캔 버스 통신 보안 위협 및 기술 동향

이민우*, 강예준*, 김원웅*, 서화정**†
*한성대학교 IT융합공학부
**† 한성대학교 IT융합공학부
minunejip@gmail.com, etus1211@gmail.com, dnjsdndeee@gmail.com,
hwajeong84@gmail.com

CAN Bus Security Threats and Technology Trends

Min-Woo Lee*, Yea-Jun Kang*, Won-Woong Kim*, Hwa-Jeong Seo**†
*Dept. of IT convergence, Hansung University
**† Dept. of IT convergence, Hansung University

요 약

캔 통신은 차량 내부의 전자장치 간 데이터 송수신 시에 사용되는 통신 방식이다. 차량 기술이 발전함에 따라 내부에 탑재되는 전자장치가 늘어나고 있고 이는 해킹의 위험성이 높아지고 있음을 의미한다. 이는 다가오는 4차 산업 혁명에서 자율주행 차량 기술의 치명적인 문제로 작용할 수 있다. 본 논문에서는 CAN Bus 통신에서의 위협 대응 방안과 안정성 향상에 대한 연구들의 동향을 살펴본다.

1. 서론

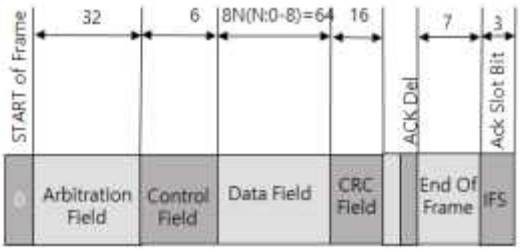
CAN(Controller Area Network) Bus 통신 프로토콜은 BOSCH(사)가 제안한 통신 방식으로 차량을 비롯하여 많은 산업기기에 사용되고 있으며, 보안이 없이 대부분 사용하고 있다[1]. 이는 최근 발전하고 있는 자율주행 차량의 보안에 있어 치명적이다. 자율주행 차량은 모든 판단이 자율주행 자동차가 외부를 인식하는 방법인 센싱 정보와 이를 해석하는 인공지능에 의해 결정되는 특징을 가지고 있다[2]. 4차 산업 혁명에서의 자율주행 자동차 프로세서 간 통신인 CAN Bus 통신이 암호화되지 않았다면 외부로부터 무단으로 접속되는 경우 해킹의 피해로 이어질 수 있다[3].

대부분의 자동차 전자장치 시스템은 ECU(Electronic Control Unit)에 의해 제어되며 CAN Bus를 통해 데이터를 주고받는다. 최근의 자동차는 편의성과 안정성을 위한 편의 장치 및 운전 보조 시스템이 대거 장착되고 있으며 이는 차량에 탑재되는 ECU의 개수가 늘어나고 있음을 의미한다.
ECU의 개수가 늘어날수록 CAN Bus의 부하가 증가하고 이로 인해 메시지의 전송 지연이나 오류가 발생한다. 이는 CAN Bus의 안정성을 떨어뜨릴 수 있다.

2. 관련 연구

2.1 CAN Bus 통신

CAN Bus는 멀티 마스터 통신 네트워크이다. 호스트인 노드가 없고 버스를 공유하고 있는 ECU와 같은 컨트롤러 노드 모두가 마스터 역할을 한다. 이는 어떤 노드라도 메시지를 전송할 수 있음을 의미하며 전송은 우선순위에 따라 순차적으로 이루어진다. 전송에서의 우선순위는 각각의 ECU마다 지니고 있는 고유의 ID 값에 따라 정해진다.



(그림 1) CAN 2.0B 패킷 구조

CAN bus는 간단한 구조를 지니고 있다. CAN-HIGH와 CAN_LOW 두 개의 신호를 이용하여 통신하며 이는 두 개의 선만 필요함을 의미한다. 케이블은 꼬임 쌍선 케이블을 이용하며 많은 모듈이 추가되더라도 추가되는 선의 양이 적다. 따라서 CAN Bus는 구성이 용이하고 가격이 저렴하며 확장성이 좋다.

CAN Bus 통신은 저비용으로 최대 1MBit/s까지

사용할 수 있으며 Multi Node 구성된 자동차 엘리베이터 등에 많이 쓰인다. Address 비트 수에 따라 11 비트 식별자를 가진 CAN 2.0A Protocol과 그림 1.과 같이 29 비트 식별자를 가진 CAN 2.0B 방식이 있다 [4,5,6].

2.2 CAN Bus 물리 계층

CAN Bus는 CAN-H와 CAN-L의 구리 선 두 줄로 이루어진다. 이 두 줄에 ECU들이 연결되어 Bus를 구성한다. ECU 모듈은 코어, 캔 컨트롤러, 캔 트랜시버로 구성된다. 정보 송수신 시 ECU core에선 송신하고자 하는 데이터를 캔 컨트롤러로 보낸다. 캔 컨트롤러에선 데이터블록 앞뒤에 헤더 파일을 추가한다. 그 후 캔 트랜시버로 포장된 데이터를 보내고 캔 트랜시버는 구리 선으로 해당 데이터를 전송한다.

CAN Bus 물리 계층인 캔 트랜시버에는 여러 종류가 있다. High-speed CAN, Low-speed CAN, 단일 와이어 CAN 하드웨어 등이 있으며 이 중 High-speed CAN이 가장 보편적으로 사용된다. High-speed CAN은 최대 1Mb/s 전송속도를 지원하지만, 신축성을 위해 500kb/s까지만 사용한다. High-speed CAN의 다른 명칭으로는 CAN C와 ISO 11898-2가 있다. 일반적인 High-speed CAN 디바이스에는 ABS(anti-lock brake systems), 엔진 컨트롤 모듈, 방출 시스템 등이 있다.

2.3 CAN 메시지 포맷

CAN Bus에 연결되어있는 장치들은 데이터를 주고받을 때 CAN 데이터 프레임이라는 패킷으로 데이터를 전송한다. CAN 프레임의 구성은 그림1.과 같이 총 7개의 필드로 구성된다.

SOF(Start Of Frame)필드는 한 개의 비트로 구성되어 있으며 메시지의 처음을 지시하고 모든 노드의 동기화를 위해 사용된다. Arbitration 필드는 11비트 혹은 29비트의 ID와 1비트의 rtr(remote transmission request)비트로 구성된다. ID 비트는 메시지를 식별하고 메시지의 우선순위를 지정한다. rtr비트가 1의 상태일 땐 해당 프레임이 데이터 프레임이 아닌 데이터 전송을 요청할 때 쓰이는 리모트 프레임임을 나타낸다. Control 필드는 데이터 필드 상의 데이터 길이를 정해주기 위한 코드로 쓰인다. Data 필드는 한 장치로부터 다른 장치로 전달하고자 하는 데이터를 포함하며 0에서 8바이트로 구성된다. CRC(cyclic Redundancy Check) 필드는 메시지 상의 에러 유무를 검사하는 데 이용된다. ACK(Acknowledge) 필드는 2비트로 구성되며 첫 번째 비트는 “0”값을 가지는 slot 비트이다. slot 비트는 메시지를 성공적으로 수신한 임의의 장치로부터 전송된 “1”값으로 기록된다. EOF(End Of Frame)필드는 7개의 비트로 구성되며 메시지의 끝을 알리는 목적으로 사용된다.

2.4 AES 암호

AES(Advanced Encryption Standard)는 미국표준연구소(NIST)에서 2001년도에 제정된 암호방식으로 1977년 공표된 DES를 대체한 AES는 암호화 복호화 과정에서 같은 KEY를 사용하는 대칭키 알고리즘이다. AES의 특징은 안전성(Security), 저비용(Cost), 알고리즘 및 구현 특성이며, KEY는 128비트, 192비트, 256비트로 확장 가능하며, 가장 널리 사용하는 미국 정보표준 암호화 알고리즘이다[7].

2.5 ARIA 암호

ARIA(Academy Research Institute Agency)는 2004년 12월에 한국산업규격 KS표준으로 제정된 것으로 대칭키 알고리즘이며 순수 국내 기술로 개발된 알고리즘이다. 블록 크기는 128비트이며 128비트, 192비트, 256비트의 확장키를 사용할 수 있다. ARIA의 특징은 경량 환경의 하드웨어에서 높은 효율성에 있으며, SEED 알고리즘보다 빠른 성능을 제공하고 있다. 객관적인 안정성 및 효율성 평가를 위하여 NESSIE(New Europen Schemes for Signature Integrity, and Encryption) 의 주관 기관인 벨기에 루벤대학에 의한 평가를 받았다[8].

2.6 HIGHT 암호

HIGHT(HIGH security ans light weigHT)는 RFID, USN 등과 같이 저전력, 경량화를 요구하는 컴퓨팅 환경에서 기밀성을 제공하기 위해 2005년 KISA와 고려대학교가 공동으로 개발한 64 비트형 블록 암호 알고리즘이다. 알고리즘의 전체 구조는 일반화된 Feistel 변형 구조로 이루어져 있으며, 64비트의 평문과 128비트 키로부터 생성된 8개의 8비트 화이닝 키와 128개의 8비트 서브키를 입력으로 사용하며 총 32라운드를 거쳐 64비트 암호문을 만든

다[9].

3. 연구 동향

3.1 CAN Bus 물리 계층 보안 기법[10]

차량에 탑재되는 ECU에는 프로세서 ID와 통신용 암호키가 고유하게 지정되어 있어서 통신을 수행할 때마다 프로그램에서 확인하며 해킹이 의심되는 경우 통신을 차단하도록 명령을 내린다. 그러나 해킹이 고도화되면 해당 ECU의 모든 소프트웨어 동작을 변조할 수 있으므로 CAN Bus 상에서 전송되는 정상적 통신 데이터를 모니터링하여 프로세서 ID 및 통신용 암호키를 유추하고 위조할 수 있으며 통신 차단 명령도 무시할 수 있다. 따라서 해킹에 의한 통신 방해 및 악의적 데이터 전송을 원천적으로 방지하기 위해서는 해킹된 노드의 통신을 CAN Bus 상에서 하드웨어적으로 차단하여야 한다.

CAN Bus에서 내부 공격에 대응하는 기법에는 [11]에서 제안된 방법을 사용한다. [11]에서는 IDS(Intrusion Detection System)와 NES(Node Expulsion System)라는 하드웨어를 사용한다. IDS는 기존 연구에서도 많이 제안된 바 있으며 데이터 프레임의 내용을 분석하여 현재 송신 중인 노드가 해킹당한 노드인지 판단한다. NES는 IDS가 해킹당한 노드로 지목한 특정 노드를 CAN Bus에서 추방하는 기능을 수행하는 블록으로 일반적인 CAN Bus에는 없는 기능이다.

IDS는 CAN Bus를 항상 모니터링하다가 어떤 노드가 악의적인 데이터 프레임을 송신하는 경우 데이터 내용을 분석하여 노드가 해킹당한 것을 감지한다. 이후 해킹당한 노드가 송신할 때마다 데이터 내용과 관계없이 NES가 에러 프레임을 발생시켜 송신을 막는다. 해킹당한 노드는 데이터를 송신할 때마다 송신 에러 카운트가 지속적으로 증가하고, 에러 패시브 상태를 지나 버스 오프 상태가 되어 더 이상 송신이 불가능하게 된다.

CAN Bus 상의 노드에는 주소가 없기 때문에 해킹을 당하여 악의적인 데이터 프레임을 전송하여도 어느 노드가 해킹당했는지 식별하기 어렵다. 따라서 기존의 CAN 컨트롤러를 수정하여 CAN Bus가 부팅할 때마다 자동으로 노드의 고유 ID를 정하고 이를 통해 CAN Bus 내부의 공격에서 안전하게 방어하는 기법이 제안되었다. 이는 Verilog HDL을 이용하여 CAN 컨트롤러를 설계하였으며 시뮬레이션을 통해 제안한 기법이 성공적으로 노드마다 ID를 자동으로 부여하고 내부 공격에 대한 방어를 수행하는 것을 확인함으로 검증되었다.

3.2 안정성 향상을 위한 CAN Bus 모니터링 기법[12]

최근 차량에 탑재되는 ECU의 개수가 증가하고 있으며 개수가 증가할수록 CAN Bus의 부하가 증가한다. 이는 차량 안정성에 심각한 영향을 미친다. 따라서 차량과 같은 고안전성(Safety Critical) 시스템의 CAN Bus를 설계할 시, 이전보다 많은 양의 통신을 해야 함에도 불구하고 CAN Bus의 통신부하를 제한하여 시스템의 안전성을 확보한다. 이는 추가적인 CAN Bus 장착이나 사용 메시지 개수의 제한 등의 문제를 야기한다.

[12]에서는 정형 기법 도구인 UPPAAL을 이용하여 모니터를 모델링하였다. 모니터는 메시지를 수신하면 PWM 레벨을 읽어 타이밍 오류를 판별하며 주기 P 동안 2번 이상의 메시지를 수신하여도 타이밍 오류를 출력한다. 시뮬레이션 환경은 Vehicle Spy3와 neoVI RED, MPC5606B를 이용하여 구축하였고 CAN bit rate는 500kbps이다. MPC5606B의 CAN 모듈에서 제공하는 16비트의 Free-Running Timer 레지스터를 이용하여 수신 메시지의 Time Stamp를 얻을 수 있다. 모니터링은 메시지 수신 ISR(Interrupt Service Routine)에 의해 실시간으로 타이밍 오류를 감지한다. 이러한 CAN Bus 모니터 기능은 타이밍 오류를 일으키는 메시지를 회복시킬 기회와 차량 안전성 향상을 위한 가능성을 제공할 수 있다.

3.3 보안 알고리즘을 반영한 확장된 CAN Bus[3]

CAN Bus 통신 표준규격은 ISO11898이며, 한 번에 보낼 수 있는 Data는 8바이트로 미국표준인 AES 암호화 방식과 한국표준인 ARIA 방식으로 암호 통신을 할 경우 최소 Data가 16바이트가 되기 때문에 한 번에 전송할 수 없다. 이로 인하여 암호화 통신할 때 성능이 감소하게 되는데, 이를 암호화 방식별로 통신성능을 비교 분석한다.

[3]에서는 32비트 CPU와 CAN Controller Device로 검증용 하드웨어를 구현하고, FreeRTOS 환경하에서 ISO11898 Protocol을 구현하여 성능시험용 알고리즘을 제작하고, AES 암호방식과 ARIA 암호방식, 64비트 HIGHT 등 3가지의 암호화에 대한 통신성능은 평문일 때, AES 128비트, 192비트, 256비트, ARIA 128비트, 192비트, 256비트 방식별로 각각 같은 길이의 암호화 패킷을 보내 수신 측에서 Bitrate 시간으로 비교 분석

하며, 암호화와 복호화에 처리 시간은 암호화 방식별로 암호화 시작 지점과 완료 지점에 하드웨어 Flag를 두어 Oscilloscope 계측 장비로 시간을 측정한 후 어떤 방식이 가장 효율이 높은지 비교 분석하여 암호화에 적합한 CAN 통신 알고리즘을 제안한다.

암호화 처리 시간은 ARIA 방식이 AES 방식보다 8배 이상 빠른 성능을 보였으며, HIGHT ECB 방식은 1ms 정도로 ARIA보다 2.5배 정도 더 소요되었다. 암호화 방식별 통신 속도를 비교해보았을 때 평문일 때는 32,046 Bitrate, HIGHT 방식은 29,539 Bitrate, AES128 비트 10,791 bitrate, ARIA128비트는 14,497 bitrate로 AES 방식보다 ARIA 방식이 134% 더 효율이 높았고, ARIA128비트 방식이 HIGHT 방식보다 49% 정도 효율이 낮았다. 128 비트 방식이 64 비트 방식보다 낮은 이유는 암호화된 최소 Packet 길이가 128 비트이기 때문에 한 번에 보낼 수 없어 두 번에 걸쳐 보내는데 많은 Overhead가 들어가기 때문이다. 따라서 통신 효율을 높이려면 한 번에 최소 16바이트 길이의 Packet을 보낼 수 있는 구조이어야 한다. CAN 2.0B Frame에서 Data Length Code가 현재는 8Byte까지 표시되는데, 16Byte까지 사용할 수 있도록 하고, Data Field는 16N(N:0-16)=128비트로 하여 길이를 확장하여야 암호화된 Packet인 경우 통신성능을 높일 수 있다.

4. 결론

본 논문에서는 CAN Bus 보안에서의 취약점과 개선 방안 및 안정성 향상 방안을 소개하였다. 물리계층에서의 해킹 위협을 탐지할 수 있는 연구가 진행되었고 CAN 통신의 안정성 향상을 위한 연구가 진행되었다. 또한 CAN 통신 암호화에 관한 연구들이 진행되고 있다. 암호화하지 않고 통신하는 CAN의 특성상 해커의 표적이 되기 쉽다. 인명 피해가 일어날 수 있는 부분인 만큼 빠르고 안정적인 CAN Bus 통신을 위한 지속적인 연구가 필요하다.

5. Acknowledgment

이 논문은 부분적으로 2021년도 정부(과학기술정보통신부)의 재원으로 정보통신기술진흥센터의 지원을 받아 수행된 연구임(No.2018-0-00264, IoT 융합형 블록체인 플랫폼 보안 원천 기술 연구, 50%) 그리고 부분적으로 2021년도 정부(과학기술정보통신부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구임(No. NRF-2020R1F1A1048478, 50%).

참고문헌

[1] O. Avatefipour and H. Malik, “State-of-the-artsurvey on in-vehicle network communication “CAN-Bus” security and vulnerabilities,” Int. J. Comput. Sci. and Netw., 2017.

[2] 서화정, 권용빈, 권혁동, 안규황."자율주행자동차 보안 동향."정보보호학회지28.5(2018):9-14.

[3] 홍봉조, 한인철, 장동원, 이남용."보안 알고리즘을 반영한 확장된 CAN Bus 통신에 관한 실증적 연구."한국통신학회논문지43.9(2018):1525-1531.

[4] O. Avatefipour and H. Malik, “State-of-the-art survey on in-vehicle network communication “CAN-Bus” security and vulnerabilities,” Int. J. Comput. Sci. and Netw., 2017.

[5] R. Došek, et al., “Secure high level communication protocol for CAN BUS,” Annals of DAAAM & Proc. 2015, vol. 26 no. 1, pp. 1009-1015, 2015.

[6] K. W. Kang, “Real time framework and platform design based on CAN communication,” Ph.D.dissertation, Dept. of Compt., Chonnam Univ., 2015.

[7] D. Selent, “Advanced encryption standard,” Rivier Academic J., vol. 6, no. 2, pp. 1-14, 2010.

[8] KISA, “Combined public-private-use block cipher algorithm ARIA algorithm specification,” pp. 4, 2004

[9] KISA, “HIGHT block encryption algorithm specification and detailed specification,” pp. 2, 2009.

[10] 강태욱, 이종배, 이성수."CAN 버스에서 노드 ID 자동 설정을 통한 물리 계층 보안 기법."전기전자학회논문지24.2(2020):294-297.

[11] T. Kang, J. Lee and S. Lee, “Counterattack Method against Hacked Node in CAN Bus Physical Layer,” j.inst.Korean.electr.electron.eng., vol.23, no.4, pp.1469-1472, 2019.

[12] 김태욱, 조범연, 최진영."안전성 향상을 위한 차량내 CAN BUS 모니터링 기법."한국자동차공학회 춘계학술대회.(2017):671-672.