블록체인을 활용한 CAN 데이터 프레임의 신뢰성 검증에 관한 연구

최수민*, 김재영**, 신용태**
*숭실대학교 융합소프트웨어학부
**숭실대학교 컴퓨터학부
e-mail : suumn1538@soongsil.ac.kr

A Study on the Reliability Verification of CAN Data Frame Using Blockchain

Su-Min Choi*, Jae-Young Kim**, Yong-Tae Shin**
*Dept. of Software Convergence, Soong-Sil University
**Dept. of Computer Science, Soong-Sil University

요 약

최근 커넥티드카, 자율주행차량 등 차량에 관한 기술이 연구개발 되어 발전함에 따라 차량의 기술이 더욱더 확장되었다. 주변 차량, 인프라, 네트워크, 스마트폰 등 다양한 통신 기기들이 차량과 연결이 가능해졌다. 다만, 차량 기술의 발전과 더불어 차량 시스템 해킹 공격 방식이 다양해지고 있지만 이에 관한 연구와 대응 방안은 미흡한 편이다. 따라서 본 논문에서는 블록체인을 활용하여 차량 통신에 사용되는 CAN(Controller Area Network) 데이터 프레임 내의 차량 ID 가 해킹 공격에 의해 위・변조 되는 것을 방지함으로써 신뢰성 검증이 가능한 방안에 대해 제안하였다.

1. 서론

최근 자율주행차량에 관한 관심이 높아짐에 따라 자율주행 기술 개발 또한 활발히 진행되고 있다. 하지만, 차량 기술의 발전과 동시에 차량 해킹 공격 방식도 차량 외부 시스템 해킹, 차량 내부 시스템 해킹, 차량 보안・안전 시스템 해킹 등 점차 다양해지고 있다. 이 중에 차량 내부 시스템 해킹에서는 차량 ECU (Electronic Control Unit)에서 주고받는 CAN(Controller Area Network) 데이터 프레임에 무작위로 값을 대입하는 반복적인 공격을 통해 ECU 접근제어 기능을 무력화시키거나 기능에 대한 권한을 획득하는 공격 방식이 있다. 이 방식은 공격자가 차량 고유의 User ID 만 알아내면 데이터 프레임의 비트를 변경하고 임의로 차량을 조작할 수 있게 된다. 하지만 차량 운전자는 해당 프레임이 조작되었는지, 누구에 의해 조작되었는지 전혀 알 수 없다. 이로써 공격자는 차량의 조작·제어 기능에 대한 권한을 쉽게 획득하여 차량의 주행을 조작 할 수 있게 되고, 운전자는 제어 기능에 대한 권한이 없으므로 만일 사고 발생 시 인명사고로 까지 이어질 수 있다[1].

따라서 본 논문에서는 공격자가 차량 ID 를 알아낼 수 없도록 차량에서 주고 받는 CAN 데이터 프레임을 해시 알고리즘을 통해 암호화한 후, 블록체인을 활용해 암호화된 값을 저장하고 관리하는 것으로 신뢰성을 검증하는 방안에 대해 제안하였다.

2. 관련 연구

본 장에서는 제안하는 방안에 기반이 되는 CAN 통신의 동작 과정, 메시지 구조, 해시 알고리즘과 블록체인에 대해 설명한다.

2.1 CAN(Controller Area Network) 통신

CAN(Controller Area Network) 통신은 높은 수준의 보안 기능을 갖춘 실시간 통신 프로토콜이며, 초기에 자동차에 적용하기 위해 설계된 직렬 네트워크 통신 방식이다. 최근에는 다양한 산업 분야에 폭넓게 적용되고 있다. 초기에는 일대일(Point to Point) 통신인 UART(Universal Asynchronous Receiver Transmitter) 방식을 사용하였다. 하지만 UART 의 일대일 방식은 서로 다른 3 개의 ECU 간의 통신을 할 수 없기 때문에 다중 통신이 가능한 CAN 통신 프로토콜을 개발하게 되었다.

2.1.1 CAN 동작 과정

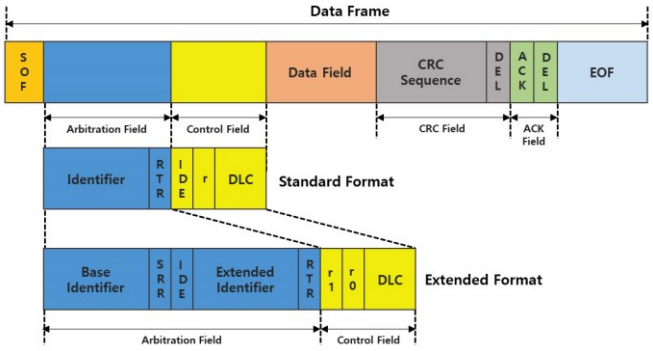
CAN 버스에는 전체 노드를 제어하는 주인 노드(Master Node)가 없는 직렬 구조이기 때문에 데이터로 비교적 쉽게 접근할 수 있다.

CAN 제어기를 사용하기 위해 CAN 버스 선이 다른 제어기에 의해 사용 중인지를 확인한다. CAN 버스 선을 해당 제어기가 사용 가능하다면 네트워크상의 모든 노드 즉, 모든 ECU 는 메시지를 수신한다. 그

후에 식별자를 통해 전송 받은 메시지가 자신에게 필요한 메시지를 확인하는 과정에서 자신에게 불필요한 메시지는 무시하고 필요한 메시지만 선택적으로 입력받아 데이터를 분석한다.

차량에서 각각의 ECU 는 고유한 ID 값을 가지고 있기 때문에 다중 노드가 동시에 메시지를 CAN 버스에 전송하려는 경우, 가장 낮은 ID 값을 가진 최우선 노드가 자동으로 버스에 접근하게 된다. 우선순위가 높은 메시지는 CAN 버스의 우선 사용 권한을 보장받을 수 있으며 순위가 낮은 다른 노드들은 대기한 후에 자동으로 다음 버스 사이클에서 재전송된다 [2][3].

2.1.2 CAN 메시지 구조



CAN 통신은 프레임이라고 하는 패킷을 통해 데이터를 전송한다. 프레임은 하나의 메시지를 이루는 필드나 비트들의 집합을 말하며 CAN 프레임은 그림 1 과 같은 분할 구조로 구성되어 있다.

- SOF(Start Of Frame) : 한 개의 dominant 비트로 구성되어 있으며, 메시지의 처음을 지시하고 모든 노드의 동기화를 위해 사용된다.
- Arbitration Field(중재 필드) : 11 비트 또는 29 비트의 크기를 갖는 ID 와 1 비트의 RTR(Remote Transmission Request) 비트로 구성되며, 이 영역은 둘 이상의 노드에서 메시지의 전송이 동시에 일어날 경우 발생하는 메시지 간의 충돌을 조정하는 데 사용된다. RTR 비트의 값은 데이터 프레임인지('d') 리모트 프레임인지('r')를 결정하는 데 사용된다.
- Control Field(제어 필드) : 2 비트의 IDE(Identifier Extension) 비트, 4 비트의 데이터 길이 코드(DLC, Data Length Code)로 구성되며, R0 는 Reserved 비트(Extended Can 2.0B R0, R1)이다.
- Data Field(데이터 필드) : 8bytes 까지 사용 가능하며, 데이터를 저장하는 데 사용된다.(특정한 노드에서 다른 노드로 전송하는 데이터를 포함)
- CRC(Cyclic Redundancy Check) : SOF 에서부터 데이터 필드까지의 비트열을 이용해 생성한 15 비트의 CRC 시퀀스와 하나의 'r'비트의 CRC 델리미터로 구성되어 있으며, 메시지 상의 에러 유무를 검사하는 데 사용된다.
- ACK(ACKnowledge) : 한 비트의 ACK 슬롯과 하나의 ACK 델리미터('d')로 구성되어 있으며, 임의의 노드에서 올바른 메시지를 수신하게 되면 ACK 필드를 받는 순간 ACK 슬롯의 값을 'd'로 설정해 버스 상에서 계속 전송하게 된다.
- EOF(End Of Frame) : 7 개의 'r'비트로 구성되어 메시지의 끝을 알리는 목적으로 사용된다.

(그림 1) CAN 메시지 구조[4]

2.2 해시(Hash) 알고리즘

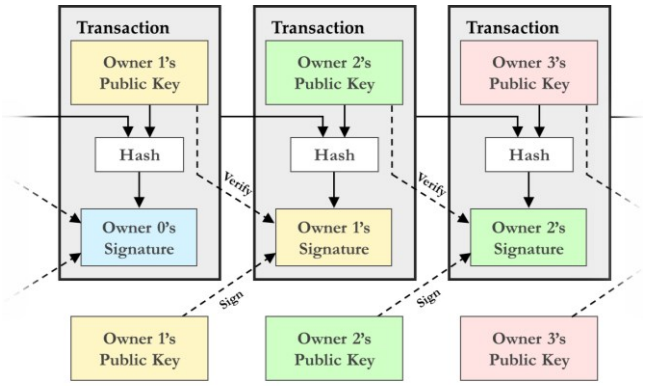
해시 알고리즘은 주로 데이터 위·변조 검사, 데이터의 빠른 검색, 통신의 안전성 증명, 패스워드의 안전한 보관 등에 사용되었다. 최근에는 전자서명, 불법 저작물 차단, 홈페이지 해킹 여부 판단, 암호 화폐의 신뢰성 확보, 전자투표 등으로 활용 범위가 점차 확대되고 있다.

임의의 비트열을 고정된 길이의 비트열로 변환시키는 함수로 해시 함수에 의한 결과 값을 해시 값(Hash value)이라고 한다. 해시 값은 입력하는 데이터의 개수와 용량에 관계없이 그 해시 함수가 정해놓은 일정한 크기의 비트열로 표현된다.

2.3 블록체인(Blockchain)

블록체인은 네트워크 참여자가 공동으로 정보를 검증하고 해시 기반으로 블록을 처리하여 기록·보관함으로써 공인된 제 3 자가 없이도 무결성 신뢰성을 확보하여 분산 원장을 가능하게 하는 기술을 말한다.

사용자간에 정보 전달이 이뤄지는 일련의 과정을 트랜잭션(Transaction)이라고 하며, 발생한 정보와 직전 블록의 정보를 암호화 시켜 하나의 새로운 블록을 만든다. 이렇게 만들어진 새로운 블록은 이전 블록의 해시 정보를 통해 연결하여 그림 2 와 같은 방식으로 체인을 이루게 된다. 새로운 블록을 생성할 때마다 직전 블록의 정당성을 검증하고 연결되기 때문에 블록의 신뢰성은 더 커지고 가치 있는 정보가 된다.



(그림 2) 블록체인의 동작 절차[5]

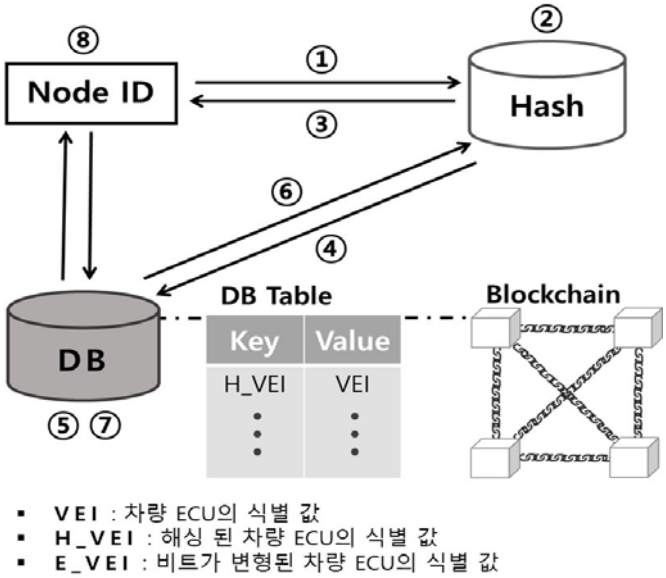
3. 블록체인을 활용한 CAN 데이터 프레임의 신뢰성 검증

본 장에서는 제안하는 기법인 블록체인을 활용한 CAN 데이터 프레임의 신뢰성 검증 방안에 대해 설명한다. 이는 신뢰성 검증을 위해 해시 알고리즘을 통해 암호화된 CAN 데이터를 블록체인을 활용하여 값

을 저장하고 관리하는 것이다.

본 논문에서는 차량 내에서 주고받는 CAN 프레임에서 Identifier 데이터 요소를 암호화하여 외부 공격자에 의해 발생하는 해킹 공격에 대한 가능성을 줄이는 방안에 대해 제안하였다. 차량 내부에서 ECU 간에 주고받는 데이터 프레임의 요소 중에 Identifier 데이터 비트에 포함되는 Node ID 즉, ECU 고유의 User ID 값을 넣지 않고 해당 값을 해시 하여 해시 된 값을 데이터 비트에 포함시킨다. 이렇게 해시 된 값을 Key 값으로 설정하고 해시 되기 전 원래의 User ID 값을 Key 값에 대한 Value 로 설정한다. 원래의 User ID 값을 보관하기 위한 DB 를 두어 해시 된 User ID 값인 Key 값과 원래의 User ID 를 일대일로 연결시킨다.

따라서 만일 사용자가 아닌 공격자가 데이터 프레임을 변형시키기 위해 차량의 User ID 를 알아내려고 해도 Identifier 에 포함되어 있는 User ID 가 해시 된 값이기 때문에 외부에서 쉽게 확인할 수 없어 공격이 불가능해진다. 또, 만일 해킹을 하여 데이터 프레임의 비트를 변형하여 전송하였다고 해도 다른 데이터 프레임과 비트를 비교하여 오류가 있음을 확인할 수 있고 정확히는 해킹 공격으로 인해 조작된 Key 값으로는 DB 에 일대일로 연결된 원래의 User ID 값을 확인하지 못하기 때문에 공격을 받아 비트가 변형되었음을 알 수 있게 된다. 이러한 과정을 통해 변형되고 조작된 데이터 프레임을 전달 받은 ECU 는 요청된 동작을 수행하지 않고 해당 메시지를 무시한다. 송신 측 ECU 에서는 수신 측 ECU 로부터 ACK 비트를 전달 받지 못함으로써 전송 과정에서 오류가 있었음을 파악하고 수신 측 ECU 에게 데이터 프레임을 재전송하게 된다. 제안한 암호화 된 CAN 프레임의 해싱 및 오류 비트 검증 절차는 그림 3 와 같다.



(그림 3) CAN 프레임 해싱 및 오류 신뢰성 검증 절차

CAN 프레임 및 오류 신뢰성 검증에 관한 절차는 다음과 같다.

① ECU 간에 메시지 전송 전에 해싱 하기 위해 송신 ECU 의 고유 ID 인 VEI 값을 전달한다.
② 전달받은 VEI 값을 해싱 한다.
③ 해싱 된 값인 H_VEI 값을 요청한 ECU 에게 전달한다.
④ 기존의 VEI 값과 H_VEI 값을 저장하기 위해 DB 로 전달한다.
⑤ DB Table 에 VEI 값과 H_VEI 값을 일대일로 연결하여 저장하고, 해당 값은 블록체인으로 활용하여 신뢰성을 높인다.
⑥ 앞의 과정을 거치고 난 후, 전송되는 비트가 변형되었을 경우, 오류 확인을 위해 해킹이 의심되는 E_VEI 값을 DB 로 전달한다.
⑦ 전달받은 E_VEI 값을 블록체인으로 연결된 DB Table 에서 확인한 후, 일치하는 Key 값을 찾을 수 없으므로 오류로 판단하고 해당 메시지를 무시한다.
⑧ DB 로부터 요청에 대한 값을 전달받지 못했으므로 전달한 E_VEI 값이 해킹 공격으로 인해 변형된 오류 프레임이라고 판단하고 해당프레임을 무시하고 재전송한다.

4. 결론

최근 차량에 대한 관심이 높아짐에 따라 여러 기업이나 정부에서 주행 기술에 대한 연구가 활발히 진행되고 있다. 하지만 조작·제어 등의 주행 기술 발전에 많은 관심을 쏟는 것에 비해 차량 해킹에 대한 대안이나 방안 연구는 아직 미흡한 부분이 있다. 이에 본 논문에서는 블록체인을 활용하여 ECU 간에 주고받는 CAN 데이터 프레임을 해시함수를 통해 암호화하였고, 이처럼 해시 된 값을 통해 외부에 차량 고유의 User ID 가 노출되거나 임의로 변경되어 공격자에 의해 차량이 조작되는 문제점을 개선하고, 신뢰성을 검증하였다.

Acknowledgment

이 성과는 2018 년도 정부(교육과학기술부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구임(No. 201817221336).

참고문헌

[1] “지능형 자동차 보안 위협 및 대응 방안 보고서”, 정보통신기술진흥센터, 2007.
[2] “Introduction to the Controller Area Network (CAN)”, Application Report, SLOA101B-August 2002-Revised May 2016.
[3] “Security Solutions for The Controller Area Network”, IEEE VEHICULAR TECHNOLOGY MAGAZINE, March 2018.
[4] “CAN(Controller Area Network) 통신 소개 및 동작 방법”, 슈어소프트테크, 2016.
[5] “ Sweden plans to adopt Blockchain for land transaction”, Anthony Wallace, 28 June, 2016