디지털산업정보학회 논문지 제14권 제4호-2018년 12월
http://dx.doi.org/10.17662/ksdim.2018.14.4.017

실시간 지능형 교통 시스템에 적합한 블록체인 기술 및 네트워크 구조

김 문 성* · 나 은 찬** · 이 장 훈** · 이 우 찬***

Blockchain Technology and Network Structure for Real-time Intelligence Transport System

Kim Moonseong · Na Eunchan · Lee Janghoon · Lee Woochan

〈Abstract〉

Connected car plays an important role on Intelligent Transport System (ITS). ITS is able to secure drivers' convenience and safety, however, the overall system can be threatened by hacking attempt. Blockchain is one strong candidate of the remedy to promote the security of the ITS network. However, there will be many challenges to adopt previously proposed blockchain technologies to ITS. This work presents a new ITS structure based on blockchain technology. Proposed scheme includes three major layers. The first layer is central manager which is initiated once to register a certain connected car. The third layer is RSU (Road Side Unit) layer which exploits PoS (Proof of Stake) for consortium blockchains and retains real-time information. In addition, this layer performs block expiration based on timers to maintain manageable block length. In the second layer, the generated blocks of the third layer without expiration are housed as private blockchains. We finally demonstrate possible merits of newly proposed scheme.

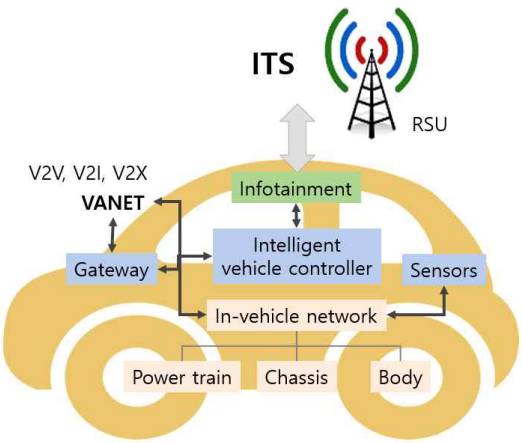
Key Words : ITS, VANET, Connected Car, Blockchain, Realtime Service

Ⅰ. 서론

지능형 교통 시스템(ITS; Intelligence Transport System)에는 커넥티드 카(Connected Car)가 중요한 역할을 하고 있다. 일반적으로 커넥티드 카는 무선 통신장치를 구비하여 차량과 차량 또는 차량과 네트워크 인프라 간에 중요 정보를 통신하며 도로를 주행하는 스마트 카의 하나이다[1].

그림1은 스마트 커넥티드 카의 개략적인 모습을 보여 주고 있다. 다양한 소프트웨어와 하드웨어의 진보된 기술은 수집한 정보들을 활용하여 지능형 컴퓨팅을 가능하게 하였다. 커넥티드 카에는 각종 센서 및 네트워크 통신 모듈들을 사용하여 차량들(V2V; Vehicle-to-Vehicle), 차량과 기반 시설(V2I; Vehicle-to-roadside Infrastructure), 차량과 모든 사물(V2X; Vehicle-to-Everything) 간의 정보를 공유 및 교환 할 수 있다[2].

* 서울신학대학교 교양학부 조교수
** 인천대학교 전자기수치해석연구실 학부연구원
*** 인천대학교 전기공학과 조교수(교신저자)



<그림 1> 스마트 커넥티드 카의 구성도 [2]

이동 차량을 위한 다양한 서비스 발전은 사용자들의 편의성과 안전성의 향상을 제공할 수 있다. 그러나 다양한 정보를 공유하는 커넥티드 카에서는 반드시 고려해야 할 정보보안 요구사항들이 존재한다. 커넥티드 카는 일반적인 차량에 다양한 형태의 통신 수단이 추가되어 차량을 제어하는 것이므로 이에 대한 인증 문제, 공유하는 데이터의 위변조, 이를 통한 차량의 불법 탈취 및 오작동 발생 등 다양한 정보보안 위협이 존재할 가능성이 크다[3-4]. 따라서 스마트 커넥티드 카의 발전에는 정보보안에 대한 중요성이 함께할 수밖에 없다.

최근에는 이러한 정보보안 취약점들을 해결하기 위한 다양한 방법들이 제안되고 있다. 예를 들어, 차량과 네트워크 기반 시설 RSU(Road Side Unit) 간 정보공유를 위해 통신하는 모든 메시지는 기밀성과 무결성이 보장되어야 한다. 만일 악의적인 공격자에게 특정 차량 ID가 노출되면 그 메시지의 기밀성과 무결성은 보장 받을 수 없다. 따라서 이러한 메시지는 보통 익명의 인증서를 통한 전자 서명이 이루어지게 된다. 그러나 참고문헌 [5]에 따르면, 익명의 인증서를 사용하여도 악의적인 공격자는 특정 차량의 ID를 추적하는 것이 가능하다고 한다. 본 논문에서는 이러한 익명성을 보장하기 위한 블록체인의 적용을 고려하였다. 또한, 기존에 제시된 블록체인 모델 [6]의 한계를 극복하고자 새로운 네트워크 기반 구조를 제안하고자 한다.

본 논문의 구성은 다음과 같다. 제2장에서는 차량 간 통신에서의 정보보안 이슈 및 블록체인 기술에 대해 소개한다. 제3장에서는 ITS에 적합한 블록체인 기법 및 네트워크 구조에 대해 제안하며, 이에 따른 성능분석을 간단히 살펴보고자 한다. 그리고 제4장에서는 본 논문을 마무리하겠다.

Ⅱ. 관련 연구

2.1 정보보안 요구사항

커넥티드 카는 무선 통신 기술을 적절히 적용하였으므로, 악의적인 사용자에 의해서 다양한 위험에 노출되어 있다. 따라서, 커넥티드 카를 지원하기 위한 ITS 환경에서는 반드시 다음과 같은 정보보안 요구사항을 수반해야 한다[4, 7].

첫째, 사용자 인증, 데이터 기밀성 및 무결성이다. 만약 비인증 사용자가 정보를 얻을 경우 악의적인 목적으로 사용자로 위장하여 개인정보에 쉽게 접근할 수 있으며 이는 데이터의 기밀성 및 무결성 또한 보장할 수 없게 된다. 이를 위해 커넥티드 카에서는 최초 인증으로 권한을 부여받은 차량만이 통신을 허용해야 한다. 또한, 메시지의 암호화 등으로 데이터의 기밀성 및 무결성을 보장해야 한다.

둘째, 개인정보 보호를 위한 익명성 보장이다. V2V, V2I, V2X에서 주고받는 정보들은 인증되지 않은 제 3자에 대해 익명성을 가져야한다. 만일 정보가 유출되면, 차량의 상태, 운전 이력, 운전 경로 및 행동 습성에 대한 공격이 가능하다. 잘 알려진 해결 방법

은 가명의 식별 정보 사용 및 인증서 발급 등이 있다.

셋째, 교통 사고 등과 같은 분쟁 해결을 위한 추적성이다. 만약 어떠한 차량 간 사고가 발생했을 경우, 공공기관(경찰, 소방서, 병원 등)에게 긴급한 사항을 전달해야 하며, 메시지를 수신한 기관에서 이들을 추적할수 있어야 한다.

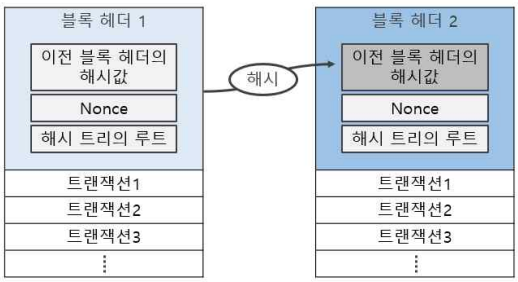
넷째, 비연결성을 고려할 수 있다. 익명성 보장으로 개인정보 유출 방지를 보장하였다 할 지라도 동일한 정보가 지속적으로 노출이 되면, 특정차량으로 지칭되어 그 경로가 노출이 될 가능성이 있다. 비연결성의 제공은 또다른 개인정보 보호로 간주할 수 있다.

마지막으로, 가용성 및 부인 방지 등 다양한 요구사항이 존재하지만, 본 논문에서는 특별히 익명성 및 추적성 보장 방법을 고려하겠다.

2.2 블록체인 연구동향

분산 장부로 대표되는 블록체인 메커니즘에서는 네트워크의 모든 노드가 동일한 거래 기록(트랜잭션; Transaction)을 처리 할 수 있다. 또한, 모든 참여자에게 기록 및 검증 등의 동일한 데이터가 존재하므로 백업에 대한 비용도 줄일 수 있다. 가장 큰 특징은 정보보안 관련 사항에 대한 중앙 기관의 역할이 줄었다는 것이며, 모든 데이터가 암호화로 공유된다는 것이다[8]. 분산장부 시스템에는 실질적으로 고장 및 점검 등으로 시스템이 멈추는 다운타임(Downtime)이 없고, 저비용이며, 어느 하나의 중앙 기관에 부여되는 높은 신뢰는 불필요하게 된다. 이를 위해 기록이 저장된 정보를 블록(Block)화 하여 체인(Chain) 모양으로 연결하는 것을 블록체인(Blockchain)이라 한다.

블록은 기록 데이터 외에 앞 블록의 정보들을 대변하는 해시값과 난스(Nonce)를 포함하고 있다. 난스는 한번 쓰이고 버려진다(**N**umber used **once**)는 의미로, 새로운 블록을 생성할 경우 사용하는 값이다[9]. 그림 2에서 새로운 블록을 생성하기 위해서는 1개 앞의 블록 헤더(1개 앞의 블록 헤더의 해시값, Nonce, 복수의 트랜잭션들을 정보로 포함해 생성한 해시값)의 해시값 정보와 생성한 Nonce 및 그 블록에 포함된 모든 트랜잭션의 해시값을 포함시켜 해시 함수 값을 구한다. 따라서 어떤 블록의 거래 기록을 변조할 경우, 해시 함수의 특성으로 이후 연결된 모든 블록의 해시값들이 변하게 된다. 만약 위조와 변조를 위해서는 모든 해시를 다시 계산해야 하는 어려움이 따른다.



<그림 2> 블록의 생성 [9]

전통적인 블록체인 모델에서는 전자 서명으로 트랜잭션의 정당성을 보증할 수 있으며, 각 트랜잭션에 한 개씩 전자 서명이 부여된다. 블록체인에는 전자 서명을 검증하기 위한 가명(Pseudonym)자들의 공개키 세트가 부여되기 때문에 네트워크의 노드들은 과거 블록체인에서 수행된 모든 트랜잭션을 순서대로 검증할 수 있다. 즉, 트랜잭션 내용을 위변조 하였는지 여부를 알 수 있다[10].

그러나 특정 가명자의 공개키로 복호화를 수행하므로, 트랜잭션을 검증할 수는 있지만 발생한 트랜잭션에 대한 추적이 가능하여 완벽한 익명성을 보장할 수 없게 된다. 즉, 차량의 현재 위치, 이동 방향, 이동 속도 등에 대한 개인정보 파일을 포함한 트랜잭션에 대한 검증은 수행하였으나, 트랜잭션을 발생한 차량을 추적할 수 있으므로 공격자가 특정 이동 차량에 커다란 위험을 가할 가능성이 생기게 된다[11].

이렇듯 블록체인의 익명성 문제를 보장하기 위해서는 다양한 방법들이 사용되고 있다. 대표적인 토르(TOR; The Onion Routing[12]) 기법은 기본적인 라우팅과는 다르게 데이터 패킷을 다수의 토르 노드를 거쳐 우회시키는 기법으로 역추적을 불가능하게 하는 방법이나, 네트워크 지연시간 문제로 실시간 ITS 시스템에는 부적합하다. 참고문헌 [6]은 Cryptonote[13]를 적용하여, 가명자의 특정한 공개키가 아닌 임의로 생성한 One-time 공개키 방식으로 트랜잭션 생성자의 익명성을 보장하였다.

이와 같이 다양한 기법들을 적용하여 트랜잭션을 검증하고 익명성을 보장할 수는 있었다. 그러나 한 개의 블록 생성시 소요되는 지연시간(10분 이상[14])에 대한 근본적인 문제를 해결하지 못한다면, 실시간 ITS에 적용할 수 있는 익명성 보장 블록체인 메커니즘을 적용하는데는 어려움이 따를 것이다. 본 논문에서는 이러한 근본적인 문제를 해결하고자 네트워크 기반 구조를 변경하여 실시간 환경에 적합한 블록체인 기반 ITS를 설계하였다.

<표 1> 블록체인의 분류

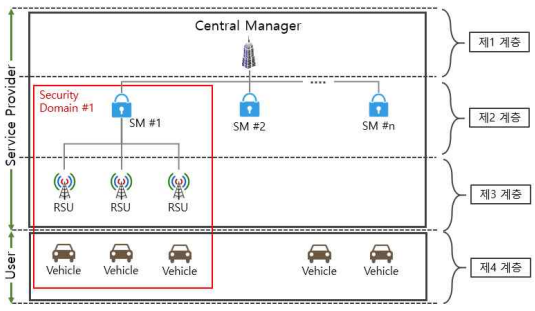
	퍼블릭 블록체인	컨소시엄 및 프라이빗 블록체인
블록 생성	불특정 다수	멤버(컨소시엄) 소유주(프라이빗)
거래 검증	참여자 누구나	승인된 기관 및 감독 기관
속도	상대적으로 느린 속도 (7~20TPS)	상대적으로 빠른 속도 (1,000TPS 이상)

블록체인 네트워크 구축시 연산 및 전파속도에 대한 지연속도 문제는 꾸준히 제기되어 오고 있다. 표1은 다양한 블록체인들의 성능을 비교하고 있다. 일반적으로 컨소시엄 및 프라이빗 블록체인의 선택은 상대적으로 빠른 인증속도 보장 및 합의 알고리즘의 규칙 변경이 간단해 확장하기도 용이하다. 또한, 지연시간 문제를 위해서 블록체인의 초기 길이 생성을 최소화하거나, 이미 생성된 블록체인의 검증 비용을 최소화 하는 것이 대안이 될 수도 있다[2, 15-16].

Ⅲ. 블록체인 기반 지능형 교통 시스템

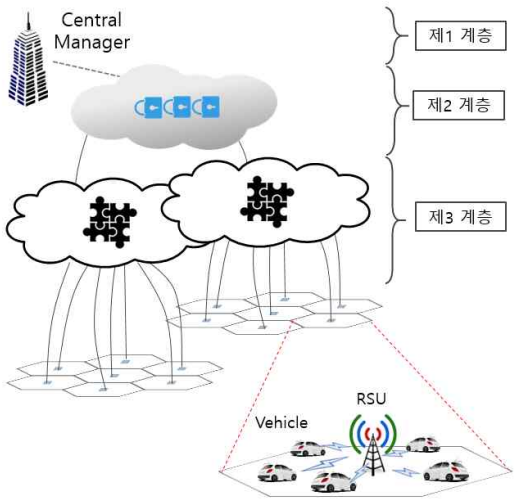
3.1 네트워크 모델

커넥티드 카를 지원하기 위한 일반적인 ITS 네트워크 계층 구조는 그림3과 같다. RSU는 제3 계층에서 IEEE 802.11p AP 역할을 하며 차량의 메시지를 상위 계층으로 라우팅할 수 있다. 또한, 최대 전송 반경을 만족할 수 있는 균일한 간격으로 도로에 설치되어 동위 계층의 라우팅도 가능하다. SM(Security Manager)은 제2 계층에 위치하여 도메인 간의 보안성을 관리한다. 가장 상위 계층 CM(Central Manager)에는 차량의 최초 등록 및 인증을 관리할 수 있는 중앙 관리자가 위치하여 있다. 그러나, 제1 및 2 계층의 CM 및 SM 그룹이 각각 다양하게 존재한다면, 이동 차량이 새로운 CM 또는 SM 그룹으로 이동 시 중앙에서 보안 정보를 관리하는 새로운 도메인의 CM에게 차량의 인증 정보 등을 교환해야 하는 지연시간 및 비용 문제가 추가 발생하게 된다.



<그림 3> 일반적인 ITS 네트워크 계층 구조 [17]

이런 문제점을 해결 할 수 있는 기법으로는 앞서 언급한 블록체인 기술이 적합하다. 블록체인 기반 구조를 고려한다면 다수의 CM을 배제할 수 있어 인증을 위한 키 전달에 대한 오버헤드를 줄일 수 있을 것이다. 물론 차량의 최초 등록을 위한 최소한의 CM은 필요할 것이다. 제안하는 기본 구조는 그림4와 같은 구조를 적용한다.



<그림 4> 블록체인 기반 ITS 네트워크 계층 구조

여기에서 CM은 차량의 초기 등록 및 블록체인 트랜잭션 전송시 사용되는 해싱된 가명 등을 저장할 수 있는 장소로 네트워크에 연결할 수 있으나, 평상시 단절되어 있는 장소로 설정하는 것이 바람직하다. 또한, 운전자는 주기적으로 자신의 가명을 익명성 보장을 위해 직접 갱신할 수 있다. 그러나, 제2 또는 3 계층의 블록체인에서는 익명성 보장을 위해 Cryptonote 트랜잭션 모델[13] 등을 적용할 수 있다. 다음 절에서는 제2 및 3 계층에서의 블록체인 적용에 대해 자세히 언급하겠다.

3.2 블록체인 기반 정보공유

도로를 주행하는 커넥티드 카는 자신의 위치에서 다양한 정보를 RSU에게 송신하기 위해 트랜잭션을 생성한다. 제3 계층에 해당하는 RSU는 트랜잭션을 수신하여 정당하게 인증받은 사용자인지 판단을 하고, 트랜잭션을 포함하는 블록을 생성하기 위해 트랜잭션 유효성에 대한 검증을 수행한다. 이때에 블록체인의 생성 및 배포를 고려할 경우 네트워크의 지연에 따른 문제점을 배제할 수가 없게 되므로, 적절한 합의 알고리즘을 고려해야 한다. 다양한 정보를 포함한 트랜잭션을 수신한 RSU에게 트랜잭션의 배포를 위촉하였으므로 블록체인 생성을 위한 네트워크에 참가할 수 있다. 이때, 블록 생성을 위한 합의 알고리즘으로는 이더리움 블록체인 환경에서의 PoS (Proof of Stake)를 사용한다. 퍼블릭 환경의 PoW(Proof of Work)를 사용할 경우 생성 및 배포 지연 등의 이유로 실시간 서비스를 필요로 하는 ITS에는 적당하지 않다.

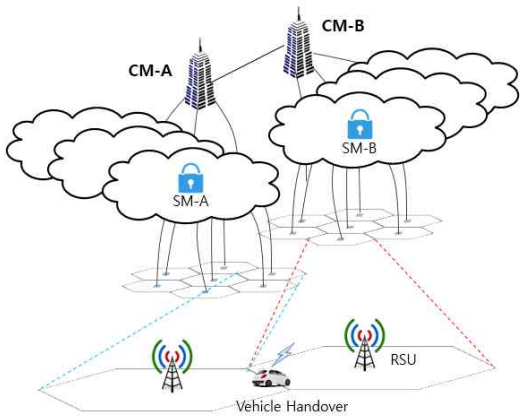
ITS에서 커넥티드 카가 사용할 수 있는 정보는 시간이라는 변수에 큰 영향을 받는다. 블록체인 생성 및 배포에 대한 시간 변수 뿐만 아니라, 블록들의 체인 크기 문제 또한 고려해야 한다[18]. 다시 말해, 현재시간 기준으로 최근의 정보를 적절히 유지하는 것이 제3 계층의 또 다른 목적일 것이다. 따라서 블록들에 적절한 타이머를 추가하여 일정시간 지난 이후 블록들의 소멸을 진행하는 것이 바람직할 것이다.

그러나 소멸된 데이터들 또한 향후 추적을 위한 자료로 쓰일 가능성은 존재한다. 따라서, 실시간 정보를 유지하는 제3 계층의 RSU에서 블록생성시 블록 소멸에 대한 타이머를 배제한 블록을 동시에 상위 제2 계층으로 전송하는 것이 필요할 것이다. 즉, 제2 계층에서는 블록들을 시간 변수에 종속시킬 이유가 없으며, 수신한 블록의 트랜잭션들을 재구성하여 단일 블록의 크기 등을 다시 고려할 수 있는 프라이빗 블록체인 환경이 적합할 것이다.

3.3 성능 비교 분석

스마트 커넥티드 카에 적합한 블록체인 기반 ITS 환경을 현재 진행 중인 각 분야의 연구 결과들과 비교하면 다음과 같다.

도로를 주행하는 차량의 사용자가 트랜잭션 전송 시 가명자의 고유 전송키를 사용하는 일반적인 블록체인 방법을 사용할 경우에는 추적이 가능하게 된다. 이를 위해 One-time 공개키 방식을 적용시키면 어떠한 트랜잭션도 일정시간 고정된 RSU 주소로 보내지는 것에 대한 연결성을 끊을 수 있다. 물론, 매번 서로 다른 주소를 생성하여 일반적인 블록체인 방법에 적용시킬 수 있으나 자신의 가명을 사용할 수 없게 되는 단점이 생겨, 추적이 가능하게 된다[6].



<그림 5> 전통적인 ITS 인증 구조 [17]

일반적인 ITS에서의 인증 메커니즘은 그림5와 같다. 다수의 RSU들을 관리하는 보안 도메인 SM-A 등을 관리하는 중앙 CM-A에서, 차량이 다른 인증 기관의 SM-B로 핸드오버 할 경우 CM-A에서 CM-B로 인증 관련된 정보들이 이동해야 할 것이다.

그림5에서 CM의 개수를 N_{CM}이라 하고, 각 CM에 연결된 SM의 개수를 N_{SM}이라고 하면, 차량이 핸드오버 이전 원소속의 CM(예를 들어, CM-A)에 리포팅하는 시간(T_{report})은 다음의 식 (1)로 결정된다.

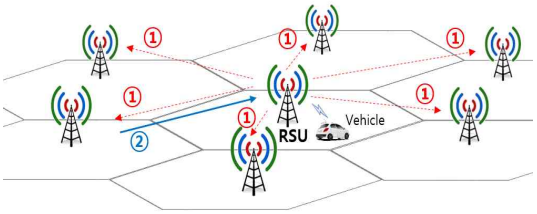
$$T_{report} = N_{SM} \times (T_{Car2RSU} + T_{RSU2SM} + T_{SM2CM}) \quad (1)$$

여기서 이동하는 차량이 각 CM의 관할 영역을 넘어 CM 간의 키교환(핸드오버)이 일어나는 경우에는 $(N_{CM} - 1) \times T_{CM2CM}$의 시간이 추가되며, 통상적인 ITS 환경에서 이동하는 차량의 총 네트워크 비용($T_{transaction}$)은 다음 식 (2)와 같다.

$$\begin{aligned} T_{transaction} &= N_{CM} \times T_{report} + (N_{CM}-1) \times T_{CM2CM} \\ &= N_{CM} \times N_{SM} \times (T_{Car2RSU} + T_{RSU2SM} + T_{SM2CM}) + (N_{CM}-1) \times T_{CM2CM} \end{aligned} \quad (2)$$

참고문헌 [6]에서는 블록체인 기법을 ITS 환경에 적용시켰으나, 블록의 생성 및 배포 지연 시간에 대해서는 전혀 언급하지 않았다. 이에 반해, 본 논문에서 제안하는 네트워크 구조에서는 RSU들이 참가하는 제3 계층에 컨소시엄 블록체인을 사용하여 지연 시간을 최소화 시키는 노력을 하였다. 제안된 네트워크 구조에서는 합의 알고리즘으로 PoS를 적용하여, 블록이 생성되는 장소를 트랜잭션을 직접 수신하는 RSU로 한정하였다. 만약 전체 네트워크에 차량이 균일하게 분포되어 있다고 간단히 가정한다면, 각각의 RSU들이 생성하는 블록들의 개수는 거의 균일하게 된다. 따라서 제3 계층 네트워크의 블록 생성이 균등하게 이루어져서 컴퓨팅 자원 배분 측면에서 유리하게 된다.

만약, PoW을 적용할 경우 그림6과 같이 수신한 트랜잭션들을 주위 네트워크에 배포(①x6)하고, 해시를 계산하여 다시 통보(②)하는 등의 합의가 이루어져서 지연 시간 뿐만 아니라 차량이 밀집된 도로에서는 매우 부적절한 합의 방법이며, 블록 하나의 합의를 위한 네트워크 비용(①x6x2+②)이 PoS를 적용할 경우



<그림 6> PoW를 적용할 경우 발생하는 메시지 흐름 [9]

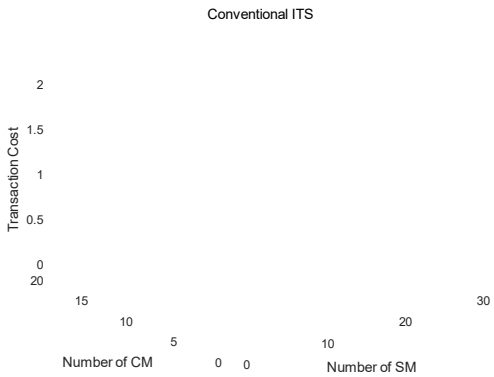
(①x6)에 비해 상대적으로 많이 발생한다.

PoW의 경우, RSU 간의 트랜잭션들 전달 비용(시간)(즉, ①과 ②)을 $T_{RSU2RSU}$라 하면, $T_{PoW}=N_{SM}\times13\times T_{RSU2RSU}$로 요약할 수 있고, PoS의 경우 $T_{PoS}=N_{SM}\times6\times T_{RSU2RSU}$로 정리할 수 있다. 본 논문에서 제안한 네트워크 구조에서는 CM 간의 키교환 비용을 생략할 수 있으므로, CM의 개수(N_{CM})에 의존하지 않는 장점이 있다.

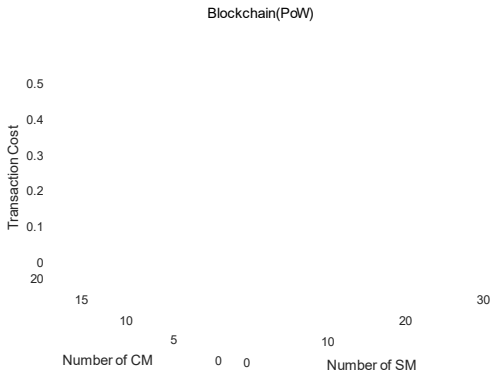
성능평가를 위한 시뮬레이션에서는 CM의 최소 개수를 2, 최대 개수를 20으로 설정하였고, 각 CM에는 SM이 최소 3개에서 최대 30개가 동일한 개수로 연결되어 있는 것으로 가정하였다. 또한, 통상적인 네트워크의 상황을 고려하여 T_{SM2SM}, T_{RSU2SM}, $T_{Car2RSU}$은 1ms의 평균과 0.1ms의 분산을 가진 정규분포로 각각 가정하였다. 또한, T_{CM2CM}은 키 교환의 오버헤드를 고려하여 10ms의 평균과 1ms의 분산을 가진 것으로 상정하였다. 다만, 본 시뮬레이션에서는 각 유닛에서 정보처리에 걸리는 시간, 예를 들어 블록체인 생성 시각은 고려하지 않았는데, 이는 컨소시엄 또는 프라이빗 블록체인을 적용했을 때의 처리속도가 상기 표 1과 같이 1,000TPS 이상임을 감안한 것이다.

그림7은 통상적인 ITS에서의 네트워크 비용을 나타내는데, 이는 CM의 개수와 CM에 연결된 SM의 개수에 의존한다.

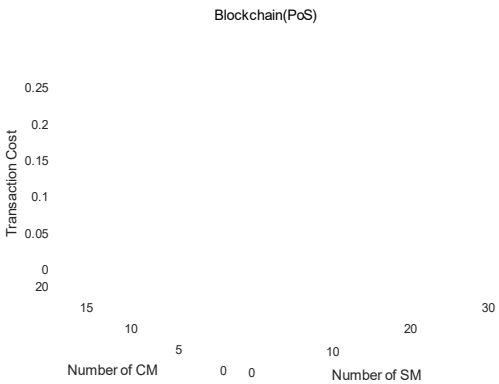
그림8은 본 논문에서 제안한 (PoW기반)블록체인을 적용한 제3계층의 네트워크 비용을 나타낸다. 그림7의 통상적인 ITS의 경우와 비교하여 보다 낮은 네



<그림 7> 일반적인 ITS에서의 네트워크 발생 비용



<그림 8> 블록체인(PoW)기반 네트워크 발생 비용



<그림 9> 블록체인(PoS)기반 네트워크 발생 비용

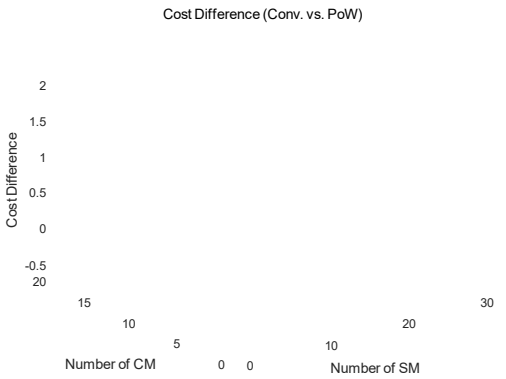
트워크 비용을 보인다.

그림9는 (PoS기반)블록체인를 적용한 제3계층의 네트워크 비용을 나타내며, 이 네트워크 비용은 통상적인 ITS(그림7) 및 PoW를 적용한 경우(그림8)보다 낮다.

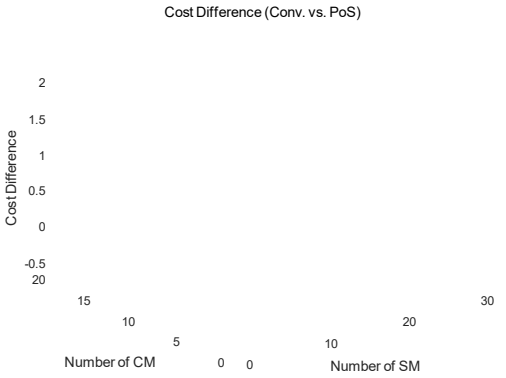
그림10 및 11은 통상적인 ITS의 네트워크 비용(그림7)과 본 논문의 PoW(그림8) 및 PoS(그림9)의 비용 간의 차이를 시각화하였다. 예상된 바와 같이 CM 및 SM의 개수가 증가함에 따라 본 논문에서 제안한 PoW 및 PoS 환경의 네트워크 비용이 적음을 확인할 수 있다.

더욱이, 제3 계층에서는 블록의 소멸을 위한 타이머를 고려하여 최대 블록들의 개수를 적절하게 유지시킬 수 있어, 블록을 소유하는 저장 비용 뿐만 아니라 컴퓨팅 시간 까지 효율적으로 관리할 수 있다는 장점이 있다.

그러나, 예기치 못한 차량의 사고 등으로 추적성을 필요 하는 경우가 생길 수 있다. 따라서 본 논문에서 제안한 네트워크 구조의 제2 계층은 프라이빗 블록체인의 생성 및 관리로 제1 계층과의 협업을 통해 메시지 이동 경로를 추적할 수 있다는 장점이 있다.



<그림 10> 통상적인 ITS vs. (PoW)블록체인 적용 구조



<그림 11> 통상적인 ITS vs. (PoS)블록체인 적용 구조

Ⅳ. 결론

지능형 교통 시스템에서 무선 통신장치를 구비한 스마트 커넥티드 카는 자신의 중요 정보 뿐만 아니라, 실시간 교통 및 기타 정보들을 RSU를 통하여 송·수신 할 수 있다. 이는 차량 운전자들을 편리하고 안전하게 지원할 수 있는 수많은 정보들을 포함할 수 있으나, 다양한 위험에 노출되어 있는 것 또한 중요한 사실이다. 그러므로, 커넥티드 카를 지원하기 위한 필수 보안 요소들을 충족시켜야 하며, 최근 이를 지원할 수 있는 방법중의 하나가 블록체인 기술이다. 그러나 블록체인 기술을 ITS에 적용한 연구들이 소개되었으나 블록체인이 가지고 있는 한계점을 여전히 극복할 수는 없었다.

이러한 문제점들을 해결하기 위하여, 본 논문에서는 ITS에서 블록체인 기술을 지원할 수 있는 네트워크 구조에 대하여 소개하였다. 제안한 네트워크 구조는 크게 3개의 계층으로 이루어 졌다. 제1 계층은 커넥티드 차량을 오프라인으로 최초 등록하여 인증을 관리하는 계층이며, 제3 계층은 RSU들이 참여할 수 있는 네트워크 계층으로 차량에서 발생하는 트랜잭션들을 수신하여 검증하고, PoS 합의 방법으로 블록을 생성 및 배포할 수 있다. 또한, 트랜잭션들을 포함하는 블록을 상위 제2 계층으로 동시에 전송하여 제3

계층에서 소멸 가능한 블록들을 백업할 수 있으며, 제1 계층과의 연결로 향후 문제가 발생하는 차량을 추적이 가능하게 고안하였다. 향후에는 제2·3 계층에서 발생하는 블록들을 실제 구현하여, 실시간 환경에 적합한지에 대한 추가 성능분석을 진행할 예정이다.

참고문헌

[1] 심현보, "커넥티드 카의 기술," 한국정보통신학회 논문지, 제20권, 제3호, 2016, pp.590-598.

[2] Kim, S., "Blockchain for a Trust Network Among Intelligent Vehicles," Elsevier, Advances in Computers, Vol.111, 2018, pp.43-68.

[3] 한국방송통신전파진흥원, "지능형 교통시스템의 차량 통신 보안 기술 동향과 전망," 방송통신기술 이슈 & 전망, 제59호, 2014.

[4] 이명렬·박재표, "스마트카 정보보안 침해위협 분석 및 대응방안 연구," 한국산학기술학회 논문지, 제18권, 제3호, 2017, pp.374-380.

[5] Wiedersheim, B., Ma, Z., Kargl, F., and Papadimitratos, P., "Privacy in inter-vehicular networks: Why simple pseudonym change is not enough," 2010 Seventh International Conference on Wireless On-demand Network Systems and Services (WONS), 2010, pp.176-183.

[6] 최석준·곽진, "차세대 ITS 환경에서 익명성을 보장하기 위한 블록체인 활용 방안," 한국인터넷정보학회 2018년도 춘계학술발표대회 논문집, 제19권, 제1호, 2018, pp.99-100.

[7] 박수민·홍만표·손태식·곽진, "VANET 프라이버시 보장 아키텍처 설계," 한국인터넷정보학회 논문지, 제17권, 제6호, 2016, pp.81-91.

[8] 김태경, "이더리움 기반 이메일 시스템 모델," 디지털산업정보학회 논문지, 제13권, 제4호, 2017, pp.99-106.

[9] 아카하네 요시하루 외 9인, "블록체인 구조와 이론," 위키북스, 2017, p.109, p.120.

[10] S. Nakamoto, "Bitcoin: A Peer-to-peer Electronic Cash System," 2008.

[11] 김인환·최형기·김정윤, "프라이버시를 보호하며 안전하고 효율적인 차량간 통신 프로토콜," 정보과학회 논문지, 제37권, 제6호, 2010, pp.420-430.

[12] Koch, R., Golling, M., and Rodosek, G. D., "How Anonymous Is the Tor Network? A Long-Term Black-Box Investigation," IEEE Computer, Vol.49, No.3, 2016, pp.42-49.

[13] Nicolas van Saberhagen, "CryptoNote v 2.0," 2013.

[14] 김영호, "미래 교통과 블록체인," 월간 교통, 제236호, 2017, pp.42-45.

[15] 김상근, "M2M 환경의 혼잡 네트워크 개선을 위한 블록체인 경량화에 대한 연구," 디지털산업정보학회 논문지, 제14권, 제3호, 2018, pp.69-75.

[16] 민병길·성영조·박원익, "비트코인과 블록체인의 쟁점 및 정책적 시사점," 경기연구원, 이슈&진단, 제307호, 2018, pp.1-27.

[17] Lei, A., Cruickshank, H., Cao, Y., Asuquo, P., Ogah, C. P. A., and Sun, Z., "Blockchain-Based Dynamic Key Management for Heterogeneous Intelligent Transportation Systems," IEEE Internet of Things Journal, Vol.4, No.6, 2017, pp.1832-1843.

[18] 임재민·김영필·유혁, "IoT 환경에서 안전한 펌웨어 인증을 위한 블록 체인의 활용 방안 및 한계점," 한국정보과학회, 2017 한국소프트웨어종합학술대회 논문집, 2017, pp.482-484.

논문접수일 : 2018년 11월 26일
수 정 일 : 2018년 12월 4일
게재확정일 : 2018년 12월 7일

■ 저자소개 ■

김 문 성
(Kim Moonseong)

2018년 9월~현재
서울신학대학교 교양학부 조교수
2009년 10월~2018년 8월
특허청 사무관
2007년 12월~2009년 10월
미국 미시간주립대학교 연구원
2007년 2월 성균관대학교 전기전자 및
컴퓨터공학부(공학박사)
2002년 8월 성균관대학교 수학과(이학석사)

관심분야 : 모바일 컴퓨팅, 정보보호 프로토콜
E-mail : moonseong@stu.ac.kr

나 은 찬
(Na Eunchan)

2018년 9월~현재
인천대학교 전자기수치해석연구실
학부연구원
2016년 3월~현재
인천대학교 공과대학 전기공학과

관심분야 : 전기공학, 머신러닝, 블록체인
E-mail : we1544@naver.com

이 장 훈
(Lee Janghoon)

2018년 9월~현재
인천대학교 전자기수치해석연구실
학부연구원
2013년 3월~현재
인천대학교 공과대학 전기공학과

관심분야 : 전기공학, 머신러닝, 블록체인
E-mail : stork741@naver.com

이 우 찬
(Lee Woochan)

2017년 9월~현재
인천대학교 전기공학과 조교수
2004년 4월~2017년 8월
특허청 사무관
2005년 7월~2008년 6월
육군사관학교 전자공학 교수사관
2016년 12월 미국 Purdue University
전기컴퓨터공학부(공학박사)
2005년 2월 서울대학교
전기컴퓨터공학부(공학석사)
2002년 2월 서울대학교 전기공학부(공학사)

관심분야 : 수치해석, 머신러닝, 블록체인
E-mail : wlee@inu.ac.kr