ISSN : 1226-7244 (Print)
ISSN : 2288-243X (Online)
논문번호 19-04-51
354

j.inst.Korean.electr.electron.eng.Vol.23,No.4,1469~1472,December 2019
http://dx.doi.org/10.7471/ikeee.2019.23.4.1469

CAN 버스 물리 계층에서 해킹된 노드의 대처 기법

Counterattack Method against Hacked Node in CAN Bus Physical Layer

강 태 욱*, 이 종 배*, 이 성 수*★

Tae-Wook Kang*, Jong-Bae Lee,* and Seongsoo Lee*★

Abstract

CAN bus in automotive applications does not assign node addresses. When a node is hacked and it transmits malicious data frame, it is difficult to resolve which node is hacked. However, this CAN bus internal attack seriously threatens the safety of a car, so a prompt counterattack is necessary in the CAN bus physical layer.

This paper proposes a counterattack method against malicious CAN bus internal attack. When a malicious data frame is detected, an intrusion detection system in the CAN bus increases the error counter of the malicious node. Then, the malicious node is off from the bus when its error counter exceeds its limit. A CAN controller with the proposed method is implemented in Verilog HDL, and the proposed method is proved to counterattack against malicious CAN bus internal attack.

요 약

자동차에 사용하는 CAN 버스는 노드에 주소를 부여하지 않기 때문에 여러 노드 중 하나가 해킹을 당하여 악의적인 데이터 프레임을 전송하여도 어느 노드가 해킹 당했는지 식별하기 어렵다. 하지만 이러한 CAN 버스의 내부 공격은 자동차의 안전에 큰 위협이 될 수 있으므로 CAN 버스의 물리 계층에서 신속하게 대처하여야 한다.

본 논문에서는 CAN 버스 상에서 악의적인 데이터 프레임이 감지되면 침입 감지 시스템이 내부 공격 노드의 에러 카운터를 증가시켜서 버스에서 분리시킴으로서 악의적인 공격을 방어하는 기법을 제안하였다. 제안한 기법을 탑재한 CAN 컨트롤러를 Verilog HDL을 이용하여 구현하였고, 이를 통해 제안한 기법이 CAN 버스의 악의적인 내부 공격을 방어할 수 있음을 확인하였다.

Key words : Controller Area Network, Internal Attack, Counterattack, Error Counter, Bus Off

* School of Electronic Engineering, Soongsil University
★ Corresponding author
E-mail : sslee@ssu.ac.kr, Tel : +82-2-820-0692

※ Acknowledgment
This work was supported by the MOTIE (Ministry of Trade, Industry & Energy) (10080649) and KSRC (Korea Semiconductor Research Consortium) support program for the development of the future semiconductor device.
Manuscript received Dec. 28, 2019; revised Dec. 30, 2019.; accepted Dec. 30, 2019.

Ⅰ. 서론

오늘날 대부분의 자동차는 CAN(Controller Area Network) 버스[1]-[4]를 기반으로 차량 내부의 ECU(Electronic Control Unit)들을 연결하고 있다. CAN 버스의 특징 중 하나는 통신에 참여하는 노드들의 주소가 존재하지 않는다는 점이다. 이는 동시 전송, 다수 전송 등 많은 장점을 가지고 있지만 동시에 보안상 취약점을 제공한다. 통신에 참여하는 노드들 중 하나를 해킹하여 악의적인 데이터 프레임을 전송하는 경우, 어느 노드가 데이터 프레임을 송신하였는지 알 수 없기 때문에 해당 노드를

차단하는 것이 매우 어렵다. 이렇게 악의적인 데이터 프레임을 막지 못할 경우 CAN 버스를 과부하 시켜서 정상적인 통신을 못하게 하거나 다른 노드를 공격하여 사용자에게 위험이 될 수 있는 동작을 하게 할 수 있다.

본 논문에서는 CAN 버스에서 발생할 수 있는 3가지 공격 시나리오를 설명하고 이를 방어할 수 있는 방법을 제안하였다. 또한 제안한 방법을 CAN 컨트롤러에 탑재하여 Verilog HDL (Hardware description Language)을 이용하여 구현하고 시뮬레이션하여 유효성을 검증하였다.

II. CAN 버스의 내부 공격 방어 기법

1. CAN 버스의 에러 관리 기법

CAN 버스의 모든 노드는 TEC(Transmit Error Counter)와 REC(Receive Error Counter)가 있으며, 이를 이용하여 에러가 자주 발생하는 노드가 다른 노드의 송수신을 방해하지 않도록 관리한다. 어느 노드든지 에러를 발견하면 에러 프레임을 발생시키는데, 이때 송신 노드의 TEC는 8만큼 증가하게 된다. 수신 노드의 경우 가장 먼저 에러 프레임을 발생시킨 노드의 REC는 8만큼 증가하고 다른 노드의 REC는 1만큼 증가한다. 메시지가 성공적으로 전송되면 송신 노드와 수신 노드의 TEC와 REC는 각각 1씩 감소한다.

그림 1은 TEC와 REC에 따라 노드 상태 변화를 나타낸 것이다. 에러 액티브 상태는 정상적인 송수신을 수행하지만 TEC 또는 REC가 128 이상이 되면 에러 패시브 상태가 되어 송수신에 다소 제약을 받는다. 여기서 주목할 것은 TEC가 256 이상이 되면 버스 오프 상태가 되어 버스에서 자동적으로 분리되며 송수신이 금지된다는 점이다. 본 논문에서

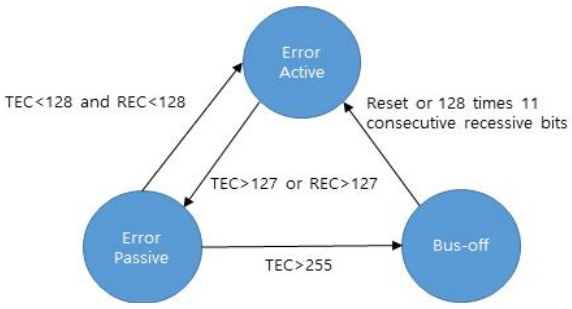

Fig. 1. Node state transition with TEC and REC.
그림 1. TEC와 REC에 따른 노드 상태 변화

는 이를 이용하여 악의적인 데이터 프레임을 전송하는 노드를 버스 오프 상태로 만들어서 해당 노드가 버스를 과부하 시키거나 다른 노드를 공격하는 것을 막는 기법을 제안한다.

2. CAN 버스 공격 시나리오

CAN 버스에서는 크게 3가지의 공격 시나리오를 생각할 수 있는데 노드를 점령한 뒤 스니핑 (Sniffing)을 통해 메시지 패턴을 파악할 수도 있고, 일반적인 공격 (Attack)을 통해 악의적인 데이터 프레임을 송신하여 버스를 과부하 걸리게 만들거나 다른 노드를 오동작 시킬 수 있다. 또한 다른 노드인 척 가장하면서 악의적인 데이터 프레임을 송신하는 스푸핑(Spoofing) 공격을 할 수도 있다.

가. 시나리오 1(스니핑) : 스니핑은 해킹을 통해 점령한 노드를 이용해서 버스 상에서 통신 중인 메시지들을 보고 패턴을 파악하는 것이다. 이 단계에서는 CAN 버스에 해를 가하지 않는다.

나. 시나리오 2(일반 공격) : 스니핑을 통해 메시지 패턴을 파악한 후 점령 한 노드를 이용하여 악의적인 데이터 프레임을 송신한다.

다. 시나리오 3(스푸핑 공격) : 일반적인 공격과 스푸핑 공격은 악의적인 데이터 프레임을 송신하는 점에서는 동일하나 스푸핑 공격에서는 점령한 노드가 다른 노드인 척 위장한다는 차이가 있다.

3. CAN 버스 공격 방어 기법

본 논문에서는 각 노드는 서로 다른 본인의 고유 ID인 NID (Node ID)를 갖고 있다고 가정하였다. 또한 CAN 버스에 노드 이외에 침입 감지 시스템인 IDS (Intrusion Detection System)가 있다고 가정하였다. IDS는 데이터 프레임의 내용을 분석하여 해킹당한 노드인지 판단하는데 이는 OSI (Open System Interconnection) 7 계층 중에서 CAN 버스보다 상위 계층에서 수행을 하는 내용이다. 따라서 본 논문에서는 IDS는 따로 구현하지 않고, 단지 IDS를 통해 해킹당한 노드의 고유 ID를 알 수 있다고 가정하였다.

에러 프레임을 보내서 해킹당한 노드를 추방하는 기능인 NES (Node Expulsion System)는 일반적인 CAN 버스에는 없고 본 논문에서 추가한 기능

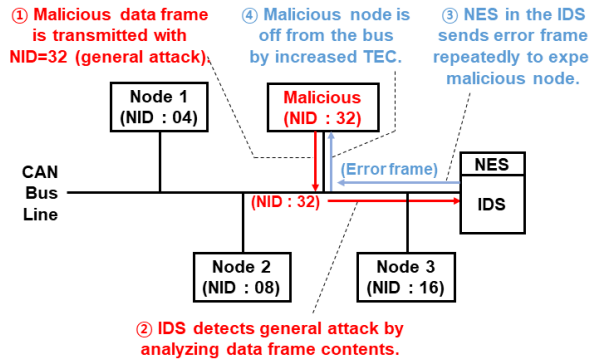

Fig. 2. Counterattack to general attack.
그림 2. 일반 공격에 대한 대처

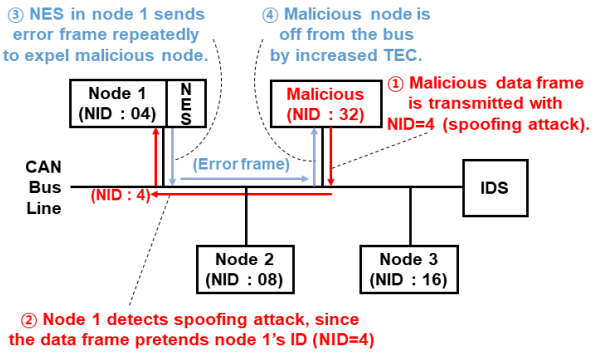

Fig. 3. Counterattack to spoofing attack.
그림 3.스푸핑 공격에 대한 대처

인데 특정 조건을 만족하면 에러 프레임을 내보내는 회로를 CAN 컨트롤러에 부가하여 간단히 구현할 수 있다. 본 논문에서는 NES를 각 노드와 IDS에 모두 장착하였다.

가. 스니핑에 대한 대처 : 스니핑은 당장 버스에 악영향을 끼치지 않기 때문에 특별한 조치를 취하지 않는다.

나. 일반 공격에 대한 대처 : 일반 공격에서는 그림 2와 같이 점령당한 노드가 악의적인 데이터 프레임을 송신할 경우 IDS에서 해당 데이터 프레임의 내용을 분석하고 해당 노드가 해킹되었음을 감지한다. 이후로는 IDS에 달려있는 NES가 해당 노드가 송신할 때마다 계속 에러 프레임을 송신하기 때문에 해당 노드는 송신을 봉쇄당하고 TEC가 증가하여 버스 오프 상태가 된다.

다. 스푸핑 공격에 대한 대처 : 스푸핑 공격에서는 그림 3과 같이 점령당한 노드가 NID를 위조하여 악의적인 데이터 프레임을 송신할 경우, 위조당한 노드 (즉 위조된 NID를 원래 쓰고 있는 노드)에서 자신과 동일한 NID를 발견하였으므로 해당 노드가 해킹되었음을 감지한다. 이후로는 위조당한 노드에 달려있는 NES가 해당 노드가 송신할 때마다 계속 에러 프레임을 송신하기 때문에 해당 노드는 송신을 봉쇄당하고 TEC가 증가하여 버스 오프 상태가 된다.

III. 시뮬레이션 결과

본 논문에서는 기존의 CAN 컨트롤러에 NES를 장착하여 Verilog HDL로 설계하고 ModelSim으로 시뮬레이션하였다. 4개 CAN 노드의 NID는 4, 8, 16, 32로 설정하였으며 스니핑은 당장 악영향을 끼치지 않기 때문에 일반 공격과 스푸핑 공격의 2가지에 대해서만 시뮬레이션을 수행하였다.

그림 4는 일반 공격에 대처하는 경우로, 처음에는 정상 동작을 하다가 일정 시간이 지난 뒤 IDS에서 점령당한 4번 노드 (NID=32)를 감지하고 4번 노드가 데이터 프레임을 송신할 때마다 IDS가 에러 프레임을 발생시켜 4번 노드의 TEC를 증가시킨다. 이후 4번 노드가 전송할 때마다 IDS가 TEC를 계속 증가시켜 버스 오프로 만든다.

그림 5는 스푸핑 공격에 대처하는 경우로, 점령당한 4번 노드(NID=32)가 1번 노드 (NID=4)를 도용하여 데이터 프레임을 송신한다. 그러나 1번 노드는 송신 중이 아닌데 자신의 NID를 감지하였으므로 공격으로 인식하고 에러 프레임을 발생시켜 4번 노드의 TEC를 증가시킨다. 이후 4번 노드가 1번 노드 (NID=4)를 도용할 때마다 1번 노드가 TEC를 계속 증가시켜 버스 오프로 만든다.

IV. 결론

CAN 버스에서는 노드들 중 하나가 해킹을 당하여 악의적인 데이터 프레임을 전송하여도 어느 노드가 문제인지 식별하기 어렵다. 본 논문에서는 기존의 CAN 컨트롤러를 수정하여 CAN 버스에서 발생할 수 있는 다양한 공격 시나리오에 대하여 대처가 가능한 방법을 제안하였다. 이를 검증하기 위해 CAN 컨트롤러와 부가 회로를 Verilog HDL로 구현하여 시뮬레이션을 통해 제안된 기법의 유효성을 검증하였다.

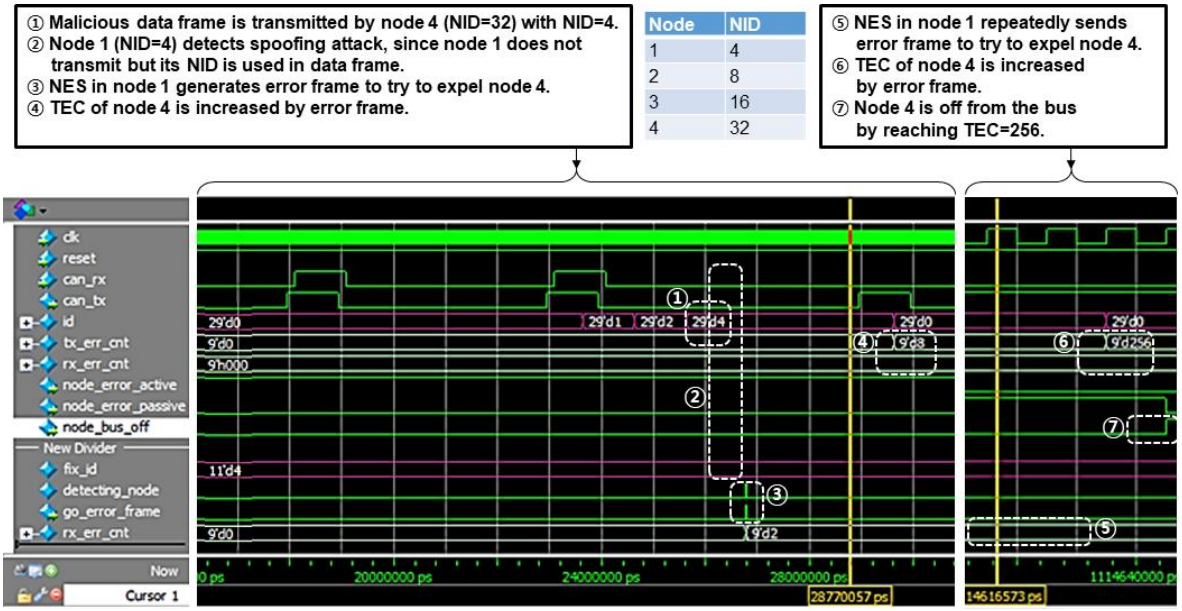

Fig. 4. Simulation waveform of counterattack against general attack.
그림 4. 일반 공격에 대한 대처 동작의 시뮬레이션 파형

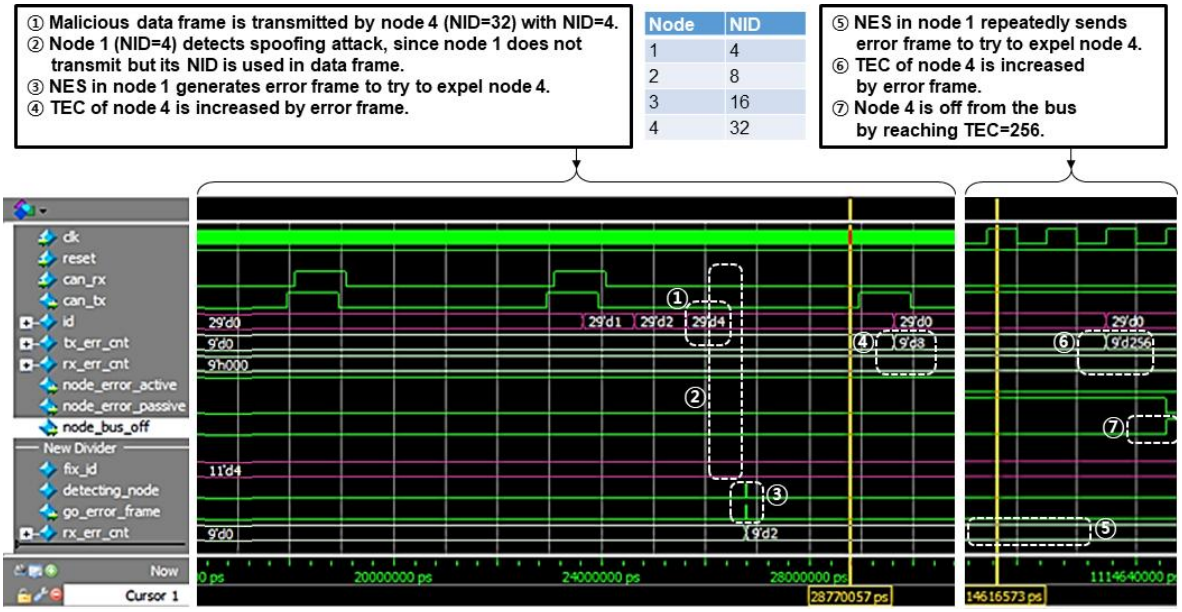

Fig. 5. Simulation waveform of counterattack against spoofing attack.
그림 5. 스푸핑 공격에 대한 대처 동작의 시뮬레이션 파형

References

[1] ISO 11898-1:2015, "Road Vehicles-Controller Area Network (CAN)-Part 1: Data Link Layer and Physical Signalling," https://www.iso.org/standard/63648.html

[2] ISO 11898-1:2015, "Road Vehicles-Controller Area Network (CAN)-Part 2: High-Speed Medium Access Unit," https://www.iso.org/standard/67244.html

[3] ISO 11898-3:2006, "Road Vehicles-Controller Area Network (CAN)-Part 3: Low-speed, Fault-tolerant, Medium-dependent Interface," https://www.iso.org/standard/36055.html

[4] J. Lee and S. Lee, "Design and Verification of Automotive CAN Controller," *j.inst.Korean.electr.electron.eng*, vol.21, no.2, 2017.
DOI: 10.7471/ikeee.2017.21.2.162