https://doi.org/10.33778/kcsa.2019.19.3.013

MANET에서 계층적 구조와 블록체인 기반 노드 인증 기법에 관한 연구★

양 환 석*

요 약

MANET은 무선을 이용한 이동 노드들로만 구성되어 있기 때문에 많은 보안 취약점이 존재한다. 특히 네트워크에 참여하는 노드들에 대한 정확한 신뢰도 측정 및 인증을 통해서 악의적인 노드들의 참여를 배제하는 것은 네트워크 성능을 좌우하는 매우 중요한 요소이다. 본 논문에서는 네트워크에 참여하는 노드들에 대한 인증 정보의 위변조를 차단하기 위하여 블록체인 기술을 적용한 기법을 제안하였다. 노드들에 대한 인증의 효율성을 높이고 블록 생성 및 교환 프로토콜의 최적 기법을 적용하기 위하여 영역기반 계층 구조를 적용하였다. 또한 블록에 노드들에 대한 인증 정보를 추가하기 위하여 4개의 데이터 payload를 블록 헤더에 추가하였다. 이동 노드들 간의 hop-by-hop 데이터 전달 방식에 블록체인 기법을 적용해 신뢰성을 높이기 위하여 트랜잭션 생성, 블록 패키징, 검증 과정을 거치는 블록체인 교환 프로토콜을 구현하였다. 이러한 과정을 통해 노드들에 대한 인증 정보의 신뢰성을 높일 수 있게 되었다. 제안한 기법의 성능을 평가하기 위하여 기존의 기법들과 비교 실험하였으며, 실험 결과를 통해 우수한 성능을 확인할 수 있었다.

A Study on Hierarchical Structure and Blockchain-based Node Authentication Mechanism in MANET

Hwanseok Yang*

ABSTRACT

MANET has many security vulnerabilities because it consists of only mobile nodes using wireless. In particular, it is a very important factor determining network performance that excludes the participation of malicious nodes through accurate reliability measurements and authentication of nodes participating in the network. In this paper, we proposed a technique applied with blockchain technology in order to prevent forgery of authentication information for nodes participating in the network. And, an area-based hierarchical structure was applied to increase the efficiency of authentication for nodes and apply the optimal technique of block generation and exchange protocol. In addition, four data payloads were added to the block header in order to add authentication information for nodes in block. To improve the reliability by applying the blockchain technique to the hop-by-hop data transfer method between mobile nodes, blockchain exchange protocol through transaction creation, block packaging and verification processes were implemented. We performed the comparative experiment with the existing methods to evaluate the performance of the proposed method and confirmed the excellent performance by the experiment results.

Key-words: Authentication Technique, Block chain, Region-based Architecture, Mobile Ad-hoc Networ

접수일(2019년 8월 29일), 게재확정일(2019년 9월 21일)

★ 이 논문은 2019년도 정부(교육부)의 재원으로 한국연구재단의 지원을 받아 수행된 기초연구사업임 (No.NRF-2018R1D1A1B07046296)

* 중부대학교 정보보호학과

1. 서 론

MANET은 고정된 인프라 없이 이동 노드로만 구성되어 있기 때문에 무선 전송 범위내의 노드들끼리 hop-by-hop 방식으로 데이터를 전달하는 구조이다[1][2]. 만약 네트워크 전송에 악의적인 노드가 참여하게 된다면 전송되는 데이터에 무결성을 보장하기 어렵고 네트워크 성능에 많은 영향을 끼치게 된다. 또한 노드들의 이동으로 인해 야기되는 동적인 토폴로지는 경로 설정의 어려움과 다양한 공격에 노출되는 원인을 제공하게 된다[3][4]. 따라서 네트워크에 참여하는 노드들에 대한 정확한 인증을 통해 악의적인 노드들에 대한 참여를 배제시키게 된다면 네트워크 신뢰성 및 성능을 향상시킬 수 있게 된다[5].

본 논문에서는 노드들의 효율적 인증을 위해 영역기반의 계층구조와 블록체인 기반 인증 기법을 제안하였다. 전체 네트워크를 일정한 크기의 영역으로 분할한 후 영역내 신뢰도가 높은 노드를 영역 인증노드(RCA, Region Certificate Authority)로 지정하고 영역 인증노드 중에서 최상위 인증노드(TCA : Top Certificate Authority)를 선출하게 된다. 먼저 RCA 노드는 TCA 노드에게 그룹키를 발급받고 RCA 노드는 영역내 멤버 노드들에게 이를 이용한 멤버키를 발급해준다. 해당 키를 발급받은 노드들만에 데이터 전송에 참여할 수 있게 된다. 그리고 노드들에 대한 인증 정보를 블록에 저장하기 위해 인증과 관련된 4개의 데이터 payload를 블록 헤더에 추가할 수 있는 구조를 적용하였다. 인증 정보를 저장한 최신 블록을 생성하고 배포하기 위하여 트랜잭션 생성, 블록 패키징, 검증의 과정을 거쳐 블록 체인을 생성하였다. 트랜잭션 생성, 블록체인 생성 및 검증을 위해 RCA 노드와 TCA 노드가 여기에 참여한다.

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

2. 관련 연구

2.1 블록체인

블록체인은 2008년 사토시 나카모토에 의해 등장했으며, 비트코인의 성공에서 비롯됐다[6]. 블록은 블록체인의 기본단위로서 일정한 시간동안에 발생한 거래 내역을 저장해 놓은 데이터베이스를 말한다. 블록은 블록헤더, 거래건수, 거래내역들에 대한 전체 크기를 나타내는 블록크기(4byte)와 이전 블록의 해시 값, 거래내역의 머클루트 등 총 6개의 정보로 구성되어 있는 헤더(80byte), 블록에 포함되어 있는 거래내역의 전체 건수를 의미하는 거래 건수(1~9 byte), 실제 발생한 거래정보인 거래내역으로 구성되어 있다. 블록체인은 거래 내역을 암호화한 뒤 네트워크 참여자간 공유를 통해 위변조를 차단함으로써 보안성과 신뢰성을 보장한다. 특히 제3자의 개입 없이 개인이나 기관 간 직접 거래가 가능하여 탈중앙화가 블록체인 기술의 대표적인 장점이라 할 수 있다[7].

2.2 블록체인 기술

블록체인은 새롭게 개발된 기술이 아닌 기존의 해시(Hash), 디지털 서명(Digital Signature), 작업증명(Proof-of-work), 피어투피어 네트워크(Peer-to-Peer Network) 기술들을 종합하여 만든 기술이라고 할 수 있다[8][9]. 먼저 해시(Hash)는 어떤 길이의 데이터라도 일정한 크기의 문자열로 매핑 시키는 기술로 해시값만 가지고는 원래의 데이터를 알 수 없기 때문에 암호화에 사용된다. 각 블록들은 2가지 해시값을 갖는데, 트랜잭션을 해시로 만들어 트리 형태로 구성한 머클트리와 작업 증명 과정에서 발견한 조건에 맞는 값인 블록 자체에 대한 해시값이 있다.

블록체인에서 디지털 서명은 트랜잭션의 송수신자를 확인하고 위변조 검증을 위해 사용한다. 송신자가 비밀키로 서명하고 수신자는 송신자의 공개키로 검증하는 방식이다. 작업 증명은 블록이 네트워크에 전파되는 과정에서 생기는 지연과 미도달, 악의적인 사용자의 위변조를 방어하기 위해 사용

된다. 블록이 생성되면 체인에 등록하기 위해 네트워크에 전파시키는데 그 과정에서 같은 시간에 생성된 다른 블록에 의해 체인에 분기가 생기는 경우가 발생하며 이를 포크(Fork)라 한다. 이를 해결하기 위해 합의 알고리즘을 이용한다[10].

3. 블록체인 기반 MANET

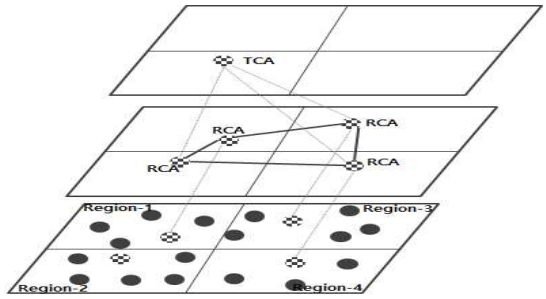
3.1 네트워크 구조

본 장에서는 MANET을 구성하는 이동 노드들에 대해 계층적 구조와 블록체인을 기반으로 한 인증 기법을 적용함으로써 네트워크의 신뢰성을 향상시킬 수 있는 방법에 대해 설명한다.

본 논문에서는 노드들에 대한 효율적 인증과 블록체인 생성시 안정된 합의를 진행하기 위해 영역기반 계층 구조를 적용하였다. 네트워크를 구성하는 노드들은 크게 최상위 인증노드(TCA : Top Certificate Authority), 영역 인증노드(RCA, Region Certificate Authority), 멤버 노드로 구성된다. 최초 네크워크 구성시 TCA와 RCA는 악의적인 노드가 아니라는 가정 하에 임의로 지정하였다.

먼저, 네트워크 구성이 시작되면 전체 네트워크를 일정한 영역으로 분할한 후, 각 영역내에서 인증 노드의 역할을 담당하는 영역인증노드(RCA, Region Certificate Authority)를 선출한다. RCA 노드의 역할을 크게 두 가지로 나눌 수 있다.

먼저 첫째는 영역내 멤버 노드들에 대한 신뢰도 측정 및 인증을 수행한다. 둘째는 노드들의 인증 정보에 대한 트랜잭션 생성 및 블록체인 생성을 위한 합의에 참여하는 역할을 담당한다. TCA 노드의 역할은 RCA 노드로부터 수집한 트랜잭션들에 대하여 블록 패키징(Block Packaging) 과정을 통해 최신 블록을 생성하는 역할과 합의를 거쳐 검증이 완료된 블록을 배포하는 역할을 수행한다. (그림 1)은 본 논문에서 작용한 영역기반 계층 구조를 보여주고 있다.



(그림 1) 영역기반 네트워크 구조

3.2 노드 인증 기법 및 절차

네트워크에 참여하는 노드들에 대한 신뢰도 검사 및 인증을 위하여 영역기반 네트워크 구조를 이용하였다. 각 영역마다 멤버 노드들의 신뢰도 검사 및 인증을 위해 RCA 노드를 지정한다. 최초에만 임의의 노드로 지정되고 그 이후부터는 노드들에 이동에 따라 새롭게 지정되어야 할 경우 영역내 가장 높은 신뢰도를 갖는 노드가 선출된다. 선출되는 과정은 다음과 같다.

1단계 : 노드들은 자신들의 신뢰도를 영역내 모든 노드들에게 방송한다.

2단계 : 신뢰도가 가장 높은 노드가 자신의 상태를 멤버 노드에서 RCA 노드로 변경한 후 TCA 노드에게 전달한다.

3단계 : TCA 노드로부터 승인을 얻은 후 이웃 RCA 노드들의 정보를 수신 받는다.

4단계 : 이웃 RCA 노드들에게 자신의 정보를 송신한다.

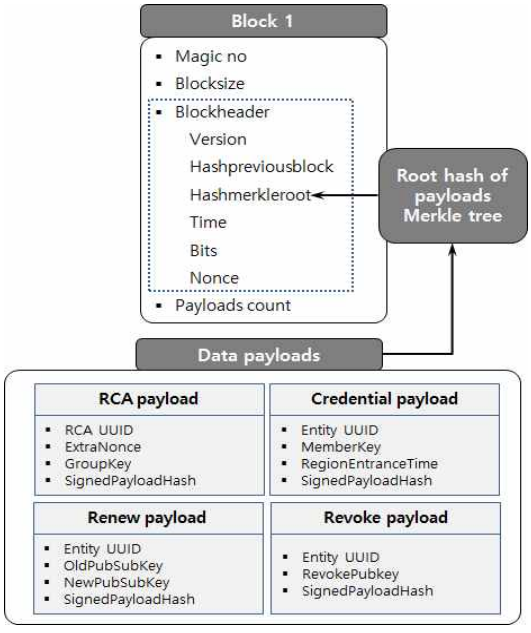
위와 같은 단계를 거쳐 선출된 RCA 노드는 자신의 영역내의 노드들에 대한 인증 과정을 거쳐 영역 그룹 멤버 키를 발급해준다. 멤버 노드에게 그룹 맴버 키를 발급해주는 과정은 다음과 같다.

RCA 노드는 TCA 노드에게 암호키쌍 $(ub_{CA}, GK_{RCA1}), P_{RCA1})$을 생성하여 그룹키 발급을 요청한다. 그룹키 요청을 수신한 TCA 노드는 RCA 노드의 신원을 확인한 후 해당 영역에서 사용될 그룹키$(GK_{RCA1}(H(M), k))$을 생성한 후

RCA 노드에게 전달한다. 그룹키를 수신한 RCA 노드는 영역내 멤버 노드에게 그룹키를 이용하여 멤버키 $K_{CA\ \ N}$)를 발급하게 된다. 이렇게 멤버 키를 발급 받은 노드들은 이를 이용하여 데이터를 암호화($GK_{RCA1}(MK_{RCA1\ \ N_i}(DATA))$)한 후 전송하기 때문에 악의적인 노드들에 의한 데이터 위변조 공격에 강건한 성능을 갖출 수 있으며, 인증을 받지 못한 노드들은 데이터 전송에서 배제될 수 있어 네트워크 신뢰도를 향상시킬 수 있다.

3.3 인증 정보 블록체인 생성 및 교환 프로토콜

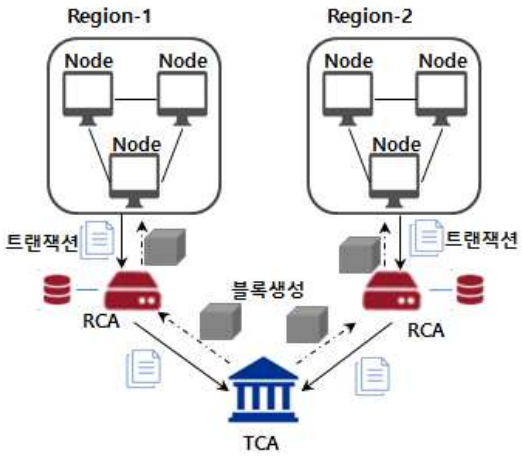
노드들에 대한 인증 정보의 높은 신뢰성을 제공하기 위해 블록체인을 적용하는 방법에 대하여 기술한다. 본 논문에서는 노드 인증에 필요한 정보를 블록체인에 저장할 수 있도록 새로운 블록체인을 설계하였다. 노드 인증 정보의 저장을 위해 블록헤더내 머클트리 루트에 인증과 관련된 새로운 데이터 payload를 적용하였다. (그림 2)는 노드 인증 정보를 위한 데이터 payload를 적용한 블록헤더 구조를 보여주고 있다.



(그림 2) 인증 payload를 적용한 블록헤더 구조

(그림 2)와 같은 블록을 이용하여 블록체인을 생성하기 위해서는 최적의 블록체인 교환 프로토콜이 필요하다. 왜냐하면 무선 이동 노드들로만 구성되어 있는 MANET은 hop-by-hop 방식으로 데이터가 전달되기 때문에 블록의 교환 및 블록체인 생성에 대한 신뢰성을 높이기 위한 기법이 필요하다. 본 논문에서 인증 정보를 블록체인으로 생성하기 위한 과정은 크게 인증 정보에 대한 트랜잭션 생성, 블록 패키징, 검증 및 배포의 단계로 구성하였다. 트랜잭션 생성 단계는 각 영역의 RCA 노드가 영역내 노드들에 대한 인증 요청을 받은 후 멤버키를 발급한 정보들을 저장하게 된다.

각 영역의 RCA 노드들로부터 인증 정보에 대한 트랜잭션을 TCA에게 전달한다. 이때 각 RCA 노드는 TCA 노드로부터 발급받은 그룹키를 함께 전송하게 된다. 트랜잭션을 전달받은 TCA는 해당 트랜잭션을 순서대로 정렬한 후 최신 블록을 생성한다. 최신 블록을 생성하는 오더링 서비스는 카프카(Kafka) 분산 메시징 방식을 적용하였다. 이 모델은 대표적인 Pub-Sub (Publish-Subscribe) 모델로서 Consumers가 Producer로부터 Topic 단위로 구분된 메시지를 수신하는 분산 메시징 시스템으로 특정 파티션을 담당하는 Broker에 장애가 발생하더라도 다른 Broker의 파티션으로부터 손실된 정보를 복구할 수 있기 때문에 안정성을 향상시킬 수 있다. 따라서 블록을 생성하는 TCA 노드는 Producer가 되고, 생성된 블록을 수신 받은 RCA 노드는 Consumer의 역할을 수행한다. 마지막 과정인 검증 및 배포 단계는 TCA가 생성한 최신 블록을 각 영역의 RCA 노드들에게 전달하고, 최신 블록을 전달받은 RCA는 해당 블록이 올바르게 생성되었는지 검증하기 위해 해당 블록을 자신의 영역내 노드들에게 배포해준다. 최신 블록을 수신한 노드들은 블록에 포함된 결과값이 정상인지와 보증정책에 부합하는지 검증 작업을 수행한 후 문제가 없다면 자신의 로컬 저장소에 저장된 블록체인에 최신 블록을 추가하고 업데이트한다. 이러한 과정을 통해 최신 블록을 생성 및 배포할 수 있게 된다. (그림 3)은 본 논문에서 제안한 인증 정보 블록체인 생성 및 교환하는 과정을 보여준다.



(그림 3) 블록체인 생성 및 배포 과정

4. 실험 및 결과

4.1 실험 환경

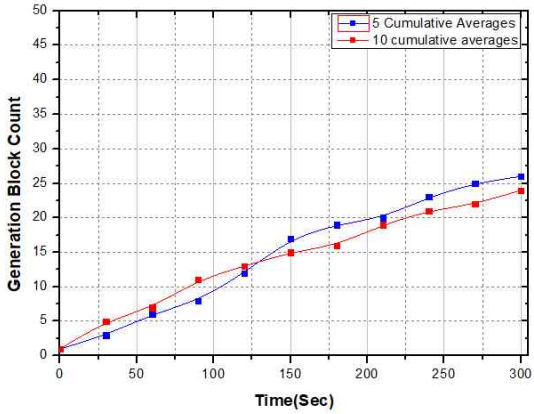
본 논문에서 제안한 계층 구조 및 블록체인 기반 인증 기법의 성능을 평가하기 위하여 다음과 같은 환경에서 실험을 진행하였다. 먼저, 전체 100개의 노드들 중 10개의 악의적인 노드를 구성하였으며, 이들 중 5개의 노드는 라우팅 정보를 수정하는 공격과 나머지 5개 노드는 일정 시간동안 패킷 전달 지연 및 폐기하는 공격을 수행하였다. <표 1>은 실험을 위해 사용한 환경변수를 보여주고 있다.

<표 1> 실험에 사용한 환경 변수

Parameter	Values
Number of Nodes	100개
MAC Protocol	IEEE 802.11 DCF
Traffic	CBR
Pause Time(sec)	20
Transmission range	250m

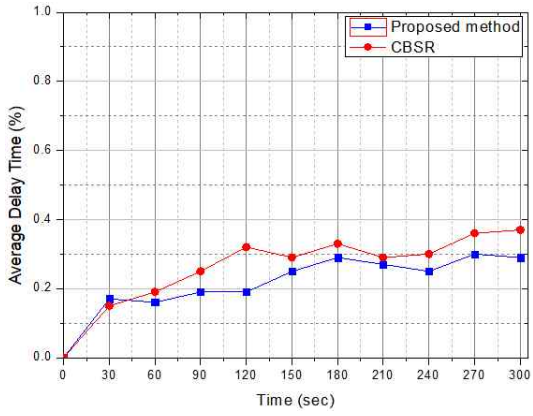
4.2 실험 결과 분석

본 절에서는 성능 평가를 위해 기존의 계층 구조 기반 보안 라우팅 기법인 CBSR(Cluster-based Sercure Routing)과 비교실험 하였으며, 성능 평가 기준은 노드들의 신뢰 정보를 저장하는 블록체인의 정상적인 생성 여부, 평균 지연시간, 처리율을 기준으로 하였다. 실험은 각 300초 동안 실시하였다.



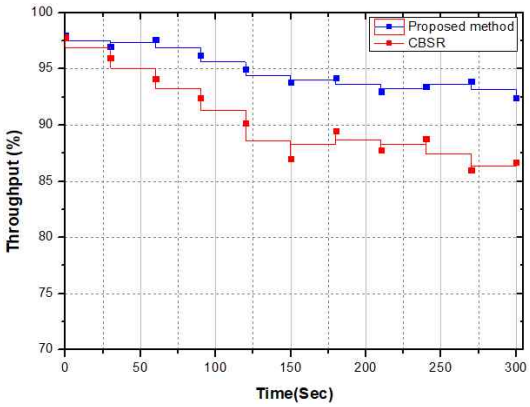
(그림 4) 블록체인 생성 측정 결과

(그림 4)에서는 영역내 노드들에 대한 인증 정보가 각 영역별 RCA 노드들에 트랜잭션으로 생성된 후 TCA 노드에 의한 블록 생성 및 합의가 원활하게 이루어지는지 그 결과를 보여주고 있다. 그래프에서 확인할 수 있듯이 본 논문에서는 트랜잭션이 지정된 일정한 크기로 되었을 때 블록 생성이 되기 때문에 시간에 따라 일정한 간격으로 생성되지는 않지만 시간 흐름에 따라 노드들에 대한 인증 정보가 정상적인 블록으로 정확하게 생성되는 것을 확인할 수 있다.



(그림 5) 평균 지연시간

노드들 사이의 평균 지연시간을 측정한 결과는 (그림 5)에서 보여주고 있다. CBSR 기법은 클러스터를 이용한 계층적 다중 경로를 이용하지만 악의적인 노드들에 의한 경로발견 비율이 증가하여 평균 지연시간이 긴 결과를 보였으며, 제안한 기법은 노드들에 대한 인증 정보가 블록체인에 의해 공유되고 영역내에서 RCA 노드들에 의해 인증 받지 못한 노드는 네트워크 참여가 배제되어 실험 시간동안 악의적인 노드에 큰 영향을 받지 않고 거의 일정한 결과를 보여주었다.



(그림 6) 패킷 처리율

(그림 6)에서는 노드들간 패킷 처리율의 결과를 보여주고 있다. 그림에서 보듯이 CBSR 기법은 경로 설정 다중화를 이용해서 악의적인 노드들의 공격에도 처리율이 많이 떨지지는 않았으며 제안한 기법에서는 각 영역별 RCA 노드들에 대한 인증과 악의적인 노드들의 이동에도 각 인증 정보가 블록체인으로 공유되기 때문에 처리율 성능에도 우수한 결과를 보였다.

5. 결 론

본 논문에서는 이동 노드로만 구성된 MANET의 안전한 노드 인증 및 관리를 위한 최적의 블록체인 구조 설계 및 교환 프로토콜 기법을 제안하였다. 제안한 기법에서는 네트워크에 참여하는 노드들에 대한 효율적인 인증 기법을 위하여 영역기반 계층 형태의 네트워크 구조를 적용하였다. 각 영역내 노드들에 대한 인증을 담당하는 노드와 이러한 인증 노드들을 인증하는 최상위 인증 노드를 선출하고, 각 영역내 멤버 노드들에 대한 인증을 위해 그룹키를 이용하였다. 그리고 노드들에 대한 인증 정보를 블록에 저장하기 위해서 4개의 데이터 payload를 저장할 수 있도록 새롭게 블록을 설계하였다. 각 영역 내에서 발생한 인증 정보에 대한 트랜잭션은 영역 인증노드가 최상위 인증 노드에 전달하면 최상위 인증 노드는 트랜잭션들을 모아 최신 블록으로 생성하는 블록 패키징을 수행하게 된다. 이러한 과정을 통해 생성된 새로운 블록은 영역기반 인증 노드를 통해 각 노드에 전달되며, 노드들은 자신의 디지털 서명과 보증 정책에 따라 해당 블록의 유효성을 판단하게 된다. 이와 같은 방법으로 각 영역 내에서 모든 노드들에 대한 인증 정보를 블록체인에 저장하여 공유함으로써 악의적인 노드들의 네트워크 참여를 배제시킴으로써 네트워크의 신뢰성과 성능을 향상시킬 수 있는 결과를 얻을 수 있었으며, 실험을 통해 그 결과를 확인할 수 있었다.

참고문헌

[1] N. W. Lo and F. L. Liu, "A Secure Routing Protocol to Prevent Cooperative Black Hole Attack in MANET," in Intelligent Technologies and Engineering Systems. vol. 234, J. Juang and Y.-C. Huang, Eds., ed: Springer New York, pp. 59-65, 2013.

[2] S. Ak, H. Rom, and S. Sharma, "A Comprehensive Review of Security Issues in Manets," International Journal of Computer Applications vol. 69 2013.

[3] J. Su and H. Liu, "Protecting Flow Design for DoS Attack and Defense at the MAC Layer in Mobile Ad Hoc Network," Applied Informatics and Communication Communications in Computer and Information Science, vol. 224, pp. 233-240, 2011.

[4] L.Yingbin, H. V. Poor, and Y. Lei, "Secrecy Throughput of MANETs Under Passive and Active Attacks," Information Theory, IEEE Transactions on, vol. 57, pp. 6692-6702, 2011.

[5] A. El-Sayed, "Clustering Based Group Key Management for MANET," in Advances in Security of Information and Communication Networks. vol. 381, A. Awad, A. Hassanien, and K. Baba, Eds., ed: Springer Berlin Heidelberg, pp. 11-26, 2013.

[6] S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," 2008, https://bitcoin.org/bitcoin.pdf.

[7] Lin Chen, Lei Xu, Nolan Shah, Zhimin Gao, Yang Lu, and Weidong Shi., "On Security Analysis of Proof-of-Elapsed Time (PoET)," In Stabilization, Safety, and Security of Distributed Systems. pp. 282 - 297, 2017.

[8] Andrew Miller, Yu Xia, Kyle Croman, Elaine Shi, and Dawn Song., "The Honey Badger of BFT Protocols," In CCS, pp. 31 - 42, 2016.

[9] Rafael Pass and Elaine Shi. [n. d.]. FruitChains: A Fair Blockchain. In PODC 2017. pp. 315 - 324.

[10] Harry Kalodner, Steven Goldfeder, Xiaoqi Chen, S. Matthew Weinberg, and Edward W. Felten. Arbitrum : Scalable, private smart contracts. In USENIX Security 2018. pp. 1353 - 1370.

〔저자소개〕

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