차량 네트워크 보안을 위한 블록체인 기반 분산 보안 프로토콜 동향

추호은 [1], 오현영 [2*]
[1] 가천대학교 인공지능전공 학부생
[2] 가천대학교 인공지능학과 교수

{hoeun8793, hyoh}@gachon.ac.kr

A Survey on Blockchain-Based Distributed Security Protocols for Automotive Network Security

Hoeun Choo, Hyunyoung Oh*
Dept. of AI, Gachon University

요 약

본 연구는 자동차 네트워크 보안을 위한 키 관리 동향을 살펴보고, 특히 블록체인 기반 분산 구조를 적용한 최신 프로토콜을 고찰한다. 기존 중앙집중형 보안의 한계를 짚은 뒤, 분산 키 관리, 메시지 보호, 트랜잭션 검증, 이상 탐지 연계 등의 핵심 설계 요소를 제시한다. 특히 최근 제안된 블록체인과 AI 융합 보안 프로토콜을 중심으로, 블록체인이 보안성과 신뢰성 강화를 어떻게 지원하는지를 논의하며, 관련 연구와의 비교를 통해 향후 연구 방향을 모색한다.

1. 서론

SOME/IP 는 자동차 내부의 서비스 지향 통신을 지원하는 핵심 프로토콜로, 최근 다양한 보안 확장 연구가 수행되어 왔다. 예컨대 Iorio et al.[1]은 서비스 메시지 보호와 ECU 관리 보안을 제안하였지만, 중앙집중식 키 관리 구조에 의존함으로써 확장성과 신뢰성 측면에서 한계가 드러났다. Khemissa et al.[5] 역시 ECU 보안 관리 아키텍처를 제안했으나 동일한 문제에서 자유롭지 않았다. 이러한 한계를 극복하기 위해 블록체인 기반 접근이 점차 주목받고 있다. Chen et al.[2]은 공급망 보안 관리에 블록체인을 도입하여 무결성과 투명성을 강화하였고, Wang et al.[3]은 VDKMS 라는 분산 키 관리 시스템을 통해 차량 네트워크에서 탈중앙화 가능성을 제시하였다. 그러나 이들 연구는 부분적 적용에 머무르거나 실시간성, 효율성 검증에 있어 미흡한 점이 존재한다.

이와 달리 Lee et al.[4]은 블록체인 기반 분산 키 관리와 딥러닝 기반 이상 탐지를 통합한 새로운 보안 프로토콜을 제안하였다. 이 연구는 블록체인의 불변성과 투명성을 차량 네트워크 환경에 적용하는 동시에, 인공지능 기반 탐지를 결합하여 기존 연구보다 실용적이고 포괄적인 아키텍처를 제시한다는 점에서 주목할 만하다. 따라서 본 논문은 [4] 연구를 중심으로 블록체인 기반 자동차 네트워크 보안 프로토콜의 구조와 특징을 심층적으로 살펴보고, 기존 연구들과 비교하여 그 의의를 밝히고자 한다.

2. 블록체인 프로토콜

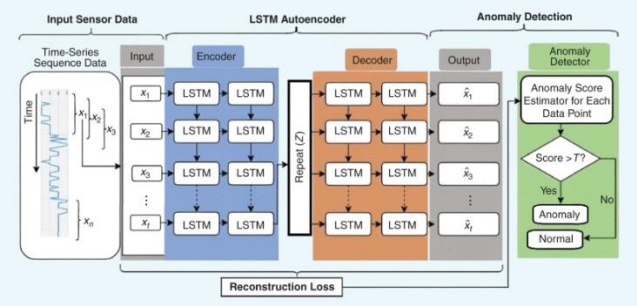
2-1. 블록체인 기술 개요

블록체인은 네트워크 내 여러 노드에 데이터가 분산 저장되고 합의 알고리즘을 통해 거래의 진위와 무결성을 보장하는 분산 원장 기술이다. 각 블록은 블록 헤더, 타임스탬프, 이전 블록의 해시 값, 거래 내역으로 구성되며, 암호학적으로 연결되어 체인 형태를 이루기 때문에 일단 기록된 데이터는 변경이 사실상 불가능하다. 이러한 구조는 데이터의 불변성을 확보하고, 중앙 서버 없이 다수의 노드가 공동으로 신뢰를 유지하는 탈중앙화를 가능하게 하며, 모든 참여자가 거래 기록을 공유하고 검증함으로써 투명성을 제공한다[2].

* 교신저자

합의 알고리즘으로는 권위 증명(Proof of Authority), 실용적 비잔틴 장애 허용(pBFT), 작업 증명(Proof of Work) 등이 널리 알려져 있다. 그러나 자동차 네트워크 환경에서는 낮은 지연 시간과 자원 효율성이 필수적이므로, 경량화된 합의 구조가 필요하다. 이러한 블록체인의 불변성, 탈중앙성, 투명성은 차량 간 신뢰성 있는 메시지 교환, 세션 키 관리, 공격 탐지 및 분석을 위한 최적화된 보안 환경을 조성하는 기반이 된다[3].

2-2. 블록체인 기반 자동차 프로토콜 설계



(그림 1) LSTM 기반 이상 탐지 동작

블록체인 기반 자동차 보안 프로토콜의 대표적 사례는 Lee et al.[4]의 연구이다. 이들은 블록체인 분산 원장 구조를 바탕으로 키 관리, 메시지 보호, 트랜잭션 검증, 그리고 인공지능 기반 이상 탐지를 통합한 프레임워크를 제안하였다. 우선 분산 세션 키 분배 단계에서는 블록체인 원장을 통해 키를 안전하고 투명하게 배포하며, 참여자 인증서를 검증하여 재생 공격과 키 노출 위험을 차단한다. 메시지 보호 단계에서는 각 메시지의 무결성과 기밀성을 확보하고, 메시지 해시와 트랜잭션 상태를 블록체인에 기록하여 위변조를 탐지한다. 또한 트랜잭션 기록 및 검증 단계에서는 모든 보안 이벤트를 블록체인에 기록하고 합의를 통해 무결성을 보장함으로써 감사 가능성과 투명성을 강화한다.

마지막으로 이상 탐지 기능은 블록체인 원장과 인공지능 기법을 결합하여 신뢰성 있는 보안 대응을 지원한다. 그림 1 은 Lee et al.[4]에서 제안한 LSTM 오토인코더 기반 이상 탐지 과정을 보여준다. 입력된 차량 네트워크 데이터는 LSTM 오토인코더를 통해 정상 패턴과 비교되며, 복원 오차가 일정 기준을 초과할 경우 잠재적 공격이나 이상 징후로 판정된다. 이 탐지 결과는 블록체인 원장에 기록되어 위변조가 불가능한 형태로 관리되고, 이후 보안 분석 및 대응의 신뢰성을 높인다. 이처럼 [4]의 아키텍처는 블록체인의 불변성과 탈중앙성을 기반으로 키 관리와 메시지 보호를 구현하는 동시에, LSTM 기반 이상 탐지를 통해 실시간 대응력을 확보함으로써 기존 연구보다 포괄적이고 실용적인 보안 체계를 제시한다.

2-3. 기존 연구와의 비교

앞서 언급한 기존 연구들은 각기 다른 측면에서 블록체인 또는 보안 아키텍처를 제안하였으나 제한된 범위에 머무른다. Iorio et al.[1]은 SOME/IP 기반 메시지 보호 방안을 제시했지만 중앙집중 구조에 의존했고, Chen et al.[2]은 공급망 관리 차원에서 블록체인의 응용 가능성을 보여주었으나 차량 네트워크 특유의 실시간성 요구에는 대응하지 못했다. Wang et al.[3]은 분산 키 관리의 가능성을 보여주었으나 실험적 검증은 부족했으며, Khemissa et al.[5]은 ECU 보안 관리 구조를 제안했으나 분산성 확보에는 한계가 있었다. 이에 비해 Lee et al.[4]은 블록체인과 인공지능을 결합하여 분산 키 관리, 메시지 보호, 트랜잭션 검증, 이상 탐지까지 포괄하는 통합적이고 실용적인 프레임워크를 제시한 점에서 차별화된다.

3. 결론

차량 네트워크 보안을 위한 블록체인 기반 분산 키 관리와 보안 프로토콜의 동향을 살펴보았다. 특히 Lee et al.[4]의 연구는 키 관리, 메시지 보호, 트랜잭션 검증, 이상 탐지를 통합한 대표적 사례로, 기존 중앙집중형 접근의 한계를 넘어서는 가능성을 제시한다. 다만 실제 차량 환경에서의 실시간성 검증과 통합적 키 관리 체계 확립은 여전히 과제로 남아 있으며, 향후 연구는 이러한 실용적 검증과 확장을 통해 블록체인 보안이 차세대 자동차 네트워크의 신뢰성을 뒷받침하는 핵심 기술로 자리잡도록 해야 한다.

사사문구

이 논문은 2025 년도 정부(과학기술정보통신부)의 재원으로 정보통신기획평가원의 지원(No. RS-2024-00337414, SW 공급망 운영 환경에서 역공학 한계를 넘어서는 자동화된 마이크로 보안 패치 기술 개발)과 한국산업기술기획평가원의 지원(No. RS-2024-00406121, 자동차보안취약점기반위협분석시스템개발(R&D))을 받아 수행된 연구 결과임.

참고문헌

[1] Marco Iorio, Massimo Reineri, Fulvio Risso, Riccardo Sisto, Fulvio Valenza, “Securing SOME/IP for In-Vehicle Service Protection,” IEEE Transactions on Vehicular Technology, vol. 69, no. 11, pp. 13450–13466, Nov. 2020.

[2] W. Chen, Y. Liu, J. Ma, “Connected Vehicle Security Blockchain Solutions for Enhancing Physical Flow in the Automotive Supply Chain,” Computers, Software and Applications Conference (TechScience), 2025.

[3] G. Wang, X. Li, Y. Qin, “VDKMS: Vehicular Decentralized Key Management System for Cellular V2X Communications,” arXiv preprint, arXiv:2310.12381, 2023.

[4] G. Y. Lee, J. H. Kim, S. H. Lee, “A Secure, Blockchain-Enabled Vehicular Sensor Communication Protocol With Deep Learning-Assisted Anomaly Detection,” IEEE Intelligent Transportation Systems Magazine, 2025.

[5] Hamza Khemissa, Pascal Urien, “Centralized architecture for ECU security management in connected and autonomous vehicles,” International Conference on Telecommunications (ICTC), 2022.