

TICN에서 데이터 가용성 향상을 위한 블록체인 기술 적용 방안 연구

이종관*, 이민우°

A Study on Application Method of Blockchain Technology to Improve Data Availability in TICN

Jongkwan Lee*, Minwoo Lee°

요 약

본 논문은 전술환경에서 운용되는 전술정보통신네트워크(이하, TICN)의 데이터 가용도를 향상시키기 위해 블록체인 기술을 적용하는 방안을 제시한다. TICN은 기존 전술통신체계에 비해 크게 향상된 전송속도를 제공한다. 하지만 임의의 시간에 데이터의 접근성을 보장하는 능력은 근본적으로 개선되지 않았다. 데이터가 특정 통신소에 집중되어 있을 뿐 아니라, 통신소의 이동 및 열악한 무선 채널 환경에 의한 링크 단절이 빈번하게 발생할 수 있기 때문이다. 따라서 동적인 네트워크 환경에서 데이터 가용성을 보장하기 위한 방안이 필요하다. 블록체인은 분산형 데이터 저장기술로 관리 대상의 데이터를 다수의 노드가 참여하는 합의 과정을 통해 블록으로 생성하고, 각 블록을 해시를 이용한 체인형태로 연결한다. 이를 통해 데이터의 무결성과 가용성을 보장한다. 제안하는 방안에서 TICN의 노드통신소들은 허가형 블록체인 네트워크를 구성한다. 각 통신소는 가입자들로부터 수신한 데이터 중 중요 데이터를 블록으로 생성하고, 블록체인 네트워크에 전파한다. 해시값 확인을 통해 검증된 블록은 기존 블록체인에 연결된다. 제안하는 방안을 TICN에 적용했을 때 데이터 가용도를 수학적으로 분석하여, 제안하는 방안의 효과를 확인하였다.

Key Words : TICN, Blockchain, Distributed Computing, Data Availability, C4I

ABSTRACT

In this paper, we propose applying blockchain technology to improve data availability in tactical information and communication networks (called TICNs) operating in tactical environments. TICN has dramatically improved the data rate of existing tactical networks. However, data availability is hardly improved because the data is concentrated on a specific node and link failures between nodes frequently occur due to poor node movement and wireless channel conditions. Therefore, we need to ensure data availability in dynamic networks such as TICN. Blockchain is a distributed data storage technology that ensures data integrity and availability. We apply blockchain technology to TICN to improve data availability. The nodes of the TICN are configured with an authority blockchain network. Each node generates a block with the required data of the subscriber and broadcasts it to the blockchain network. The identified block is connected to the existing blockchain by checking the hash value. Numerical analysis verifies the effectiveness of the proposed method.

* 이 논문은 한국연구재단(No.NRF2021R111A1A01047914)과 육군사관학교 화랑대연구소의 지원으로 수행되었음

• First Author : Korea Military Academy Department of Computer Science, jklee64@kma.ac.kr, 정희원

° Corresponding Author : Ajou University Department of Military Digital Convergence, iminu@ajou.ac.kr, 종신회원
논문번호 : 202203-041-0-SE, Received March 24, 2022; Revised May 2, 2022; Accepted May 6, 2022

I. 서 론

전술정보통신체계(이하 TICN)는 저속 데이터 전송 및 음성 서비스 중심의 전술통신 기반체계(SPIDER)를 고속 데이터 전송과 데이터 서비스 중심의 기반체제로 발전시켰다.^[1,2] TICN은 통신소간 고속 데이터 링크를 제공하고, 대대급 이하 제대의 이동간 지휘통제(OTM)를 실현하기 위해 전투무선체계를 디지털 무선기로 전환하였다. 또한, All IP 기반의 통신망을 구축함으로써 정보체계의 접근성 및 활용성을 향상시켰다.

한편, TICN은 육군 군단급 이하 제대의 C4I 체계인 ATCIS 운용을 위한 가장 핵심적인 기반체계 역할을 한다. 전장에서 발생하는 전술데이터의 유형 및 크기가 급증하고 이를 신속히 처리하여 상·하급 제대간 실시간 공유하고자 하는 작전운용 측면에서의 필요성은 지속적으로 증대하고 있다. TICN의 향상된 전송속도를 통해 이러한 요구를 일부 충족하고 있다. 하지만 민간 이동통신기술과 유사하게 전장 환경에서의 새로운 서비스의 출현(인공지능, 빅데이터, 블록체인 등)으로 보다 빠른 전송 속도에 대한 요구는 끊임없이 계속될 것이다. 이러한 이유 때문에 전술 네트워크의 전송 속도 향상을 위한 연구개발과 투자는 많은 관심을 받고 있다.

작전운용 측면에서는 고속의 데이터 전송 뿐 아니라 작전 수행 중 언제든지 필요시 데이터에 접근할 수 있는 가용성도 중요한 요구능력이다. TICN 전력화를 통해 전술환경에서의 데이터 전송속도가 크게 향상되었으나 데이터 접근에 대한 가용성은 근본적으로 개선되지 않았다.

일반적으로 ATCIS 서버는 특정 부대통신소에 우선으로 접속되어 있으며 부대통신소와 물리적으로 동일한 지점에 설치된다. 그리고 ATCIS의 생존성 향상을 위해 주서버와 예비 서버를 운용한다. 만약 ATCIS가 접속한 부대통신소가 이동해야 하는 상황이라면 주·예비 ATCIS 서버들은 차례대로 해당 부대가 이동하는 차후 지점으로 이동되어 설치되어야 한다.^[3] 이때, 다소 복잡한 주·예비 서버 전환 절차를 거쳐야 하며 ATCIS 사용자들도 접속해야 하는 서버의 IP 주소 정보를 직접 변경해야 하는 불편함이 발생한다. 뿐만 아니라 ATCIS 서버가 이동 중에는 데이터 접근이 부분적으로 제한될 수밖에 없다. 또한, ATCIS 서버가 접속한 특정 통신소에 트래픽이 집중될 수밖에 없고, ATCIS 서버 파괴 또는 서버에 접근하기 위한 네트워크 경로가 단절되었을 때 필요한 데이터에 접근할 수

있는 대안이 마땅치 않다. 즉, 데이터 가용성이 높지 않다고 할 수 있다. 가용성을 높이기 위한 연구개발 및 투자는 고속 통신을 구현하기 위한 노력에 비해 상대적으로 미흡한 실정이다.

TICN과 같이 서버가 자주 이동해야 하고 데이터가 집중되는 전술 네트워크 환경에서는 블록체인과 같은 분산형 데이터 처리 기술이 필요하다. 하지만 전술 네트워크 환경에 데이터 가용성 향상을 위해 블록체인 기술을 적용하는 연구는 아직까지 많지 않다. 일부 연구를 제외하고 대부분 블록체인 기술의 개념적인 적용방안과 증명되지 않은 기대효과를 제시하는 수준이며, 기술적 구체성이 결여되어 있다. 유인덕 등 5인은 블록체인 기술에 대한 기술적 설명과 더불어 전술 네트워크에서 블록체인 기술을 인증, 무결성 보장, 전술 명령 관리, 권한통제 등에 활용할 수 있음을 제시하였다. 하지만 어떻게 적용해야 하는지에 대한 구체적인 설명은 포함되어 있지 않다.^[4] Yang 등 5인은 합동작전에서 운용되는 다양한 전술데이터링크(TDL)간의 데이터 동기화와 분산된 데이터 전송 통제 시스템 구축을 위해 TDL-Chain을 제안하였다.^[5] TDL-Chain은 블록체인과 스마트 컨트랙트 기능을 이용하여 다양한 전장 요소들간의 정보 동기화를 보장하고 자동화된 데이터 전송을 가능케 하였다. 하지만 가변적인 전장 환경에서의 채널 조건을 고려하지 않아 TICN과 같은 지상통신체계에 적용하는 것은 제한적이다. 본 논문에서는 TICN의 전형적인 네트워크 구조에서 블록체인 기술을 적용하여 전술정보에 대한 접근 가용성을 향상시키는 방안을 제시한다.

본 논문의 구성은 다음과 같다. 2장에서 TICN 구조 및 블록체인 등에 대한 배경지식을 살펴보고 3장에서는 제안하는 블록체인 기술 적용방안을 설명한다. 4장에서는 제안하는 방안을 적용했을 때의 데이터 가용도를 수학적으로 분석한다. 마지막으로 5장에서 결론 및 향후 연구계획을 살펴본다.

II. 배경 지식

본 장에서는 제안하는 방안의 이해를 돕기 위해 TICN의 기본 구조와 블록체인에 대해 간략히 소개한다.

2.1 TICN 구조

그림 1은 TICN의 전형적인 네트워크 구조를 나타낸다. TICN의 중요 장비들은 모두 차량화되어 있어 필요시 이동하여 임의의 지역에서 통신소 개소가 가

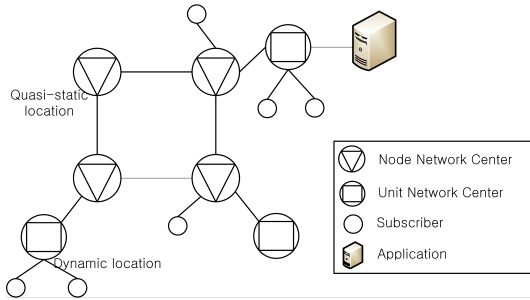


그림 1. TICN 구조 개념도
Fig. 1. Conceptual figure of TICN structure

능하다. 하지만 이동 중에는 정상적인 통신소 운용은 불가능하다.

통신소는 노드통신소와 부대통신소로 구분된다. 노드통신소는 네트워크 생존성을 보장하기 위해 격자 형태의 네트워크를 구성하며 TICN의 백본 역할을 한다. 그리고 노드통신소 인근에 배치된 부대와 전투원에게 통신 기능을 제공한다. 즉, 노드통신소는 특정 부대 중심이 아닌 지역 중심의 통신소라 할 수 있다. 반면 부대통신소는 특정 부대를 직접지원하기 위해 운용되는 통신소이며, ATCIS와 같은 응용체계는 사용자의 접속 편의성을 고려하여 일반적으로 부대통신소에 접속한다. 그리고 부대통신소는 작전수행간 전술 부대의 이동에 따라 함께 이동해야 한다. 이는 부대통신소에 접속해 있는 응용체계들도 연쇄적으로 이동해야 한다는 것을 의미한다. 한편, 지역 중심으로 운용되는 노드통신소는 부대통신소에 비해 이동해야 하는 상황이 상대적으로 적다.

일반 가입자는 노드통신소 또는 부대통신소에 접속하여 운용되는 개체이다. 모든 가입자는 특정 통신소에 있는 응용체계를 통해 데이터에 접속해야 하기 때문에 해당 통신소에 트래픽이 집중될 수 있다. 또한, 응용체계가 접속한 통신소의 기능이 제한되거나 트래픽 경로상의 네트워크 구간이 단절된 경우 해당 체계를 통한 데이터 접근이 불가능하게 된다.

2.2 블록체인 기술

블록체인은 분산형 데이터 저장 기술이라 할 수 있다. 분산된 네트워크 환경에서 관리 대상의 데이터를 다수의 노드가 참여하는 합의 과정을 통해 블록으로 생성하고, 각 블록을 해시를 이용한 체인 형태로 연결하여 각 노드별로 저장함으로써 데이터의 무결성과 가용성을 보장한다.^[5] 블록체인은 기존에 존재하지 않았던 새로운 기술이라기 보다는 이미 보편적으로 활용되고 있는 P2P 네트워크, 합의 알고리즘, 전자서명,

해시 등의 기술들이 적절히 융합된 기술이라 할 수 있다.^[6,7]

블록체인은 크게 공개형과 허가형으로 구분할 수 있다. 두 유형의 근본적인 차이점은 블록체인 네트워크에 참여할 수 있는 권한의 제한 여부이다. 공개형 블록체인은 누구나 블록체인 네트워크에 참여하여 블록생성, 검증 등을 수행할 수 있으나, 허가형 블록체인은 승인된 사용자들만 참여할 수 있다. 전술 네트워크는 기본적으로 승인된 사용자들만 가입할 수 있으므로 전술 네트워크에 적용되는 블록체인의 형태는 허가형이 되어야 한다.

분산된 노드에 동일한 데이터를 안전하게 저장할 수 있게 하는 핵심 기술은 합의 알고리즘이다. 합의 알고리즘은 다수의 참여자가 분산된 환경에서 통일된 의사결정을 하기 위해 사용하는 알고리즘으로, 블록체인에서는 분산된 시스템에 동일한 데이터를 저장하기 위해 사용된다. 공개용 블록체인에는 대표적으로 PoW(Proof of Work), PoS(Proof of Stake), DPoS(Delegated PoS) 등이 사용되며, 허가용 블록체인에는 PBFT(Practical Byzantine Fault Tolerance), Raft 등의 알고리즘이 사용된다.^[8-11] PBFT는 이상 노드가 n 개 있을 때 총 노드의 개수가 $3n+1$ 개 이상이면 정상적인 합의가 가능하다는 것이 수학적으로 증명되었다. Raft가 적용된 각 노드는 3개의 상태(Follower, Candidate, Leader)를 가지며, 최초 Follower로 시작한다. 그리고 Leader로부터 일정시간 동안 사전에 정해진 정보를 수신하지 못하면 Candidate 상태로 전환된다. Candidate 상태에서 리더 선정 절차를 통해 Leader 상태로 전환될 수 있다. Raft는 Leader를 통해 모든 클라이언트의 요청을 처리하며, Follower는 단지 수동적으로 Leader의 요청에 응답만 한다. 클라이언트로부터의 요청을 Leader가 접수하여 Follower들에게 전달하고 이에 대한 응답이 과반수 이상이면 해당 데이터를 각 노드들이 저장하는 방식으로 동작한다.^[12]

III. 블록체인 기술 적용방안

본 장에서는 전술 네트워크 환경에서 데이터의 가용도 향상을 위해 제안하는 방안의 블록체인 네트워크 구성, 블록의 생성, 전파 및 관리, 블록의 구조, 블록체인 노드 추가에 따른 조치 등에 대한 세부사항을 설명한다. 표 1은 본 논문에서 사용되는 주요 기호와 의미를 나타낸다.

표 1. 주요 기호와 의미
Table 1. Notation

Symbol	Meaning
BN_i	i th node of a blockchain network
S_i	Subscribers connected to BN_i
BC_i	Blockchain for BN_i
BC_i^j	BC_j maintained by BN_i
B_i^m	m th block of BC_i
$Seq(BC_i)$	Number of blocks in BC_i
REQ(l, m)	Packet to request from the l th block to the m th block
VAL	Packet to inform that the received block is valid
FIN	Packet to inform that the block is finalized

3.1 블록체인 네트워크 구성

제안하는 방안에서 블록이 유통되는 네트워크는 노드통신소들로만 구성되며 허가형 블록체인이다. 노드통신소는 모두 개별적으로 자신의 블록체인을 유지한다. 해당 블록체인은 블록체인 네트워크를 구성하는 모든 노드통신소와 동일하게 유지한다. 따라서 블록체인 네트워크에 참여하는 노드통신소의 수가 n 개일 때, 각 노드통신소는 n 개의 블록체인을 유지한다.

3.2 블록 생성 및 전파

전술네트워크의 용량이 충분하지 못할 수 있기 때문에 노드통신소 BN_i 는 S_i 로부터 수신한 데이터 중 중요 전술데이터를 선별하여 블록 B_i^m 을 생성한다. 이때, 어떤 전술데이터를 블록체인에 포함할지는 작전 목적, 유형 그리고 가용한 네트워크 용량 등을 종합적으로 고려하여 사전에 정의한다. BN_i 는 B_i^m 을 BC_i 에 추가하고 $Seq(BC_i)$ 와 함께 블록체인 네트워크에 브로드캐스팅한다. 이를 수신한 BN_j 는 $Seq(BC_i)$ 가 $Seq(BC_j^i)$ 와 일치하는지 확인한다. 만약 일치하지 않는다면 REQ(l, m)를 BC_i 에게 전송한다. 이때 l 은 $Seq(BC_j^i) + 1$ 이다. 일치한다면 B_i^m 이 정당한 블록인지를 해시를 통해 검사한다. B_i^m 이 정당한 블록이라면 BC_j^i 에 B_i^m 를 추가하고 BN_i 에게 VAL을 전송한다.

한편, BN_i 가 REQ(l, m)를 수신했다면 BN_j 에게 l 번째 블록부터 m 번째 블록을 전송한다. 한편, BN_j 에

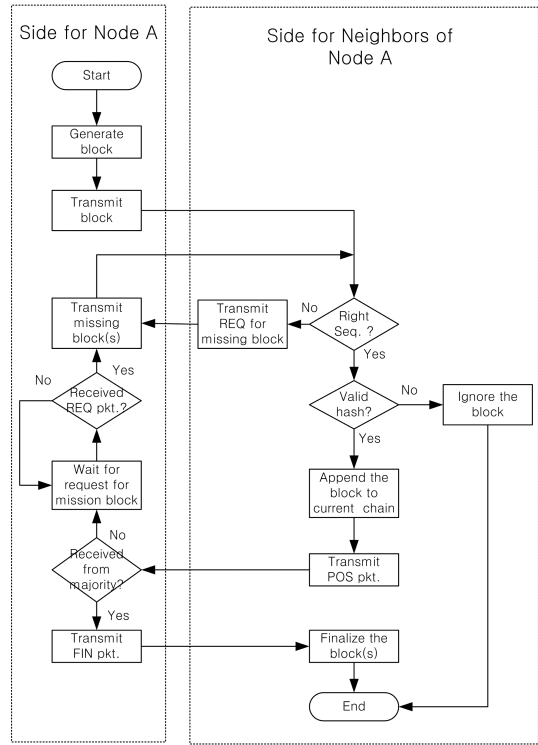


그림 2. 블록 생성 및 전파 절차에 대한 흐름도
Fig. 2. Flowchart for process of block generation and broadcasting

게 과반수 이상의 VAL을 수신했다면 BN_j 에게 FIN을 전송한다. FIN을 수신한 BN_j 는 B_i^m 을 확정한다. 만약 일정 시간 이내에 과반수 이상의 FIN을 수신하지 못했다면 B_i^m 을 다시 브로드캐스팅한다.

그림 2는 블록의 생성, 전파, 검증, 확정되는 과정을 개념적으로 나타낸다.

3.3 블록 및 블록체인 구조

블록체인 BC_i 의 구조는 그림 3과 같다. 첫 번째 블록은 블록체인 네트워크에 참여하기 위한 인증정보, BN_i 의 ID 정보, 블록체인에 대한 구조정보 등의 메타데이터와 공유하고자 하는 전술데이터 그리고 메타데이터와 전술데이터의 해시값으로 구성된다. 두 번째 블록 이후부터는 이전 블록의 해시값, 공유하고자 하는 전술데이터 그리고 이전블록의 해시값과 전술데이터에 대한 해시값으로 구성된다.

블록들은 해시값으로 서로 연결되어 있을 뿐 아니라 해당 블록체인을 모든 노드통신소들이 공유하기 때문에 특정 블록의 전술데이터를 임의로 위·변조하거나, 기존 블록체인을 보유하고 있지 않은 악의적인

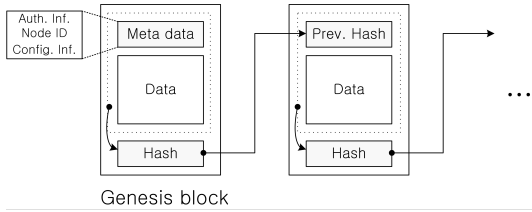


그림 3. 제안하는 방안에서의 블록 구조
Fig. 3. Block structure in proposed scheme

노드가 가져야 할 블록을 기존 블록체인에 추가하는 것이 현실적으로 불가능하다.

3.4 새로운 노드통신소의 추가

전술 네트워크 환경에서는 다양한 이유로 기존 노드통신소가 임무수행이 불가능할 수 있어 새로운 노드통신소가 기존 노드통신소를 대체할 수 있다. 그리고 작전 지역 내에 새로운 전력이 추가 배치됨에 따라 노드통신소가 추가 운용될 수 있다. 이때, 대체되거나 추가된 노드통신소가 블록체인 네트워크에 참여하기 위해서는 기존 노드통신소들이 유지하고 있는 블록체인들을 모두 수신해야 한다. 그런데 블록체인 길이가 매우 긴 경우에는 블록체인을 그대로 수신받는 것은 비효율적이다. 많은 트래픽 발생을 유발할 수 있을 뿐 아니라 과거 전송데이터가 현재 작전수행에 불필요할 수도 있기 때문이다. 따라서, 제안하는 방안에서는 BN_i 가 BC_i 를 그대로 전송하는 것이 아니라, 기존 전송데이터의 요약정보와 가장 최근에 확정된 블록의 해시값이 포함된 블록을 생성하고 이를 전송한다. 이를 통해, 새로운 노드통신소는 보다 신속히 블록체인 네트워크에 참여할 수 있다.

그림 4는 새로운 노드가 블록체인 네트워크에 참여할 때 기존 블록체인을 압축적으로 수신하여 운용하는 개념을 나타낸다.

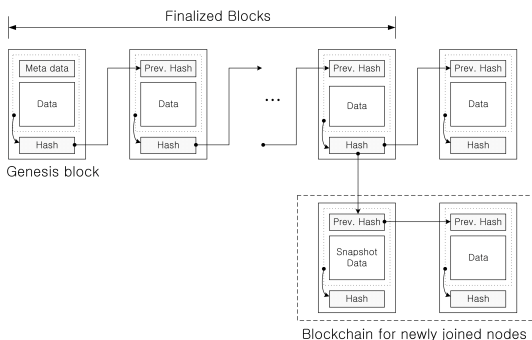


그림 4. 신규 노드통신소의 블록체인
Fig. 4. Blockchain for newly joined nodes

IV. 성능 분석

기존 방안과 제안하는 방안의 근본적인 차이는 기존 방안은 중요 전송데이터에 접근하기 위해 특정 서버에 접속해야 하지만 제안하는 방안은 인근 노드통신소까지만 접속하면 된다는 것이다. 본 장에서는 수학적 분석을 통해 제안하는 방안을 TICN에 적용했을 때 데이터 가용도 측면에서의 성능을 살펴본다.

4.1 성능 지표 및 분석 환경

데이터 가용도는 임의의 시간에 일반 가입자가 전송데이터에 접근할 수 있는 확률로 정의한다. 제안하는 방안이 적용된 경우에는 전송데이터가 모든 노드통신소에 저장되어 있다. 반면 기존 시스템에서는 전송데이터가 특정 부대통신소의 서버에 저장되어 있다.

일반가입자는 서버에 접근하기 위해 여러 링크를 경유해야 한다. 이때, n 번째 링크가 단절될 확률을 p_i 라 하자. TICN 구조의 특징을 고려했을 때 링크 단절 확률은 구간별로 다를 수 있다. 하지만 정확한 단절 확률을 추정하는 것이 쉽지 않고 성능분석의 용이성을 고려하여 구간별 단절 확률을 동일하게 적용한다. 그리고 총 경로를 그림 5와 같이 가입자~노드통신소, 노드통신소~노드통신소, 노드통신소~서버 등 3개 구간으로 구분한다. 각 구간을 각각 가입자 구간, 노드 구간, 서버 구간이라 하자. TICN에서 가입자 구간, 서버 구간은 일반적으로 우회경로가 존재하지 않지만, 노드 구간은 독립적인 우회경로가 존재할 수 있다.

이처럼 본 논문에서는 데이터 가용도를 성능 지표로 삼아, 가입자가 전송데이터에 성공적으로 접근할 수 있는 확률을 각 구간별로 구분하여 성능을 분석한다.

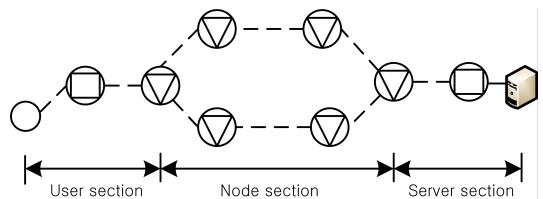


그림 5. TICN에서 데이터 전송 경로의 구간
Fig. 5. Sections of data transmission path in TICN

4.2 분석 결과

4.2.1 사용자 구간

일반사용자가 노드통신소에 직접 접속(Case 1)하거나 부대통신소를 경유하여 접속(Case 2)하는 두 가지 경우를 고려한다. Case 1인 경우에는 사용자 구간에

서 한 개의 링크(부대통신소~노드통신소)만 단절되지 않으면 되지만, Case 2인 경우에는 2개의 링크(사용자~부대통신소, 부대통신소~노드통신소)가 모두 단절되지 않아야 데이터 접근이 가능하다. 따라서 사용자 구간에서 각 Case별로 링크가 단절되지 않을 확률 P_U 는 다음과 같다.

$$P_U = \begin{cases} 1-p_1, & \text{Case 1} \\ (1-p_1) \times (1-p_2), & \text{Case 2} \end{cases} \quad (1)$$

4.2.2 노드 구간

TICN은 생존성 보장을 위해 노드 구간에서 최적경로를 구성한다. 즉, 임의의 두 노드통신소 간에 독립적인 경로가 다수 존재할 수 있다. l -홉 이격되어 있는 노드통신소 사이에 독립적인 경로가 r 개 있다고 가정하자.

l -홉 이격되어 있는 노드통신소 사이의 특정 경로가 단절되지 않을 확률은 다음과 같다.

$$P_r = \prod_{i=1}^l (1-p_i) \quad (2)$$

그런데 노드 구간에는 독립적인 여러 경로가 존재할 수 있다. r 개의 경로가 존재하는 노드 구간에서 모든 링크가 단절되지 않을 확률 P_N 은 다음과 같다.

$$P_N = 1 - \prod_{i=1}^r (1-P_{r,i}) \quad (3)$$

식 (3)에서 $P_{r,i}$ 는 노드구간에서 다수의 독립적인 경로 중 r 번째 경로가 단절되지 않을 확률을 의미한다.

4.2.3 서버 구간

서버는 일반적으로 부대통신소와 유선으로 접속된다. 따라서 서버와 부대통신소간의 링크가 단절될 확률은 0이라고 가정한다. 하지만 부대통신소와 노드통신소는 무선링크이다. 따라서 서버 구간에서의 접속 성공확률은 다음과 같다.

$$P_S = 1 - p_m \quad (4)$$

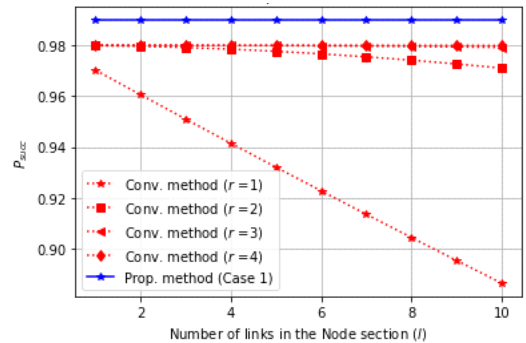
식 (4)에서 p_m 은 서버가 접속되어 있는 부대통신소와 노드통신소 간의 링크가 단절될 확률이다.

최종적으로 가입자로부터 서버까지의 데이터 가용도는 각 구간에서 링크가 단절되지 않을 확률들의 곱

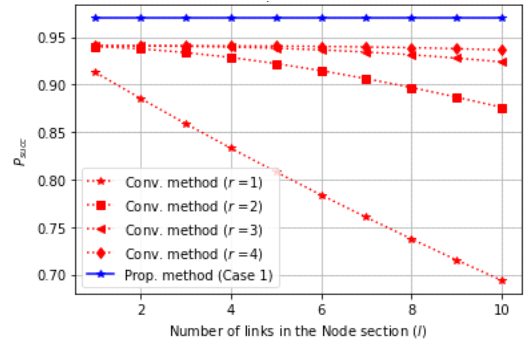
으로 표현된다. 그런데 제안하는 방안은 데이터에 접근하기 위해서 서버가 아니라 인근 노드통신소에만 접속하면 된다. 따라서 기존 시스템의 데이터 가용도 P_{suc}^c 와 제안하는 방안을 적용한 시스템의 데이터 가용도 P_{suc}^p 는 각각 다음과 같다.

$$P_{suc}^c = P_U \times P_N \times P_S \quad (5)$$

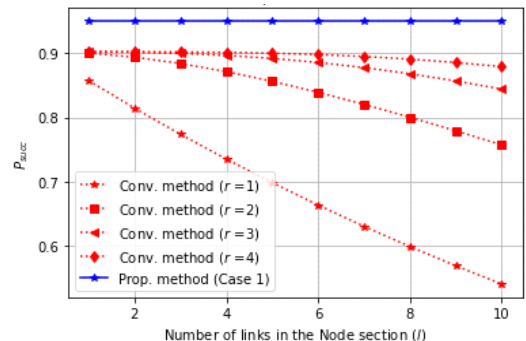
$$P_{suc}^p = P_U \quad (6)$$



(a) Data availability for Case 1 with $p_f=0.01$



(b) Data availability for Case 1 with $p_f=0.03$



(c) Data availability for Case 1 with $p_f=0.05$

그림 6. 기존 시스템과 제안 방안의 데이터 가용도 비교
Fig. 6. Comparison of data availability between proposed method and existing system

식 (5)와 (6)을 통해 제안하는 방안의 접속 성공확률은 기존 시스템보다 항상 높거나 같다는 것을 알 수 있다.

그림 6은 Case 1에서 링크의 수, 링크 단절 확률, 노드 구간에서의 우회경로의 수 등에 따른 데이터 가용도를 나타낸다. 용이한 분석을 위해 각 링크별 단절 확률은 p_j 로 동일하게 설정하였다. 그림 6을 통해 다음과 같은 4가지 사실을 확인할 수 있다.

첫째, 제안하는 방안은 어떤 조건에서도 기존 시스템의 데이터 가용도를 향상시킨다. 이는 식 (5)와 (6)을 통해서도 확인할 수 있다.

둘째, 링크 단절 확률이 클수록 제안하는 방안에 의한 데이터 가용도의 향상 효과가 증대된다. 안정적인 채널 조건을 보장하기 어려운 전술 환경에 적용했을 때 제안하는 방안이 효과적일 수 있다는 것을 의미한다.

셋째, 노드 구간에서 경유해야 하는 노드통신소의 수가 증가할수록 데이터 가용도는 감소한다. 특히 우회경로가 없는 경우(즉, $r=1$)에 데이터 가용도는 급격하게 감소한다. 따라서, 충분한 우회경로 구성이 필요하다. 하지만 전술환경에서 노드통신소가 공유되지 않는 독립적 우회경로를 다수 구성하는 것은 제한적이다. 한편, 제안하는 방안을 적용했을 때는 노드 구간에서의 우회경로 수와 무관하게 데이터 가용도를 일정 수준으로 유지할 수 있다.

한편, Case 2는 Case 1에 사용자 구간에서의 링크만 한 개 추가된 것이기 때문에 Case 2에 대한 결과도 Case 1과 유사한 경향을 나타낸다.

결론적으로 채널 환경이 제한적이고 다수의 우회경로를 구성하는 것이 쉽지 않은 전술환경에서 제안하는 방안을 적용했을 때 데이터 가용도를 효과적으로 증대시킬 수 있다.

V. 결론 및 향후 연구

본 논문은 데이터 가용도를 향상시키기 위해 TICN에 블록체인 기술을 적용하는 방안을 제안하였다. 제안하는 방안은 TICN의 운용 특징을 고려하여 노드통신소들이 블록체인 네트워크를 구성하고 각 노드통신소들이 중요한 전술데이터를 블록으로 생성하여 이웃 노드통신소와 블록체인 형태로 공유함으로써 데이터 가용도를 향상시킨다. 수학적 분석을 통해 TICN에 제안하는 방안을 적용했을 때 데이터 가용도가 크게 향상될 수 있음을 확인하였다. 뿐만 아니라 일반가입자의 트래픽이 특정 서버가 접속한 노드통신소에

집중되지 않기 때문에 노드 구간의 트래픽을 완화시키는 효과를 기대할 수 있다.

한편, 제안하는 방안을 적용하면 블록체인을 유지, 관리하는 기능이 노드통신소에 추가되어야 한다. 또한, 각 노드통신소는 블록을 블록체인 네트워크에 브로드캐스팅하고 블록 검증 및 확정을 위한 제어 패킷을 발생킨다. 즉, 부가적인 트래픽과 오버헤드가 발생한다. 따라서 제안하는 기법을 적용했을 때 데이터 가용도 향상과 트래픽 증가, 오버헤드 등의 상관관계에 대해 향후 연구를 진행할 예정이다.

References

- [1] J. Lee, et al., "Study on development of tactical networks using artificial intelligence technique," *J. KICS*, vol. 45, no. 1, pp. 191-200, 2020.
- [2] T. Woo, J. Seo, and C. Lee, "A study on the tactical echelon network applying a content-centric networking," *J. KICS*, vol. 46, no. 3, pp. 499-507, 2021.
- [3] H.-H. Lee and D.-S. Ko, "A study on improvement of transition speed between main/standby system for ground tactical C4I system(ATCIS)," *J. KIIT*, vol. 17, no. 9, pp. 49-56, 2019.
- [4] I.-D. Yoo, et al., "Blockchain technology and utilization schemes in tactical communication network," *J. KSCI*, vol. 23, no. 12, pp. 49-55, 2018.
- [5] X. Yang, Y. Li, L. Chen, W. Feng, and Z. Yan, "TDL-Chain: An intelligent data transmission control system in tactical data link based on blockchain," in *Proc. 2020 IEEE Blockchain*, pp. 305-312, 2020.
- [6] Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang, "An overview of blockchain technology: Architecture, consensus, and future trends," in *Proc. 2017 IEEE Int. BigData Congress*, pp. 557-564, Honolulu, HI, 2017.
- [7] L. Bahri and S. Girdzijauskas, "Blockchain technology: Practical P2P computing (Tutorial)," in *Proc. 2019 IEEE 4th FASW*, pp. 249-250, 2019.

- [8] S. Pahlajani, A. Kshirsagar, and V. Pachghare, "Survey on private blockchain consensus algorithms," in *Proc. 2019 1st ICICT*, pp. 1-6, 2019.
- [9] S. J. Alsunaidi and F. A. Alhaidari, "A survey of consensus algorithms for blockchain technology," in *Proc. 2019 ICCIS*, pp. 1-6, 2019.
- [10] W. Gu, J. Li, and Z. Tang, "A survey on consensus mechanisms for blockchain technology," in *Proc. 2021 CAIBDA*, pp. 46-49, 2021.
- [11] G.-T. Nguyen and K. Kim, "A survey about consensus algorithms used in blockchain," *JIPS*, vol. 14, no. 1, pp. 101-128, 2018.
- [12] D. Ongaro and J. Ousterhout, "In search of an understandable consensus algorithm (Extended Version)," in *Proc. USENIX ATC 14*, pp. 305-319, 2014.

이 종 관 (Jongkwan Lee)



2000년 2월 : 육군사관학교 전자공학과 학사
2004년 2월 : 한국과학기술원 전기 및 전자공학과 석사
2014년 2월 : 아주대학교 일반대학원 NCW공학과 박사
2017년 12월~현재 : 육군사관학교 컴퓨터과학과 부교수

<관심분야> 인공지능, 사이버전, 전술네트워크
[ORCID:0000-0003-2195-2417]

이 민 우 (Minwoo Lee)



1998년 2월 : 한국항공대학교 항공통신정보공학과 졸업
2013년 2월 : 아주대학교 일반대학원 NCW공학 박사 졸업
2019년 3월 : 아주대학교 국방디지털융합학과 대우교수
<관심분야> 위성통신, 네트워크 보안, 사이버전자전

[ORCID:0000-0001-7109-4700]