CAN ID 오류 검출이 가능한 차량용 네트워크 신뢰성 향상 기법

이승한, 김현빈, 이영우*
인하대학교 전기컴퓨터공학과

sh_lee@inha.edu, hbkim@inha.edu, *yw.lee@inha.ac.kr

MISR-based CAN ID Error Detection Scheme for High Reliability of Automotive Network

Seunghan Lee, Hyunbeen Kim, Young-woo Lee
Department of Electrical and Computer Engineering, Inha University

요 약

차량의 CAN(Controller Area Network) 통신은 안정적인 고속 통신이 가능한 반면, 실시간으로 데이터를 송수신하는 네트워크이므로 운전자의 안전을 보장하기 위한 보안성 확립이 필수적이다. 본 논문에서는 외부 공격으로 인해 발생하는 CAN ID 의 오류를 검출하여 차량용 네트워크 신뢰성을 향상시키는 기법을 제안한다. 제안하는 방식은 MISR(Multiple-Input Signature Register) 구조를 활용하여 산출된 Golden Signature 를 확인하여 오류를 검증한다. 모의실험을 통한 시뮬레이션을 진행한 결과 ECU ID 의 오류를 검출하여, 통신 네트워크의 보안성을 유지할 수 있음을 증명하였다.

Ⅰ. 서 론

차량용 네트워크의 UART(Universal Asynchronous Receiver/Transmitter) 통신은 Point-To-Point 방식으로, ECU(Electronic Control Unit)마다 통신 선을 연결해야 하므로 차량에 탑재되는 ECU 의 개수가 늘어날수록 배선 증가로 인한 비용이 상승하고 차량의 무게가 증가하는 단점이 있다[1]. 이를 해결하기 위해 개발된 CAN(Controller Area Network) 통신은 모든 ECU 를 하나의 CAN BUS 에 연결함으로써 데이터를 공유하는 네트워크로, 전체 통신 선을 효과적으로 줄임과 동시에 고속 통신을 보장하여 효율적인 데이터 송수신을 가능하게 하였다[2]. 하지만 모든 ECU 가 BUS 를 통해 메시지를 주고 받는 구조이기 때문에 CAN BUS 자체에 결함이 발생할 경우 전체 통신이 중단되며, 각각의 ECU 에서 오류가 발생하면 메시지 일부 기능이 수행되지 않아 정밀한 차량 제어가 불가능하다. 이는 ECU 간에 송수신하는 데이터를 실시간으로 처리하여 차량을 제어하는 시스템에 결함을 야기할 수 있다.

Ⅱ. 본 론

이전 연구에서는 안정적인 통신을 유지하기 위해 CAN BUS 를 모니터링하여 전송된 데이터가 중단 없이 수신되는지 확인하고, ECU 와 CAN BUS 사이의 케이블이 정상적으로 연결되어 데이터 비트 전송이 원활한지 테스트하였다[3],[4]. 그러나 외부에서 접근하여 통신 시스템을 공격하는 경우에는 오류 검출이 불가능하여 CAN 통신의 완전한 무결성을 보장할 수 없다. 차량의 CAN 통신은 각 ECU 에 할당된 고유 ID 의 값을 기준으로 낮은 순서부터 우선 순위를 정하여 이에 따라 송신한 메시지의 명령으로 차량을 통제하는데, 시스템에 침입하여 거짓된 ECU 를 삽입하거나 기존의 ECU 를 수정 및 제거하는 등의 외부 공격에 의해 ECU 메시지에 오류가 발생하면 주행 중인 운전자의 안전에 큰 위협을 가하게 된다. 따라서 본 논문에서는 CAN ID 를 비교하여 오류 검출을 통해 차량의 네트워크 신뢰성을 향상시키는 기법을 제안한다.

1.MISR-based CAN ID Error Detector

본 논문에서는 MISR(Multiple-Input Signature Register)의 output 으로 최종 출력된 Golden Signature 를 일정 시간 후에 최신화시켜 기존의 값과의 비교를 통해 오류를 검출하는 모듈을 제안한다. 모듈의 구조는 그림 1 과 같으며, CAN BUS 를 모니터링하여 BUS 가 IDLE(유휴) 상태일 때, free 신호를 받는다. IDLE 상태에서 MISR-based CAN ID Error Detector 는 Q0 부터 Qn-1 까지의 모든 레지스터를 '0' 으로 초기화한다. 이후 활성화된 모든 ECU ID 의 MSB 를 XOR 연산하지 않고, 순차적으로 Q 레지스터에 저장하여 Signature 1 을 생성한다. 즉, 활성화된 ECU ID 의 MSB 로 구성된 비트가 Signature 1 이다. MSB 다음 비트부터 LSB 에 이르는 연산은 Q 레지스터에 저장된 비트와 XOR 연산한 값이 Signature 값으로 저장된다. 이 단계부터 Signature 산출 연산은 최종 레지스터인 Qn-1 의 값이 처음과 마지막의 XOR gate 에 피드백되는 과정을 포함한다. 이 과정을 거쳐 최종 산출되는 Signature 가 Golden Signature 이다. MISR-based CAN ID Error Detector 는 CAN BUS 가 IDLE 상태에 진입한 시점과 우선 순위가 가장 높은 ECU 의 메시지 전송이 시작되는 시점에, 총 2 개의 Golden Signature 를 산출하여 비교함으로써 활성화된 모든 ECU ID 의 변동이 없음을 확인한다. ECU ID 는 고정된 11 비트이기 때문에 외부 공격이 발생하지 않으면

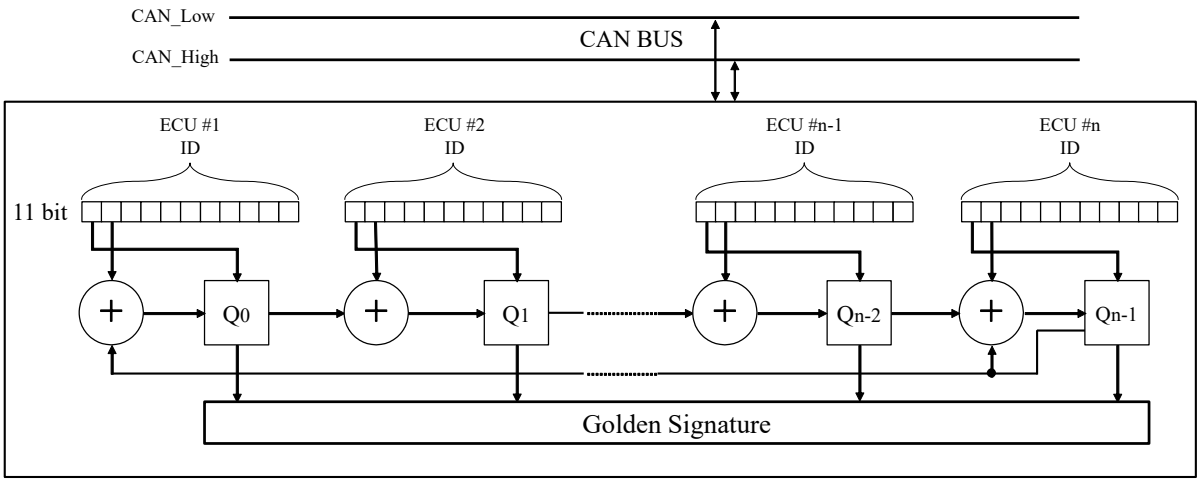
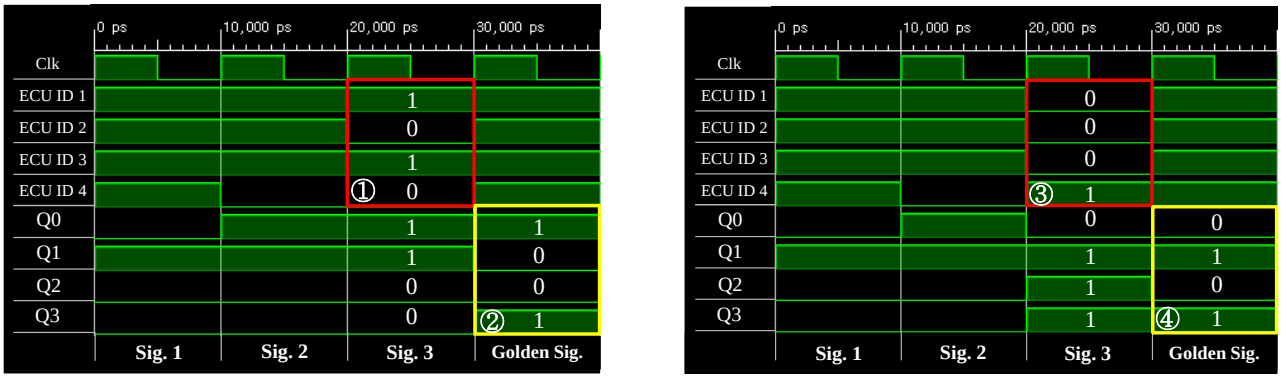


그림 1. 제안하는 MISR-based CAN ID Error Detector 구조



(a)정상 ECU ID 의 Golden Signature (b)손상된 ECU ID 의 Golden Signature

그림 2. 제안하는 구조의 Timing diagram

변동되지 않지만, 외부에서 접근하여 임의로 생성한 ECU ID 를 추가하거나 기존의 ECU ID 를 수정 및 삭제하는 경우, 도중에 산출되는 Signature 값이 변경되고 최종적으로 Golden Signature 값이 바뀌어 오류를 검출한다.

2. 모의실험 결과

본 연구에서 제안하는 구조의 Golden Signature 산출 기능 동작의 검증은 Xilinx 사의 Zynq Ultrascale+에서 진행하였고, implementation 을 통해 Total On-Chip Power 가 6.952W 로 측정됨을 확인하였다. 모의실험은 차량의 ECU 를 4 개로 설정하였으며, 이에 따라 Golden Signature 가 4 비트로 산출됨을 그림 2 의 Timing diagram 을 통해 확인할 수 있다. 그림 2.(a)는 활성화된 ECU 의 ID 가 정상적으로 입력되었을 때의 Golden Signature 를 보여준다. 그림 2.(b)에서는 외부 공격으로 인한 ECU ID 가 손상되어 기존과 다른 Golden Signature 가 산출된다. ①은 정상 ECU 의 ID 이며, ③에서 ECU 의 ID 가 손상되어 정상 ID b '1010' 가 b '0001' 로 변경되었다. 결과적으로 오류가 발생하지 않았을 경우 ②에서 보여지는 정상 Golden Signature b '1001' 이 산출되는 반면, ECU ID 가 손상된 그림 2.(b)의 ④에서는 b '0101' 로 산출되어 오류 발생을 감지할 수 있음을 확인하였다.

Ⅲ. 결 론

본 논문에서는 MISR 구조를 기반으로 CAN ID 오류 검출이 가능한 차량용 네트워크 신뢰성 향상 기법을 제안하였다. 제안한 구조는 ECU 의 ID 를 Q-레지스터에 저장하고 Golden Signature 를 산출한 후, 비정상 ECU ID 로 인한 Golden Signature 값의 변동을 확인하여 오류를 검출하는 방식이다. 본 기법은 외부 접근 공격자에 의한 ECU ID 오류를 검출하여 CAN 통신의 신뢰성 및 보안성을 향상시킬 수 있다.

ACKNOWLEDGMENT

본 연구는 과학기술정보통신부 및 정보통신기획평가원의 지역지능화혁신인재양성사업의 연구결과로 수행되었음(IITP-2023-RS2022-00156287). 본 연구는 IDEC 에서 EDA Tool 을 지원받아 수행하였음.

참 고 문 헌

[1] Gupta, Ashok Kumar, et al. "Design and implementation of high-speed universal asynchronous receiver and transmitter (UART)." 2020 7th International Conference on Signal Processing and Integrated Networks (SPIN). IEEE, 2020.

[2] Palaniswamy, Basker, et al. "An efficient authentication scheme for intra-vehicular controller area network." IEEE Transactions on Information Forensics and Security 15 (2020): 3107-3122.

[3] Kelkar, Supriya, and Raj Kamal. "Adaptive fault diagnosis algorithm for controller area network (AFDCAN)." IEEE Transactions on Industrial Electronics (2013).

[4] Altaha, Ibraheem Raed Abdulsalam, Duc NM Hoang, and Jong Myung Rhee. "Fault-Tolerant Optical Controller Area Network (FTO-CAN) Based on Heartbeat Signal Termination." 2022 IEEE 27th International Conference on Emerging Technologies and Factory Automation (ETFA). IEEE, 2022.