한국빅데이터학회지
제8권 제2호, 2023, pp. 141-148 https://doi.org/10.36498/kbigdt.2023.8.2.141

# 안전한 위성-IoT 네트워크를 위한 블록체인 기반 SDN 분산 컨트롤러 구현

## Blockchain based SDN multicontroller framework for Secure Sat_IoT networks

박준범[1] · 박종서[2†]

한국항공대학교 컴퓨터공학과[1], 한국항공대학교 소프트웨어학과[2]

**요 약**

인공위성과 IoT를 연결하는 연구가 활발히 진행됨에 따라 통합된 네트워크를 구축되고, 얻어진 빅데이터들은 다양한 분야에서 활용되고 있다. 하지만 통합 네트워크 생태계는 제한된 대기 시간과 낮은 필요 전력 및 다양한 이기종 장치들의 구성 등으로 인해 심각한 보안 문제를 겪고 있다. 이를 해결하기 위해 SDN(Software Defined Networking)을 활용한 위성-IoT 네트워크를 구축하는 연구가 진행되었다. 하지만 기존 SDN에서 발생하는 보안 문제들이 여전히 존재하기 때문에 본 논문에서는 블록체인 기반 SDN 환경을 구현하여 추가적인 문제점을 해결하고자 한다. 블록체인 기반의 SDN 분산 컨트롤러를 운용하고, 블록체인 인증시스템을 통해 IoT 단말 및 노드들을 검증하도록 구현하였다.

본 논문에서는 우리가 개발한 구현의 계획을 제안하고, 향후 연구로 인공지능과의 융합과 위성-IoT 기기에서 얻을 수 있는 빅데이터들을 활용할 수 있는 방안을 제시한다.

■ 중심어 : 소프트웨어 정의 네트워킹, 블록체인, IoT, 네트워크 보안, 이더리움, 스마트 컨트랙트

**Abstract**

Recent advancements in the integration of satellite technology and the Internet of Things (IoT) have led to the development of a sophisticated network ecosystem, capable of generating and utilizing vast amounts of big data across various sectors. However, this integrated network faces significant security challenges, primarily due to constraints like limited latency, low power requirements, and the incorporation of diverse heterogeneous devices.

Addressing these security concerns, this paper explores the construction of a satellite-IoT network through the application of Software Defined Networking (SDN). While SDN offers numerous benefits, it also inherits certain inherent security vulnerabilities. To mitigate these issues, we propose a novel approach that incorporates blockchain technology within the SDN framework. This blockchain-based SDN environment enhances security through a distributed controller system, which also facilitates the authentication of IoT terminals and nodes.

Our paper details the implementation plan for this system and discusses its validation through a series of tests. Looking forward, we aim to expand our research to include the convergence of artificial intelligence with satellite-IoT devices, exploring new avenues for leveraging the potential of big data in this context.

■ Keyword : Software Defined Networking, Blockchain, IoT, Network Security, Ethereum, Smart Contract

2023년 11월 24일 접수; 2023년 12월 05일 수정본 접수; 2023년 12월 08일 게재 확정.

† 교신저자 (jspark@kau.ac.kr)

## Ⅰ. 서론

현대 통신 및 빅데이터 관리 분야에서 위성 기술과 IoT 기술의 융합과 관련된 다양한 연구들[1]이 진행되고 있다. 특히 인공위성 기기와 IoT 기기에서 얻어지는 많은 데이터를 활용하기 위해 다양한 기술들을 융합하기 위한 연구가 제시되었다. SAR 이미지, 영상, 기후 등에 대한 데이터들을 활용하기 위해 인공지능 기술, 네트워크 기술 등 다양한 분야의 기술들이 위성-IoT에 융합되는 상황이다. 하지만 이러한 융합과 발전에도 불구하고 위성기기와 IoT 장치들이 구성하는 통합 네트워크 생태계에는 많은 어려움이 존재하고 있다. 가장 중요한 어려움 중 한 가지는 시스템의 본질적인 한계로 인해 발생하는 심각한 보안 문제이다. 특히 통합된 네트워크에는 대기시간을 효과적으로 관리해야 하는 필요성, IoT 장치의 저전력 소비에 대한 필수 사항, 수많은 이기종 장치를 통합하는 데 따른 복잡성 등으로 인해 발생하는 새로운 문제점들이 존재한다. 이러한 각각의 문제점들은 통합된 네트워크의 취약성에 기반하여 빅데이터의 무결성과 신뢰성을 무너트릴 수 있다.

이러한 보안 문제를 해결하기 위해 본 논문에서는 위성과 IoT 장치 간 구성되는 통합 네트워크에 Software Defined Networking(SDN)을 적용하는 연구를 진행하였다. 고전적인 네트워크에서는 데이터 플레인과 컨트롤 플레인이 통합된 단일 스위치 또는 기기를 사용하였기에 관리가 어렵고 복잡하였다. 하지만 SDN을 적용하여 데이터 플레인과 컨트롤 플레인을 분리하고, 네트워크를 소프트웨어적으로 관리할 수 있도록 구성하여 네트워크 스위치는 단순한 포워딩 기기가 되고 패킷과 플로우에 대한 컨트롤 로직은 중앙화된 컨트롤러에서 관리하여 네트워크 구성을 단순화하고 관리하기 쉽게 만들었다. 컨트롤러 프로그램을 통해 소프트웨어적으로 네트워크 상태를 파악하고 오작동, 악의적인 공격 등에 대해 자동으로 반응할 수 있는 SDN이지만 여전히 보안 문제점을 가지고 있다. 단일 컨트롤러를 운용하는 경우 컨트롤러가 탈취되는 경우 모든 네트워크 권한을 상실할 수도 있고, DoS 공격 등을 통해 컨트롤러가 공격당하면 네트워크 과부화 및 스위치 권한 상실, 데이터 탈취 등의 문제가 발생할 수 있다.

이러한 SDN에서의 보안 취약점을 해결하기 위해 본 연구에서는 블록체인[2] 기술을 SDN 프레임워크에 통합하는 접근 방식을 도입하였다. 블록체인 기술을 통해 데이터의 무결성과 프라이버시를 보장하고, 통합된 네트워크 안에서의 기기들을 관리하고 데이터를 기록할 수 있도록 하였다. 여기에 추가로 블록체인 기반 SDN 분산 컨트롤러를 구현하여 IoT 단말기와 노드를 검증할 수 있도록 블록체인 기반의 인증, 암호화 과정을 거치도록 하였다. 그리고 컨트롤러들을 하나의 블록체인 노드로 구성시켜 플로우 테이블과 패킷들을 블록체인에 기록하고 악의적인 노드는 참여하지 못하도록 스마트 컨트랙트를 작성하였다.

본 연구에서는 단순히 현재의 위성과 IoT 장치 간의 통합된 네트워크 보안 문제를 해결하고 보안을 강화하는 것에 더하여 이 통합으로 생성되는 방대한 양의 빅데이터를 효과적으로 활용할 수 있는 기반을 마련하는 통합 시스템에 대한 포괄적인 구현 계획을 제안하고자 한다. 위성-IoT 네트워크에서 획득 가능한 빅데이터들은 특정 지역이 아닌 전 세계적으로 넓은 범위에서 수집되는 다양한 데이터들이라는 특징이 있다. 그렇기 때문에 지역적인 중앙집중화된 시스템에서는 관리가 어렵고, 특히 위성통신의 경우 해킹이나 주파수 간섭에 노출될 확률이 높고, 그에 대한 관리가 지상국 통신에 비해 상대적으로 어렵기 때문에 보안 요소를 반드시 고려해야한다. 그래서 본 논문에서는 블록체인 기술을 활용하여 위

성-IoT 네트워크에서 수집된 데이터들의 무결성을 보장하고 모든 기록과 데이터의 투명성을 얻을 수 있었다. 그리고 분산화된 스마트 컨트랙트를 활용하여 위성-IoT 네트워크의 효율적인 관리와 자동화된 운용을 가능하도록 하였다.

나아가서 우리는 이 빅데이터가 인공지능(AI)의 기능과 결합될 때 위성 IoT 장치의 기능과 효율성을 기하급수적으로 향상시킬 수 있을 것이라 생각하고 향후 연구 방향을 제시하였다. 이러한 기술들의 새로운 융합과 적용은 빅데이터 분석 및 응용 분야의 새로운 지평을 열어 다양한 분야에 크게 기여할 수 있는 잠재력을 가지고 있다.

결론적으로, 본 논문은 블록체인 기반의 SDN 분산 컨트롤러를 구축하여 기존 방식과 비교하여 더 안전하고 효율적인 위성-IoT 네트워크를 위한 기반을 마련하는 동시에 향후 연구를 위한 다양한 가능성을 제시한다. 이러한 가능성을 바탕으로 항공우주 및 빅데이터 분야가 다양한 기술들과의 융합을 거쳐 새로운 연구와 기술 개발이 이루어질 수 있도록 향후 연구 진행 방향을 소개하면서 본 논문을 마무리한다.

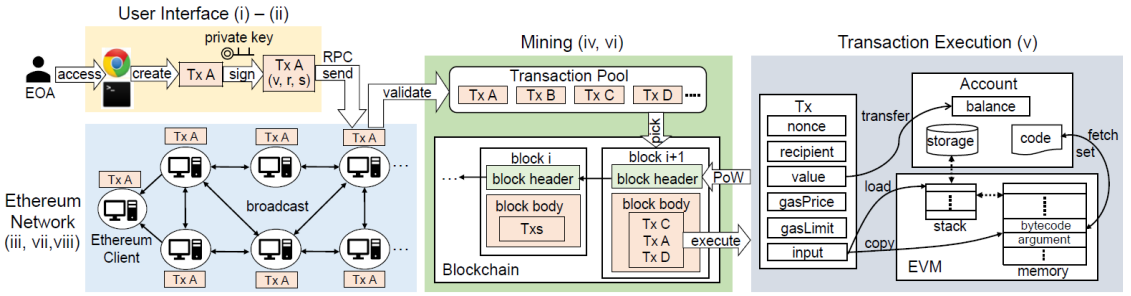
## Ⅱ. 제안 방법

### 2.1 이더리움 블록체인 네트워크

분산원장시스템인 블록체인 기술은 디지털 거래를 기록하고 데이터를 확인하는 시스템으로, 가상화폐와 데이터 저장에 있어 혁신을 가져온 새로운 기술이다. 블록체인 기술은 인증 정보를 저장하고 공유하기 위한 분산화 및 변조 방지 방법을 제공함으로써 분산 인증의 보안 및 효율성을 향상시키는 데 활용될 수 있다. 블록체인 기반 분산 인증시스템에서는 시스템의 각 장치나 컴퓨터가 블록체인의 복사본을 가지며 저장된 인증 정보에 액세스할 수 있습니다. 이를 통해 각 거래가 암호화되고 이전 거래들과 체인처럼 연결되므로 거래에 대한 변조 및 사기에 대해 안전할 수 있다. 그림 1과 같이 이더리움 블록체인[3]의 블록에 거래 기록 및 데이터, 스마트 컨트랙트 코드들이 담기게 된다. 그리고 블록체인의 모든 데이터는 참여하는 모든 노드들과 컴퓨터에 분산되어 있기 때문에 중앙/단일 실패 지점이 없어서 기존 방식보다 안전하다고 할 수 있다. 그리고 여러 종류의 블록체인은 각각 다른 합의 알고리즘을 사용하고 있는데 본 논문에서 채택한 이더리움 블록체인의 PoS 합의 알고리즘은 기존 PoW 방식과 비교하여 효율적인 에너지 활용과 향상된 보안을 보장하고 있다.

PoS 합의 알고리즘에서는 검증인이 새로운 블록을 생성하고 컴퓨팅 능력보다는 보유한 코인 수와 담보로 '스테이킹'하려는 의지를 기반으로 거래를 확인하도록 선택된다. 이 접근 방식은 네트워크 보안에 필요한 계산 작업량을 대폭 줄여 에너지 소비 및 관련 비용을 줄일 수 있다. 위성-IoT 네트워크에 적용되는 많은 기기들은 사용 가능한 최대 전력량이 크지 않기 때문에 네트워크 운용 및 데이터 처리에 관한 전력소모량을 줄여야 효율적으로 네트워크를 운용할 수 있다. 비트코인에서 사용하는 PoW 합의 알고리즘의 경우 한 개의 트랜잭션 처리에 드는 전기량이 약 1,135,000 Wh에 해당하고, 이더리움의 PoS 합의 알고리즘의 경우 약 35 Wh가 소모된다[4]. 그렇기 때문에 위성-IoT 네트워크에서의 PoS 합의 알고리즘은 효율적인 전력 소모의 이점을 가져올 수 있다. 그리고 대표적인 PoW 합의 알고리즘인 비트코인에서는 초당 7개 정도의 트랜잭션 처리가 가능하지만 이더리움의 PoS 알고리즘에선 현재 초당 20개 정도의 트랜잭션 처리가 가능하다[5]. 비트코인은 블록 생성시간이 10분이기 때문에 데이터의 처리가 10분마다 진행되지만 이더리움에서는 약 5초 정도마다 블록에 생성되기 때문에 보다 빠르게 데이터의 전송이 가능하다.

또한 PoS 방식은 네트워크 보안과 탈중앙화를



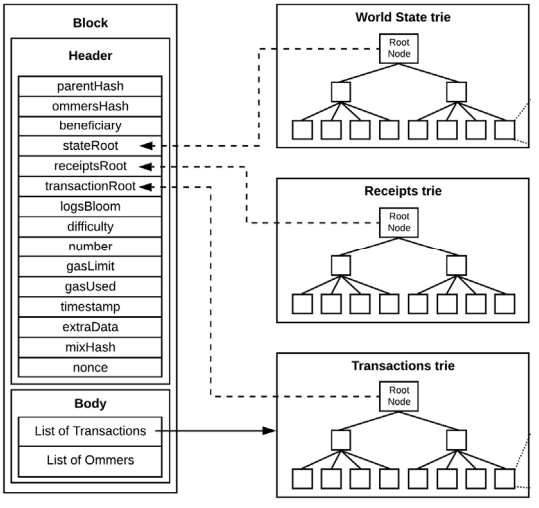

〈그림 1〉 이더리움 트랜잭션 처리 과정

강화한다. 더 큰 검증자 풀에 인센티브를 제공함으로써 보다 분산되고 민주적인 프로세스를 보장하고, PoW 시스템에서 종종 우려되는 중앙화의 위험은 PoS에서 크게 완화된다. 단일 주체가 스테이킹된 토큰의 대부분을 제어하는 것이 실용적이지 않기 때문이다.

기존에 다른 연구들은 SDN에 프라이빗 블록체인을 사용하고 IoT 장치를 인증하거나 네트워크를 구축하는 방향으로 진행되었다. 본 논문에서는 이전 연구와 달리 이더리움 퍼블릭 블록체인을 사용하였다. 퍼블릭 블록체인을 선택하는 주된 이유는 투명성, 분산화, 신뢰성과 같은 블록체인 속성의 이점을 유지하기 위해서이다. 본 논문에서 제안하는 방식은 블록체인을 사용해 데이터를 기록하는 것만이 아니라 연결된 IoT 장치들을 인증하고 검증하는 단계를 거치기 때문에 프라이빗 블록체인을 사용하는 경우 다양한 IoT 기기의 참여가 어려울 수 있어 이더리움 퍼블릭 블록체인을 채택하였다.

IoT 기기들의 경우 다양한 종류의 기기와 여러 위치에 분산되어서 작동하기 때문에 중앙화된 하나의 시스템에서 관리하기는 어려운 점이 있다. 그리고 대부분의 IoT 기기들은 처리능력과 저장공간, 전력소모량이 많거나 크지 않기 때문에 중앙화된 프라이빗 블록체인과 처리량과 전력소모량이 많은 PoW 방식의 퍼블릭 블록체인은 적용하기에 적합하지 않다. 그리고 퍼블릭 블록체인을 사용하여 IoT 기기 자체가 아닌 블록체인 네트워크에서 데이터 처리와 저장이 이루어지기 때문에 제한된 자원을 가진 IoT 기기에서 사용하기에 적합하다.

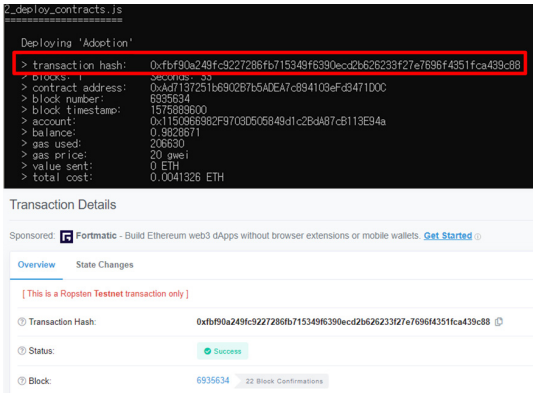
추가적으로 IoT 기기들은 상대적으로 보안 이슈가 많이 발생하기 때문에 블록체인 활용으로 얻는 데이터 무결성, 투명성 확보에서 보안 이점을 가져올 수 있다. 퍼블릭 블록체인을 사용하기 때문에 다양한 노드들이 참여할 수 있고 트랜잭션 처리 및 데이터의 기록이 모든 노드에 분산되어 저장되기 때문에 데이터의 신뢰성과 무결성을 프라이빗 블록체인과 비교하여 더 확보할 수 있었다.




〈그림 2〉 이더리움 블록 구조

본 연구에서는 블록체인 기술을 SDN 컨트롤러에 적용하고, IoT 장치를 인증하는 것에 관련된 솔루션을 제안하였다. 컨트롤러의 패킷 전송, 플로우 테이블 기록 및 IoT 장치 인증 등의 모든 데이터 전달이 그림 2와 같이 블록체인의 트랜잭션과 스마트 컨트랙트를 통해 이루어진다.

따라서 그림 3과 같이 트랜잭션에 비용이 소모되는 블록체인에서는 악의적인 노드들이 DoS, DDoS 공격을 시도하는 것이 거의 불가능하다. 공격을 시도하더라도 블록체인 노드들이 해당 트랜잭션을 탐지하고 처벌할 수 있도록 PoS 합의 알고리즘이 구성되어 있다. 그리고 블록체인에서는 블록을 변경하거나 제거하려면 상당한 양의 컴퓨팅 성능이 필요하고 체인의 블록이 이전 블록과 가지고 있는 암호화 링크로 인해 비용이 매우 많이 들기 때문에 공격에서 얻는 것에 비해 시도하는 비용이 더 크다고 볼 수 있다.




〈그림 3〉 이더리움 블록체인 스마트 컨트랙트

이러한 블록체인 기술을 활용하여 위성-IoT의 통합된 네트워크에 적용하고, SDN 컨트롤러의 연결을 블록체인으로 연동하여 보안적 이점을 가져올 수 있었다.

### 2.2 SDN 분산 컨트롤러

SDN(소프트웨어 정의 네트워킹)[6]은 네트워크 관리 및 아키텍처의 새로운 혁신을 이루어냈다. 기본적으로 SDN은 네트워크 컨트롤 플레인을 데이터 플레인에서 분리한다. 기존에는 두 계층이 네트워크 장치 내에 통합되어있기 때문에 관리가 복잡하고 문제가 발생했을 경우 유연하게 대처하기 어려웠다. SDN에서는 이 플레인을 분리하여 네트워크 리소스를 보다 유연하고 효율적으로 관리할 수 있게 되었다.

SDN의 아키텍처는 세 가지 기본 계층으로 구성된다. 네트워크 서비스와 애플리케이션을 운용하는 애플리케이션 계층, SDN 컨트롤러들 사이의 연결과 스위치로의 명령 전달, 플로우 테이블 관리 등이 포함되는 컨트롤 계층, 제어 계층의 명령에 따라 트래픽을 전달하는 물리적 및 가상 네트워크 장치(예: 스위치 및 라우터)로 구성된 인프라 계층으로 구성된다. 컨트롤러는 애플리케이션 계층의 요구 사항을 데이터 플레인 구성으로 변환하는 역할을 담당하고 있다. SDN 스위치들은 인프라 계층에 속하여 패킷 등의 데이터들이 전송되는 데이터 플레인에 속하게 된다.

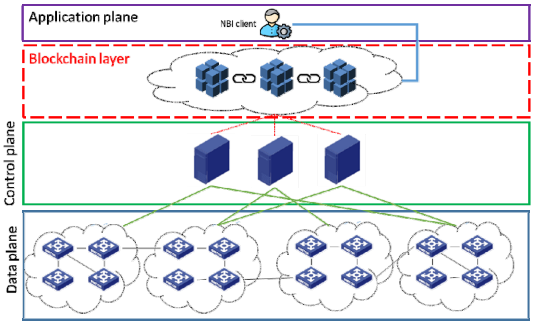
SDN의 가장 큰 장점은 중앙 집중식 제어 메커니즘에 있다. 네트워크 관리자는 중앙 집중식 SDN 컨트롤러에서 네트워크와 트래픽을 형성하여 효율적인 관리와 문제 발생 시 민첩한 대처가 가능해졌다. 특히 기존의 네트워크와 달리 SDN에서는 소프트웨어를 활용하여 전체 네트워크를 관리할 수 있을뿐더러 효율적인 리소스 관리와 모니터링까지 할 수 있어서 비용과 효율 측면에서 커다란 이점을 가져올 수 있다. 하지만 이런 중앙 집중화된 컨트롤러의 보안 문제점이 발생하기 때문에 SDN 연구에서는 멀티 컨트롤러를 운용하는 방향으로 연구들이 진행되었다.

더 크고 복잡한 네트워크 환경에서는 단일 SDN 컨트롤러가 증가된 로드와 복잡성을 처리하기에는 충분하지 않을 수 있다. 이러한 문제로 인해 네트워크의 다양한 세그먼트 또는 계층을 관리하기 위해 여러 컨트롤러를 배포하는 접근 방식인

SDN 다중 컨트롤러라는 개념이 탄생하였다.

SDN 아키텍처의 다중 컨트롤러 접근 방식은 네트워크 확장성과 안정성을 향상시킨다. 여러 컨트롤러에 컨트롤 플레인을 분산함으로써 네트워크는 더 많은 장치와 더 많은 양의 트래픽을 관리할 수 있다. 이렇게 컨트롤러를 분산하여 운용하게 되면 하나의 컨트롤러에 장애가 발생하더라도 다른 컨트롤러가 그 책임을 대신할 수 있어 중단 없는 네트워크 운영이 보장된다. 하지만 SDN 다중 컨트롤러는 여러 컨트롤러에서 일관되고 일관적인 네트워크 정책을 보장하기 위해 신중하게 조정되어야 한다. 그래서 일반적으로 컨트롤러 간의 통일된 데이터 무결성을 위해서는 분산 시스템의 합의 알고리즘을 도입하여 컨트롤러 간의 일관성과 동시성을 유지한다. 다른 많은 연구에서 RAFT, PBFT[7] 등 다양한 합의 알고리즘을 SDN 컨트롤러에 적용하여 분산 컨트롤러를 운용하는 것을 제안하였다. 이렇게 분산 컨트롤러를 운용하게 되면 SDN의 기능이 더욱 향상되어 대규모의 복잡한 네트워크 인프라에 적합한 솔루션이 될 수 있다. 기존의 모든 데이터와 리소스가 단일 개체에 의해 제어되는 중앙 집중식 아키텍처는 보안, 확장성 및 분산화가 부족했기 때문에 블록체인과 같은 분산형 시스템을 적용시켜 여러 개체에 제어권을 분산시켜 더욱 안전하고 확장 가능하며 장애에 대한 복원력을 높일 수 있었다.

하지만 이렇게 기존 방식의 합의 알고리즘과 프라이빗 블록체인으로 구현된 분산 컨트롤러는 여전히 보안 문제점을 가지고 있다. 그리고 위성-IoT 네트워크와 같이 다양한 이기종 기기들과 많은 노드들이 네트워크에 참여하게 되면 프라이빗 블록체인은 유연하게 대처하기 어려운 점이 있다. 그래서 본 논문에서는 멀티 컨트롤러의 합의 방식을 퍼블릭 블록체인 이더리움의 PoS 합의알고리즘으로 채택하였다. 그림 4와 같이 블록체인 기반 SDN 분산 컨트롤러를 설계하여 위성과 IoT 기기 통합 네트워크를 운용할 수 있도록 하였다. SDN을 적용하여 IoT 환경에서의 리소스 관리를 보다 쉽게 할 수 있도록 구성하였고, 소프트웨어를 활용하여 많은 기기들을 효율적으로 관리할 수 있도록 제안한다.



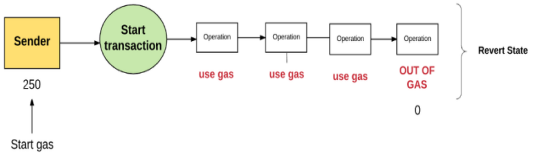

〈그림 4〉 블록체인 기반 SDN 컨트롤러 아키텍쳐

## Ⅲ. 제안방법 분석 및 이점

본 논문에서 제안하는 블록체인 기반 SDN 분산 컨트롤러를 위성-IoT 통합 네트워크에 적용하게 되면 다음과 같은 이점들이 있다.

- 향상된 보안 및 신뢰성: 블록체인 기술의 데이터 무결성과 신뢰성, 투명성은 SDN 아키텍쳐의 보안을 크게 강화한다. SDN 컨트롤러가 관리하는 모든 네트워크 구성의 거래와 변경 사항들이 블록체인에 기록되기 때문에 변조 방지 및 악의적인 노드들의 구분이 가능하게 된다. 특히 컨트롤러 운용에 있어 발생 가능한 보안 문제들을 완화할 수 있다. 시스템 또는 컨트롤러 일부가 오류가 발생하더라도 다른 부분은 영향을 받지 않는다.
- 확장성: 퍼블릭 블록체인 이더리움의 P2P 네트워크를 사용하기 때문에 다양한 이기종 IoT 장치들이 네트워크에 참여하기 쉽고, 관리 또한 간편하다.

- 인증 및 메시지 무결성: 네트워크에 참여하는 노드 및 기기들은 모두 이더리움 블록체인에 속하기 때문에 교환된 모든 트랜잭션은 ECDSA 알고리즘을 사용하여 인증서와 연결된 개인 키를 사용하여 서명된다. 결과적으로 서명은 장치의 신뢰성과 메시지의 무결성을 보호하여 인증 없이는 어떤 장치도 네트워크에 연결할 수 없도록 보장하게 된다.
- DoS/DDoS 보호: 블록체인은 분산형 아키텍처로 인해 DoS/DDoS 사이버 공격에 대응할 수 있다. 블록체인의 데이터가 담긴 블록들은 복사되어 여러 네트워크 노드에 분산되기 때문에 공격자가 하나의 노드를 비활성화하더라도 다른 모든 노드를 비활성화할 수는 없다. 게다가 그림 5와 같이 이더리움 블록체인에서 트랜잭션은 비용이 많이 들기 때문에 공격자가 대량의 트랜잭션을 보내는 것을 막을 수 있다. 사용자가 공격을 위해 트랜잭션으로 요청을 보내어서 소모되는 비용이 공격하여 얻게 되는 비용보다 많기 때문에 공격자들은 블록체인 기반 네트워크에 공격하는 것을 시도하지 않는다. 공격을 시도하는 경우가 발생하더라도 PoS 합의 알고리즘에서 트랜잭션을 검증할 때 악의적인 트랜잭션은 마이너들이 검토하고 삭제시키기 때문에 공격에 대처할 수 있다.




〈그림 5〉 블록체인 gas 소모 시나리오

## Ⅳ. 결론 및 향후 연구

본 논문에서는 통합된 위성-IoT 네트워크의 보안과 효율성을 향상시키기 위한 혁신적인 접근 방식을 제시하였다. SDN 컨트롤러의 운영을 분산시키기 위해 이더리움 블록체인을 활용하는 블록체인 기반 SDN 분산 컨트롤러를 구현하였다. 통합 네트워크에 참여하는 IoT 장치들이 이더리움의 피어로 참여시키고, 블록체인의 인증 시스템 걸쳐 트랜잭션 전송시킬 수 있도록 스마트 컨트랙트를 구현하였다. 그리고 SDN의 플로우 테이블과 패킷을 블록체인 네트워크에 기록함으로써 분산 관리할 수 있도록 설계하였다. 이를 통해 하나의 컨트롤러가 문제에 발생하더라도 다른 분산 컨트롤러가 네트워크 작업을 유지할 수 있도록 보장하여 루트 컨트롤러의 로드를 줄이고 SDN의 탄력성을 보장할 수 있게 되었다. 또한 스마트 컨트랙트를 사용하면 잠재적으로 악의적인 노드의 요청을 효과적으로 관리할 수 있어 DoS/DDoS 공격에 대한 대응을 제공할 수 있었고, 네트워크에서 발생하는 모든 데이터의 기밀성 또한 보장할 수 있었다.

향후 연구로 본 논문에서의 블록체인 기반 SDN 프레임워크를 활용하여 발전 가능한 몇 가지 부분을 제시한다.

먼저 인공지능 기술을 적용하여 네트워크 트래픽을 실시간으로 분석하고 모니터링하여 보안 강화를 할 수 있도록 AI 기반 패킷 분석 프로그램을 구현하는 것이다. 자동화된 실시간 네트워크 관리 및 보안 강화를 위한 AI 기반 패킷 분석 프로그램을 구현하여 현재의 SDN 프레임 워크와 통합하여 운용해야 할 것이다. 이를 통해 네트워크에서 발생 가능한 위협을 탐지하고 대응할 수 있을 것이다.

그리고 위성과 IoT에서 얻을 수 있는 빅데이터를 활용하는 것이다. 특히 SAR, 영상, 위성영상 등과 같은 빅데이터들이 많기 때문에 이를 활용

하는 종합적인 연구가 필수적인데 향후 연구에서 IoT 장치에 Federated Learning을 적용하여 이 광범위한 데이터 풀을 처리하고 학습할 수 있도록 하는 연구가 필요할 것이다.

마지막으로 블록체인 기반 SDN 프레임워크의 보안 문제를 해결하는 것이다. 다양한 연구들이 진행되고 있음에도 SDN 프레임워크 내의 보안 문제는 여전히 발생하고 있다. 향후 작업에는 위성 네트워크에서의 예측할 수 없는 지연 시간과 노드 안정성에 중점을 두고 관련된 공격에 대한 대응을 연구가 진행되어야 할 것이다.

제로데이 공격과 기타 새로운 위협에 대응하기 위한 솔루션을 개발하여 네트워크의 견고성을 보장해야 할 것이다. 결론적으로, 위성-IoT 네트워크의 보안과 효율성을 향상시키기 위해서 패킷 분석을 위한 AI의 통합, 빅데이터의 효과적인 사용, 네트워크 보안 문제해결 연구가 진행된다면 항공우주와 빅데이터 분야의 발전을 이룰 수 있을 것이다.

## 참 고 문 헌


[1] C. Liu, W. Feng, Y. Chen, C.-X. Wang, and N. Ge, “Cell-free satellite-UAV networks for 6G wide-area Internet of Things,” IEEE J. Sel. Areas Commun. 39(4), pp.1116-1131, 2021.

[2] S. Nakamoto, “Bitcoin: A Peer-to-Peer Electronic Cash System”, Oct. 2008.

[3] V. Buterin, “A next-generation smart contract and decentralized application platform”, cryptorating.eu, 2014.

[4] London stock exchange group. Proof-of-Stake: A crypto path to lower energy consumption and yield [online] [17.02.2023].

[5] https://beaconscan.com/

[6] T. Hu, Z. Guo, P. Yi, T. Baker, and J. Lan, “Multi-controller based software-defined networking: A survey,” IEEE Access 6, pp.15980-15996, 2018.

[7] D. Chattaraj, S. Saha, B. Bera and A. K. Das, “On the Design of Blockchain-Based Access Control Scheme for Software Defined Networks,” IEEE INFOCOM 2020 - IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS), Toronto, ON, Canada, 2020.


## 저 자 소 개


**박 준 범(June Beom Park)**

- 2018년: 한국항공대학교 컴퓨터공학과 학사
- 2020년: 한국항공대학교 컴퓨터공학과 석사
- 2020년~현재: 한국항공대학교 컴퓨터공학과 박사과정

<관심분야> 블록체인, SDN, 빅데이터, 정보보안

**박 종 서(Jong Sou Park)**

- 1983년: 한국항공대학교 항공통신공학과 학사
- 1986년: North Carolina State University 전기컴퓨터공학 석사
- 1994년: Pennsylvania State University 컴퓨터공학 박사
- 1996년~현재: 한국항공대학교 소프트웨어학과 교수

<관심분야> 정보보안, 블록체인, 인공지능, 빅데이터