# MANET 환경에서 데이터 무결성 보장을 위한 블록체인 적용에 관한 연구★

양 환 석*, 최 대 수**

## 요 약

MANET은 어떠한 인프라스트럭처의 도움 없이 이동 노드들로 구성되어 hop-by-hop 방식으로 데이터가 전달되는 구조가 블록체인과 매우 유사하다. 하지만 MANET은 이러한 특징 때문에 악의적인 노드에 의한 데이터 변조 또는 폐기 등 다양한 위협에 노출되어 있다. 이러한 이유로 전송 데이터에 대한 무결성 보장은 MANET의 중요한 보요 요소이다. 본 논문에서는 네트워크를 구성하는 노드들에 대한 신뢰도 값을 악의적인 노드들로부터 보호하기 위하여 블록체인 기술을 적용하는 방법을 제안하였다. 이를 위하여 클러스터 형태의 계층 구조를 이용하였으며, 클러스터 헤드만이 노드들의 신뢰도 정보를 블록에 저장하고 이를 전파할 수 있도록 하였다. 또한 잘못된 블록의 전파를 차단하기 위하여 클러스터 헤드 선출에 참여하는 노드들의 수와 클러스터 헤드의 신뢰도를 이용한 블록생성 난이도 자동 설정 기법을 적용하였다. 이렇게 되면 악의적인 노드에 의한 블록 생성 및 전파를 차단할 수 있게 된다. 제안한 기법의 우수한 성능은 SAODV 기법과 비교 실험을 통해 확인할 수 있었다.

# A Study on the Application of Block Chain to Ensure Data Integrity in MANET Environment

Hwanseok Yang*, Daesoo Choi**

## ABSTRACT

MANET transmits data by hop-by-hop method because it is composed of mobile nodes without support of any infrastructure. Its structure is very similar to a block chain. However, it is exposed to various threats such as data tampering or destruction by malicious nodes because of transmission method. So, ensuring the integrity of transmitted data is an important complement to MANET. In this paper, we propose a method to apply the block chain technique in order to protect the reliability value of the nodes consisting the network from malicious nodes. For this, hierarchical structure of a cluster type is used. Only cluster head stores the reliability information of the nodes in a block and then, this can be spread. In addition, we applied block generation difficulty automatic setting technique using the number of nodes selecting cluster head and the reliability of cluster head to prevent the spread of wrong blocks. This can prevent block generation and spread by malicious nodes. The superior performance of the proposed technique can be verified by comparing experiments with the SAODV technique.

Key words : Geographic Information, Multicast Routing, Virtual Group, Mobile Ad-hoc Network

접수일(2018년 11월 29일), 수정일(1차: 2018년 12월 17일), 게재확정일(2018년 12월 30일)

★ 이 성과는 2018년도 정부(과학기술정보통신부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구임(No.2018R1D1A1B07046296)

* 중부대학교 정보보호학과

** 중부대학교 소프트웨어공학부 (교신저자)

# 1. 서 론

MANET에서 무선 매체를 이용한 이동 노드들로만 구성되어 있기 때문에 많은 보안 취약점이 존재한다. 이러한 보안 취약점에 대해 많은 분야에서 연구가 진행되어 왔다[1]. 특히 데이터 전송이 hop-by-hop 방식으로 이루어지기 때문에 전송되는 데이터 무결성 보장에 많은 연구가 진행되어 왔다[2]. 하지만 데이터 전송 경로에 존재하는 노드들의 대한 신뢰 평가 및 정보의 위변조 때문에 많은 문제가 야기되어 신뢰 정보 전달을 위한 보안 기법이 필요한 상황이다[3].

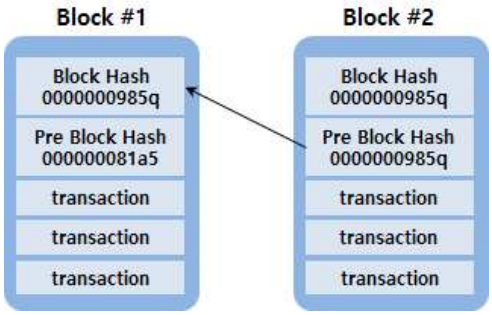
본 논문에서는 중앙의 개입 없이 P2P 형태로 이루어지는 구조인 블록체인이 MANET과 유사한 구조를 갖고 있기 때문에 블록체인 기술의 강점인 신뢰성 보장과 거래 내역들의 무결성을 MANET에 적용하여 보았다. 먼저 블록체인을 MANET에 적용하기 위하여 네트워크는 클러스터 형태의 계층 구조를 이용하였다. 클러스터 헤드가 자신의 클러스터 내의 노드들의 신뢰 정보를 블록에 저장한 후 이웃 클러스터 헤드에게 전파하게 된다. 선출된 클러스터 헤드 중 선출에 참여한 노드가 가장 많은 클러스터 헤드가 genesis 블록을 생성하게 된다. 그리고 잘못된 블록의 전파를 차단하기 위한 기법으로 클러스터 헤드 선출에 참여한 노드들의 수와 선출된 클러스터 헤드의 신뢰도 값을 이용하여 블록생성 난이도 자동 조절 기법을 적용하였다.

본 논문의 구성은 다음과 같다. 2장에서는 블록체인 기술에 대하여 살펴보고 3장에서는 본 논문에서 제안한 블록체인 기반 MANET과 난이도 자동 조절 기법에 대해 기술하였다. 4장에서는 제안한 기법의 성능 평가를 위해 실험하고 마지막으로 5장에서 결론을 맺는다.

# 2. 관련연구

## 2.1 블록체인 기술

블록체인은 블록이라는 분산된 디지털 장부에 그 이력을 저장하여 누구라도 임의로 수정할 수 없고 누구나 변경의 결과를 열람할 수 있는 분산 컴퓨팅 기술로서 탈중앙화된 전자장부에 쓰이기 때문에 개인간의 자유로운 거래가 가능하다[4[5]]. 블록체인의 동작 과정은 크게 5단계로 이루어진다. 첫 번째 단계는 블록체인 네트워크가 미리 정의한 트랜잭션 모델인 트랜잭션 정의이다. 두 번째 단계는 트랜잭션 인증은 노드가 유효성을 검증하는 단계이다. 세 번째 단계는 블록생성 단계로서 생성 시간을 기준으로 트랜잭션 풀에서 노드별로 블록을 생성하는 과정이다. 네 번째 단계인 블록 검증 단계에서는 이전 해시 및 작업 증명을 제공하는 난수가 있는지 확인하여 블록의 유효성을 검사한다. 마지막 블록 체이닝 단계는 모든 노드의 합의가 이루어지면 블록을 블록체인에 추가하는 과정이다[6][7]. (그림 1)은 블록체인의 형태을 보여주고 있다.




(그림 1) 블록체인의 형태

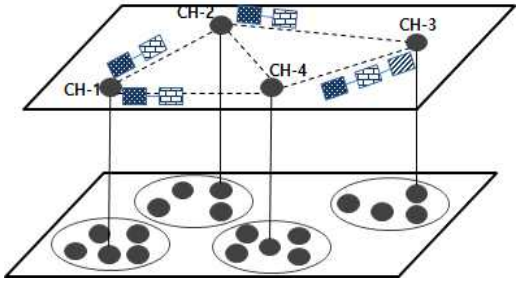
블록체인의 종류는 네트워크 상호작용에 따라 퍼블릭 블록체인과 프라이빗 블록체인으로 구분할 수 있다[8]. 퍼블릭 블록체인은 누구든지 블록 생성에 참여할 수 있으며, 분산합의를 통해 신뢰할 수 있는 블록으로 인정하는 구조이다. 이것은 블록을 공유해야 하는 시간이 많이 소요되고, 분산합의를 위해 작업증명이나 지분증명과 같은 방식이 적용된다[9]. 프라이빗 블록체인은 읽기, 쓰기, 합의 과정에 대한 권한이 미리 정의되어 있으며, 설계자의 의도에 따라 다양한 형태를 설계할 수 있다. 따라서 보안성 면에서도 충분한 가치를 제공한다[10].

# 3. 블록체인 기반 MANET

## 3.1 네트워크 구조

본 장에서는 이동 노드들로만 구성되어 데이터 전송이 hop-by-hop으로 이루어지는 MANET에 네트워크 신뢰도를 높이고 악의적인 노드들에 의한 피해를 줄이기 위한 데이터 무결성 향상을 위하여 블록체인 기법 적용을 설명한다.

본 논문에서 제안한 MANET 환경에서의 무결성 보장을 위한 블록체인 적용은 이를 구현하기 위하여 클러스터 형태의 계층 구조를 적용하였다. 즉, 각 클러스터내의 노드들에 대한 수집된 신뢰 정보를 블록에 저장하여 이를 이웃 클러스터 헤드들에게 배포한다. 본 논문에서는 클러스터 헤드들 간에 신속한 블록 전파를 위하여 프라이빗 블록체인 기법을 적용하였다. 각 클러스터내의 노드들에 대한 신뢰도 측정은 이웃 노드들로부터 수신한 패킷의 양을 기초로 측정하였으며, 해당 패킷이 이웃 노드에 의한 생성 패킷인지 포워딩 패킷인지를 검사하여 이루어진다. (그림 2)는 본 논문에서 제안한 네트워크 구조를 보여주고 있다.




(그림 2) 블록체인 적용을 위한 네트워크 구조

## 3.2 신뢰정보 측정 모델

네트워크내의 노드들에 대한 신뢰 정보 수집의 효율성을 높이기 위하여 클러스터 구조를 이용하였다. 클러스터내의 모든 노드들에 대한 신뢰도 값을 블록에 저장하고 이를 이웃 클러스터 헤드에게 전달하는 역할은 클러스터 헤드가 담당하고, 클러스터내 노드들에 대한 신뢰도 측정은 모든 노드들이 에이전트 역할을 수행하면서 이루어진다. 신뢰도 측정의 신빙성을 높이기 위하여 단순이 전송되는 패킷의 양을 측정하는 것이 아니라 패킷 포워딩의 질을 반영하였다. 신뢰도 측정을 위한 첫 번째 단계는 수신한 패킷의 생성 노드에 대한 판단이다. 즉, 이웃 노드가 생성한 패킷인지 아니면 포워딩하는 패킷인지 IP 헤더를 검사하게 된다. 두 번째 단계는 패킷을 전달한 이웃 노드에 대한 신뢰도를 측정하는 단계이다. 신뢰도 측정은 식 (1)에 의해 이루어진다.

$$i) = w \begin{matrix} F_P_i(N_j) \\ G_P_i(N_j) \end{matrix} \times w_2 \begin{matrix} F_D_i(N_j) \\ G_D_i(N_j) \end{matrix} \qquad (1)$$

여기서 $G_P_i(N_j)$는 노드 $j$에서 생성한 패킷을 노드 $i$에게 전달한 양을 의미하고, $F_P_i(N_j)$는 노드 $j$에서 이웃으로부터 전달받은 패킷을 노드 $i$에게 포워딩하는 것을 의미한다. 그리고 $w_1$과 $w_2$는 노드들이 네트워크에 참여한 시간에 따른 가중치를 나타낸다. 노드들의 이기적인 행동을 차단시키기 위하여 특정 노드에 의해 생성된 데이터와 전달되는 패킷을 신뢰도 계산에 이용하였다. 클러스터 헤드에서는 클러스터내 모든 노드에서 수집된 신뢰 정보를 전달받아 식 (2)에 의해 다시 계산하게 된다.

$$T) = \begin{matrix} n \\ = 0 \end{matrix} \frac{N_i(T)}{n+1} \qquad (2)$$

이렇게 계산된 클러스터내 노드들에 대한 신뢰 정보는 이웃하는 클러스터 헤드에 전달하여 네트워크 전역에 안전하게 전달하여 모든 노드들의 데이터 전송을 위한 경로 설정 과정에서 이를 활용할 수 있도록 블록에 저장한 후 배포하는 단계로 넘어가게 된다.

## 3.3 블록체인을 이용한 신뢰정보 전달

네트워크에 참여하는 모든 노드들이 블록체인을 생성할 수 있는 게 아니고 클러스터 헤드로 선정된 노드들만 블록체인 네트워크에 참여시켜 한정적으

로 탈중앙화를 구현하면서 안정성을 확보하였다. 이전의 단계에서 클러스터내 모든 노드들에 대한 신뢰정보가 수집되고 클러스터 헤드에서 각 노드들에 대한 신뢰도에 대한 계산이 완료되면 해당 정보를 악의적인 노드들에 의한 변조 없이 안전하게 전체 네트워크에 전달될 수 있도록 신뢰 정보를 블록에 저장하게 된다. (그림 3)은 본 논문에서 구현한 블록체인 구조의 모습을 보여주고 있다.

```
class Block:
    def __init__(self, overload, index, data, time,hash_, nonce,bits,
                 trust, merkleroot='2'):
        self.index = index
        self.data = data
        self.time = time
        self.be_hash = hash_
        self.nonce = nonce
        self.bits = bits
        self.trust = trust # Node 신뢰 정보
        self.merkleroot = merkleroot
        self.wal_pas="dkdl"+str(index)
        self.money=100 * (self.index+1)
        sha = hashlib.sha256((str(self.wal_pas)).encode('utf-8'))
        self.wal_pas=sha.hexdigest()
        sha = hashlib.sha256()
        sha.update(str(self.index).encode('utf-8') +
                   str(self.time).encode('utf-8') +
                   str(self.data).encode('utf-8') +
                   str(self.be_hash).encode('utf-8'))
        self.my_hash = sha.hexdigest()
        sha = hashlib.sha256((str(self.wal_pas)+"3").encode('utf-8'))
        self.wal_addr = sha.hexdigest()
```

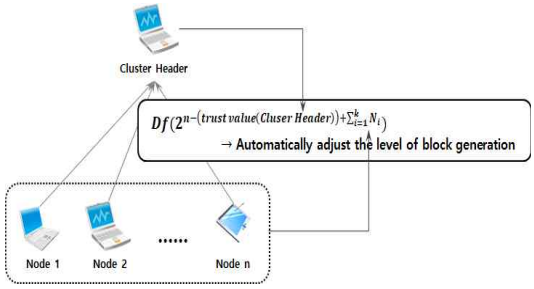
(그림 3) 신뢰 정보를 담은 블록체인 구조

(그림 3)에서 보여준 블록 구조로 네트워크 초기 구성시 선출된 클러스터 헤드 중 링크 값이 가장 높은 노드가 genesis 블록을 생성하게 된다. 그 이후 각 클러스터 헤드는 신뢰도 정보가 수집이 되면 블록에 각 노드들의 신뢰 정보를 담아 블록을 전파하게 된다. (그림 4)는 클러스터 헤드들에 의해서 블록체인이 전파되는 과정을 보여주고 있다.

| | |
|---|---|
| Step 1 | Select nodes in the cluster heads to generate the Genesis Block after broadcasting their own link values |
| Step 2 | Generated and distributed Genesis Block |
| Step 3 | Measure the reliability values of the cluster nodes and store them in a block |
| Step 4 | Use the reliability value of the block received as the weight when setting the path |

(그림 4) 블록체인 생성 및 전달 과정

이렇게 블록체인을 통해 노드들에 대한 신뢰도가 전송된다면 악의적인 노드들에 의해 위변조는 쉽게 이루어질 수 없게 된다. 하지만 악의적인 노드들에 의해 잘못된 블록이 생성되고 전파가 된다면 노드들의 신뢰도 평가는 의미가 없게 되고, MANET은 커다란 혼란에 빠질 수밖에 없다. 이는 블록을 생성할 수 있는 클러스터 헤드가 악의적인 정보를 블록에 삽입하여 전파하게 되는 것을 차단하기 위해서 난이도 자동 설정 블록 생성 기법을 적용하였다. 이를 위해서 블록을 생성하는 클러스터 헤드 노드를 선출에 참여하는 노드들의 수, 즉 클러스터내의 노드들의 수와 클러스터 헤드 노드의 신뢰도 값을 반영하여 일의 증명 난이도가 자동으로 조절되게 하였다. 이렇게 된다면 신뢰도가 높은 노드들로부터 지지를 받고 신뢰도가 높은 노드일수록 난이도 값이 작게 되어 블록 생성 속도가 높아지기 때문에 잘못된 블록 전파를 차단할 수 있게 된다. (그림 5)는 블록생성 난이도 자동 조절 방법을 보여주고 있다.




(그림 5) 블록생성 난이도 자동 조절

## 4. 실험 및 결과

### 4.1 실험 환경

본 장에서는 MANET 환경에서 데이터 무결성 보장을 위한 블록체인 적용 기법의 성능을 평가하기 위하여 다음과 같은 환경에서 실험하였다. 가상화 환경에서 네트워크를 구축하였으며, 블록체인은 파이썬 언어로 구현하였다. 실험에 사용한 PC는 CPU I7-8700K, 메모리 16GB이며, VMware 가상

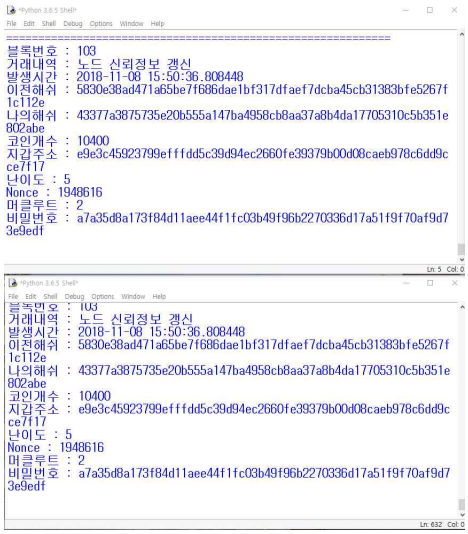
화 프로그램을 이용하였다. <표 1>은 MANET 구성 실험에 사용한 환경변수를 보여주고 있다.

<표 1> 환경 변수 값

| Parameter | Values |
|---|---|
| Number of Nodes | 50개 |
| MAC Protocol | IEEE 802.11 DCF |
| Traffic | CBR |
| Transmission range | 200m |

### 4.2 실험 결과 분석

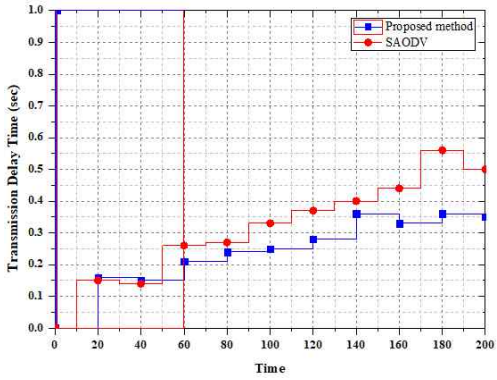
MANET을 구성하는 노드들의 신뢰 정보를 저장하는 블록 생성 및 배포의 정상 동작여부를 측정하였으며, 블록체인 기반 신뢰도 공유를 통한 원활한 라우팅 성능 평가를 위해 SAODV와 비교 실험하였으며, 실험시간 동안 10번의 Jellyfish 공격을 발생하였다.




(그림 6) 신뢰도 저장 블록체인 생성 과정

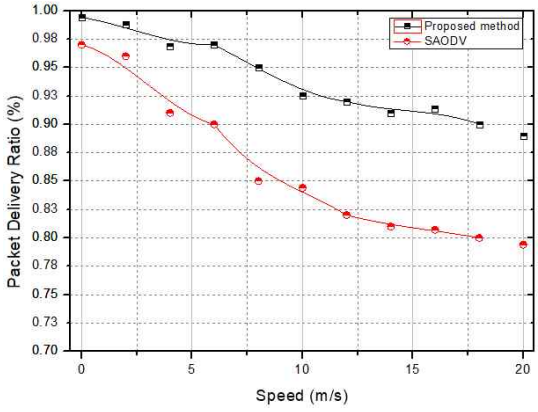
(그림 6)에서는 노드들의 신뢰 정보를 저장하고 있는 블록체인의 생성 및 각 노드에서 수신한 블록의 정보 출력 모습을 보여주고 있다. 그림에서 보듯이 노드들의 신뢰정보를 수정한 블록의 생성 및 배포가 정상적으로 이루어짐을 확인할 수 있었다.

(그림 7)은 노드들 사이의 전송 지연시간의 측정 결과를 보여주고 있다. SAODV 기법은 TTL과 전자서명을 이용한 경로 설정 때문에 공격 발생시 지연시간이 길게 나타나는 결과를 보였으며, 제안한 기법은 블록체인에 의한 안전하게 전달된 신뢰 정보를 기반으로 라우팅을 설정하기 때문에 공격에 의한 지연시간이 크게 늘지 않는 것을 확인할 수 있었다.




(그림 7) 전송 지연시간

SAODV 기법은 RREQ와 RREP에 대한 인증을 통해 경로 설정을 수행하고 그 이후에는 특별한 보안 기법이 적용되지 않아 경로 설정이후에 공격이 이루어지는 Jellyfish 공격에는 성능이 좋지 않았으며, 제안한 기법에서는 경로 설정시 노드들의 신뢰도를 가중치로 활용하기 때문에 공격 발생시에도 우수한 실험 결과를 보여주었다.




(그림 8) 패킷 전달 비율

## 5. 결 론

본 논문에서는 중앙 집중 관리가 아니면서 어떠한 인프라의 도움 없이 P2P 형태로 동작하는 블록체인 기술을 MANET에 적용하여 데이터의 무결성을 향상시키기 위한 기법을 제안하였다. 제안한 기법은 노드들의 신뢰도를 측정하고 이 정보를 블록에 담아 네트워크 전체 노드들에게 배포한다. 노드들 간의 경로 설정시 이렇게 배포된 블록체인의 신뢰도 정보를 이용하게 된다. 즉, 블록체인 담긴 신뢰 정보는 악의적인 노드들에 의해 수정이 불가능하기 때문에 신뢰도가 낮은 노드들은 네트워크에서 배제될 수밖에 없기 때문에 신뢰성을 높일 수 있었다. 그리고 잘못된 블록의 생성 및 배포를 차단하기 위하여 일의 증명 자동 난이도 조절 기법을 적용하였다. 즉, 블록을 생성하는 클러스터 헤드 노드를 선출에 참여하는 노드들의 수와 클러스터 헤드 노드의 신뢰도 값을 반영하여 일의 증명 난이도가 자동으로 조절되게 하였다. 이와같이 블록체인 기술을 MANET에 적용함으로써 전송되는 데이터의 무결성을 향상시킬 수 있는 결과를 얻을 수 있었으며, 실험을 통해 그 결과를 확인할 수 있었다.

## 참고문헌


[1] Kashihara S, H. T., “Data delivery method based on neighbor nodes information in a mobile ad hoc network,” The Scientific World Journal, pp. 1-13, 2012.

[2] Biradar RC, M. S., “Ring mesh based multicast routing scheme in MANET using bandwidth delay product,” Wireless Personal Communication, pp. 117-146, 2012.

[3] Han-Chao Lee, Shin-Ming Cheng, Kuo-Ping Wu, “A responsive probing approach to detect dynamic intrusion in a MANET,” IEEE, Vol. 3, No. 2, pp. 243 - 259, 2016.

[4] Satoshi Nakamoto, “Bitcoin: A Peer-to-Peer Electronic Cash System”, 2008.

[5] FROYSTAD, P. HOLM, Jarle., “Blockchain: powering the internet of value,” EVRY Labs, 2016.

[6] THAKUR, Mukesh, et al., “Authentication, Authorization and Accounting with Ethereum Blockchain,” 2017.

[7] 유헌우, “블록체인 방식의 전자투표 시스템 구현 및 성능 개선 방안 연구”, 아주대학교 석사학위 논문, 2016.

[8] Huh, Seyoung; Cho, Sangrae; Kim, Soohyung. Managing IoT devices using blockchain platform. In: Advanced Communication Technology (ICACT), 2017 19th International Conference on. IEEE, p. 464-467, 2017.

[9] 이수환, “oneM2M 아키텍처에서 강화된 보안 서비스를 위한 Blockchain 기술”, 한국통신학회, 2016.

[10] Brooklyn, NY:Apress, "Introducing Ethereum and Solidity : foundations of cryptocurrency and blockchain programming for beginners", 2017.


〔저 자 소 개〕

양 환 석 (Hwan-seok Yang)
1998년 2월 조선대학교 이학석사
2005년 2월 조선대학교 이학박사
2007년 3월 호원대학교 연구교수
2011년 9월 ~ 현재 중부대학교 정보보호학과 부교수
email : yanghs@joongbu.ac.kr

최 대 수(Dae-Soo Choi)
2001년 2월 고려대학교 문학사
2011년 8월 서강대학교 경제학석사
2018년 8월 동국대학교 기술창업학박사
2014년 4월 ~ 현재 중부대학교 소프트웨어공학부 조교수
email : daesooc100@gmail.com