Journal of the Korea Academia-Industrial cooperation Society
Vol. 25, No. 8 pp. 15-21, 2024

https://doi.org/10.5762/KAIS.2024.25.8.15
ISSN 1975-4701 / eISSN 2288-4688

Controller Area Network의 침입 탐지 시스템을 위한 제어 명령과 센서 데이터의 상관관계를 이용한 공격 탐지 알고리즘

사공상욱
계명대학교 컴퓨터공학과

Attack Detection Algorithm Exploiting Correlation between Control Command and Sensor Data for Intrusion Detection System in Controller Area Network

Sang Uk Sagong
Division of Computer Engineering, Keimyung University

요 약 현대의 차량은 센서와 액츄에이터를 제어하는 제어기를 장착하고 있다. 이들 제어기는 차량 내부 네트워크에 연결되어 있고, Controller Area Network (CAN)과 같은 차량 내부 네트워크 프로토콜을 이용하여 센서 및 제어 데이터를 교환한다. 차량 내부 네트워크는 데이터를 암호화하지 않고 메시지를 인증하지 않는다. 그러나 더 많은 제어기들이 전화망과 같은 외부 네트워크에 연결되어 있으며, 이런 제어기들이 현대의 차량에 탑재되고 있다. 외부 접점을 가지고 있는 제어기는 차량 내부 네트워크와 다른 제어기에게 공격 표면을 제공한다. 이 공격 표면을 통한 사이버 공격으로부터 차량을 보호하기 위해서, 제어기의 물리적인 특성과 차량의 물리적인 이동을 이용하여 공격을 탐지하는 침입 탐지 시스템이 개발되었다. 기존의 침입 탐지 시스템은 센서 데이터를 이용한다. 그 결과, 공격자는 한 메시지 내에 있는 모든 센서 데이터를 변경할 수 있다. 본 논문에서, 변조 메시지를 전송하는 제어기가 변경되지 않더라도, 제어 명령과 센서 데이터 간 상관도를 추적하여 공격을 탐지할 수 있는 침입 탐지 시스템을 제안한다. 하나의 제어 명령을 하나의 센서 데이터와 상관도를 가지게 만드는 수학적인 방법을 개발한다. 제안한 침입 탐지 시스템의 성능을 실제 차량에서 수집된 데이터를 이용하여 검증한다.

Abstract Modern automobiles have electronic control units (ECUs) that control sensors and actuators. ECUs are connected to in-vehicle networks and exchange sensors and control data using in-vehicle network protocols, such as controller area network (CAN) protocols. These in-vehicle protocols do not encrypt data or authenticate messages. On the other hand, an increasing number of ECUs are connected to external networks, such as cellular networks, and these ECUs are installed in modern automobiles. These ECUs with outward-facing interfaces provide attack surfaces to in-vehicle networks and other ECUs. Intrusion detection systems (IDSs) that detect attacks using the physical properties of ECUs or the physical movement of a car have been developed to protect cars from cyber attacks through these attack surfaces. A conventional IDS exploits only sensor values. As a result, an adversary may spoof all sensor values in the same CAN message. This paper proposes an IDS that can detect an attack even if the transmitter of the spoofing message remains the same by tracking the correlation between control signals and sensor values. A mathematical methodology that correlates a control command with sensor data was developed. The detection performance of the proposed IDS was evaluated using CAN message data collected from a real car.

Keywords : Controller Area Network, Intrusion Detection System, Data Falsification Attack, Correlation, Control Data, Sensor Data

본 논문은 계명대학교 연구과제로 수행되었음.
*Corresponding Author : Sang Uk Sagong(Keimyung Univ.)
email: susagong@kmu.ac.kr
Received May 20, 2024 Revised June 17, 2024
Accepted August 2, 2024 Published August 31, 2024

1. 서론

현대 차량은 제어기(ECU)를 탑재하고 있으며, 제어기를 이용하여 차량 자세 제어, 연비 향상 및 인포테인먼트 기능을 승객에게 제공한다. 제어기는 차량 제어 신호 및 센서 데이터를 차량 내부 네트워크를 통해서 교환한다. CAN 프로토콜을 포함하여 차량 내부 네트워크 프로토콜은 차량 내부 네트워크가 외부 네트워크와 연결되어 있지 않은 환경을 고려하여 개발되었다. 무선으로 새로운 기능을 추가하고, 내비게이션 지도를 실시간으로 업데이트하는 등 다양한 편의 기능을 승객에게 제공하기 위해서, 전화망, Wi-Fi, 블루투스 등 외부 네트워크와 연결할 수 있는 외부 접점을 보유한 제어기들이 차량에 탑재되고 있다. Fig. 1은 다수의 제어기가 CAN 버스 네트워크에 연결되어 있는 것을 보여주며, 주황색으로 표시한 제어기가 외부 접점인 On-Board Diagnostic(OBD)-II 포트, 텔레매틱스, 인포테인먼트 시스템이다. 이들 외부 접점을 보유한 제어기는 차량 내부 네트워크 및 해당 제어기에 대한 공격 표면을 발생한다[1,2]. 공격자는 공격 표면을 이용하여, 제어기 소프트웨어 또는 차량 내부 네트워크에 접근할 수 있다. 공격자가 제어기 소프트웨어에 접근하여 해당 소프트웨어를 변조할 수 있는 범위에 따라서, 차량 내부 네트워크에 메시지가 전송되지 못하도록 하거나, 변조 메시지를 주입할 수 있다[3]. 정상 메시지가 전송되지 못하면, 제어기는 과거 데이터를 사용하는 문제가 발생한다. 공격자는 변조 메시지를 주입하여, 차량을 임의로 제어할 수 있다. 다양한 차량 내부 네트워크 프로토콜 중에서, 본 논문에서는 보편적으로 양산 자동차에 적용되고 있는 CAN 프로토콜을 고려한다. 다른 차량 내부 네트워크에도 본 연구에서 제안한 알고리즘을 적용할 수 있다.

제어기의 물리적인 특성을 이용하여 공격을 탐지하는 기존의 침입 탐지 시스템은 데이터 필드만 변조하는 공격을 탐지할 수 없다. 데이터 필드만 변조하는 공격을 탐지하기 위해서, 차량의 물리적 신호 데이터 간의 상관도를 이용하는 침입 탐지 시스템이 개발되었다[4]. 하지만, 기존의 침입 탐지 시스템은 동일한 유형의 센서 데이터 2개를 이용하였으며, 해당 센서 데이터는 하나의 CAN 메시지를 통해서 전송된다. 그 결과, 공격자가 하나의 CAN 메시지 내의 모든 센서 데이터를 변조하면, 기존의 침입 탐지 시스템은 이런 유형의 공격을 탐지할 수 없다는 한계가 있다. 본 논문의 주요 연구 내용은 아래와 같이 기존의 연구와 차별성을 가지고 있다.

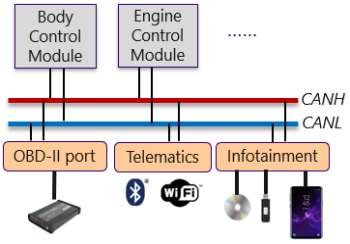

Fig. 1. ECUs are connected to CAN bus. ECUs in orange boxes have outward-facing interfaces whereas ECUs in gray boxes do not have outward-facing interfaces.

SOF	Arbitration		Control			Data	CRC	ACK		EOF
SOF	Message ID	RTR	IDE	RB0	DLC	Data	CRC	CDREL	ACK	ADCEKL	EOF
0	11 bits	0	0	0	4 bits	8-64 bits	15 bits	1	1 bit	1	1111111

Fig. 2. Data frame of the CAN protocol is composed of seven fields that are SOF, Arbitration, Control, Data, CRC, ACK, and EOF. The number of bits in Data field can variable from 1 to 8 bytes.

- 기존의 상관도 기반 침입 탐지 시스템의 한계를 분석하고, 해당 침입 탐지 시스템이 탐지할 수 없는 데이터 변조 공격 모델을 만든다.
- 기존의 침입 탐지 시스템이 동일한 유형의 센서 데이터만 사용했지만, 본 논문에서는 제어-센서 신호 간의 상관도를 이용하여 공격을 탐지하는 침입 탐지 시스템을 제안한다.
- 토요타 캠리에서 수집된 CAN 메시지 데이터를 이용하여, 제안한 침임 탐지 시스템의 공격 탐지 성능을 분석한다.

본 논문은 아래와 같이 구성되어 있다. 2장은 CAN 프로토콜과 공격 모델을 설명한다. 3장은 기존의 침입 탐지 시스템에 대한 연구를 정리한다. 4장은 제어-센서 신호 상관도 기반의 침입 탐지 시스템을 제안한다. 5장 실제 차량에서 수집된 CAN 메시지 데이터를 이용하여, 제안한 침임 탐지 시스템의 성능을 실험적으로 분석한다. 6장은 본 논문의 결론이다.

2. 배경

2.1 CAN 프로토콜

Fig. 2는 CAN 프로토콜의 데이터 프레임의 구조이며, Start of Frame (SOF), Arbitration, Control, Data,

Cyclic Redundancy Check (CRC), ACK, End of Frame (EOF) 필드로 구성되어 있다. Control 필드의 DLC는 데이터 필드의 크기를 나타낸다. 해당 데이터 프레임을 수신하는 제어기는 SOF 필드부터 데이터 필드까지의 비트를 이용하여 CRC 값을 계산하고, 수신한 CRC 값을 비교한다. CRC 값이 서로 같으면, ACK 필드의 ACK 영역은 해당 데이터 프레임을 정상적으로 수신한 제어기가 0으로 작성한다. ACK 영역이 0이 아니면, 송신 제어기는 전송 과정에서 오류가 발생했다고 판단하고 해당 데이터 프레임을 재전송한다. 제어기가 전송하는 CAN 메시지는 CAN 버스에 연결된 모든 제어기로 전송된다. 동시에 다수의 제어기가 각각의 CAN 메시지를 전송하고자 할 경우, 메시지 ID가 가장 작은 CAN 메시지가 우선 전송된다.

Fig. 2에서 볼 수 있듯이 CAN 메시지를 송신한 제어기를 확인하는 인증 필드는 존재하지 않으며, 데이터 필드의 내용은 암호화하지 않는다. 공격자는 다른 제어기가 전송하는 CAN 메시지의 내용을 확인하여, 주요 센서 및 제어 신호를 추출할 수 있다. 변조된 CAN 메시지를 주입하여, 차량의 가속, 제동 등을 악의적으로 조정할 수 있다[5].

제어기의 연산 능력과 메모리 크기의 한계로 인해서, 제어기는 복잡한 암호화 및 복호화 연산을 실시간으로 수행할 수 없다. 그러므로, CAN 버스와 제어기에 대한 공격을 방어하기 위해서, 데이터 필드를 암호화하기 매우 어렵다[6]. 또한, 기존의 제어기 및 부품과의 호환성을 확보하기 위해서, 메시지 인증을 위한 새로운 필드를 CAN 프로토콜에 추가하지 못한다. 그래서, CAN 버스에 전송되는 메시지의 주기, CAN 버스의 전압 및 신호 간의 상관도 등 물리적 고유 특성을 추적하여 공격을 탐지하는 침입 탐지 시스템이 차량에 적용되고 있다.

2.2 공격 모델

이 장에서 본 연구에서 고려한 공격 모델을 설명한다. 두 제어기 A와 B가 CAN 메시지 0x001과 0x002를 각각 전송한다고 가정한다. Fig. 3은 공격자는 제어기 B가 제어기 A인 것처럼 CAN 메시지 0x001을 같은 주기로 주입하고, 제어기 A가 0x001을 전송하지 못하도록 하는 위장 공격을 보여준다[7]. CAN 메시지를 전송하는 제어기를 식별하는 침입 탐지 시스템은 위장 공격을 탐지할 수 있다[7,8]. 공격자가 제어기 A를 해킹하여 데이터가 변조된 CAN 메시지 0x001을 전송하는 데이터 변조 공격을 Fig. 4가 보여준다[4]. 변조된 CAN 메시지 0x001

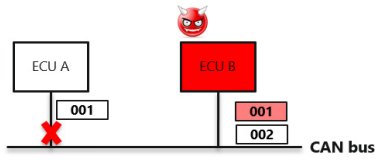

Fig. 3. Masquerade attack. An adversary suspends transmission of 0x001 from ECU A whereas 0x001 is transmitted from ECU B. ECU B pretends ECU A.

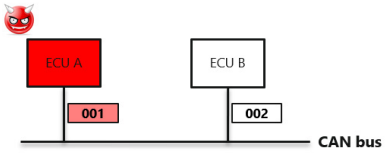

Fig. 4. Data falsification attack. Adversary maliciously modifies data field of 0x001, and the transmitter of 0x001 remains the same after the data falsification attack is launched.

을 제어기 A가 계속해서 전송하므로, CAN 메시지를 전송하는 제어기를 식별해서 공격을 탐지하는 침임 탐지 시스템은 데이터 변조 공격을 탐지할 수 없다. 데이터 간의 상관도를 이용하여 공격을 탐지하는 침입 탐지 시스템은 데이터 변조 공격을 탐지할 수 있다[4].

각 바퀴 속도 센서 데이터와 같이 동일한 유형의 센서 데이터는 하나의 CAN 메시지를 통해서 전송된다. 공격자는 하나의 센서 데이터만 변경하지 않고, 모든 센서 데이터를 함께 변경하는 데이터 변조 공격을 수행할 수 있다. Fig. 4와 같이, 공격자는 메시지 0x0B0를 송신하는 제어기를 해킹하여, 이 메시지의 데이터 필드를 임의로 변경할 수 있다. 메시지 0x0B0에 바퀴 속도가 모두 포함되어 있으므로, 공격자는 두 개 바퀴 속도를 변경한다. 그러나 공격자가 차량의 모든 제어기를 해킹하지 못하므로, 가속 명령이 전송되는 메시지 0x2C1의 데이터 필드까지 임의로 변경할 수 없다.

3. 기존의 침입 탐지 시스템

CAN 버스에서 전송되는 메시지 트래픽을 분석하여 공격을 탐지하는 침입 탐지 시스템이 제안되었다. 실제 차량에서 대부분의 CAN 메시지는 주기적으로 전송된다. 그러므로, CAN 메시지의 주기가 변경되는 것을 이용하여 공격을 탐지하는 침입 탐지 시스템이 제안되었다[9]. 또한 CAN 메시지 트래픽의 엔트로피를 측정하여, 정상

트래픽의 엔트로피보다 증가하면 공격으로 판단하는 침입 탐지 시스템이 개발되었다[10]. 공격자가 공격하려는 차량의 CAN 메시지 트래픽과 유사하게 공격 메시지를 주입하면, 이 두 가지 유형의 침입 탐지 시스템을 무력화할 수 있다.

공격자가 정상 CAN 메시지 트래픽과 유사하게 공격 메시지를 주입하더라도, CAN 메시지를 전송하는 제어기의 물리적인 특성을 이용하면 공격을 탐지할 수 있다. CAN 버스의 전압을 변경하여, 제어기는 CAN 메시지를 전송한다. CAN 버스 전압의 고유한 특성은 제어기의 CAN 트랜시버의 물리적 특성으로 결정된다. 그래서, 각 제어기가 보유한 전압 특성을 이용하여 공격을 탐지하는 침입 탐지 시스템이 제안되었다[8]. 시간 기반의 침입 탐지 시스템은 각 제어기의 클록 스큐(clock skew)를 이용하여, CAN 메시지를 전송하는 제어기를 식별할 수 있다[7]. 클록 스큐가 변경되면, 해당 CAN 메시지를 송신하는 제어기가 변경된 것이므로, 공격이 발생한 것이다.

4. 제어-센서 신호 상관도 기반의 침입 탐지 시스템

4.1 제어-센서 신호 데이터

각 메시지에 하나의 데이터만 존재하는 경우도 있지만, 모든 신호 데이터를 하나의 CAN 메시지를 통해서 전송하면, 메시지 ID의 개수가 부족하여 CAN 버스를 효과적으로 사용할 수 없다. 제어기는 다수의 제어및 센서 신호 데이터를 1~8바이트 사이의 비트시퀀스로 만들어서 하나의 CAN 메시지를 통해서 전송한다. CAN 메시지에서 우리가 원하는 제어 또는 센서 데이터를 추출하여 물리 신호 값으로 변환하는 과정은 아래와 같다.

- 대상 신호가 전송되는 메시지 ID, 신호를 저장하기 위한 비트 수, 데이터 필드 내의 비트 위치를 확인한다. Table 1은 토요타 캠리에서 수집한 CAN 메시지에서 주요 신호에 대한 메시지 ID, 비트 수 및 위치정보를 보여준다.
- 신호에 대한 비트 시퀀스를 십진수로 변환한다. 십진수 값에 스케일 팩터를 곱하고 오프셋을 더하면, 물리 값으로 변환할 수 있다.

메시지 ID, 비트 수 및 위치, 스케일 팩터, 오프셋, 단위는 역공학 또는 데이터베이스를 통해서 제한적으로 확인할 수 있다.

Table 1. Control and sensor signal in Toyota Camry. Speed-related control and sensor signals are embedded in a CAN message.

Signal	Message ID	Bit location	Number of bits	Unit
Wheel speed 1	0x0B0	0	16	km/h
Wheel speed 2	0x0B0	16	16	km/h
Engine speed	2C4	0	16	Unknown
Brake pressure	224	32	16	Unknown
Throttle	2C1	48	8	Unknown
Vehicle speed	610	24	8	km/h

4.2 두 벡터의 상관도

두 벡터 $\overrightarrow{A}=\{a_1,\dots,a_n\}$와 $\overrightarrow{B}=\{b_1,\dots,b_n\}$를 고려하자. $\overrightarrow{A}$와 $\overrightarrow{B}$의 i번째 요소를 각각 a_i와 b_i로 나타낸다. $\overrightarrow{A}$와 $\overrightarrow{B}$의 상관도 ρ는 Eq. (1)과 같이 계산한다.

$$\rho=\frac{\sum_{i=1}^{n}(a_i-\mu_a)(b_i-\mu_b)}{\sqrt[2]{\sum_{i=1}^{n}(a_i-\mu_a)^2}\sqrt[2]{\sum_{i=1}^{n}(b_i-\mu_b)^2}} \quad (1)$$

Where, μ_a and μ_b denote means of $\overrightarrow{A}$ and $\overrightarrow{B}$, respectively.

Table 1의 바퀴 속도(wheel speed) 1과 바퀴 속도 2의 상관도를 계산하면, 0.99이다.

4.3 제안하는 침입 탐지 시스템

제안하는 침입 탐지 시스템은 Fig. 5와 같이 CAN 메시지 필터 블록, 배열 생성 블록, 상관도 계산 블록, 누적합(CUSUM: cumulative sum) 블록으로 구성되어 있다. CAN 메시지 필터 블록은 상관도 계산에 사용될 제어 및 센서 신호 각 1개를 추출하여 물리 값으로 변경한다. 대상 제어 및 센서 신호를 각각 C와 S로 나타낸다. 효과적인 수식 분석을 위해서, 두 신호의 주기가 같다고 가정한다. 배열 생성 블록은 C 와 S의 데이터를 배열에 저장하고, 새로운 메시지를 수신할 때마다 각각의 배열을 Eq. (2)와 같이 갱신한다.

$$C=\{c_1,c_2,\dots,c_i,\dots\},S=\{s_1,s_2,\dots,s_i,\dots\},i\geq 1 \quad (2)$$

Where, w denote the window size.

$i \geq w$이면, $C_{w,i} = \{c_{i-w+1}, \cdots, c_{i-1}, c_i\}$와 $S_{w,i} = \{s_{i-w+1}, \cdots, s_{i-1}, s_i\}$를 상관도 계산 블록은 생성한다. Eq. (1)을 이용하여, 두 배열 $C_{w,i}$와 $S_{w,i}$ 간 상관도 ρ_i를 계산한다. $i < w$이면, 슬라이딩 윈도우 크기만큼 데이터가 없으므로, 상관도를 계산하지 않는다.

누적합 블록은 상관도를 추적하여, 상관도가 정상 범위를 벗어나는지 확인한다. 상관도가 정상 범위를 벗어나면, 데이터 변조 공격이 발생했다고 판단한다. 누적합 블록은 ρ가 입력되면, 이전 모든 ρ의 평균 μ_ρ과 분산 σ_ρ을 이용하여, Eq. (3)을 계산한다. ρ_{norm}을 누적하여, 사전에 정한 임계값보다 커지거나 작아지면, 공격이 발생한 것이다.

$$\rho_{norm} = \frac{\rho - \mu_\rho}{\sigma_\rho} \tag{3}$$

Where, μ_ρ and σ_ρ denote mean and standard deviation of previous ρ values, respectively.

제안하는 침입 탐지 시스템은 가속 명령과 바퀴 속도를 제어-센서 신호 짝으로 만들어 공격을 탐지한다. 가속 명령이 0보다 크면, 바퀴 속도는 증가하며, 가속 명령이 0이면 바퀴와 도로의 마찰력으로 바퀴속도가 감소한다. 바퀴 속도의 변화율은 가속 명령에 비례하므로, 가속 명령의 적분값을 Eq. (2)의 C로 사용한다.

5. 실험 결과

2010년식 토요타 캠리의 CAN 메시지 데이터를 이용하여, 제안한 침입 탐지 시스템의 공격 탐지 성능을 분석한다. 해당 CAN 메시지 데이터는 디어본 그룹 그리폰 장치를 이용하여 무선으로 CAN 메시지를 수집하였다[11].

Fig. 6은 토요타 캠리의 바퀴 속도 및 가속 명령을 추출한 예시이다. Table 1에 정리한 것과 같이, 바퀴 속도의 단위는 km/h이고, 스케일 팩터는 0.01이며, 오프셋은 0이다. 그러나, 가속 명령은 해당 비트를 십진수로 변환하여 임의 단위(AU: Arbitrary Unit)를 사용한다. 바퀴 속도는 동일한 제어기에서 송신되므로, 공격자는 4개의 바퀴 속도를 변경할 수 있다. 그러나 다른 제어기가 전송하는 가속 명령은 해당 공격자가 변경할 수 없다. 평균이 0이고 표준편차가 0, 4, 8, 12인 가우시안 잡음을 바퀴 속도에 더해서, 공격 데이터를 생성한다. 표준편차

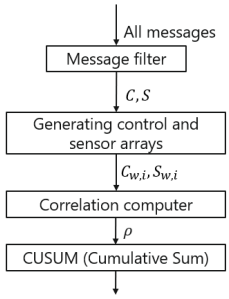

Fig. 5. Proposed IDS is composed of message filer, generating control and sensor arrays, correlation computer, and CUSUM blocks.

가 0이면 정상 데이터와 동일하다. Fig. 7은 가속 명령 적분값과 바퀴 속도의 상관도를 나타내며, 공격은 샘플 인덱스가 1000에서 시작한다. 정상 상황에서 두 데이터의 상관도는 0.98 이상이다. 표준편차가 4, 8, 12인 각각의 공격이 발생하면, 샘플 인덱스 2000에서, 두 데이터의 상관도는 0.64, 0.39, 0.24로 감소한다.

Fig. 8은 잡음의 표준편차가 12인 데이터 변조 공격이 발생하였을 때, CUSUM 블록의 상위 및 하위 제어한계(Control Limit)를 나타낸다. 상위 및 하위 제어한계 중 하나라도 임계값보다 커지면 공격이 발생한 것으로 판단하며, 이 임계값은 4로 설정하였다[3]. 샘플 인덱스가 1000부터 공격이 발생하면 상관도가 감소하므로, 하위 제어한계가 증가하고, 제안하는 침입 탐지 시스템이 데이터 변조 공격을 탐지한다.

6. 결론

본 연구에서 기존의 물리 기반의 침임 탐지 시스템의 한계를 분석하였다. 동일한 제어기가 송신하는 센서 데이터만을 사용하는 기존의 알고리즘은 공격자 해당 센서 데이터를 모두 변경하는 데이터 변조 공격을 탐지하지 못한다. 제안하는 침임 탐지 시스템은 운전자가 생성한 제어 명령과 그 결과 변화하는 센서 데이터의 상관도를 이용한다. 서로 다른 제어기가 송신하며 다른 유형의 물리 신호들의 상관도를 이용하기 위해서, 신호를 선처리하는 방법을 제안하였다. 토요타 캠리 차량에서 수집된 실제 CAN 메시지 데이터를 이용하여, 데이터 변조 공격에 대한 제안하는 침임 탐지 시스템의 성능을 분석하였다. 본 연구는 서로 다른 유형의 물리 신호인 제어 및 센서 신호를 이용하여 공격을 탐지할 수 있음을 보여준다.

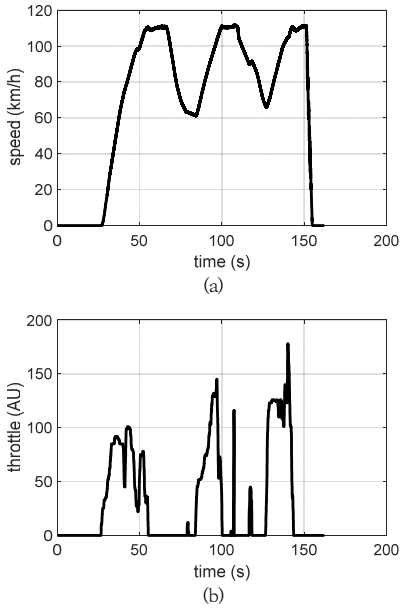

Fig. 6. Wheel speed 1 and throttle status of Toyota Camry are extracted from messages 0x0B0 and 0x2C1, respectively.
(a) Wheel speed 1 (b) Throttle status

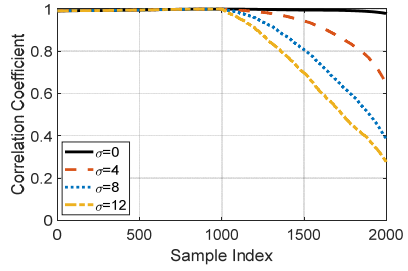

Fig. 7. Correlation coefficients between wheel speed 1 and throttle for various values of σ (σ= 0, 4, 8, 12).

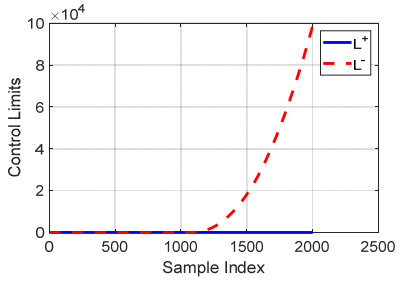

Fig. 8. Upper and lower control limits when is σ=12. The lower control limit increases above the threshold value of 4 after the attack occurs.

현대의 자동차에는 차량의 조향 장치, 공조 장치, 인포테인먼트 시스템 등 차량 상태를 확인하기 위한 다수의 센서가 장착되어 있다. 다양한 종류의 센서 데이터와 운전자 및 승객이 내린 명령을 조합하여, 속도 뿐만 아니라 차량의 종합적인 상태를 근거로 공격을 탐지하는 장치를 개발 과정에 활용할 수 있다. 또한, 본 논문에서 제안한 알고리즘은 CAN 통신을 포함하여, Local Interconnect Network 통신과 플렉스레이 통신에 확대 적용할 수 있다.

References

[1] A. Berdich and B. Groza, "Cyberattacks on Adaptive Cruise Controls and Emergency Braking Systems: Adversary Models, Impact Assessment, and Countermeasures," *IEEE Transactions on Reliability*, Vol.73, No.2, pp.1216-1230, June 2024.
DOI: https://doi.org/10.1109/TR.2024.3373810

[2] Stephen Checkoway, Damon McCoy, Brian Kantor, Danny Anderson, Hovav Shacham, *et al.*, "Comprehensive experimental analyses of automotive attack surfaces," *Proceedings of the 20th USENIX Conference on Security*, San Francisco, CA, USA, pp.77–92, August 2011.

[3] K. Cho and K. Shin, "Fingerprinting electronic control units for vehicle intrusion detection," *Proceedings of the 25th USENIX Conference on Security*, Austin, TX, USA, pp.911–927, August 2016.

[4] S. Sagong, R. Poovendran, and L. Bushnell, "Inter-Message Correlation for Intrusion Detection in Controller Area Networks," *Proceedings of the 17th Embedded Security in Cars Europe*, Stuttgart, Germany, pp.215–229, October 2019.
DOI: https://doi.org/10.13154/294-6677

[5] C. Miller and C. Valasek, "Remote exploitation of an unaltered passenger vehicle," *Proceedings of the 18th Black Hat USA*, Las Vegas, NV, USA, S91, August 2015.

[6] P. Murvay and B. Groza, "Source Identification Using Signal Characteristics in Controller Area Networks," *IEEE Signal Processing Letters*, Vol.21, No.4, pp.395–399, April 2014.
DOI: https://doi.org/10.1109/LSP.2014.2304139

[7] S. Sagong, X. Ying, A. Clark, L. Bushnell, and R. Poovendran, "Cloaking the clock: Emulating clock skew in controller area networks," *Proceedings of the 9th ACM/IEEE International Conference on Cyber-Physical Systems*, Porto, Portugal, pp.32–42, April 2018.
DOI: https://doi.org/10.1109/ICCPS.2018.00012

[8] K. Cho and K. Shin, "Viden: Attacker Identification on In-Vehicle Networks," *Proceedings of the ACM SIGSAC Conference on Computer and Communications Security*, Dallas, TX, USA, pp.1109–1123, October 2017.

DOI: https://doi.org/10.1145/3133956.3134001

[9] T. Hoppe, S. Kiltz, and J. Dittmann, "Security Threats to Automotive CAN Networks-Practical Examples and Selected Short-Term Countermeasures," Elsevier Reliability Engineering & System Safety, Vol.96, No.1, pp.11-25, January 2011.
DOI: https://doi.org/10.1016/j.ress.2010.06.026

[10] M. Muter and N. Asaj, "Entropy-based Anomaly Detection for In-vehicle Networks," *Proceedings of IEEE Intelligent Vehicles Symposium*, Baden-Baden, Germany, pp.1110-1115, June 2011.
DOI: https://doi.org/10.1109/IVS.2011.5940552

[11] University of Tulsa Crash Reconstruction Research Consortium [Internet]. Available From: http://tucrrc.utulsa.edu (accessed May 2, 2019)

사 공 상 욱(Sang Uk Sagong) [정회원]

- 2011년 2월 : 연세대학교 공과대학 전기전자공학과 (공학석사)
- 2019년 12월 : 워싱턴주립대학교 공과대학 전기공학과 (공학박사)
- 2020년 6월 ~ 2023년 7월 : 현대자동차 책임연구원
- 2023년 9월 ~ 현재 : 계명대학교 컴퓨터공학과 조교수

〈관심분야〉
임베디드시스템, 자동차보안, 정보보안