차량 내부 네트워크에서 메세지 인증을 이용한 사이버 공격 탐지

이수윤, 박서희, 송호진, 백영미*

창신대학교

Cyber Attack Detection Using Message Authentication for Controller Area Networks

Suyun Lee, Seo-Hee Park, Ho-Jin Song, Youngmi Beak*

Changshin University

E-mail : ymbeak@cs.ac.kr

요 약

본 논문은 차량 내부 네트워크에서 메시지 인증을 사용하여 사이버 공격을 탐지할 수 있는 보안 시스템을 제안한다. 자동차 내부 네트워크는 브로드캐스트 방식으로 메시지를 전송하고 노드의 식별자를 사용하지 않으므로 송신자를 식별할 수 없다. 송신 노드는 제어 데이터를 암호화 해시함수를 사용하여 메시지인증코드를 생성하여 제어 데이터와 같이 전송한다. 메시지인증코드 생성 시, 결과의 임의성을 증가시키기 위해서 다차원 카오틱 맵을 적용하였다. 수신 노드는 수신한 메시지의 제어 데이터에 대해 생성된 메시지인증코드를 수신 메시지에 존재하는 메시지인증코드 값과 비교하여 전송된 메시지의 위조 여부를 탐지한다. CANoe와 CAPL(Communication Access Programming Language)을 사용하여 차량 내부 네트워크 환경을 구성하고 사이버 공격을 수행하여 성능을 평가하였으며 탐지율 100%의 성능을 보였다.

ABSTRACT

This paper proposes a new security system to detect cyber-attacks based on message authentication in a in-vehicle network. In the in-vehicle network, when a sending node transmits messages in a broadcast manner, it only uses a message identifier, rather than a node's identifier. It leads to a problem not identifying the source. In the proposed system, the sending node generates a message authentication code (MAC) using a cryptographic hash function to the control data and transmits it with the control data. When generating the MAC for each message, a multidimensional chaotic map is applied to increase the randomness of the result. The receiving node compares its MAC generated from the control data in the received message with the MAC of the received message to detect whether the message transmitted from the sending node is forged or not. We evaluate the performance of the proposed system by using CANoe and CAPL (Communication Access Programming Language). Our system shows a 100% of detection rate against cyber-attacks injected.

키워드

In-Vehicle Network, Controller Area Network, Cyber-Attacks, Chaotic Map, Message Authentication Code

Ⅰ. 서론

차량의 안전성과 편의성을 개선하기 위해서 차량 내부 네트워크는 다수의 여러 전자제어장치(Electronic Control Unit; ECU)를 연결하여 정보를 공유한다. 전자제어장치는 바디, 파워트레인, 새시 등의 차량 주요 시스템에서 각 구성 요소들을 제어하는데 사용한다. 차량의 전정화로 현대 차량에 들어가는 전자제어장치의 수가 늘어남에 따라 전자제어장치의 중요도는 커지고 있다.

최근 들어 차량 제조사들은 자율주행차, 스마트카, 커넥티드 카를 위해서 외부 플랫폼과의 연결에 열을 올리고 있다. 1985년 Bosch사에서 개발된 CAN(Controller Area Network)은 지금까지 상용차의 주요시스템을 위한 제어네트워크로 사용되고 있다. 즉, 수십 년 이상 사용되고 신뢰성과 안정성이 검증된 시스템이다. 그러나 외부와의 연결을 고려하지 않은 과거에 개발된 CAN은 각종 사이버 공격에 취약함이 드러났다.

본 논문은 차량 내부 네트워크에서 메시지 인증을 통한 사이버 공격 탐지 기법을 제안한다. 이 기법은 제어 데이터에 대해서 암호화 해시 함수를 적용하여 생성한 인증정보를 제공함으로써 수신 측에서 전송된 메시지에 대해 무결성을 검증하는 방식으로 사이버 공격을 탐지한다. 제안한 기법은 메시지 전송주기를 고려하여 최소 전송주기 내에서 빠르게 인증을 완료할 수 있는 경량의 보안 메커니즘으로, 소프트웨어로 구현하여 별도의 추가 하드웨어 장비 없이 사용할 수 있다. 작은 크기를 가지는 인증정보의 한계점을 극복하고 사이버 공격으로부터 견고한 시스템을 제공하기 위해서, 생성된 결과의 임의성을 높이는 방법을 채택하여 높은 보안성을 제공한다.

* Corresponding author

II. CAN 프로토콜의 취약점

CAN 프로토콜이 등장하기 전에는 각종 전자제어장치는 일대일(Point-to-Point) 방식으로 연결되었다. 이러한 방식은 장치를 연결하기 위한 배선의 양이 늘어나고 이로 인해 유지보수의 어려움 및 차량 무게증가 문제로 이어졌다. CAN은 각종 전자제어장치(노드)들을 단일 인터페이스로 통일하여 안정적인 네트워크 기능을 제공하고 상기된 문제들을 해결하였다. 송신 노드는 CSMA/CD(Carrier Sense Multiple Access/Collision Detection) 방식을 사용하여 CAN 버스 상에 메시지 전송 여부와 충돌 가능성을 파악한 후 자신의 메시지 전송 시기를 결정한다. 그러나 CAN은 메시지 전송 시에 송신 노드나 수신 노드의 주소를 사용하지 않는다. 다만, 브로드캐스트 전송 방식으로 인해 연결된 전자제어장치들이 전송된 메시지를 수신하므로, 전자제어장치들은 수신한 메시지의 식별자(Identifier; ID)를 확인하는 필터링을 수행한다. 필요한 메시지를 식별하고 필요 없는 메시지는 무시하는 것이다.[1] 메시지 전송 시 송수신 노드의 주소를 사용하지 않는 방법은 수신 노드가 수신한 메시지의 출처를 알 수 없고 위조와 도용을 구분하기 어렵다. 또한, 브로드캐스트 전송 방식을 사용하기 때문에 공격자는 손쉽게 CAN 버스 상의 데이터를 열람할 수 있다. 이러한 점이 CAN이 사이버 공격의 취약에 취약한 이유이다.

III. 암호화 해시 함수를 이용한 메시지 인증

본 논문에서는 암호화 해시 함수 기반의 메시지인증코드(Message Authentication Code; MAC)를 송신 노드가 CAN 프레임을 통해 제공하면, 수신 노드는 수신한 CAN 프레임에 대한 메시지 인증을 수행함으로써 사이버 공격 여부를 탐지한다. 다시 말하면, 송신 노드는 전자제어장치 간에 제어를 위해 공유되어야 하는 제어 데이터에 대해서 암호화 해시 함수를 통해 생성된 MAC을 제어 데이터와 맵 번호와 함께 전송한다. 이 세 가지 정보의 전송은 CAN 프레임의 8바이트 크기의 데이터 필드를 이용한다. 수신 노드는 수신한 제어 데이터에 대해 송신 노드와 동일한 방법으로 MAC을 생성하고 제어 데이터와 비교하여 사이버 공격을 탐지한다. 예를 들어, 제어 데이터의 크기가 1바이트로 주어지면, CAN 프레임의 데이터 필드는 제어데이터를 위한 1바이트, 카오틱 맵(Chaotic map) 번호를 위한 1바이트를 할당하고, 나머지 6바이트의 공간에 MAC를 할당한다. 만약 제어 데이터가 1바이트 이상일 경우, 제어 데이터와 1바이트의 카오틱 맵 번호를 할당하고 남은 공간에 생성된 MAC을 할당함으로써 제어데이터의 크기에 따른 MAC 길이의 가변성을 고려한다. 이러한 가변성을 고려한 방법은 MAC 길이 축소에 따른 보안성 약화에 대한 우려가 있으므로, 다중 카오틱 맵 선택과 Salt 생성을 통해서 보안성을 강화한다.

암호화 해시 함수의 초기 입력값은 제어 데이터와 카오틱 맵 기반의 Salt를 사용한다. 카오틱 시스템은 매개변수에 대한 민감도, 에르고딕성을 가지고 있다.[2] 즉, 임의성(Randomness)을 극대화하기 위해 다차원 카오틱 맵을 Salt 생성에 사용한다. 송수신 노드 간에 명시적인 동기화 없이 다중 카오틱 맵을 사용하기 위해서는 초기 조건, 반복 횟수 값이 필요하다. 단, 다중 카오틱 맵에서 하나를 선택하기 위해서 사용되는 카오틱 맵 번호는 송신 노드가 명시적으로 CAN 프레임을 통해 제공한다. 초기 조건은 CAN 노드에 미리 배포된 비밀 키를 사용하여 생성[2]하였으며, 이 비밀키는 본 논문에서는 초기 조건 생성에 한 번만 사용된다. 비밀키로 초기 조건이 만들어지고 그 값이 한 번 사용되면, 이후의 초기 조건은 마지막으로 생성된 카오틱 맵의 결과값으로 재설정된다. 카오틱 맵에 두 번째 주요한 파라미터는 반복 횟수인데 이 값은 [2]에서 수정된 선형합동법을 사용하여 생성한다. 선택된 카오틱 맵과 초기 조건, 반복 횟수를 이용하여 생성된 Salt 값과 제어 데이터에 대해서, 송신 노드는 암호 해시 값인 MAC을 생성하고 전송한다. 여기서 사용한 암호화 해시 함수는 MD5이고 암호화 해시 함수의 반복 횟수는 앞서 생성한 Salt를 재사용하였다. 수신 노드는 메시지의 ID 값을 확인하고 자신에게 유효한 제어 데이터가 있는 메시지를 수신한다. 수신 메시지에 포함되어있는 카오틱 맵 번호와 이미 배포된 비밀키로부터 생성된 초기 조건, 수정된 선형합동법에서 생성된 반복 횟수를 사용하여 수신 측의 MAC을 생성하고 메시지 내의 송신 측의 MAC과 비교한다. 두 개의 MAC이 동일한 경우, 무결성을 만족한 것으로 간주하고 수신 노드는 제어 데이터를 사용한다. 만약 다를 경우, 수신한 메시지를 사이버 공격으로 판단하고 제어데이터를 무시한다.

IV. 성능평가

CANoe와 CAPL(Communication Access Programming Language)을 이용하여 차량 내부 네트워크 환경을 구현한다.[4] 이때 실제 차량에서의 CAN 버스 내에서 메시지 이동하는 혼잡한 상황을 고려해서 SAE 벤치마크의 CAN 네트워크 구성을 참고하여 환경을 구성하였다.[3] 우선 SAE 벤치마크에 따라 노드를 6개 설정한다. 그림 1과 같이, 운전자의 시각에서 운전 환경을 패널을 이용하여 구현한 후 패널과 각 기능의 노드들을 연결시킨다.

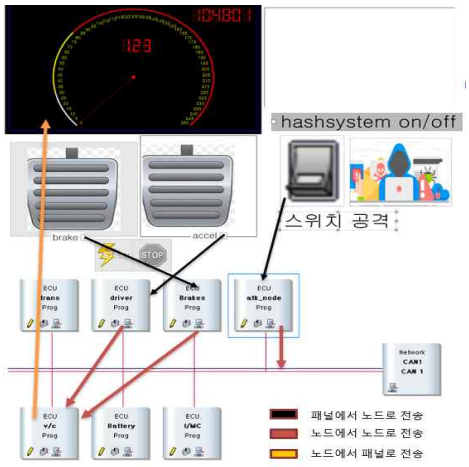

그림 1. 차량 내부 네트워크 구성 및 패널과 노드의 관계

그림 1에 나타난 바와 같이 패널의 brake와 accel은 각 ECU Brakes와 ECU driver로 연결되어 있다. 각 패널의 이미지를 클릭하면 각 연결된 노드로 신호가 전송된다. 이때 전송되는 메시지는 제안한 보안 메커니즘이 적용되지 않아서 사이버 공격에 취약한 CAN 메시지이다. 패널에서 신호를 받은 각 ECU들은 ECU v/c로 패널의 제어 데이터를 지속해서 송신하고 ECU v/c는 패널에 있는 계기판으로 현재 차량의 속도 데이터를 전송한다. Hashsystem on/off의 체크박스를 활성화하면, 차량 내에 송수신되는 노드들의 메시지들 전송 시, 본 논문이 제안한 보안 시스템이 적용된 상태로 전환이 된다. 사이버 공격을 주입하기 위해서는 체크박스 밑에 있는 스위치 공격의 스위치 컨트롤을 활성화하면

지속적으로 랜덤한 제어 데이터를 전송하는 퍼지 공격(Fuzzy attack)을 실행한다. 우리는 총 8초 동안 시뮬레이션을 실행하였다. ECU driver는 accel 컨트롤을 위한 제어 데이터를 50 ms 주기로 전송하고 사이버 공격은 300 ms 주기로 공격을 수행하였다. 총 8초 동안 전송된 186번의 메시지 전송에서, 사이버 공격은 26회 발생하였다. 메시지 인증을 수행하여 정상적인 신호로 판단한 것은 160회, 사이버 공격은 26회 탐지하여 사이버공격에 대한 제안한 보안 시스템의 탐지율은 표 1과 같다. 제안한 보안 시스템을 사용하지 않았을 때는 무작위로 속도계기판이 변하는반면, 제안한 보안 시스템을 사용하였을 때에는 사이버 공격을 감지하고 차단하는데 성공하였다.

표 1. 사이버공격 탐지율

전송 메시지 수	사이버 공격 비율	탐지율
186	13.9%	100%

Ⅴ. 결 론

우리는 차량 네트워크의 내에서 사용되는 CAN 메세지에 대해서 발생하는 사이버 공격을 탐지하기 위해서 암호화 해시함수를 이용한 메시지 인증 기법을 제안하였다. 이 방법은 특별한 추가 하드웨어의 장착 없이 구현이 가능하다는 장점과 제어 데이터의 크기에 따른 MAC 길이의 가변성을 고려하였다. 또한 작은 크기를 가지는 MAC의 한계점을 극복하고 사이버 공격으로부터 견고한 시스템을 제공하기 위해서 생성된 결과의 임의성을 높이는 다중 카오틱 맵을 채택하여 높은 보안성을 제공하였다. 그러나 보안 메커니즘의 효율성을 높이고 단순화하기 위해서 카오틱 맵을 통해 생성된 Salt를 암호화 해시 함수의 초기 값과 반복 횟수에 동일하게 사용하였으므로 개선이 필요하다.

Acknowledgement

This work was supported by the Gyeongnam SW Convergence Cluster 2.0 (Specialized Industry Reinforcement) and the National Research Foundation of Korea (NRF) grant funded by the Korea government (MSIT) (No. 2021R1F1 A1048179).

References

[1] Lim Myung-seop, “차량 통신 네트워크 기술,” *Information and Communications Magazine*, Vol. 24, No. 9, pp. 86-95, 2007.

[2] Pareek, N. K., Vinod Patidar, and K. K. Sud, “Cryptography using multiple one-dimensional chaotic maps,” *Communications in Nonlinear Science and Numerical Simulation*, Vol. 10, No. 7, pp. 715-723, 2005.

[3] Tindell, K., & Burns, A., “Guaranteed message latencies for distributed safety-critical hard real-time control networks,” Dept. of Computer Science, University of York, 1994.

[4] Vector. CANoe Product Information [Internet]. Available: https://cdn.vector.com/cms/content/products/canoe/canoe/docs/Product%20Informations/CANoe_ProductInformation_EN.pdf