IDEC Chip Design Contest

물리적 보안 기능이 탑재된 차량용 ECU

Chan-goo Lee and Sun-Woo Jung and Jin-Hyuk Choi

And Seong-Soo Lee

서론

* 사용자의 안전과 밀접하게 관련된 차량 내 주요 ECU는 CAN 버스를 기반으로 구성되어 있다.

* CAN 버스에 연결되는 노드들은 Address가 존재하지 않아 통신에 참여하는 노드들 중 하나가 해킹을 당하여 악의적인 데이터 프레임을 송신해도 어느 노드가 문제인지 식별하기 어렵다.

* 악의적인 프레임을 식별하고 대처할 수 있도록 CAN Controller의 수정이 필요하다.

* 이와 같은 기능을 수행하는 CAN Controller 버스를 가진 차량용 ECU를 설계한다.

CAN 버스 고장 시뮬레이션

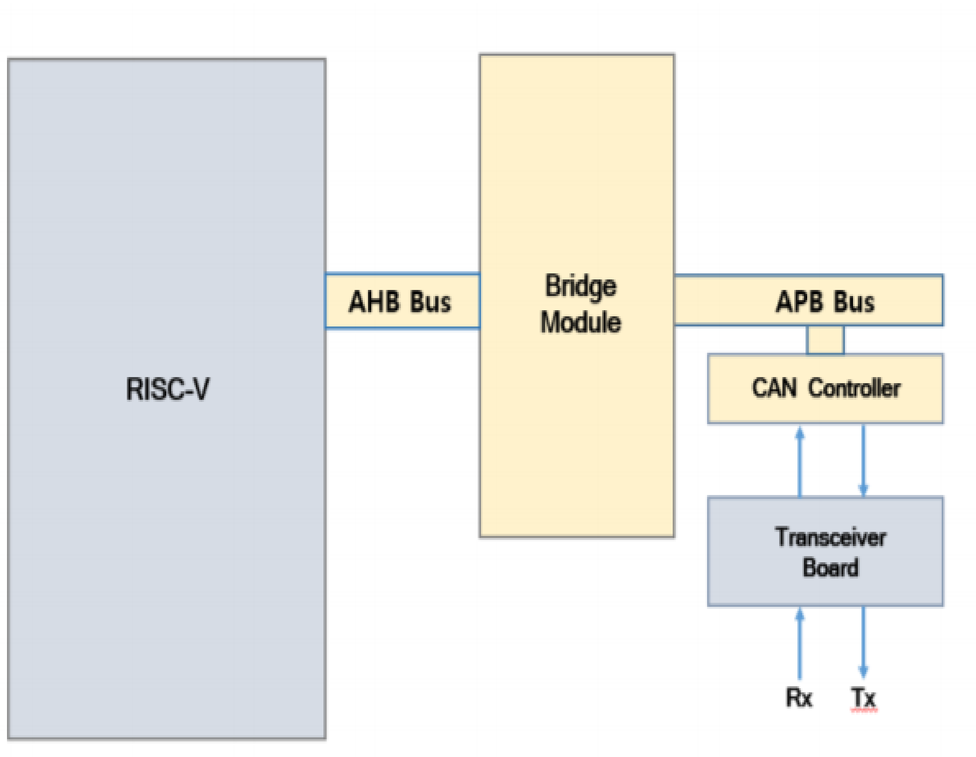

Fig. 1 ECU 블록도

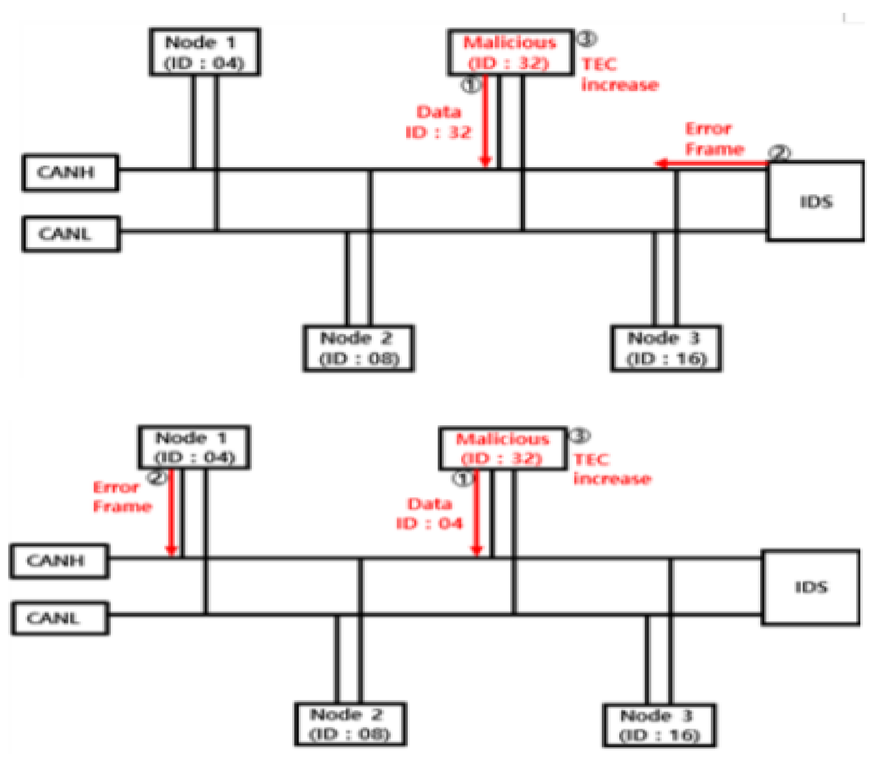

Fig. 2 CAN 버스 공격 시나리오 대처 방법

- 차량 내 통신을 수행 할 수 있는 통신 블록, CPU CORE(RISC-V)와 인터페이스를 위한 AMBA 버스 블록으로 구성
- 통신 블록은 CAN 버스 내부 보안을 고려한 CAN Controller로 구성
- OSI 7-Layer 중 CAN 표준보다 상위 Layer에서 데이터 프레임을 분석, 해킹 당한 노드인지 판단
- CAN 버스를 점령한 다음 악의적 데이터 프레임을 송신하는 경우 에러 프레임을 발생시켜 점령당한 노드의 TEC를 증가, 점령당한 노드가 계속해서 악의적인 데이터 프레임을 전송하는 경우 TEC가 계속 증가하여 결국 버스 오프

결론

- CAN 보안 문제가 발생하는 가장 큰 이유는 CAN 통신 Protocol에 참여하는 노드들의 Address가 존재하지 않아 어느 노드에서 데이터 프레임을 송신한 것인지 알 수 없기 때문
- 노드들 중 하나가 해킹을 당하여 악의적인 데이터 프레임을 전송 하여도 어느 노드가 문제인지 식별하기 어렵고 사용자에게 위험이 될 수 있음
- 기존의 CAN 컨트롤러를 수정하여 CAN 통신 Protocol에서 발생할 수 있는 공격 시나리오에 대하여 대처가 가능한 방법을 제안

본 연구는 IDEC에서 MPW를 지원받아 수행하였습니다.