자동차 데이터 보안을 위한 효율적인 분산형 암호 키 관리 연구 동향

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

Hoeun8793@gachon.ac.kr, hyoh@gachon.ac.kr

Efficient Distributed Encryption Key Management for Automotive Data Security: Research Trends

Hoeun Choo[1], Hyunyoung Oh[2]
[1]Dept. of Artificial Intelligence, Gachon University
[2]Dept. of Artificial Intelligence, Gachon University

요 약

본 연구는 자동차 데이터 보안을 위한 키 관리 기법의 최신 동향을 분석한다. 중앙집중형, 분산형, 그리고 블록체인 기반의 키 관리 방식을 비교 분석하며, 각 방식의 기술적 특징과 장단점을 심도 있게 고찰한다. 특히 차량 내부 통신과 차량 간 통신 보안을 통합적으로 고려하는 접근 방식의 필요성을 강조한다.

1. 서론

자동차 산업의 급속한 발전으로 커넥티드 카와 자율주행차량의 보급이 확대되면서, 차량 데이터의 보안이 중요한 이슈로 대두되고 있다. 특히 차량 내부 네트워크와 차량 간 통신의 복잡성 증가로 인해, 효율적이고 안전한 키 관리 기법의 필요성이 더욱 강조되고 있다. 현재 차량 네트워크 보안 접근 방식은 크게 중앙집중형과 분산형으로 나뉘며, 최근에는 블록체인 기술을 활용한 새로운 방식도 제안되고 있다. 본 논문에서는 이러한 다양한 접근 방식의 기술적 특징과 장단점을 분석하고[1-4], 차량 내/외부 통신을 아우르는 통합적 보안 솔루션의 필요성을 제시한다.

2. 키 관리 기법

2-1. 중앙집중형 키 관리

중앙집중형 키 관리 방식은 하나의 중앙 관리 장치가 모든 ECU 의 키를 관리하는 방식이다. Khemissa 와 Urien [1]이 제안한 중앙집중형 아키텍처는 안전한 세션 키 합의를 보장하며, 공격자가 비밀 키 없이는 세션 키를 계산할 수 없도록 설계되었다.

이 방식의 주요 장점은 키 관리의 효율성과 구현의 단순성이다. 중앙 장치가 모든 키를 관리하므로 키 분배와 갱신이 용이하며, 각 ECU 는 중앙 장치와의 통신만 고려하면 되어 구현이 상대적으로 간단하다. 또한, ECU 에 요구되는 계산 능력과 저장 공간이 적어 리소스 효율성이 높다.

그러나 이 시스템의 주요 단점은 중앙 데이터 센터에 과도하게 의존한다는 점이다. 데이터 센터에 문제가 발생하면 전체 네트워크가 위험에 처할 수 있는 단일 장애점(Single Point of Failure) 문제가 존재한다. 또한, 네트워크 규모가 커질수록 중앙 서버의 부하가 증가하여 확장성에 제약이 생길 수 있다.

2-2. 분산형 키 관리

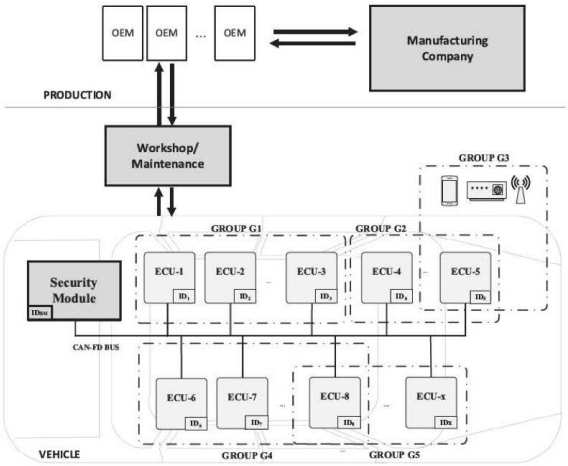
분산형 보안 관리는 중앙 서버 없이 각 ECU 가 자체적으로 키를 관리하는 방식으로, 중앙집중형 보안 관리보다 더 높은 보안성을 제공한다. 그림 1 은 전자제어 장치(ECU)가 기능별로 CAN-FD 버스를 통해 통신하는 차량 내 네트워크 구조를 보여준다.

Carvajal Roca 등 [2]이 제안한 준중앙화 프레임워크의 주요 장점은 높은 보안성과 유연성이다. 각 ECU 가 독립적으로 키를 관리하므로 단일 장애점 문제를 해결할 수 있으며, 차량 운행 중에도 동적으로 키를 생성하고 관리할 수 있다. 또한, 제조 및 유지보수 과정에서 중앙 키 관리 시스템을 재구성할 필요 없이

* 교신저자

ECU 를 업데이트하거나 서비스할 수 있어 시스템의 유연성이 높다.

그러나 이 방식의 단점으로는 각 ECU 의 계산 부하 증가와 키 동기화의 복잡성을 들 수 있다. 또한, ECU 간 직접 통신이 증가함에 따라 전체 네트워크 트래픽이 증가할 수 있으며, 완전한 탈중앙화가 아닌 준중앙화 구조이기 때문에 여전히 부분적인 중앙 관리 요소가 존재한다.



(그림 1) CAN-FD 버스를 통해 통신하는 차량 내 네트워크

2-3. 블록체인 기반의 분산형 키 관리

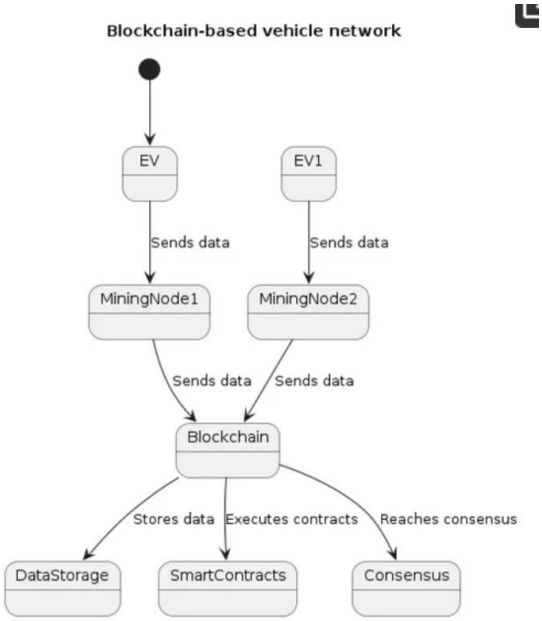
블록체인 기술을 적용한 키 관리 방식은 대규모 차량 네트워크를 위한 기존 보안 조치의 한계를 극복하는 것을 목표로 한다. 그림 2 는 The Proof of Authority (PoA) 합의 메커니즘을 사용한 블록체인 기반 차량 네트워크 아키텍처를 보여준다.

Aldweesh [3]와 Lin [4]이 제안한 블록체인 기반 접근 방식의 주요 장점은 높은 보안성, 투명성, 그리고 확장성이다. 분산 원장 기술을 통해 데이터의 무결성을 보장하고, 모든 거래가 투명하게 기록되어 추적 가능하다. 또한, 중앙 관리 주체 없이도 대규모 네트워크에서 효율적인 키 관리가 가능하다.

그러나 이 방식의 단점으로는 실시간 처리 요구사항을 충족시키기 어려울 수 있다는 점이다. 블록체인의 합의 과정으로 인한 지연이 발생할 수 있으며, 스토리지 수요가 증가하여 리소스 관리에 부담이 될 수 있다. 또한, 기존 차량 시스템에 블록체인 기술을 도입하기 위해서는 상당한 인프라 변경이 필요할 수 있다.

3. 결론

자동차 데이터 보안을 위한 키 관리 기법은 중앙집중형에서 분산형, 그리고 블록체인 기반으로 빠르게 발전하고 있다. 각 접근 방식은 고유한 장단점을 가지고 있어, 차량 시스템의 특성과 요구사항에 따라 신중히 선택해야 한다.



(그림 2) 블록체인 기반 차량 네트워크 아키텍처

중앙집중형 방식은 구현이 간단하고 효율적인 키 관리가 가능하지만, 단일 장애점 문제와 확장성 제약이 있다. 분산형 방식은 높은 보안성과 유연성을 제공하지만, ECU 의 계산 부하 증가와 키 동기화의 복잡성이 단점으로 작용한다. 블록체인 기반 방식은 탈중앙화, 투명성, 부인 방지 등의 장점을 제공하지만, 실시간 처리 요구사항 충족과 리소스 관리에 대한 과제가 남아있다.

현재 연구들은 차량 내부 통신과 차량 간 통신 보안을 개별적으로 다루는 경향이 있다. 그러나 향후 연구에서는 이 두 영역을 통합적으로 고려하는 접근 방식이 필요하다. 차량 네트워크의 전체 생태계를 강화하는 총체적인 보호 전략을 제공하기 위해서는 내부와 외부 통신을 아우르는 통합적 키 관리 솔루션 개발이 필수적이다.

사사문구

이 논문은 2024 년도 정부(산업통상자원부)의 재원으로 한국산업기술기획평가원의 지원(No. RS-2024-00406121, 자동차보안취약점기반위협분석시스템개발(R&D))과 정부(과학기술정보통신부)의 재원으로 한국연구재단의 지원(No. RS-2022-00166529)을 받고 과기정통부 정보통신기획평가원의 정보보호핵심원천기술개발사업(No. RS-2024-00337414)으로 수행한 결과임.

참고문헌

[1] Hamza Khemissa, Pascal Urien, “Centralized architecture for ECU security management in connected and autonomous vehicles,” ICTC, 2022

[2] I. E. C. Roca et al., "A Semi-centralized Security Framework for In-Vehicle Networks," IWCMC, 2020

[3] Amjad Aldweesh, "A Blockchain-Based Data Authentication Algorithm for Secure Information Sharing in Internet of Vehicles," World Electric Vehicle Journal, 2023

[4] Hua Yi Lin, "Secure Data Transfer Based on a Multi-Level Blockchain for Internet of Vehicles," Sensors, 2023