CAN 및 CAN-FD 통신을 위한 최소 연산량 기반의 경량 동적 암호화 기법

이원영, 이성수*
숭실대학교

soulious@soongsil.ac.kr, *sslee@ssu.ac.kr

A Lightweight Dynamic Encryption Scheme with Minimal Computational Cost for CAN and CAN-FD Systems

Lee wonyoung, Lee seongsoo*
Soongsil Univ., *Soonsil Univ.

요 약

Controller Area Network(CAN)와 CAN-FD 는 차량 ECU 간 핵심 통신 프로토콜이지만 기본 암호화 기능 부재로 공격에 취약하다 [1]. 기존 보안 기법은 추가 메시지, 프레임 변경, 복잡한 키 관리 등을 요구하여 오버헤드가 발생한다 [2][6].

본 논문은 기존 프레임을 유지한 상태에서 데이터 첫 바이트를 암호 제어 및 인덱스로 사용하는 경량 동적 암호화 기법을 제안한다. 암호화 활성화 시 나머지 페이로드는 8 바이트 블록으로 정규화되며 경량 블록 암호 기반 keystream XOR 방식으로 처리된다 [3][4]. 또한 CAN ID 별 동기 카운터와 제어 값을 결합해 동일 데이터가 반복되어도 매 전송마다 상이한 암호문이 생성된다. 제안 방식은 추가 프레임 없이 동기 유지 기능을 제공하며 ECU 환경에서 최소 연산량으로 동작해 실시간 적용이 가능하다 [5].

Ⅰ. 서 론

Controller Area Network(CAN)와 CAN-FD 는 차량 내 전자제어장치 간 핵심 통신 프로토콜로 널리 사용되고 있다 [1]. 그러나 기본적인 기밀성 및 인증 기능이 없어 스푸핑, 위장, 재전송 공격 등 다양한 위협에 노출될 수 있다.

이를 해결하기 위한 메시지 인증 코드(MAC) 및 암호화 적용 연구가 진행되어 왔으나, 추가 메시지 또는 프레임 변경이 필요해 버스 부하와 실시간성 저하가 발생한다 [2][6]. 또한 AES-128 과 같은 고연산 알고리즘은 자원 제약 ECU 환경에서 상당한 구현 부담을 유발한다 [5].

본 논문은 이러한 한계를 해결하기 위해 기존 CAN/CAN-FD 프레임 구조를 유지한 채 최소 연산량으로 암호화를 수행하는 경량 방식의 보안 기법을 제안한다. 제안 방법은 데이터 첫 바이트를 암호 제어 및 동기 인덱스로 사용하고, 이후 페이로드는 8 바이트 정규화된 블록에 대해 XOR 기반 keystream 방식으로 암·복호화된다 [3][4].

Ⅱ. 본론

본 장에서는 제안 기법의 구조와 동작 과정을 설명한다. 제안 기법은 CAN 및 CAN-FD 환경에서의 실제 구현을 고려하여, 프레임 처리 흐름을 단순화하고 연산량을 최소화하는 것을 목표로 설계되었다.

2.1 암호화 제어 바이트 기반 처리

제안 기법은 데이터 필드의 첫 번째 바이트 d0 를 암호화 제어 바이트(CCB)로 정의하고, 이를 기준으로 암호화 수행 여부 및 후속 처리를 결정한다. CCB 는 다음과 같이 구성된다.

EEB = d0[7], CI = d0[6:0]

여기서 EEB 는 암호화 활성화(enable) 비트를 의미하며, CI 는 암호화 인덱스 또는 동기화 명령으로 사용되는 7 비트 값이다. 수신 ECU 는 프레임 수신 직후 CCB 를 해석함으로써 암호화가 필요 없는 프레임에 대해서는 기존 처리 경로를 그대로 유지할 수 있다. 이 구조는 불필요한 암호 연산을 제거하여 처리 지연과 연산 오버헤드를 최소화한다.[2]

2.2 페이로드 정규화 방식

암호화가 활성화된 경우, CCB 를 제외한 데이터 영역은 항상 8 바이트 블록으로 정규화 된다.

$$P = Norm(d1, d2, ..., dDLC-1)$$

여기서 P 는 정규화된 8 바이트 페이로드 블록을 의미하며, 데이터 길이가 8 바이트보다 작은 경우 실제 페이로드는 블록의 하위 바이트에 우측 정렬되고, 나머지 상위 바이트는 0 으로 채워진다. 이와 같은 방식은 블록 길이에 따른 조건 분기를 제거하여 구현 복잡도를 낮추고 일정한 실행 시간을 보장한다.[6]

2.3 Keystream 기반 암·복호화

정규화된 페이로드 P 는 keystream 과의 XOR 연산으로 암·복호화된다. Keystream 입력 X 는 다음과 같이 구성된다.[4]

$$X = CTR\_ID \oplus (CI << 56) \oplus (ID << 16)$$

CTR_ID: 동기 카운터, CI: 암호화 인덱스, ID: CAN ID

keystream 생성 및 암호문 생성은 다음과 같다.

$$KS = E\_K(X), \quad C = P \oplus KS$$

CTR 구조를 사용하므로 복호화도 동일 연산

$$P = C \oplus E\_K(X)$$

2.4 동기 카운터 관리

제안 기법은 CAN ID 별 동기 카운터 CTR_ID 를 유지하여 전송 순서에 따라 암호문이 매번 달라지도록 한다. 카운터 값은 각 프레임 암·복호화가 완료된 시점에 갱신되며, 암호화 인덱스 CI 가 특정 예약 값(CI_reset)인 경우 카운터를 즉시 초기화한다. 이 동작은 다음 조건식 한 줄로 표현된다.[6]

$$CTR_{ID} \leftarrow \begin{cases} 0, & \text{if } CI = CI_{reset} \\ CTR_{ID} + 1, & \text{otherwise} \end{cases}$$

이를 통해 송·수신 측은 추가 메시지나 신호 교환 없이 자체적으로 동기 상태를 유지할 수 있으며, 프레임 손실이나 순서 변경으로 인한 동기 불일치를 효율적으로 해소할 수 있다.

2.5 구현 효율성

고정 길이 블록 처리, XOR 중심 연산, 경량 블록 암호 사용을 통해 연산량과 구현 복잡도를 최소화한다. 프레임당 동일한 암호 연산량을 요구하므로 실행 시간 예측이 용이하며, 차량용 ECU 와 같은 자원 제약 환경에서 실시간 처리에 적합하다.[5]

Ⅲ. 결론

본 논문은 기존 CAN/CAN-FD 프레임을 유지하면서 데이터 필드 내부 정보만으로 암호화를 수행하는 경량 보안 방식을 제안하였다. 첫 번째 바이트를 암호 제어 및 동기 정보로 사용하고, 나머지 페이로드는 경량 블록 암호 기반 keystream XOR 방식으로 처리함으로써 추가 헤더나 인증 태그 없이 기밀성을 제공한다. 또한 CAN ID 별 동기 카운터를 적용하여 동일 메시지도 매 전송마다 다른 암호문이 생성되며, 내재된 제어 값으로 동기 복구가 가능해 별도 메시지가 필요 없다.

<표 1>은 AES-128 및 MAC 기반 방식과 비교해 제안 방식의 처리 구조와 자원 요구를 요약하며, 자원 제약 ECU 에서의 구현 이점을 확인한다. 또한 연산량 수치는 AES-128 및 MAC 표준 구현을 Python 으로 직접 수행하여 측정한 결과에 기반한다.

항목	AES-128 방식	MAC 기반 방식	제안 기법
추가 메시지 전송	경우에 따라 필요	필수 (인증 태그 포함)	없음
암호/태그 크기	128-bit 블록	태그 길이에 의존 (64~128bit)	64-bit 경량 암호
평균 CPU 연산량	약 1,800–2,400 cycles/frame	약 1,200–1,600 cycles/frame	약 300–400 cycles/frame
복호화/검증 수행 방식	AES 역연산 필요	MAC 재계산 후 비교	XOR 동일 연산
동기 복구 방식	별도 관리 필요	경우에 따라 필요	CCB 기반 즉시 반영
ECU 구현 난이도	중~상	중	하

표 1 AES-128 및 MAC 방식 대비 제안 기법 비교 요약

본 기법은 낮은 연산량과 구현 부담으로 실시간 차량 네트워크 환경에 적합하며, 향후 인증 결합, IDS 연동뿐 아니라 FPGA/MCU 기반 하드웨어 구현 및 실차 환경 테스트를 통해 실제 성능을 검증하는 연구로 확장 가능하다.

ACKNOWLEDGMENT

본 연구는 대한민국 정부(산업통상자원부, MOTIE)의 재원으로 한국 산업기술평가관리원(KEIT)의 지원을 받아 수행되었으며(RS-2023-00232192, RS-2024-00403483), 또한 과학기술정보통신부(MSIT)의 재원으로 정보통신기획평가원(IITP)의 지원을 받아 수행되었다(RS-2025-02214672).

참 고 문 헌

[1] Checkoway S. et al., “Comprehensive experimental analyses of automotive attack surfaces,” USENIX Security, pp. 447-462, 2011.

[2] Kim H. and Kim S., “Efficient message authentication for CAN using truncated MAC,” IEEE Transactions on Vehicular Technology, vol. 66, pp. 2560-2572, 2017.

[3] Banik S. et al., “GIFT: A small PRESENT,” CHES, pp. 321-345, 2017.

[4] Bogdanov A. et al., “PRESENT: An ultra-lightweight block cipher,” CHES, pp. 450-466, 2007.

[5] NIST, “FIPS-197: Advanced Encryption Standard (AES),” National Institute of Standards and Technology, 2001.

[6] T. Kim, H. Cho, and J. Park, “Lightweight cryptography for automotive CAN-FD networks,” IEEE Access, vol. 9, pp. 90030-90042, 2021.