Vehicular Ad-hoc Network 환경에서 IPFS 와 블록체인을 활용한 안전하고 효율적인 교통정보시스템

박한울 [1], 허가빈 [2], 도인실 [1]
[1] 이화여자대학교 사이버보안전공
[2] 이화여자대학교 인공지능 · 소프트웨어학부
nanometre380@ewhain.net, gjrkqls@ewhain.net, isdoh1@ewha.ac.kr

Secure and Efficient Traffic Information System Utilizing IPFS and Blockchain in Vehicular Ad-hoc Network

Hanwool Park[1], Gabin Heo[2], Inshil Doh[1]
[1]Dept. of Cyber Security, Ewha Womans University
[2]Division of Artificial Intelligence and Software, Ewha Womans University

요 약

현재의 교통정보시스템은 수집된 정보를 서버에서 가공하여 서비스하는 형태로 이루어져 있다. 이러한 형태는 네트워크 구성이 비교적 단순하고 유지관리 비용이 적게 든다는 장점이 있지만, 반면에 실시간성이 저하되고 보안이 제대로 보장되지 않을 수 있다는 문제가 있으며, 최근 많은 연구가 이루어지고 있는 VANET 환경에서의 교통정보시스템도 broadcast storm 의 가능성을 안고 있다. 본 연구에서 제안하는 교통정보시스템은 자동차가 수집한 돌발 상황에 대한 데이터를 RSU(Road Side Unit)가 수신하고, 이후 메시지를 노드들에게 보낼 때 블록체인에 업로드함으로써 보안성과 broadcast storm 문제들을 해결할 수 있으며, raw data 를 IPFS 에 저장하여 시스템 고도화에 사용할 수 있어 참여자들이 교통 상황에 대해 신속하게 대응할 수 있도록 하는 장점을 갖는다.

1. 서론

ITS(Intelligent Transport System)는 무선 통신 기술을 통해 도로 안전을 개선하고 사용자에게 편리함을 제공하기 위한 지능형 교통 시스템으로써, 자율주행차량의 한계를 극복할 수 있어 자율주행차량의 발전과 함께 그 필요성이 더해지고 있다[1]. 그중에서도 교통정보시스템은 도로 상황, 재난 정보 등을 실시간으로 수집 분석하여 그 정보를 시민과 관련 기관에 제공할 수 있다. 따라서 다양한 교통 상황에서 돌발 상황 혹은 사고에 대응하도록 하여 교통정보시스템은 현대의 교통 체계에서 필수적인 요소가 되고 있다. 하지만 현재의 교통정보시스템은 교통 정보 수집 카메라나 CCTV 등의 장치로부터 수집된 정보를 서버에서 가공하여 갱신 주기에 맞추어 사용자에게 서비스하는 형태로 이루어져 있다. 이러한 구조는 중앙 서버에서 일련의 과정을 거쳐 개별 사용자에게 보내지므로 지연시간이 존재하게 되는데, 이는 교통정보시스템에서 필수 요소인 실시간성이 제대로 보장되지 않는다는 문제점이 존재한다. 또한, 이러한 구조는 서버를 공격하여 제대로 동작하지 못하는 DDoS 공격에 취약하며, 사용자에게 전달되는 정보의 위 · 변조 가능성과 정보 탈취로 인한 재전송 공격의 가능성이 항상 존재하여 혼란을 야기할 수 있다.

차량 ad-hoc 네트워크인 VANET(Vehicular Ad-Hoc Network)을 기반으로 한 교통 정보 시스템이 연구되고 있는데, 이는 차량이 통신 노드의 역할을 하도록 하여 운전자가 인지하는 대처와 더불어 자동차의 자체적인 대응까지도 가능할 수 있도록 한다. 하지만 VANET 또한 위 · 변조 위험을 피할 수 없고, 위조 공격, 재전송 공격에 노출되어 있다. 그뿐만 아니라 뒤늦게 네트워크에 합류한 경우 메시지가 누락될 위험이 있으며, multi-hop broadcast 방식으로 인해 하나의 메시지가 주변의 노드에 broadcast 되고, 해당 메시지를 수신한 노드가 다시 주변 노드에 broadcast 를 하면서 많은 양의 트래픽을 발생시켜 정상적인 동작이 힘들어지도록 하는 Broadcast storm 의 가능성 또한 안고 있다[2]. 이에 본 논문에서 앞에서 언급된 네트워크 및 보안 문제를 해결하고 더욱 안정적인 시스템을 만들기 위해 VANET 환경에서 IPFS 와 블록체인을 활용하여 데이터를 안전하고 신속하게 노드들에 전달할

수 있고, 학습을 통한 고도화가 가능한 효율적인 교통정보시스템을 구축하고자 한다.

2. 관련 연구

1) VANET

VANET 은 무선 통신 기술을 갖춘 차량들에 의해 형성된 ad-hoc 네트워크이다. 차량과 RSU(Roadside Unit)라는 도로 옆 기반시설로 구성되어 있으며, 차량과 RSU, 차량과 차량 간의 통신이 가능토록 하여 ITS 의 핵심기술이라고 할 수 있다. VANET 을 통해 노드가 교통 정보를 다른 노드로 전달하며, 차량의 이동 특성으로 인해 지연에 민감하고 빠른 판단이 필요하다.

2) 블록체인

블록체인은 분산형 데이터 저장기술을 말한다. 노드들은 동일한 사본을 저장하며, 한번 기록되고 나면 데이터의 변조 및 위조가 불가능하다는 특징이 있어 정보 신뢰성, 투명성, 추적성 등의 이점을 제공한다[3].

블록체인은 개방형(Public) 블록체인과 전용(Private) 블록체인으로 나뉜다. 이 때 전용 블록체인은 허가를 받은 경우에만 블록체인 네트워크에 참여할 수 있으며, 트랜잭션 속도가 개방형 블록체인에 비해 굉장히 빠르고, 비용이 낮다는 장점이 있다. 해당 시스템에서는 지연 시간을 최소화하기 위해 전용 블록체인을 채택한다[4].

<표 1> 개방형 블록체인과 전용 블록체인의 비교

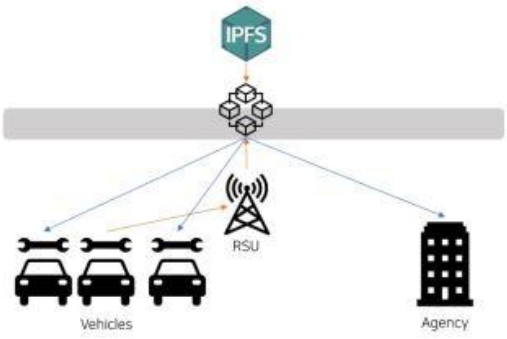
	Public Blockchain	**Private Blockchain**
네트워크	P2P network	Private network
열람권한	누구나 가능	허가된 사용자만
속도	낮음	빠름
비용	높음	낮음

3) IPFS(Inter-Planetary File System)

IPFS 는 상호 연결된 분산 파일 시스템으로 콘텐츠 자체가 주소 역할을 하는 content-addressing 방식을 사용한다. IPFS 를 활용하면 고용량의 파일을 빠르고 효율적으로 저장할 수 있다는 이점이 있으며, 무결성, 위조방지 및 탈중앙화의 효과를 얻을 수 있다. IPFS 는 주로 블록체인에 담기에는 무거운 파일들을 저장하는 오프체인 저장소의 역할을 한다[5].

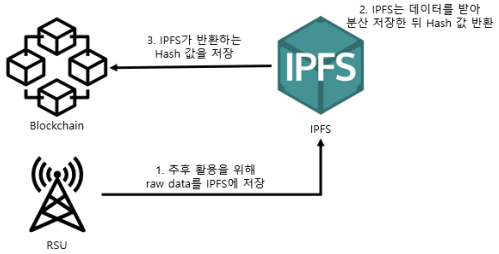
3. VANET 환경에서의 블록체인 기반 교통정보시스템

본 논문에서는 VANET 환경에서의 블록체인 기반 교통정보시스템을 제안한다. (그림 1)은 제안하는 시스템의 구조를 간략하게 나타낸 그림이다.



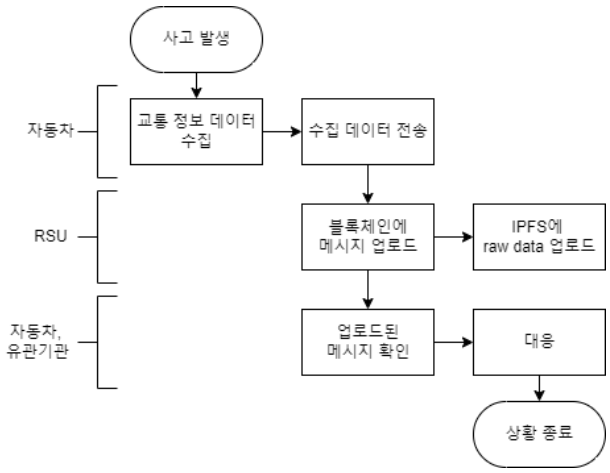
(그림 1) 제안하는 시스템의 구조

해당 시스템은 VANET 의 자동차, RSU, 유관 기관이 블록체인 네트워크로 연결되어 있고, 상위에는 IPFS 가 존재하는 구조이다. 자동차 센서가 실시간으로 이벤트를 감지하면 RSU 에 해당 센서 데이터들을 보낸다. RSU 는 데이터를 받아 이를 다른 자동차와 유관 기관에 알려야 한다. 이때, RSU 는 자동차와 유관 기관이 알아야 하는 메시지를 블록체인에 업로드한다. RSU 가 블록체인에 메시지를 업로드하면 블록체인 내의 모든 네트워크가 해당 내용을 확인할 수 있다. 또한, RSU 는 컴퓨팅 능력이 충분하지 않은 통신만을 위한 장치이므로 자동차가 전달한 raw data(원시 데이터)를 IPFS 에 업로드한다. 이러한 방식을 통해 데이터를 안전하게 저장하여 이후 더 고도화된 시스템을 목표로 하는 학습에 사용될 수 있도록 한다. (그림 2)는 RSU 가 raw data 를 IPFS 에 저장하는 과정을 간단하게 도식화한 그림이다.



(그림 2) 학습을 위한 raw data 저장 과정

RSU 는 자동차가 전달한 raw data 를 IPFS 에 저장한다. IPFS 는 RSU 로부터 데이터를 받아 분산 저장한 뒤 데이터에 접근할 수 있도록 hash 값을 산출하여 반환하고, 이 hash 값은 블록체인에 저장된다. 이렇게 IPFS 에 저장된 다양한 차량의 센서 데이터들은 학습 데이터로 사용이 가능하며, 이러한 학습 데이터들을 통해 교통 흐름 예측 모델 등을 구축하여 시스템의 효율성과 편의성, 정확도 등을 개선할 수 있다.



(그림 3) 블록체인을 기반으로 한 시스템 흐름도

(그림 3)은 데이터 수집 및 전송, 블록체인을 통한 메시지 업로드와 확인을 포함한 일련의 과정을 나타낸 흐름도이다. 위의 흐름도와 함께 예상 시나리오를 제시하고자 한다. 특정 위치에서 차량 추돌 사고가 발생했다고 가정했을 때, 차량 센서는 사고를 감지하고 센서가 수집한 데이터를 RSU 에 전송한다. RSU 는 해당 데이터를 수신하고 사고를 인지하여 해당 내용을 전달하기 위해 사고 발생 메시지를 블록체인에 업로드할 뿐만 아니라, Raw data 를 IPFS 에 업로드한다. 블록체인에서 RSU 가 추가한 메시지를 확인한 네트워크 내의 노드들은 사고 발생 정보를 확인하여 조치한다. 자동차는 차선을 변경하거나 경로를 우회할 수 있고, 유관 기관은 사고 수습을 위한 인력을 보내는 등의 대응을 할 수 있을 것이다. IPFS 를 통해 저장되는 데이터들은 시스템 개선 및 발전을 위한 학습에 사용된다.

Transaction (Tx)
TIME
Message ID
RSU ID
Message Type
Message Content
Sensor ID
IPFS Hash

(그림 4) 트랜잭션 구성 요소

(그림 4)는 블록체인 원장에 기록되는 트랜잭션의 구성을 보여준다. 블록체인 원장에서 트랜잭션에 포함되는 구성요소이다. 먼저 데이터를 수집한 센서에 대한 정보와 RSU 가 전달하고자 하는 메시지의 ID 가 필요하다. 또한, 트랜잭션에 RSU 의 ID 를 기록하여 메시지의 발생위치를 확인할 수 있도록 한다. 블록체인에 참여하는 노드들은 메시지의 Type 과 Content 를 통해 어떤 유형의 상황인지와 그 자세한 내용을 확인하여 대응할 수 있다. 그뿐만 아니라 IPFS 에 업로드하는 데이터의 주소를 함께 저장하여 이후 활용할 수 있도록 한다. 용량이 큰 데이터는 오프체인 스토리지를 사용하여 별도로 저장함으로써 속도를 향상시킬 수 있다.

4. 성능 분석

본 시스템은 기존 중앙서버 시스템 대신 VANET 과 블록체인을 적용하여 실시간성을 보장한다. 제안 시스템의 효율성 및 보안성에 대한 분석은 다음과 같다.

1) 효율성 분석

가장 먼저 기존의 교통정보시스템과 비교하였을 때, 중앙 서버에 의지하는 방식이 아니기 때문에 비교적 신속하게 정보를 주고받을 수 있다. 기존의 VANET 환경 시스템은 노드 간에 통신하며 메시지를 전달하는 방식이었으나, 본 시스템의 경우 메시지를 전달하고 수신하는 것이 아닌 블록체인에 업로드 된 메시지를 확인하는 방식으로, 노드 간의 통신이 불필요하여 네트워크 오버헤드를 감소시킬 수 있으며 이를 통해 현재 VANET 의 가장 근본적인 문제인 broadcast storm 문제를 해결할 수 있다[2]. 또한, 기존의 VANET 시스템의 경우 원거리의 노드들까지는 메시지가 도착하지 않거나, 뒤늦게 네트워크에 합류한 경우 이전 메시지가 누락될 위험이 있다. 본 연구는 이러한 문제를 블록체인을 활용함으로써 비교적 원거리의 노드에도 메시지가 전달되도록 하고, 합류 시점에 관계없이 필요 정보를 제공함으로써 서비스의 질을 향상시킬 수 있다는 장점을 갖는다.

2) 보안성 분석

보안 측면에서는 RSU 가 직접 노드에 전송하는 것이 아니라 블록체인에 기록함으로써 RSU 가 네트워크 내의 다른 노드로 전달하고자 하는 메시지의 위조 공격을 방어할 수 있으며 같은 이유로 공격자가 메시지를 다시 재생하여 전송하는 재전송 공격을 방어할 수 있다[1]. 또한, 기존 시스템의 경우 중앙 서버에 의지하고 있어 서버가 DDoS 와 같은 공격을 당할 경우 교통정보를 실시간으로 받지 못할 수가 있다. 하지만 본 시스템은 VANET 환경에서 블록체인을 도입하여 중앙 서버에 의지하지 않은 탈중앙화 환경을 만듦으로써 서버 공격에 의한 서비스의 지연 및 마비를 방지할 수 있다.

<표 2> 보안 측면에서의 성능 분석

공격	설명	방어 방법
위조 공격	전송되는 데이터를 변경하는 공격	RSU 가 전달하고자 하는 메시지를 블록체인에 올려 메시지의 무결성 보장
재전송 공격	유효한 데이터를 가로채서 재전송하는 공격	메시지를 주고받지 않고, 블록체인에 올라간 메시지를 열람하는 방식으로 방어
DDos 공격	중앙 서버에 대량의 트래픽을 발생 시켜 서버가 제대로 동작하지 못하도록 하는 공격	중앙 집중 서버를 사용하지 않고, 분산화시켜 단일 서버를 노리는 공격 불가

5. 결론

자율주행자동차의 발전과 함께 지능형 교통 체계 ITS 의 필요성이 점차 커지고 있다. 특히 돌발 상황과 사고에 대응이 가능하도록 하는 교통정보시스템은 현대의 교통 체계에서 필수적인 요소가 되었다. 기존 교통정보시스템의 중앙화로 인한 문제 뿐만 아니라 VANET 기반의 시스템이 가지고 있는 네트워크 문제들을 완화하고 보안성을 높이기 위해 본 논문에서는 VANET 환경에서 블록체인을 적용하여 노드들에 돌발 상황을 알리는 교통정보시스템을 제안하였다. 해당 시스템은 블록체인과 IPFS, VANET 노드들로 이루어져 있으며, 차량의 데이터를 RSU 가 받아 네트워크 내의 다른 노드들에 전달하기 위해 블록체인에 메시지를 담은 트랜잭션을 기록하는 방식으로 동작한다. 이후 서비스 고도화를 위하여 데이터를 별도로 IPFS 에 저장한다. 본 시스템을 통해 노드 간 메시지 전송으로 인한 네트워크 오버헤드를 줄일 수 있고, 분산화로 인한 단일 서버 공격을 방어할 수 있으며 이외에도 위조 공격, 재전송 공격 등을 방어할 수 있다. 뿐만 아니라 앞으로 기존 차량을 빠르게 대체할 자율주행 자동차를 서비스하는 교통정보시스템에서 매우 효율적인 구조로 활용될 수 있다. 향후, 제안 시스템의 시뮬레이션을 통해 좀 더 구체적인 성능 분석을 수행하고, IPFS 에 저장된 data 를 이용한 학습을 통해 교통흐름 예측 모델을 구축하여 교통시스템의 효율성을 더 높일 수 있는 방안에 대한 연구를 진행하고자 한다.

Acknowledgement

이 논문은 2020 년도 정부(과학기술정보통신부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구임 (No. 2020R1A2C1006497). (교신저자: 도인실)

참고문헌

[1] Abdul Quyoom, Aftab Ahmad Mir, Dr.Abid Sarwar, “Security Attacks and Challenges of VANETs : A Literature Survey”, Journal of Multimedia Information System, VOL. 7, NO.1, pp.45-54, 2020.

[2] 박상면, 문영성, "VANET 에서 Clustering 기법을 이용한 Emergency 메시지 전달 방안”, 한국차세대컴퓨팅학회 논문지, vol.15, no.2 pp.29-38, 2019.

[3] Chao Wang, Xiaoman Cheng, Jitong Li, Yunhua He and Ke Xiao, “A survey: applications of blockchain in the Internet of Vehicles”, EURASIP Journal on Wireless Communications and Networking, 77, 2021.

[4] 김문성, 나은찬, 이장훈, 이우찬, “실시간 지능형 교통 시스템에 적합한 블록체인 기술 및 네트워크 구조”, 디지털산업정보학회 논문지, 제 14 권 제 4 호, pp.17-26, 2018.

[5] R.Wang, W. – T. Tsai, J. He, C. Liu, Q. Li and E. Deng, “A Video Surveillance System Based on Permissioned Blockchains and Edge Computing”, 2019 IEEE International Conference on Big Data and Smart Computing (BigComp), pp.1-6, 2019.