real-time by reducing the time required for data sharing compared to the consensus algorithm method applied to the existing blockchain. In addition, it was shown that data inside the naval combat can be distributed and stored in the blockchain to improve reliability and security through data integrity and change tracking compared to the existing data sharing method.

※ 본 연구는 금오공과대학교 학술연구비로 지원되었음(202001790001)
◆ First Author : BMTech System R&D Team, whddn4547@kumoh.ac.kr, 정회원
° Corresponding Author : Kumoh National Institute of Technology, Dept. of IT Convergence Eng., dskim@kumoh.ac.kr, 종신회원
* NSLab R&D Team, haengg@nslab.tech, 학생회원
** Kumoh National Institute of Technology, Dept. of IT Convergence Eng., ljmpaul@ kumoh.ac.kr, 종신회원
*** Kumoh National Institute of Technology, Dept. of Computer Software Eng., taesoo.jun@kumoh.ac.kr, 정회원
논문번호 : 202106-132-B-RN, Received June 15, 2021; Revised September 27, 2021; Accepted March 26, 2022

Ⅰ. 서 론

함정 전투 시스템에서는 다양한 센서 및 장비와 같은 무기체계 간의 데이터 공유를 위해 DDS(Data Distribution System) 미들웨어를 사용한다. DDS는 이기종에 대한 통신 문제를 해결하고 테이블이 변경되어도 개발자가 일일이 수정하지 않아도 되는 장점이 있지만, DDS가 사용되는 국방 및 사회 기간 사업 분야에서 보안에 대한 위협이 지속적으로 증가하고 있다[1]. 더욱이 이기종 무기체계 간 통합이 확대되면서 외부로부터 사이버 공격으로 인한 사이버보안 취약점이 새로운 이슈로 대두되고 있다[2].

한편 최근 국방 영역에서 미래전을 위해 블록체인 기술이 방어 목적으로 적용될 수 있다는 연구들이 대두되면서 항공우주 및 방위사업 분야에 블록체인에 관한 연구가 활발히 진행되고 있다[3,4]. 블록체인에 저장된 데이터는 누구도 수정할 수 없고 악의적인 노드의 공격으로부터 데이터를 보호할 수 있어 프라이빗 블록체인을 적용함으로써 신뢰성 및 보안성 향상을 기대할 수 있다. 이러한 프라이빗 블록체인에서는 다양한 합의 알고리즘이 존재한다. 그중 PBFT (Practical Byzantine Fault Tolerance) 합의 알고리즘은 비동기 시스템 내부에서 합의에 참여한 노드가 성공적인 합의를 할 수 있도록 하는 알고리즘이며 네트워크 내에 배신자가 있더라도 합의에 다다를 수 있다. 따라서 노드 간 합의를 통해 신뢰성이 향상된 데이터를 블록체인에 저장함으로써 데이터 무결성 보장을 통해 보안성을 향상시킬 수 있다[5].

그러나 일반적인 프라이빗 블록체인 기법을 함정 전투 시스템에 적용한다면 PBFT 합의 알고리즘을 처리하는 과정이 필수적으로 추가된다. 따라서 노드 수의 증가에 따라 데이터 공유가 이루어지는 소요 시간이 증가하며 실시간성을 만족할 수 없다.

이러한 문제점을 해결하기 위해 DDS를 이용한 블록체인 기반의 데이터 공유기법을 제안한다. 제안하는 기법은 PBFT 합의 알고리즘의 실시간성을 만족시키며 DDS 미들웨어 기반의 데이터 공유기법의 신뢰성 및 보안성을 향상시켰다.

본 논문의 구성은 다음과 같다. 1장 서론에서 본 논문에서 제안하는 기법을 소개하고 2장에서 관련 연구 및 기존 기법의 문제점에 대해 분석한다. 3장에서 블록체인 기반의 데이터 공유 기법에 대해 서술하고 4장에서 모의실험 및 성능 평가를 통해 제안하는 기법에 대한 적합성을 평가한 뒤 5장에서 결론 및 향후 연구에 관해 서술한다.

Ⅱ. 관련 연구 및 문제점 분석

2.1 함정 전투 시스템의 개요 및 기존 데이터 공유기법의 문제점 분석

함정 전투 시스템에서 사용되고 있는 DDS 미들웨어를 이용한 데이터 공유기법은 다수의 처리장치 및 센서 내부에서 다양한 애플리케이션으로 구현되어 있다. 따라서 이기종 센서 및 장비 간 통신을 위해 소프트웨어의 복잡성과 연결성이 증가하고 있다. 최근에는 무기체계가 자동화되고 네트워크를 통한 상호연결성이 높아지며 소프트웨어의 비중과 중요성이 강조되고 있다. 하지만 함정전투 시스템은 사이버보안의 중요성이 다른 무기체계에 비해 상대적으로 낮게 평가되고 있으며 소프트웨어에 대한 체계적인 보안성 시험이 시행되지 않고 있다[6].

또한 함정 전투 시스템과 같은 내부망으로 이루어진 분산 시스템에서는 분산 컴퓨팅 구성을 기반으로 데이터를 저장하며 이렇게 저장된 데이터는 보안과 직접 관련되어 있다[7]. 이러한 분산 컴퓨팅 구성을 기반으로 한 데이터 저장기법은 중앙 서버가 존재하기 때문에 데이터의 보안성 및 무결성에 대해 취약하다.

2.2 DDS 미들웨어의 구조 및 보안성 분석

DDS는 발간/구독(publish/subscribe) 기반의 실시간성, 확장성, 신뢰성을 갖는 OMG(Object Management Group) 표준 미들웨어이다. 프로그래밍 모델에 대한 표준화를 위해 개발되었으며 최근 군에서뿐만 아니라 민간기업과 같은 다양한 분야에서 활용되고 있다[8].

DDS는 그림 1과 같이 애플리케이션, DCPS(Data Centric Publish Subscribe), RTPS(Real Time Publish Subscribe), Transport 계층으로 나뉜다. DCPS는 데이터를 교환할 다른 애플리케이션에 대한 정보 없이 Topic 기반의 통신을 수행할 수 있다. RTPS는 OMG에 의해 표준화된 데이터 중심구조를 위한 데이터 전송 프로토콜로써 발간/구독 통신 모델을 지원하며 UDP와 같이 신뢰성이 부족한 전송 계층에서도 동작이 가능하다. 이러한 구조는 자료구조(Queue) 기반의 데이터 전송을 하지 않기 때문에 함정 전투 시스템과 같은 실시간 시스템에 적합하며, 22가지의 QoS(Quality of Service)를 지원하여 노드 관리에 용이하다.

기존의 DDS는 도메인 분리 취약성, 응용프로그램 무결성 등의 보안에 대한 취약점을 갖는다. 도메인 분리 측면에서는 DDS 내부에 자체적인 보안 기능이 없

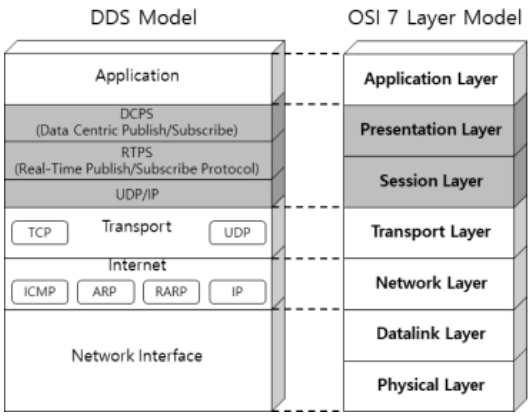


그림 1. TCP/IP 상의 DDS 구조
Fig. 1. DDS Structure on the TCP/IP

으므로 동일한 네트워크 도메인에 포함된 참여자는 누구나 통신 패킷의 탈취, 위조, 변조 등이 가능하다. 또한, 응용프로그램 무결성에 대한 취약성 측면에서는 DDS 운용을 위해 필요한 다수의 실행 파일, 설정 파일, 라이브러리, 감사 로그 등 데이터에 대한 보호가 필요하다. 최근 이러한 보안 취약점에 대응하기 위해 DDS에 보안 기능을 추가한 DDS Security에 관해 연구되고 있다[9]. 하지만 DDS Security의 경우 디스커버리 과정에서 인증 관련 절차가 복잡하여 부하를 급증시키는 문제가 있다[10]. 또한, 도메인 내부에서 인증받은 참여자 정보 접근 여부와 중요 데이터에 대한 암호화 수행 여부가 검증되지 않았기 때문에 데이터 무결성이 보장되지 않는다.

2.3 블록체인 합의 알고리즘의 실시간성 분석

블록체인이란 데이터 분산 처리를 통해 블록체인 네트워크에 연결된 노드에 데이터를 저장 및 보관하는 기술이다. 블록체인은 최근 데이터 공유기법과 같은 다양한 분야에서 연구되고 있으며 블록체인이 높은 보안성을 갖는 이유는 모든 블록 해시값들이 상관관계에 놓여있기 때문에 데이터에 대한 무결성을 확보할 수 있기 때문이다[11].

이러한 블록체인은 다수의 노드가 통일된 의사결정을 위해 합의 알고리즘을 사용한다. 합의 알고리즘을 통해 저장된 데이터는 무결성이 증명된 데이터이며 기존에 저장된 데이터를 변경 및 수정할 수 없다는 점에서 높은 신뢰성을 가진다. 합의 알고리즘 중 PBFT 합의 알고리즘은 미리 정의된 행동을 하지 않는 비동기 시스템일 경우 합의에 참여한 노드가 성공적인 합의를 할 수 있도록 하는 알고리즘이다. PBFT 알고리즘은 P2P 통신을 이용하여 그림 2와 같이 진행된다.

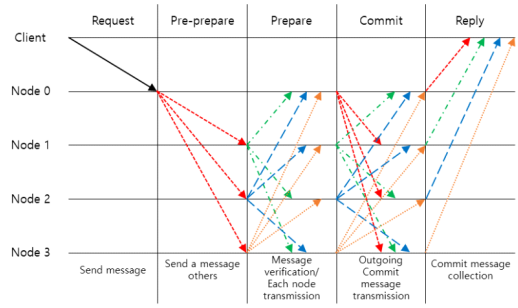


그림 2. PBFT 합의 알고리즘
Fig. 2. PBFT Consensus Algorithm

먼저 클라이언트가 네트워크의 모든 노드에게 현재 상태에 관한 확인을 요청한다. 모든 노드 중 선정된 대표 노드인 Node 0은 클라이언트로부터 받은 트랜잭션(Transaction)을 블록으로 생성 후 다른 나머지 노드들에 블록을 전송한다. 다른 노드들은 블록을 수신하고 블록을 수신했다는 사실을 다른 노드들에 전송한다. 각 노드는 다른 노드들이 블록을 수신했는지에 대한 여부를 취합한다. 이러한 PBFT 알고리즘을 이용하여 일부 노드의 합의 결과가 달라도 66% 이상의 합의 결과가 같다면 합의가 성공적으로 이루어졌다고 할 수 있다.

이와 같이 PBFT 알고리즘은 데이터에 대한 높은 신뢰성을 보장하지만, 네트워크 내부의 전체 노드 수의 증가에 따라 사용되는 전체 통신량이 지수 함수로 급격하게 증가한다는 단점이 있다. 따라서 다수의 노드를 사용하는 함정 전투 시스템에 일반적인 PBFT 합의 알고리즘을 적용할 경우 함정 전투 시스템의 실시간성 요구사항(1 ms ~ 100 ms)을 만족하지 못하는 문제가 발생한다.

Ⅲ. 함정 전투 시스템의 신뢰성 및 보안성 향상을 위한 블록체인 기반의 데이터 공유기법

3.1 B-DSS의 시스템 모델

그림 3은 본 논문에서 제안하는 블록체인 기반의 데이터 공유기법(B-DSS, Blockchain-based Data Sharing Scheme)의 데이터 흐름에 대한 구성도이다. 각 노드는 Topic을 갖고 있으며 발간/구독(pub/sub) 기반의 통신이 이루어진다. 또한, 블록체인 데이터 및 Topic은 전역 데이터 공간(Global Data Space)에서 관리된다. 각 노드가 통신할 때 같은 Topic을 가진 노드들은 블록체인 데이터를 공유한다. 예를 들어 Node 1이 Topic A를 갖고 있다면 같은 토픽을 가진 Node

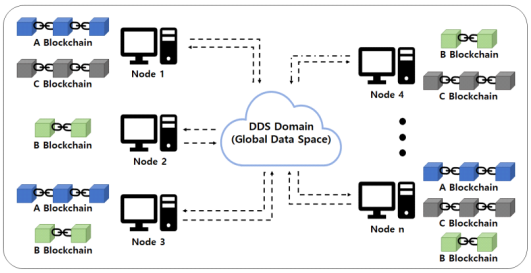


그림 3. 블록체인 기반의 데이터 공유 기법 구성도
Fig. 3. Configuration diagram of B-DSS

3에서 데이터를 수신하고 블록체인 데이터를 공유한다.

B-DSS는 기존 DDS 미들웨어 기반의 데이터 공유 기법에서 공유될 데이터를 합의 알고리즘을 통해 신뢰성이 향상된다. 합의가 이루어진 데이터는 블록체인에 분산저장을 통해 데이터의 보안성이 향상된다. 블록체인을 기반으로 하는 데이터 공유기법의 트랜잭션이 생성되는 과정은 그림 4와 같이 동작한다.

① : 기존 데이터 공유기법 환경에서 데이터를 변경 및 수정하고 변경된 데이터는 다른 노드들에게 PBFT 합의 알고리즘을 진행해야 한다는 Topic으로 발간한다.

② : 다른 노드들이 합의 알고리즘을 수행하기 위해 발간된 데이터를 구독할 수 있다. 또한, 서버는 마지막 트랜잭션에 데이터가 추가되는 과정에서 처음 생성된 데이터와 합의 알고리즘의 결과를 비교 후 데이터를 트랜잭션에 추가해야 하므로 데이터를 구독한다.

③ : 각각의 노드는 PBFT 합의 알고리즘을 실행하기 위해서 처음 구독한 데이터를 발간한다. 그 후 다른 노드들이 그 데이터를 구독한다.

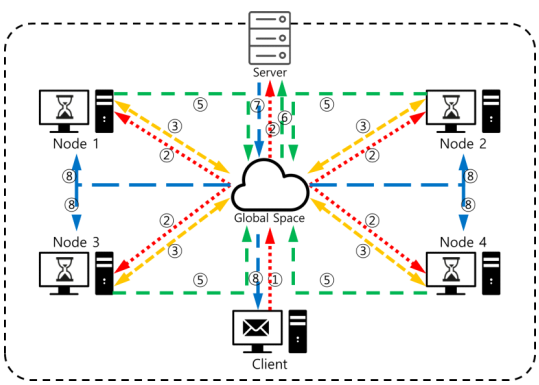


그림 4. B-DSS의 트랜잭션 생성 과정
Fig. 4. Transaction creation process of the B-DSS

④ : 다른 노드들이 처음 구독한 데이터와 자신이 처음 구독한 데이터를 비교하여 PBFT 합의 알고리즘을 진행하고 결과를 도출한다.

⑤ : 각자의 노드에서 받은 데이터들을 비교하여 PBFT 합의 알고리즘 결과를 출력한 뒤 발간한다.

⑥ : 서버는 각 노드로부터 발간된 PBFT 합의 알고리즘의 결과를 토대로 과반수인지 확인하고 과반수일 경우 합의가 이루어졌다고 판단하여 트랜잭션에 추가한다.

⑦ : 데이터가 트랜잭션에 추가되고 추가된 최종 블록체인 데이터를 발간한다.

⑧ : 각각의 노드들은 최종 데이터를 구독함으로써 데이터의 분산저장이 이루어진다.

3.2 B-DSS의 시퀀스 다이어그램 및 유효성 검토 알고리즘

B-DSS의 시퀀스 다이어그램은 그림 5와 같다.

① : 클라이언트는 getDomain 함수를 통해 domainID 값을 얻어내고 환경변수 해석 등 최초 동작에 필요한 초기화를 수행한다.

② : create_manager 함수로 domainID에 소속될 Manager를 생성한다.

③ : 생성된 Manager에 Listener를 등록한 후 데이터베이스를 생성한다. 클라이언트는 과거 데이터 유무에 따라 구분된 데이터베이스의 특성에 따라 데이터베이스를 생성할 수 있다.

④ : 데이터베이스 생성 및 초기 동작을 완료했다면 데이터베이스에 변경사항 발생 시 클라이언트에게 알림을 주기 위한 수단으로 on_changed_data

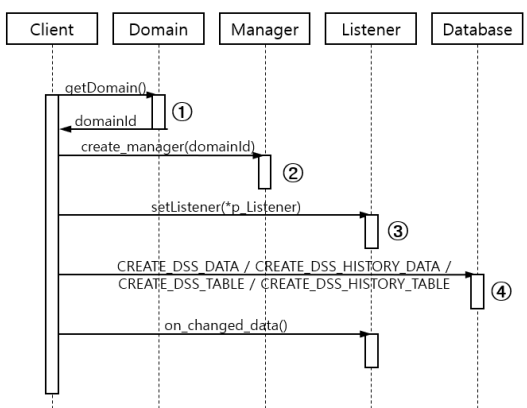


그림 5. B-DSS의 시퀀스 다이어그램
Fig. 5. Sequence Diagram of B-DSS

```
Algorithm1 : The validity of generated blocks
Input : Blockchain, output : Boolean
 1: procedure
 2:     for (i = 1, i < Blockchain.size(), i++) do
 3:         CurrentBlock = Blockchain.get(i)
 4:         PreviousBlock = Blockchain.get(i-1)
 5:         if (CurrentBlock.previoushash ≠ PreviousBlock.hash) then
 6:             return false
 7:         end if
 8:         if (CurrentBlock.substring(difficulty) ≠ HashTarget) then
 9:             return false
10:         end if
11:     end for
12:     for (j = 0, j < CurrentBlock.transactions.size(), j++) do
13:         CurrentTransaction = CurrentBlock.transactions.get(j)
14:         if (!CurrentTransaction.verifySignature()) then
15:             return false
16:         end if
17:     end for
18:     return true
19: End procedure
```

그림 6. 생성된 블록의 유효성 검토 알고리즘
Fig. 6. Validation algorithm of generated blocks

함수를 이용하여 데이터에 대한 위변조 상황을 확인할 수 있다.

그림 6의 알고리즘은 생성된 블록의 무결성 및 데이터가 트랜잭션에 문제없이 잘 저장되었는지를 파악하는 B-DSS의 유효성 검토 알고리즘이다. 해당 알고리즘은 현재 블록에 저장된 previoushash 값과 이전 블록에 저장된 해시값을 비교하고 트랜잭션의 유효성 및 무결성을 검토함으로써 기존에 저장된 데이터의 변동 여부를 확인할 수 있다. 또한, 생성된 블록이 특정 기준 해시값을 만족하는지 파악하여 올바른 블록인지에 대한 여부를 확인할 수 있다.

Ⅳ. 모의실험 및 성능 평가

본 장에서는 제안하는 기법을 성능 평가하고 결과를 분석하고자 한다. 성능 평가는 합정 전투 시스템을 위한 블록체인 기반의 데이터 공유기법을 기존 데이터 공유기법, 프라이빗 블록체인과의 성능을 비교 분석한다. 성능 평가를 통해 저장되는 데이터에 대한 위변조가 없는지 파악하여 신뢰성, 보안성 및 실시간성 만족 여부를 확인한다.

4.1 시험 환경 구성

본 논문에서는 B-DSS의 실시간성 분석을 위해 데이터 공유가 이루어지는 시간을 측정하고 신뢰성 및 보안성 분석을 위해 데이터 위변조 여부에 대해 파악한다. 따라서 위와 같은 성능 평가를 위해 본 논문에서는 세 가지 환경을 설정한다.

첫 번째로는 합정 전투 시스템의 분산 시스템 환경이 내부망이라는 조건이다. 기존 데이터 공유기법은 DDS를 사용하고 이를 사용하기 위해서는 내부망에서 사용되어야 하기 때문이다.

두 번째로 합의 알고리즘이 진행될 동안 데이터를 처리하는 속도를 고려하지 않고 합의 알고리즘이 이루어지기 위한 통신 소요 시간을 측정하였다.

세 번째로는 데이터 무결성 평가를 위해 실제 블록체인 데이터가 저장되는 JSON 파일을 캡쳐하여 데이터가 변경 여부를 확인하고 평가한다. 모의실험을 위해 사용한 장비의 성능은 표 1과 같다.

표 1. 모의실험 장비 성능
Table 1. Specification of equipment for simulation

Performance	Specifications
CPU	Intel(R) Core(TM) i5-7400 CPU @ 3.00GHz
Operating System	Windows 10
Graphic Card	NVIDIA GeForce GTX 1050
RAM	8GB

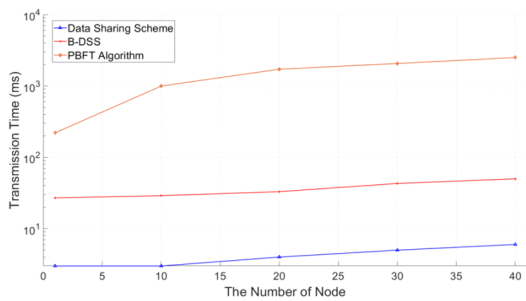
4.2 B-DSS의 실시간성 비교 및 분석

4.2장은 B-DSS의 신뢰성 및 실시간성 성능 비교 및 분석에 대해 다룬다. 성능분석을 위한 성능지표는 다음과 같다.

(1) 노드 수에 따른 데이터 공유 소요 시간

(2) 데이터 크기에 따른 데이터 공유 소요 시간

그림 7은 데이터가 공유되는 데 걸리는 시간을 노드 수에 따라 기존의 PBFT 알고리즘과 데이터 공유 기법을 B-DSS와 비교한 그래프이다. 기존 PBFT 알고리즘은 노드 수가 증가할수록 데이터 공유 소요 시간이 눈에 띄게 증가한다. 따라서 PBFT 알고리즘을



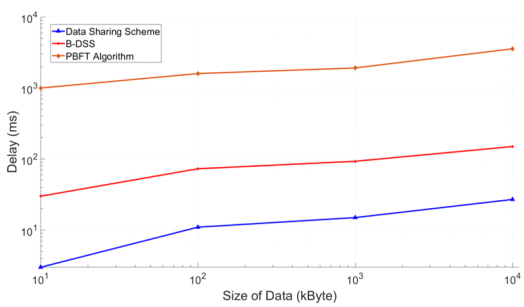
The Number of Node	1	10	20	30	40
PBFT Algorithm [ms]	220	997	1715	2064	2501
B-DSS [ms]	27	29	33	43	50
Data Sharing Scheme [ms]	3	3	4	5	6

그림 7. 노드 수에 따른 데이터 공유 소요 시간 비교
Fig. 7. Comparison of data sharing time according to the number of nodes

그대로 함정 전투 시스템에 적용할 경우 실시간성을 만족하지 못한다. 제안하는 기법은 기존 데이터 공유 기법과 비교하여 노드 수 대비 소요 시간 증가율이 15% 감소하였다. 따라서 노드 수가 많은 함정 전투 시스템에서 제안하는 기법이 적합함을 확인할 수 있다. 또한, 제안하는 기법의 합의 과정을 통해 데이터의 유효성을 검증할 수 있기 때문에 기존 데이터 공유 기법에 비해 신뢰성을 증가시켰다.

그림 8은 데이터가 공유 소요 시간을 데이터 크기에 따라 비교한 그래프이다. 기존의 PBFT 알고리즘은 비교하여 데이터 크기가 커질수록 데이터 공유 소요 시간이 2,500 ms 증가하였다. 제안하는 기법은 그림8의 결과와 기존 기법 대비 소요 시간 증가율이 감소함을 보였다.

또한, 본 논문에서 제안하는 B-DSS는 기존 데이터 공유기법 대비, 데이터 유효성 검증을 통해 신뢰성을 확보하였다. 그림 8에 도시한 시험 결과를 통해, 신뢰성을 최대로 확보할 수 있는 PBFT 방식 대비 지연시간 개선을 통해 사용성 및 적용 가능성을 확보하였고, 기존의 데이터 공유 방식 대비, 지연시간은 증가하지만, 유효성 검사를 통해 신뢰성을 확보하였다. 즉, 데이터 공유 지연시간과 신뢰성 사이의 trade-off 관계를 확인할 수 있다. 그리고, 본 실험을 통해서, 제안하는 기법의 데이터 공유 시간의 증가율이 기존 데이터 공유기법보다 감소하여 데이터 크기가 클수록 공유 지연시간 차가 작아질 것으로 보인다. 따라서, B-DSS는 데이터 유효성 검증을 통해 기존 데이터 공유기법보다 높은 신뢰성 확보가 가능하며, 함정 전투 시스템에서 요구하는 실시간성을 만족할 수 있다.



Size of Data (kByte)	10	100	1000	10000
PBFT Algorithm [ms]	990	1597	1915	3564
B-DSS[ms]	30	73	93	150
Data Sharing Scheme [ms]	3	11	15	27

그림 8. 데이터 크기에 따른 데이터 공유 소요 시간 비교
Fig. 8. Comparison of data sharing time according to the size of data

4.3 B-DSS의 보안성 분석

4.3장에서는 B-DSS의 보안성에 대해 분석한다. 표 2는 기존 데이터 공유기법과 제안하는 기법의 보안성 검증을 비교한 결과이다. 데이터 가용성 및 복구, 외부 및 내부로부터 공격에 관한 항목은 기존 데이터 공유기법이 중앙 서버를 통해 데이터가 저장되기 때문에 데이터를 분산 저장하는 제안하는 기법에 비해 외부/내부로부터의 해킹과 같은 위협으로부터 위험하다. 또한, 기존 기법은 무결성 검증 및 데이터가 변경되는지 추적할 수 없지만 제안하는 기법은 해시값의 변화를 통해 무결성을 검증할 수 있고 데이터가 변경 여부의 추적이 가능하다.

데이터 위변조를 확인하기 위해 블록체인에 저장되는 블록의 구조와 트랜잭션의 데이터는 그림 9와 같이 구성하였다. 저장되는 데이터는 "키-값(Key-Value)"으로 구성된 데이터를 사용하는 블록체인에 저장하기에 적절한 JSON 형태를 이용하였다. 블록의 데이터 중 해시 값은 현재 블록에 저장된 merkleRoot, previousHash을 이용하여 얻을 수 있다. previousHash는 현재 블록 바로 직전 블록의 해시값이다. merkleRoot는 트랜잭션의 각각의 데이터마다 고유의 ID를 사용하여 가장 가까운 트랜잭션 데이터 2개를 한 쌍으로 묶어 합친 뒤 해시값으로 변환하는 과정을 반복하여 마지막에 남는 해시값이다.

그림 10은 데이터에 대한 위변조를 확인하기 위해 실제 블록체인 데이터가 저장되는 JSON 파일을 캡쳐한 그림이다. B-DSS를 이용하여 공유된 데이터를 블록체인에 저장하고 JSON 형태를 이용하여 저장하였

표 2. 기존 데이터 공유기법과 제안하는 기법의 보안성 검증 비교
Table 2. Comparison of security verification between the existing data sharing scheme and B-DSS

Comparison factor	Data Sharing Scheme	B-DSS
Data availability and recovery	Weak (Central server)	Strong (Distributed and save)
Security against external attacks	Weak (Central server)	Strong (Distributed and save)
Security against internal attacks	Weak	Strong
Integrity verification	X	O
Tracking data changes	X	O

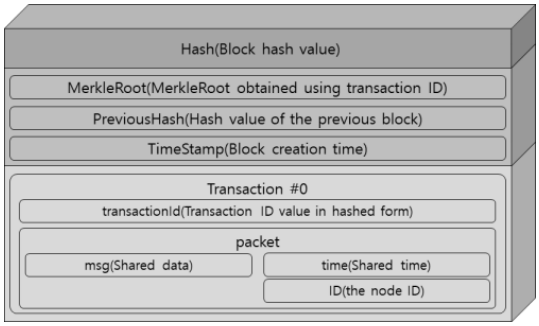


그림 9. JSON 형태의 블록 및 트랜잭션 데이터 구조
Fig. 9. Structure of block and transaction data in JSON format

그림 10. JSON 형태로 저장된 실제 블록체인 데이터
Fig. 10. Blockchain data stored in JSON format

다. 프라이빗 블록체인은 중앙 서버에서 블록의 생성 시점을 설정할 수 있고 날짜가 변경될 때를 기준으로 신규 블록이 생성되도록 하였다. 그림 10의 결과를 보면 첫 번째 제네시스 블록의 해시와 두 번째 블록의 previousHash가 동일하다는 것을 확인할 수 있고 두 번째 블록의 해시와 세 번째 블록의 previousHash가 동일하다는 것을 확인할 수 있으며 블록체인 형태의 저장이 설계된 데이터 구조에 따라 저장이 잘 되었음을 확인할 수 있다. 따라서 기존에 저장된 데이터의 변경이 불가능하며 기존 데이터가 변경된다면 트랜잭션의 ID 값이 변경됨을 알 수 있다. 즉 외부 공격 또는 내부의 악의를 가진 노드들로부터 데이터의 무결성을 보장하여 보안성을 확보할 수 있음을 확인하였다.

V. 결론 및 향후 연구

본 논문에서는 함정 전투 시스템에서 보안성 및 신뢰성을 향상하기 위해 블록체인 기반의 데이터 공유 기법을 제안하였다. B-DSS는 공유하는 데이터를 합의 알고리즘을 사용하여 블록체인에 저장하고 해시값 비교를 통해 기존에 저장된 데이터의 변동에 대한 유무를 확인할 수 있다. 또한, 유효성 검토 알고리즘을 사용하여 블록체인 적용으로 의해 발생할 수 있는 지연을 감소하여 실시간성을 만족할 수 있음을 보였다. 모의실험 결과 기존 합의 알고리즘 대비, 데이터 공유 소요 시간을 감소시켜 실시간성을 확보하였고 블록체인 데이터의 무결성 및 변경 추적을 통해 신뢰성 및 보안성 향상을 기대할 수 있음을 보였다. 또한, 제안하는 기법을 방위산업에 적용하여 신뢰성 및 보안성 개선을 통한 사이버 보안 공격 등의 미래전에 효과적으로 대비할 수 있을 것으로 판단된다.

향후 연구에서는 실제 경항모급 군함에서 운용되는 노드 수를 고려하여 수백, 수천 개의 노드가 포함된 네트워크에서 성능 평가를 진행하고 이에 따른 데이터 병목 현상, 실시간성을 개선하고자 한다.

References

[1] D.-R. Yoo, “North Korea’s cyber threats and countermeasures,” *The J. Strategic Stud.*, vol. 28, no. 3, pp. 7-36, 2021.

[2] J. A. Bullock, G. D. Haddow, and D. P. Coppola, “Chapter 8 - Cybersecurity and critical infrastructure protection,” *Introduction to Homeland Secur.*, pp. 425-497, 2021.

[3] R. W. Ahmad, H. Hasan, I. Yaqoob, K. Salah, R. Jayaraman, and M. Omar, “Blockchain for aerospace and defense: Opportunities and open

research challenges," *Comput. & Ind. Eng.*, vol. 151, pp. 1-14, 2021.

[4] K.-H. Lee and H.-S. Park, "Study on trends and strategies for defense blockchain and ICT technologies," *Electron. and Telecommun. Trends*, vol. 35, no. 1, pp. 12-24, 2020.

[5] J. Dattani and H. Sheth, "Overview of blockchain technology," *Asian J. Convergence in Technol.*, vol. 5, no. 1, pp. 1-3, 2019.

[6] C.-G. Yi and Y.-G. Kim, "A study on software security test of naval ship combat system," *J. KICS*, vol. 45, no. 3, pp. 628-637, 2020.

[7] J.-S. Im and S.-J. Lee, "A survey on decentralized storage," *Commun. KIISE*, vol. 36, no. 6, pp. 30-36, 2018.

[8] J.-H. Cha, J.-W. Lee, J.-M. Lee, and D.-S. Kim, "Real-time middleware application and trend research for civilian and military ICT convergence technology," *J. KICS*, vol. 37, no. 10, pp. 47-54, 2020.

[9] OMG Std., *DDS Security Version 1.1*, OMG, 2018.

[10] J.-W. Lee, J.-H. Cha, J.-W. Lee, G.-S. Kim, and D.-S Kim, "PFDP-Based DDS security lightweight discovery scheme," *J. KICS*, vol. 45, no. 12, pp. 2123-2131, 2020.

[11] H. Guo and X. Yu, "A survey on blockchain technology and its security," *Blockchain: Research and Applications*, pp. 1-23, 2022.

이 종 우 (Jong-Woo Lee)

2018년 2월 : 금오공과대학교 전자 공학과 졸업
2020년 2월 : 금오공과대학교 IT 융복합공학과 석사졸업
2021년 2월~현재 : ㈜비엠텍시스템 연구개발팀 대리
<관심분야> 블록체인, 미들웨어, 실시간 시스템
[ORCID:0000-0002-1978-1877]

김 형 진 (Hyeong-Jin Kim)

2020년 2월 : 금오공과대학교 전자 공학과 졸업
2021년 8월 : 금오공과대학교 IT 융복합공학과 석사졸업
2022년 2월~현재 : ㈜엔에스랩 연구개발 팀장
<관심분야> 블록체인, 미들웨어, 항공기 네트워크
[ORCID:0000-0002-7648-9805]

이 재 민 (Jae-Min Lee)

1997년 2월 : 경북대학교 전자공학과 학사졸업
1999년 2월 : 경북대학교 전자공학과 석사졸업
2005년 3월 : 서울대학교 전기 및 컴퓨터공학부 박사졸업
2004년~2016년 : 삼성전자 수석연구원
2016년~2017년 : 금오공과대학교 ICT융합특성화 연구센터 산학협력중점교수
2017년~현재 : 금오공과대학교 전자공학부 조교수
<관심분야> 산업용 통신망, 네트워크 기반 임베디드 시스템 설계 및 성능분석
[ORCID:0000-0001-6885-5185]

전 태 수 (Tae-Soo Jun)

1998년 2월 : 서울대학교 전기공학부 졸업
2000년 2월 : 서울대학교 전기공학부 석사 졸업
2009년 12월 : University of Texas at Austin, Computer Engineering 박사졸업
2010년 : University of Texas at Austin, 박사후연구원
2000년~2005년 : 삼성SDS 정보기술연구소 선임연구원
2010년~2022년 : 삼성전자 Samsung Research 수석연구원/PL
2022년 3월~현재 : 금오공대 컴퓨터소프트웨어공학과 조교수
<관심분야> 모바일 컴퓨팅, Context-Aware 컴퓨팅, IoT 플랫폼, 실시간 시스템
[ORCID:0000-0002-1435-3769]

김 동 성 (Dong-Seong Kim)

1992년 2월 : 한양대학교 전자공학과 졸업
2003년 3월 : 서울대학교 전기 및 컴퓨터공학부 박사졸업
2004년 : Cornell 대학교 ECE 박사 후 연구원
2004년 3월~현재 : 금오공대 전자공학부 정교수
2015년~2018년 : 금오공과대학교 융합기술원 원장
2014년 6월~현재 : ICT 융합특성화연구센터 센터장(과기정통부 ITRC 및 연구재단 중점연구소)
2019년~2022년 2월 : 금오공과대학교 산학협력단장
2014년 9월~현재 : IEEE/ACM Senior 회원
<관심분야> 실시간 S/W, 실시간 통신망 및 IoT 시스템, 네트워크 기반 분산 제어 시스템
[ORCID:0000-0002-2977-5964]