차량 네트워크의 침입감지장치의 장애 복구

장현탁*
*아주자동차대학교 미래자동차공학부
e-mail:wslong@motor.ac.kr

Fault Recovery of Intrusion Detection System for In-Vehicle Network

Hyun-Tak Jang*
*Division of Mobility Engineering, Ajou Motor University

요 약

자동차에서 안전, 편안함, 자동화에 대한 수요가 계속 증가함에 따라 사이버 보안 위험과 공격에 대한 취약성이 증가했다. 자동차는 다양한 기능을 수행하기 위해 여러 전자 장치를 내장하고 있으며 시스템의 설계 복잡성이 증가했다. 이러한 장치는 컨트롤러 영역 네트워크(CAN) 및 로컬 상호 연결 네트워크와 같은 차량 네트워크를 통해 통신하며 이는 사이버 공격자의 대상이다. CAN 버스 침입을 목표로 하는 메시지 공격을 탐지하고 복구하는 새로운 알고리즘을 제안한다. 복구 프로세스에서 CAN 메시지 프레임의 침입감지장치로 오류를 감지하고 재부팅 기반 복구 프로세스 활용이 가능하다.

1. Introduction

자동차에서 임베디드 장치와 인터넷 연결을 사용하는 방식이 발전하면서 차량이 전자 장치에 주요 기능을 의존하는 차량은 보안에 대한 우려를 불러일으킨다. 자동차는 차량의 기능과 작동을 증가로 다양한 전자 제어 장치(ECU)를 내장할 자동차 시스템의 복잡성 증가에 비례하여 공격 가능성이 증가하고 있다. ECU는 컨트롤러 영역 네트워크(CAN), 로컬 상호 연결 네트워크(LIN), FlexRay, 미디어 지향 시스템 전송(MOST)을 포함한 차량 내 네트워크를 통해 통신한다.

CAN 버스는 자동차에서 가장 일반적으로 사용되는 네트워크 시스템이며 메시지 브로드캐스트 프로토콜을 통해 ECU를 연결한다. CAN 버스는 ECU 간에 전송된 메시지 프레임이 암호화되거나 인증되지 않기 상태에서 허가되지 않은 통신을 허용하므로 원격 및 물리적 공격에 취약하다.

물리적 공격은 온보드진단(OBD-II) 포트와 무선 네트워크 연결을 사용하여 원격 공격이 가능하다. 다른 위협이 여전히 발생하고 있지만 이러한 위협의 탐지 및 방어와 관련된 경험은 여전히 부족한 실정이다. 처음엔 CAN 보안 설계는 보안 요구 사항이 명확히 정의하지 않았고 차량 네트워크 프로토콜의 사용 가능한 대역폭 제약을 고려하지 않았다. 최근 ISO/SAE 21434 표준이 개발되고 있으며 자동차 엔지니어 협회(SAE)에서 발표한 J3061 사이버 물리적 차량 시스템을 위한 사이버 보안 규정의 표준으로 되었다. 자동차 차량의 보안 메커니즘을 고려할 때 필수적인 요구 사항은 시스템의 제한된 계산 능력과 메모리 용량을 고려한 알고리즘이다. 따라서 CAN 보안 메커니즘은 내결함성이 중요하며 알고리즘 계산이 효율이다.

CAN 버스에 대한 수많은 침입 탐지 장치의 다양한 방식과 대응 메커니즘을 이해하고 자동차 시스템에서 경보의 활용 방안을 제시한다.

Bus Off는 ECU가 네트워크에서 분리되어 재설정을 거칠 때까지 메시지를 전송할 수 없는 상태이다. CAN 버스의 고유한 오류 처리 기능인 Bus Off 모드를 활용하여 활성 공격을 받는 동안 손상된 노드를 정상 상태 복구한다.

본 논문에서는 CAN 버스에서 전송되는 동안 악성 메시지 공격을 차단하고 종료하기 위한 실용적인 접근 방식, 그리고 CAN 버스의 오류 처리 기능이 공격을 받는 노드를 복구하는 방법을 제안한다.

2. 공격 시나리오

공격 시나리오는 악의적인 노드가 네트워크의 다른 노드 공격을 시작하거나 네트워크 운영에 침입하는 가정이다. 침입자가 버스에 액세스하여 수신 및 전송 작업을 수행할 수 있다고 가정한다. 액세스는 버스에서 원격으로 액세스할 수 있는 노드를 통해 CAN 버스에 침입한다. 일반적으로 주로 저속 CAN 버스에서 가능하며, 이것을 이용하여 고속 CAN 버스에 액세스하여 주행 기능을 제어하는 안전이 중요한 노드의 작동에 영향을 준다. 고속 CAN 버스에서 안전이 중요한 노드를 제어하는 것인 다단계 공격 시나리오를 살펴보자. 침입자는 저속 버스에서 전송하는 정상 노드의 메시지를 가로채고 악의적인 노드가 메시지 프레임을 읽는 것이 액세스가 설정된다. 공격자는 고속 CAN 버스에서 안전에 중요한 노드를 대상으로 하는 가장된 메시지를 보낸다. 모든 노드가 CAN 버스에서 메시지를 브로드캐스트할 수 있고 각 수신 노드가 이제 메시지가 자신에게 전송 여부를 판단하기 때문에 침입자는 인증 없이 차량의 중요한 작업을 제어하는 특정 노드를 대상으로 하는 메시지를 성공적으로 스푸핑 가능하다. 이러한 대상 노드가 스푸핑 메시지를 수락하면 침입자는 공격에 완수된다.

3. CAN 보안

컨트롤러 영역 네트워크는 자동차 애플리케이션에서 사용하기 위해 개발된 표준 직렬 통신 버스로, 브로드캐스트 버스를 통해 ECU를 상호 연결한다. 메시지 우선순위(CSMA/CD+AMP)에 대한 충돌 감지 및 중재를 통해 캐리어 감지 다중 액세스를 통신 프로토콜이다.

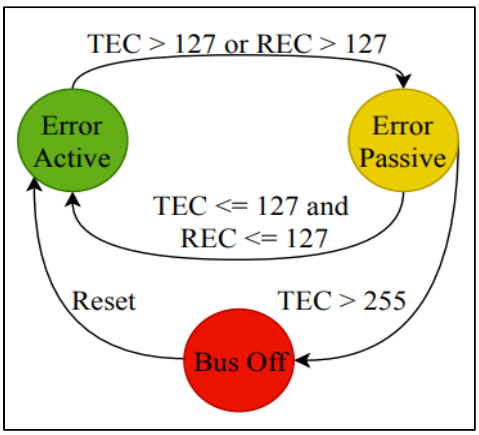
CAN은 버스 중재를 통해 메시지 프레임의 고정 우선순위 스케줄링을 효율적으로 구현한다. 버스에서 전송된 메시지 프레임은 네트워크의 모든 노드(ECU)에 브로드캐스트 한다. 모든 메시지 브로드캐스트에 우선순위와 의미를 나타내는 고유한 ID가 포함된다. 버스에서 ID가 낮은 메시지는 우선순위가 높고 메시지 먼저 전송한다. 메시지 프레임은 네 가지 프레임의 연결되어 있다. 노드 간에 데이터를 전송하기 위한 데이터 프레임, 식별자를 가진 데이터 프레임의 전송을 요청하기 위한 원격 프레임, 감지된 오류를 나타내는 데 사용되는 오류 프레임, 프레임 간에 추가 지연을 제공하는 데 사용되는 오버로드 프레임이다. CAN 버스는 0 또는 1의 신호를 전송하는데, 여기서 우세한 비트라는 용어는 논리적 0을 나타내고, 열성적인 비트는 논리적 1 신호를 나타낸다. 통신용 와이어 (CAN 하이 및 로우) 간의 전압 차이가 크면 우세한 상태이다. 두 와이어 간의 전압 차이가 작으면 열성적인 상태이다. 노드가 우세한 비트를 전송하고 다른 노드가 열성적인 비트를 전송하면 우세한 비트가 전송된다. 자동 중재는 모든 노드가 전송 중에 버스의 상태를 감시하고 열성적인 비트를 전송할 때 우세한 비트가 관찰되면 전송을 중단해야 하므로 CAN 프로토콜에 내장되어 있다.

CAN 아키텍처는 차량 내에서 통신하는 노드의 폐쇄된 시스템이다. 따라서 CAN 버스는 인증 프로토콜 없이 구현되어 모든 노드로 메시지를 자유롭게 흐르게 하고 이러한 메시지는 일반 메시지로 전송된다. 노드가 메시지를 받으면 해당 메시지가 자신에게 적합 여부를 결정한다. CAN의 브로드캐스트 특성 덕분에 버스에 연결된 각 노드는 소스와 목적지를 확인하지 않고 전송된 메시지를 브로드캐스트하고 수신할 수 있다. 버스에 액세스할 수 있는 침입자는 암호화되지 않은 메시지를 도청할 수 있다. 버스는 분할되지 않아 안전에 중요한 노드와 안전에 중요하지 않은 노드가 같은 버스에서 통신할 수 있다. 이는 무단 노드가 안전에 중요한 노드를 손상에 스푸핑 메시지를 전송하는 심각한 공격이 가능하다. CAN 버스는 공격에 취약하며, 이는 버스의 중재 프로세스를 활용하여 버스의 작동을 마비시키기 위해 가장 높은 우선순위 메시지를 계속 전송하여 실현할 수 있다. CAN 버스의 이러한 취약성을 악용하여 데이터 주입, 스푸핑, 재생 공격을 포함한 여러 공격을 수행할 수 있다. 악성 노드를 버스에 배치하여 버스의 전체 작동을 손상되는 비정상적인 메시지를 전송할 수 있다.

4. 침입감지장치

성능, 신뢰성 및 안전성은 자동차 네트워크와 같은 안전이 중요한 애플리케이션의 중요한 특징이다. 자동차 개발의 과제는 안전, 보안 및 기능성의 요구사항을 균형 있게 조정하는 것입니다. 안전의 우선순위는 운전자의 생명을 최악의 상황에서도 안전을 보장하기 위해 에어백 및 충돌 방지 시스템과 같은 차량의 특정 기능은 계속 작동해야 한다. 이는 중요한 기능과 작동의 안전성이 보안보다 우선함을 의미한다. 그러나 이러한 안전 기능 중 하나가 손상되거

나 공격의 대상이 되는 상황에서는 어떻게 될까요? 이러한 상황에서 차량의 보안을 보장하기 위해 차량 시스템이 작동 안전을 유지하는 동안 일부 기능과 작동을 제한해야 한다. 네트워크 노드의 임의적 오류를 포괄하고 CAN 버스에서 공격 전파의 영향을 고려하는 보안을 위한 재부팅 기반 침입 방지 접근 방식을 제시한다. 재부팅 기반 복구는 원격 침입자에 의해 손상된 ECU에 대한 실용적인 복구 방법이다. 목표는 침입자의 공격 메시지를 네트워크로 더 멀리 전파하는 것을 방지하고 안전에 중요한 CAN 버스 작업을 제어한다. 복구 방법은 메시지가 버스에 릴리스, 탐지기 노드를 포함하여 네트워크의 모든 노드에 브로드캐스트 된다. 버스에 브로드캐스트 메시지를 모니터링을 위해 전략적으로 배치된 IDS를 나타내는 탐지기 노드는 보낸 메시지가 비정상적이면 검사를 수행하고 오류 프레임을 전송한다. 손상된 노드는 전송오류 카운터는 증가하고, 건강한 노드는 수신오류 카운터는 증가한다. 오류 카운터가 증가하면 재부팅 복구 프로세스가 수행한다.



[Fig. 1] Flow of CAN error counter

5. 장애 복구

IDS가 공격을 감지하면 오류 프레임을 대기열에 넣는다. 이 프레임은 6개의 연속된 우세한 비트로 시작하며, 다음 버스 중재에서 가장 높은 우선순위를 갖는다. 오류 프레임을 수신한 노드는 수신한 메시지를 버린다. 버스 오프 상태의 ECU는 버스에서 128번 11개의 연속적인 열성 비트를 관찰해야 오류 활성 상태로 다시 전환할 수 있다. 이 전환 전에 ECU는 재설정하거나 재부팅할 수도 있다. 원격 인터페이스 기능이 있는 모든 ECU는 버스 오프 상태에 도달하면 재부팅 프로세스를 거치는 것이 좋다. 재부팅 프로세스는 초기 시스템 상태를 복원은 자동화하기 쉽고 소프트웨어를 초기 상태로 되돌린다.

전원 사이클은 빠르며 시스템이 복구되는 데 걸리는 시간에 미치는 영향이 최소화되며 감지 알고리즘이 오경보에 취약하거나 재부팅 프로세스가 오류를 수정할 수 있어 ECU 고가용성을 제공할 수 있다. ECU 재부팅의 영향은 장치 안전에 영향은 없지만, 운전자에게 부정적인 영향을 미칠 수 있다. 재부팅 프로세스는 노드를 버스 꺼짐 상태로 유지하는 데 중요한 역할을 하며 실제 재시작을 수행하려면 재부팅이 필요하다. 자동 재설정에서 재설정은 CAN 컨트롤러가 버스 꺼짐 상태로 전환된 직후에 시작되지만 대기 후 재설정은 애플리케이션 계층이 재설정을 시작하기 전에 오류 조건에서 복구하기 위해 사전 정의된 대기 기간을 준수해야 한다. 주파수 제한 재설정에서 두 개의 재설정 사이의 시간은 미리 정해진 시간 간격보다 커야 한다. CAN 컨트롤러가 버스 오프 상태일 때, 애플리케이션 계층의 재설정 벡터가 트리거되고 재설정을 초기화하고, CAN 컨트롤러는 네트워크에 다시 가입하기 전에 미리 정해진 수의 열성 비트를 관찰한다.

6. 결론

원격 메시지 주입 공격이 성공하는 것을 방지하고 원격으로 손상된 ECU의 재부팅 기반 복구를 트리거 할 수 있는 CAN 버스용 새로운 침입방지 장치를 제시했다.

참고문헌

[1] Brooke Lampe, “can-logic: Automotive Intrusion Detection via Temporal Logic”, IoT 2023, November 07 - 10, 2023, Nagoya, Japan