ITS 환경에서 신속하고 안전한 노드 검증을 위한 블록체인 기반 인증 시스템

김윤아, 허가빈, 도인실*
이화여자대학교
yunakim@ewhain.net, gjrkqls@ewhain.net, *isdoh1@ewha.ac.kr

Blockchain-based Authentication System for Rapid and Secure Node Verification in ITS Environments

Yuna Kim, Gabin Heo, Inshil Doh*
Ewha Womans University

요 약

데이터의 송수신 및 가공이 실시간으로 일어나는 ITS 환경에서는 대량의 데이터를 수집하고 활용해야 하며 이에 높은 비용이 요구된다. 본 연구에서는 ITS의 구성 노드에 대한 인증 절차를 경량화 및 가속화 하기 위하여 블록체인 시스템을 도입하고 Challenge-Response 인증 방식과 해시 함수를 활용하는 방안을 제안하고자 한다. 제안하는 시스템에서는 ITS의 중앙 관리 주체이자 신뢰 기관인 TA와 차량의 인증을 담당하는 RSU가 블록체인을 통해 노드의 주요 인증 정보를 공유한다. RSU는 인증 과정에서 차량에게 Challenge를 전송하고, 차량은 이를 적절히 활용하여 해시 함수 계산값인 Response를 도출한 뒤 RSU에게 제출한다. 이후, RSU는 스스로 계산한 해시값과 차량으로부터 수신한 Response를 비교하여 인증 여부를 결정한다. 제안 기법은 블록체인을 통해 개별 차량에 대한 민감한 데이터를 보호할 수 있으며, Challenge-Response 인증 방식의 장점인 빠른 인증 속도와 보안성 증대, 통신 비용 절감을 보장한다. 또한, Response 계산 시 해시 함수를 사용함으로써 계산 비용을 낮추고 개별 데이터의 무결성과 기밀성을 보장하여 신속하고 안전한 인증이 가능하도록 하였다.

Ⅰ. 서 론

ITS(Intelligent Transportation Systems)는 교통 인프라 및 제어 시스템에 정보 통신 기술을 접목하여 교통정보의 종합적인 수집, 가공 및 전파를 통해 심각한 교통 문제에 효과적으로 대응하는 시스템이다. ITS에서는 대량의 데이터가 실시간으로 수집 및 활용되는데, 이 과정에서 상당한 통신 비용과 계산 비용이 소모된다. 따라서 교통 체계의 혁신이라는 ITS의 목표를 효과적으로 달성하기 위해서는 구성 노드의 인증에 드는 비용을 절감하여 데이터 공유와 활용에 더 많은 자원을 할당하여야 한다.

기존 이동통신 환경에서 사용되는 셀룰러 기술은 서비스 공간을 정육각형의 셀로 분할하여 각 셀의 중심에 기지국을 배치한다. 각 셀 안에 존재하는 사용자는 해당 셀의 기지국과 통신하는데, 사용자가 하나의 셀 영역을 벗어나 인접 셀로 진입하면 통신하던 기지국이 변경되어야 한다. 이 작업을 핸드오버라고 부르는데, 일반적인 이동통신 환경의 경우 사용자가 빠른 속도로 이동하는 상황에서 핸드오버가 지연되거나 실패하고 Ping-pong 효과가 발생하는 문제점이 있어 이동장치의 원활한 신호 수신을 방해한다. ITS는 차량을 중심으로 교통정보를 수집하고 상호교환하는 시스템인 만큼 고속으로 이동하는 차량에서도 이동장치가 원활한 신호 수신을 할 수 있도록 적절한 핸드오버가 보장되어야 한다[1]. 또한, 민감한 데이터를 실시간으로 주고받을 수 있어야 하므로 통신과 계산에 자원을 우선 배분하는 한편 차량을 인증하는 비용을 반드시 절감해야 한다.

이러한 문제를 해결하기 위해 본 연구에서는 신속하고 안전한 노드 인증을 위해 블록체인 기술을 적용하고자 한다. 데이터가 분산된 원장에 암호화 및 연결되어 저장된 데이터 사슬인 블록체인은 저장된 트랜잭션이 블록체인 시스템의 모든 참여자에게 투명하게 공개된다는 특징을 가진다[2]. 이와 같은 특성으로 인해 본 연구에서 ITS 환경의 RSU와 TA(Trusted Authority)가 노드의 인증 정보를 신속하고 안전하게 공유할 수 있다. 또한, 해시 함수가 가지는 단방향성을 통해 민감한 데이터의 노출을 막고 계산과 검증 과정을 경량화하였다. 나아가 인증 주체가 송신한 Challenge에 대해 인증 대상이 올바른 Response를 제시함으로써 인증을 승인받게 되는 방식인 Challenge-Response 메커니즘을 통해 인증 과정에서 통신 속도와 비용을 개선하고 보안성을 강화하였다. Challenge-Response 방식을 사용하면 사용자 토큰과 Clock, Counter와 같은 동기를 유지할 필요가 없으며 빠른 인증이 가능하다는 장점이 있다. 또한 인증에 사용되는 Challenge 및 Response는 일회성으로 사용되는 값으로 발급 시점에서만 유효하기 때문에 공격자가 이러한 인증 정보를 탈취하더라도 이를 재사용하는 것이 불가능하여 재전송 공격이 불가하며 정보 유실에 대한 2차 피해가 발생하지 않는다[3].

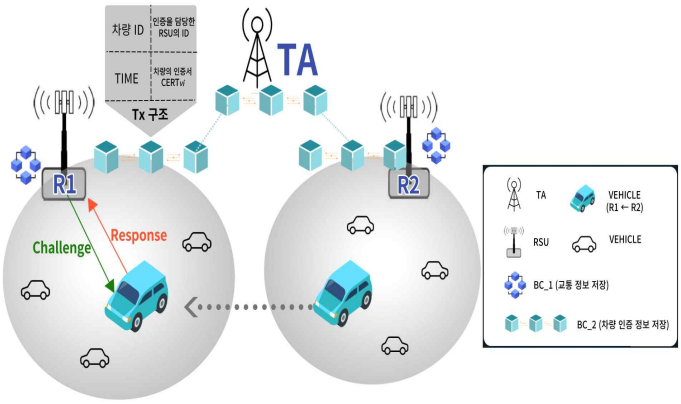
본 연구는 기존의 차량간 통신 네트워크 환경의 연구 동향과는 상이하게 RSU를 온전히 신뢰하지 않는다고 가정한다. RSU를 신뢰한다고 가정하는 기존 연구들[4]에서는 침입에 성공한 공격자가 RSU에 저장된 데이터를 추가, 삭제 및 변조할 수 있으므로 악의적인 차량에 대한 인증을 수행하는 등 심각한 보안 문제가 발생할 수 있었다[5]. 따라서 본 논문에서는 RSU가 공격 당하는 최악의 경우까지 모두 고려한 인증 메커니즘을 제안하고자 한다.

Ⅱ. 블록체인 기반 인증 메커니즘

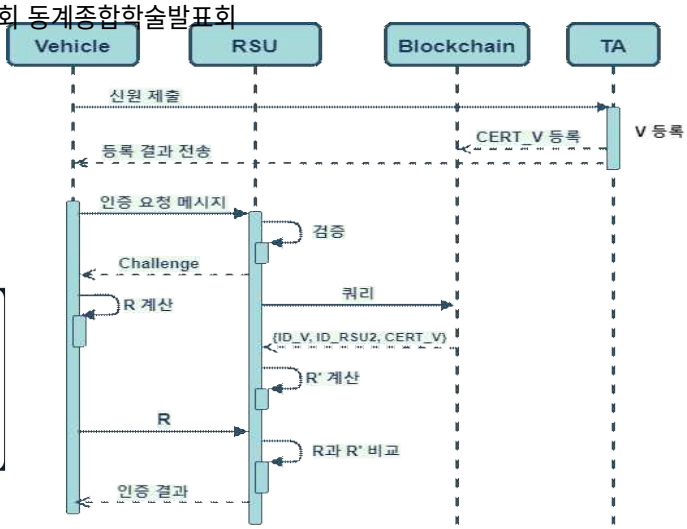
1. 시스템 환경 정의

본 논문에서 설정한 ITS 환경의 구성 요소로는 블록체인, TA(Trusted Authority), RSU(Road Side Unit), 차량이 있다.

먼저, 블록체인 시스템을 도입하여 민감한 데이터에 대한 무결성과 기밀성, 가용성을 보장하고자 하였다. 노드의 인증 과정에서 사용되는 정보는 블록체인상에 안전하게 저장되는데, 트랜잭션은 [그림 1]과 같이 차량의 ID, 해당 차량을 인증한 RSU의 ID, 차량의 인증서, 인증이 성사된 시각 정보로 구성되어 있다.



[그림 1] ITS 환경에서 차량의 구역 이동 발생 시 인증 절차



[그림 2] 제안하는 인증 시스템

ITS 전체를 통합 관리하는 단일 기관인 TA는 온전히 신뢰할 수 있으며 ITS가 처음 구축될 때 시스템을 초기화하며 TA와 RSU가 참여하는 블록체인을 구축한다. 또한, 새로운 차량을 시스템에 등록하고, 인증서를 발급하여 블록체인에 기록한다. 모든 차량은 ITS에 최초로 진입할 때 TA에 신원을 제출하고 등록 후 인증서를 발급받는 과정을 거쳐야 한다. ITS의 모든 서비스 공간은 구역 단위로 분할되며 각 구역은 단일 RSU에 의해 관리된다. RSU는 차량과의 통신을 통해 인증을 담당하며 인증이 끝나면 해당 정보가 담긴 트랜잭션을 발행한다. 이때 블록체인상에 저장된 인증 정보는 ITS 환경 내의 모든 참여자에게 공유되므로 RSU는 특정 차량이 어떤 구역을 거쳐서 진입하였는지 파악할 수 있다. RSU가 차량의 인증을 완료하면 해당 RSU의 ID가 블록체인에 기록된다. 이후 해당 차량이 새로운 구역으로 이동하여 재인증을 받을 때, 직전 구역에서 인증을 수행한 주체인 RSU의 ID는 Response 계산을 위한 입력값 중 일부로 사용된다.

2. 인증 과정

[그림 1]과 같이, RSU 2의 관리 구역인 R2(Region 2)에서 RSU 1의 관리 구역인 R1(Region 1)으로 이동한 차량 V가 RSU 1에 의해 새롭게 인증을 받는 과정은 다음과 같다.

(1) 가장 먼저 V가 RSU 1에 인증 요청 메시지를 전송하면 RSU 1은 이를 수신하여 검증한 다음, V에게 Challenge 값을 보낸다.

(2) Challenge를 수신한 V는 *R*(Response)을 계산하여 RSU 1에 전송한다. *R*의 계산식은 다음과 같다.

$$R = H(Challenge||ID\_V||ID\_RSU2||time||CERT\_V)$$

이때 H는 시스템 초기화 단계에서 TA가 지정한 해시 함수며 *Id_V*는 V의 ID, *ID_RSU2*는 V의 직전에서 V를 인증해준 RSU 2의 ID, *time*은 현재 시각, *CERT_V*는 TA가 V에 부여한 인증서이다.

(3) 만약 기존 인증 이력이 없는 차량일 경우, 직전에 자신을 인증해준 RSU의 ID를 TA의 ID로 대체하여 계산을 수행한다.

(4) RSU 1이 블록체인에 *Id_V*, *ID_RSU2*, *CERT_V*를 쿼리하고, 쿼리 결과를 바탕으로 R' 값의 계산을 수행한다.

(5) RSU 1이 스스로 계산 결과와 V로부터 수신한 *R*값의 비교를 통해 V의 인증 여부를 결정한다.

(6) RSU 1이 V에 인증 성공 또는 거부 결과를 전송하고, 인증이 정상적으로 이루어졌을 경우 블록체인에 해당 정보를 담은 트랜잭션을 올린다.

[그림2]는 제안하는 인증과정을 간단히 표현한 것이다. 이와 같이 신속하고 안전한 인증 절차를 거친 각 노드는 ITS에서 수집한 정보를 상호교환하고 재가공하여 교통의 질을 높이는 데 기여한다.

Ⅲ. 결론 및 향후 연구

본 연구에서는 블록체인 시스템을 도입하여 인증에 사용되는 데이터를 저장함으로써 RSU와 TA 간의 통신에 드는 비용을 절감하였으며, 데이터의 무결성을 보장하고 접근 속도를 향상하고자 하였다. 또한 해시 함수가 가지는 단방향성이라는 특성을 이용하여 차량의 ID나 인증서와 같은 민감한 데이터가 공격에 노출되는 것을 막았으며 response 값의 계산과 검증에 드는 시간과 비용을 줄여서 인증 과정을 경량화하였다. 마지막으로, Challenge - Respnse 인증 방식을 통해 RSU와 차량 사이의 통신 비용을 감소시켜서 기존의 차량 인증 메커니즘보다 가볍고 빠른 인증이 가능하도록 하였다. 나아가 Challenge - Respnse 인증 방식을 사용하면 공격자가 중간에서 response 값을 스니핑 하더라도 이를 재사용 하는 것이 불가능하기 때문에 재전송 공격을 막을 수 있으므로 안전한 인증이 이루어질 수 있다.

향후 연구로는 시뮬레이션을 통해 제안된 환경을 구축하여 안전성 및 신속성을 검증할 예정이며, challenge-response 인증 단계에서 발생할 수 있는 취약점을 추가 분석하여, 이에 대한 대응 방안을 도출하고자 한다.

ACKNOWLEDGMENT

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

참 고 문 헌

[1] 정영교. (2015). 고속 환경에서 원활한 LTE 핸드오버를 위한 기법, 한국컴퓨터정보학회 동계학술대회 논문집, 23(1), 255-258.

[2] 이동영, 박지우, 이준하, 이상록, 박수용. (2017). 블록체인 핵심 기술과 국내외 동향, 정보과학회지, 35(6), 22-28.

[3] Young Soo Kim, Byoung Yup Lee. (2018). Challenge-Response based Authentication Model for Cloud Computing. 한국콘텐츠학회 ICCC 논문집, (), 237-238.

[4] Wang, S., Yao, N. (2019). A RSU-aided distributed trust framework for pseudonym-enabled privacy preservation in VANETs. Wireless Netw 25, 1099 - 1115.

[5] Z. Yang, K. Yang, L. Lei, K. Zheng, V. C. M. Leung. (2019). Blockchain-Based Decentralized Trust Management in Vehicular Networks, IEEE Internet of Things Journal, 6(2), 1495-1505.