Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.33, NO.2, Apr. 2023 ISSN 2288-2715(Online)
https://doi.org/10.13089/JKIISC.2023.33.2.325

실차기반 LIN-CAN 연계 통합 분석 테스트베드 개발과 초음파센서 물리적 오류주입 및 분석을 통한 효용성 검증*

김 윤 지,[1†] 고 예 지,[1] 오 인 수,[1] 임 강 빈[2‡]
[1,2]순천향대학교 (대학원생, 교수)

Commercial ECU-Based Test-Bed for LIN-CAN Co-Analysis and Proof on Ultrasonic Sensors through Physical Error Injection*

Yoon-ji Kim,[1†] Ye-ji Koh,[1] In-su Oh,[1] Kang-bin Yim[2‡]
[1,2]Soonchunhyang University (Graduate student, Professor)

요 약

자율주행 기술이 발전함에 따라 차량에 탑재되는 외부접점 센서의 수가 증가하고 있으며 특히 차량용 초음파 센서는 버스 토폴로지 형태로서 LIN 프로토콜을 사용하여 연결되며 주변을 감지하고 상태 메시지를 전송하여 차량 내부 네트워크에 접근한다. LIN은 프로토콜의 보안성이 검증되지 않아 공격에 취약하기 때문에 안전성을 평가하기 위한 테스트가 필요하지만, 물리적인 제약으로 인해 실제 차량을 이용한 분석에 한계가 있으며 이를 위한 테스트 환경이 부족하기 때문에 테스트에 어려움이 있다. 따라서, 본 논문에서는 LIN 프로토콜 분석 및 테스트를 위해 CAN과의 연동 분석이 가능한 테스트베드를 개발하고 초음파 센서를 이용하여 그 효용성을 검증하였다.

ABSTRACT

With the development of autonomous driving technology, the number of external contact sensors mounted on vehicles is increasing, and the importance is also rising. The vehicular ultrasonic sensor uses the LIN protocol in the form of a bus topology and reports a status message about its surroundings through the vehicle's internal network. Since ultrasonic sensors are vulnerable to various threats due to poor security protocols, physical testing on actual vehicle is needed. Therefore, this paper developed a LIN-CAN co-analysis testbed with a jig for location-specific distance test to examine the operational relation between LIN and CAN caused by ultrasonic sensors.

Keywords: LIN, CAN, Ultrasonic Sensor, Advanced Driving Assistance System, Test-bed

I. 서 론

미래 최첨단 기술 중 하나인 자율주행 기술은 운전자의 조작 없이 차량이 주변 상황을 인지하고 판단하여 스스로 주행하고 운전자가 설정한 목적지까지 도달하는 자동화 시스템이다. 현재까지는 특수한 경우에 운전자 개입이 필요한 레벨 3 정도의 자율주행 기능을 수행할 수 있도록 개발이 완료되었으며 상용화

Received(01. 06. 2023), Accepted(02. 20. 2023)
* 이 논문은 2022년도 한국정보보호학회 호남지부 학술대회에 발표한 우수논문을 개선 및 확장한 것임
* 본 연구는 정부(과학기술정보통신부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구임(2021R1A4A2001810)
* 본 연구는 2022년도 교육부의 재원으로 한국연구재단의 지원을 받아 수행된 지자체-대학 협력기반 지역혁신 사업(2021RIS-004)의 결과임
* 본 연구는 2022년도 정부(과학기술정보통신부)의 재원으로 정보통신기획평가원의 지원을 받아 수행된 연구임(No. 2022-0-01197, 융합보안대학원(순천향대학교))
† 주저자, rladbswl7@sch.ac.kr
‡ 교신저자, yim@sch.ac.kr(Corresponding author)

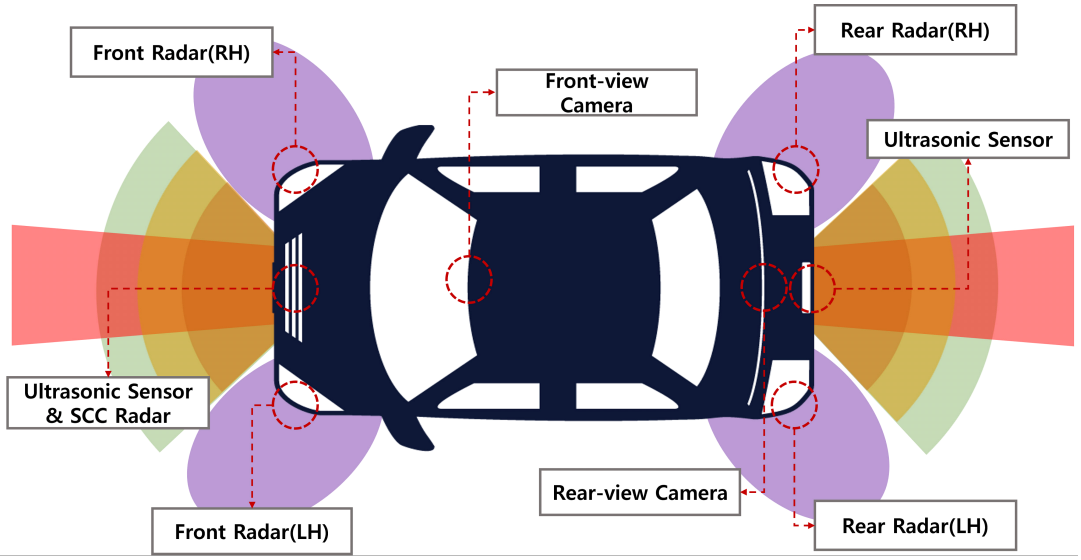

Fig. 1. Advanced Driving Assistance System for self-driving vehicle

되는 시점이다. 따라서 최근 출시되는 차량에는 안전한 자율주행 기술을 보장하기 위해 운전자의 편의성과 안전성을 제공하는 시스템인 첨단 운전자 보조 시스템(ADAS: Advanced Driver Assistance System)이 사용된다. 첨단 운전자 보조 시스템은 전방 충돌 방지 보조(FCA), 차로 이탈 방지 보조(LKA), 후측방 충돌 경고(BCW), 후측방 충돌 방지 보조(BCA), 주차 거리 경고(PDW) 등의 여러 가지 기능을 지원하고 주행 및 주차 시에 경고나 시야 확보 및 차량을 제어하며 해당 시스템이 구현되기 위해서는 외부접점 센서가 필수적으로 탑재된다[1].

외부접점 센서는 차량에 장착되어 주변 상황을 인식하고 생성된 데이터가 차량에 입력되며 차량의 자율주행 기능을 제공한다. 또한, 전·후방 장애물 및 차량의 거리를 측정하고 충돌을 방지하는 기능을 제공하기 위해서 차량 내부 네트워크에 메시지를 송신하게 된다. 차량에 탑재되는 외부접점 센서는 대표적으로 라이다(LiDAR), 차량용 카메라, 차량용 레이더(Radar), 근거리 측정 초음파 센서(Ultrasonic Sensor)의 네 가지로 분류할 수 있다.

그러나 이러한 외부접점 센서가 악의적인 공격자로부터 외부에서 공격을 받거나 차량 내부에 오류가 생겨 결함이 발생할 경우 큰 사고로 이어질 수 있기 때문에 보안 안전성을 평가하기 위한 테스트가 필요하다. 특히 차량용 초음파 센서는 모델과 옵션에 상관없이 모든 차량에 탑재되어 있으며 전·후방에 설치되어 운전자가 자주 사용하는 기능이다. 따라서 본 논문에서는 외부접점 센서 중에서 차량 주차 보조 시스템에 사용되는 차량용 초음파 센서를 선택하여 차량용 초음파 센서에 대한 물리적인 오류주입을 통한 차량 내부 네트워크의 변화를 분석한다.

초음파 센서는 외부로부터 입력받은 정보를 LIN(Local Interconnect Network) 프로토콜을 사용하여 차량 내부 네트워크에 상태 메시지를 보고하는 저비용 데이터 버스 토폴로지로 구성되어 있다. 저전력 통신이며 저렴한 비용으로 효율적인 설계를 할 수 있다는 장점을 가진 LIN 프로토콜은 보안 안전성이 고려되지 않은 문제점이 지적되고 있다. 따라서 본 논문에서는 차량 외부접점 센서인 초음파 센서를 분석하기 위한 테스트베드 환경을 구축한 다음, 발생할 수 있는 보안 위협을 도출하고 다양한 환경에서의 데이터 셋을 확보하며 초음파 센서에서 사용하는 LIN 프로토콜의 구조적 특성과 기능 분석을 진행한다.

본 논문의 2장에서는 차량 외부접점 센서인 라이다, 레이더, 초음파, 카메라에 관해 서술하고 3장에서는 LIN 프로토콜에 관한 내용을 설명한다. 4장에서는 차량용 초음파 센서의 보안 위협에 관한 관련 연구를 설명하고 5장에서는 차량용 초음파 센서용 LIN-CAN 통합 분석 테스트베드 구현과 지그 개발에 관한 내용을 서술한다. 6장에서는 차량용 초음파 센서 LIN 네트워크 테스트 및 테스트베드 검증에

대해 설명한 다음 결론으로 마무리한다.

II. 자동차 외부 접점 센서

2.1 LiDAR 센서

LiDAR(Light Detection and Ranging) 센서는 최근 차량에 부착되어 자율주행 자동차의 핵심 센서로 주목받고 있다. 라이다는 펄스 광파를 방출하여 주변 사물에서 반사되고 돌아오는 시간을 측정하여 물체까지의 거리를 계산하는 원리로 공간을 탐지한다. LiDAR에서 방출되는 펄스 광파의 수를 일반적으로 채널 수라고 불리며 높은 채널일수록 스캐닝할 수 있는 범위가 넓어지기 때문에 mm 단위의 오차범위를 가지고 있으며 정밀도 및 해상도가 높다는 장점을 가지고 있다. 2D LiDAR는 하나의 펄스 광파를 방출하여 회전하고 스캔하지만, 3D LiDAR는 수백만 개의 펄스 광파를 방출하여 주변 3D 공간을 스캔하고 실시간으로 3D 지도가 생성된다[2]. 하지만, LiDAR 센서에 레이저 공격이 가해지는 재밍 공격이 시행되면 주변을 인식하지 못할 가능성이 커진다.

2.2 차량용 카메라 센서

차량용 카메라 센서는 차량의 전방과 후방에 탑재되어 차량의 눈의 역할로서 차선, 차량, 보행자 등의 주변 환경을 인식한다. 전방에 탑재된 카메라는 차선을 인식하여 조향을 자동으로 제어하고 차량이나 보행자를 인지하여 충돌 위험 가능성을 줄인다. 후방에 탑재된 카메라는 후진 및 주차 시에 사각지대에 있는 장애물이나 차량으로부터 충돌을 피하고자 영상정보를 운전자에게 제공한다.

차량용 카메라 센서는 취득한 이미지 데이터를 통해 차량의 신호정보인 CAN(Controller Area Network) 이나 Automotive Ethernet 통신으로 차량 내부 네트워크에 실시간으로 상태 메시지가 전달되며 수집된 데이터를 사용하여 운전자의 주행이나 주차의 편의성 기능을 제공한다. 차량용 카메라는 외부접점 센서 중 유일하게 색상에 대한 정보를 제공하며 저렴한 가격대로 차량에 탑재할 수 있다[3]. 하지만, 이물질에 오염되거나 기상악화 및 환경 변화에 민감하고 악의적으로 공격자가 카메라를 향해 빛의 세기를 강하게 노출하면 카메라는 제 기능을 하지 못하며 카메라 관련 시스템이 제한될 수 있다.

2.3 차량용 레이더(Radar) 센서

차량용 레이더는 1980년대 후반부터 미국, 유럽 및 일본을 중심으로 밀리미터파를 이용한 레이더 방식이 널리 보급되기 시작하였으며, 현재는 자율주행 차량에 중요한 외부접점 센서로 주목받고 있다. 차량용 레이더는 운전자의 차량에서 전파 신호를 상대 물체에 송신하여 반사되어 온 신호를 수신하고 두 신호 간의 시간 차이와 도플러 주파수 변화량을 이용해 상대 물체와의 거리, 이동 속도, 진행 방향 등을 감지할 수 있다.

차량용 레이더는 차량의 전방, 후방, 측방에 탑재되어 있어 상대 차량과 장애물의 위치 정보를 운전자에게 제공하며 자율주행 자동차에 있어서 차량을 제어하고 운전자가 안전하게 주행할 수 있도록 돕는 역할을 한다. 또한, 야간이나 악천후 상황, 50m 이상의 측정 거리에서도 사용이 가능하다는 장점을 가지고 있다[4].

하지만, 레이더 센서에 전파를 발사하여 공격하는 재밍 공격이나 차량 시스템을 위변조하여 공격하는 스푸핑 공격을 통해 레이더 센서의 오작동을 유발하게 되면 주변 장애물을 인식하지 못하게 되어 치명적인 사고가 발생할 수 있다.

2.4 차량용 초음파 센서(Ultrasonic Sensor)

초음파 센서는 초음파 펄스를 방출하여 전·후방의 장애물이나 차량으로부터 반사되어 오는 시간을 측정하여 거리를 감지하는 원리로 작동한다. 차량용 초음파 센서는 일반적으로 차량 전후방에 4개씩 탑재되어 있으며 최신 차량에는 측면에도 부착되어 있다. 전방과 후방에서는 각각 최대 10km/h 이내에서 초음파 센서가 활성화되며 주로 저속 전/후진 및 주차 상황에서 운전자가 발견하지 못하는 사각지대의 물체나 차량을 감지하는 데에 사용되어 경고 알람을 통해 운전자에게 주의하도록 하는 기능을 한다. 초음파에 감지되는 장애물에 대한 정보는 총 3단계로 구분하며 1, 2단계에서는 단순 경보로 주의를 주는 반면, 3단계의 경보는 연속적인 경고음을 통해 충돌을 방지한다[5]. 이러한 초음파 센서에도 스푸핑 공격이나 물리적인 오류주입을 통해 장애물이 있지만 없는 것처럼 인식할 수 있거나 장애물과의 거리 감지를 식

별하지 못하여 추돌 사고가 발생할 수 있다.

III. 차량용 LIN 프로토콜

차량 내부 네트워크에는 CAN, LIN, MOST, Flexray 등 다양한 프로토콜을 사용하지만 주로 차량의 내부 네트워크인 CAN 프로토콜에 중점을 두었다. 그러나 첨단 운전자 보조 시스템에 사용되는 초음파 센서는 로컬 통신에서 LIN 프로토콜을 주로 활용하고 있으며 LIN의 경우 마스터-슬레이브(Master-Slave) 구조로 이루어져 필요한 데이터를 즉각 송신하여 센서 데이터 값을 주고받는데 효율적이다. 그동안 차량 내부 네트워크 데이터를 분석하고 취약점을 발굴하기 위한 연구는 다양하게 이루어지고 있으나 차량 외부접점 센서를 분석하기 위한 데이터 수집은 자동차의 로컬에서 이루어지기 때문에 물리적으로 쉽지 않아 아직 연구가 활발하지 못하다. 다음은 차량 센서 데이터 셋을 수집하여 분석하는 방법으로서 초음파 센서의 보안 위협을 파악하기 위한 기존 연구들에 대해 소개한다.

차량에 사용되는 초음파 센서는 최대 20kbit/s의 비트 속도를 가지는 LIN 프로토콜을 사용하여 차량 내부에 메시지를 전달하는 역할을 하며 버스 토폴로지의 형태를 갖추고 있다. 주로 차량에서 고대역폭을 필요로 하지 않고 저전력으로 사용할 수 있는 파워 윈도우 모듈, 와이퍼 모듈, 초음파 센서 모듈 등에 사용되며 효율적인 버스 통신을 제공한다.

3.1 차량용 초음파 센서 표준 (ISO17987)

차량 내부 네트워크인 LIN 프로토콜과 관련한 대표적인 표준으로 국제표준화기구(International Organization for Standardization)에서 제정한 ISO 17987 표준은 총 8가지로 구성되는데 LIN 프로토콜의 정의, LIN 기반 차량 네트워크 시스템의 전송 프로토콜, 네트워크 계층 서비스 명시, LIN 프로토콜 지정, 전기 물리적 계층 명시, 식별 서비스 등과 관련된 규정을 지정한다[6]. 명시된 8가지 표준에 대한 설명은 Table 1.과 같다.

3.2 마스터-슬레이브 구조

LIN 버스 프로토콜은 모든 노드가 마스터이며 브로드캐스팅(broadcasting) 방식으로 수행되는 CAN 프로토콜과 다르게 하나의 마스터와 여러 개의 슬레이브로 이루어져 간단한 구조의 형태로 단일 와이어를 통해 구성되어 있다. 마스터 노드에는 마스터 태스크와 슬레이브 태스크 두 개를 포함하며 슬레이브 노드에서는 슬레이브 태스크만이 포함된다. 마스터 노드는 주로 명령 및 데이터 요구 역할을 수행하며 슬레이브 노드는 데이터를 제공한다. 마스터가 헤더 부분에 마스터 태스크와 슬레이브 태스크를 동시에 포함하여 송신할 시에는 슬레이브 노드에게 명령하는 메시지를 전달하며, 마스터 태스크만 송신 시에는 슬레이브 노드에게 현재 어떤 상태인지 보고하라는 의미로 해석할 수 있다[7].

Table 1. ISO 17987 standard[6]

Standard	Contents
ISO 17987-1	LIN Protocol General Definitions and Use Cases
ISO 17987-2	Specify transport protocols and network layer services that are tailored to meet the requirements of the LIN-based vehicle network system
ISO 17987-3	Provides LIN protocol specifications including signal management, action, LIN master, and slave nodes
ISO 17987-4	Define 12V and 24V electrical and physical layers for LIN communication systems
ISO 17987-5	Specify the LIN API and node configuration and identification services
ISO 17987-6	Specify LIN protocol conformance tests and provide the required technical information
ISO 17987-7	Conformity testing of the electrical and physical layers of the LIN communication system is prescribed
ISO 17987-8	Specify the requirements for implementation of DC Power Line Electrical Physical Layer (EPL) for LIN communication systems and the conformity test plan for EPL

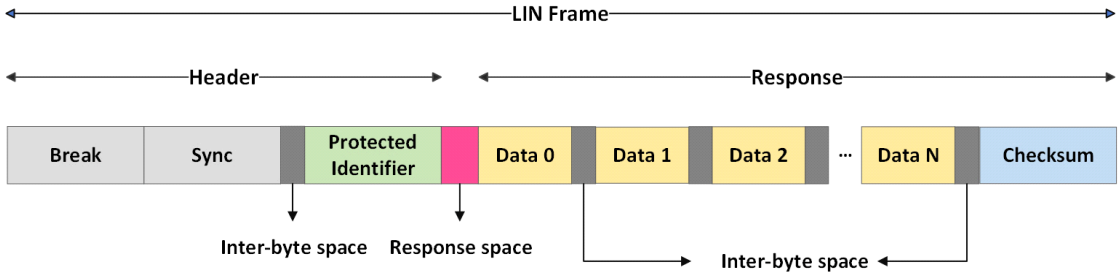

Fig. 2. LIN protocol frame format

3.3 LIN 프레임 구조

LIN 프로토콜에서의 메시지는 프레임을 의미하기 때문에 본 논문에서는 LIN 프레임을 정의한다. LIN 프레임의 구조는 Fig. 2.와 같다.

LIN 프레임은 헤더와 응답으로 구분할 수 있으며 헤더 프레임에는 Break 필드, Sync 필드, PID(Protected Identifier) 필드로 구성된다. Break 필드는 새 프레임의 시작을 알리는 데에 사용이 되며 Sync 필드는 동기화를 위해 0x55의 데이터 값을 정의하고 버스와 동기화하기 위해 내부 전송 속도를 조정한다. PID 필드는 헤더에서 마지막으로 마스터 노드가 보내는 필드로서 LIN 메시지의 고유한 식별 값을 정의하며 노드의 수신과 응답을 결정한다. 또한, 0~59(0x3B)의 값은 신호 전달 프레임에 사용되고, 60(0x3C) 및 61(0x3D)은 진단 및 구성 데이터를 전달하는 데 사용된다.

응답 프레임에서는 데이터 필드와 체크섬 필드로 구성된다. 데이터 필드는 슬레이브 노드가 전송하는 데이터 값으로 최소 1개 이상의 데이터가 전송되며 데이터 필드의 페이로드는 최대 8바이트까지 제공된다. 체크섬 필드는 외부 노이즈로 인한 프레임의 훼손 여부를 판단한다[7].

3.4 체크섬 계산 방법

체크섬은 에러 검출이나 데이터를 송신할 시에 무결성을 보장하기 위해 적용하는 필드이다. LIN 프로토콜에서 응답 필드에 포함되어 있는 체크섬 필드는 클래식 체크섬(Classic Checksum)과 향상된 체크섬(Enhanced Checksum)으로 분류할 수 있다. 클래식 체크섬은 LIN 1.x 슬레이브와의 통신에 사용되며 데이터 필드끼리의 합만을 이용하여 계산한다. 또한, 향상된 체크섬은 LIN 2.x 슬레이브와의 통신에 사용되며 PID와 데이터 필드의 합을 이용하여 계산하며 클래식 체크섬 또는 향상된 체크섬의 사용은 마스터 노드와 프레임 식별자에 따라 결정된다. 클래식 체크섬의 수식은 다음과 같다[7].

$$\begin{aligned} &\mathrm{if}(A_{n+1} > 0XFF(255), A_{n+1} - 0XFF) \\ &D_0 + D_1 = A_1 \\ &A_1 + D_2 = A_2 \\ &A_2 + D_3 = A_3 \\ &\quad\vdots \\ &A_n + D_{n+1} = A_{n+1} \end{aligned} \tag{1}$$

향상된 체크섬의 수식(2)은 다음과 같다.

$$\begin{aligned} &\mathrm{if}(A_{n+1} > 0XFF(255), A_{n+1} - 0XFF) \\ &PID + D_0 = A_1 \\ &A_1 + D_1 = A_2 \\ &A_2 + D_2 = A_3 \\ &\quad\vdots \\ &A_n + D_{n+1} = A_{n+1} \end{aligned} \tag{2}$$

만약 두 개의 데이터 필드끼리의 합이 255(0XFF)를 넘어가게 되면 데이터 필드의 합에서 255를 감소시켜 255 이하 값의 결과를 얻어야 한다. 전부 계산되어서 나오는 마지막 A_{n+1}의 값을 1의 보수로 변환해주면 체크섬 값이 나오게 된다.

IV. 차량용 초음파 센서 보안 위협

4.1 차량 내부 네트워크 데이터 셋 수집 방법 및 확보

고에지 외 3명은 차량 내부 네트워크인 CAN 프로토콜의 데이터 셋을 수집하는 방법과 두 가지 방법으로 수행된 데이터 수집의 비교 분석에 대해 설명한

다. 차량의 CAN 메시지를 수집하기 위해서는 차량에 탑재되어 있는 OBDⅡ를 통해 이루어지고 있지만, 진단 포트의 기능을 가지고 있는 OBDⅡ에서는 차량 전체 메시지를 확인하기에는 한계점이 존재한다. 따라서, 해당 논문에서는 직접 ECU(Electronic Control Unit)에 접근하여 차량 내부에서 송수신 되고 있는 CAN 메시지를 스니핑하는 EDA(ECU Direct Approach) 방식을 서술한다. 이러한 접근 방식은 모든 채널에서 대량의 데이터를 수집할 수 있으며 실시간으로 지연 없는 정확한 데이터를 확보할 수 있다[8].

국내 한 연구팀은 LIN 버전 2.2A를 기반으로 Verilog HDL을 이용하여 LIN 제어기를 설계하였다. 해당 논문에서 제안한 LIN 제어기는 Verilog HDL로 기술한 후 Modelism을 이용하여 시뮬레이션 하였다. 주변 회로인 마이크로 컨트롤러(MCU)와 LIN 송수신기(LIN transceiver)는 상용 칩인 Atmel사의 Atmega128과 Freescale사의 MC33662를 사용한다. LIN 제어기는 MCU로부터 해당 레지스터들의 설정 값들을 입력받아 마스터 모드 또는 슬레이브 모드로 동작하게 되고 identifier ID를 16진수 값 0x02으로 설정하게 되면 마스터가 슬레이브에게 4바이트 값을 전송하게 설계하였다. 오실로스코프를 이용하여 측정한 결과 정상적으로 LIN 버스에 데이터가 전송되었음을 보여준다[9].

4.2 LIN 프로토콜의 취약점 분석 방법

Joseph M. Ernst 외 2명은 CAN 버스는 모든 노드가 마스터인 반면, LIN은 하나의 마스터 노드에 의해 제어되는 특성으로 인해 다양한 유형의 공격이 가능함을 보여준다. LIN 버스는 차량 센서와 보조 시스템 개수 증가에 따라 이를 연결하기 위한 효율적인 저비용 데이터 버스 의도로 제작되어 다른 차량 데이터 버스에 비해 비용이 적게 들지만 안전성이 떨어지는 것을 확인하였다. 또한, LIN 버스 상에서 마스터 노드가 손상되면 전체 LIN 버스가 손상될 수 있으며 마스터 노드는 슬레이브 노드에 잘못된 데이터를 보낼 수 있다. 해당 논문에서는 테스트베드를 설계하여 LIN 버스 인터페이스의 물리적 계층을 테스트하도록 설계되었으며 수행한 실험은 악성 LIN 버스 장치가 LIN 버스의 메시지를 손상시키고 잘못된 유효 패킷을 생성할 수 있음을 보여준다. 악성 LIN 장치가 메시지 패킷 파괴를 통해 네트워크 메시지를 손상시킬 수 있으며 마스터에서 슬레이브 1로의 메시지 전송을 슬레이브 2가 방해할 수 있는 것을 확인하였다. 따라서, LIN 장치 중 일부는 ECU에 연결되어 있어서 보안이 우려되며, LIN 버스 보안 분야의 연구는 LIN 버스의 특징에 맞춰 차량 네트워크 설계를 저비용의 보안으로 고려해야 한다고 언급하였다[10].

4.3 초음파 센서 보안 위협

Bing Shun Lim 외 2명은 실생활에서 발생할 수 있는 네 가지의 공격 시나리오를 설계하여 반자율 차량에 대한 초음파 센서 변조의 영향을 보여준다. 네 가지 공격 시나리오에 대한 결과는 각각 초음파 센서가 물체를 정확하게 감지하지 못하거나 범위를 벗어난 판독 값을 반환하며 센서의 정확도에 상당한 영향을 미치는 것을 입증하였다. 테스트 결과를 바탕으로 초음파 센서는 외부 영향에 민감하고 쉽게 손상될 수 있으며 주행이나 주차 시에 많은 제약이 생긴다는 것을 보여준다. 이러한 테스트 케이스에 발생하는 오류를 완화하기 위해서는 감지 정확도를 향상하기 위해서 다른 유형의 센서와 협력하여 사용하는 다중 센서 융합을 채택해야 함을 강조한다[11].

Chen Yan 외 2명은 외부 접점 센서인 카메라, 레이더, 초음파 센서에 대해 재밍 공격, 스푸핑 공격 등의 다양한 공격을 시도한 후 외부 접점 센서의 취약점을 도출하였다. 자동차에 탑재된 초음파 센서와 동일한 주파수로 초음파를 생성하고 센서의 작동 패턴을 에뮬레이트(emulate)하기 위해 초음파 펄스를 제작할 수 있는 공격 시스템을 설계한다. 해당 논문에서는 초음파 센서를 대상으로 재밍 공격과 스푸핑 공격을 통해 초음파 센서에 소음을 발생시키고 측정이 불가능하도록 하는 것을 목표로 하며 장애물을 감지하지 못하도록 시나리오를 설계하였다. 8개의 서로 다른 초음파 센서를 테스트하였고 초음파 센서에 공격을 수행한 결과 차량이 장애물을 감지하지 못하는 상황을 초래하였다. 따라서, 자율주행차량의 안전에 대한 현실적인 문제점을 보여주고 시스템의 오작동을 임의로 일으켜 자율주행 자동차의 안전성에 대한 문제점을 지적하였다[12].

상기와 같이 초음파 센서의 보안 위협을 분석하기 위한 기존 연구가 진행되었으며 기존 연구에서는 다양한 상황을 가정하여 공격 시나리오를 설계하였고 실제 차량의 초음파 센서에 접근하여 공격을 수행하

거나 시뮬레이션 환경에서 공격을 수행하여 초음파 센서의 오작동 결과를 도출한다. 그러나 실제 차량에서의 실험이 차량 시스템의 오작동 및 결함을 유발할 수 있는 우려가 있다. 또한, 실제 초음파 센서에 물리적인 공격이 수행되었을 때 차량 내부 네트워크의 변화를 실차를 가지고 분석하기에는 역부족이다. 그러므로 초음파 센서 계통을 안전하게 분석할 수 있는 환경이 요구된다. 따라서 본 논문에서는 초음파 센서를 분석할 수 있는 실차 기반의 테스트 프레임워크를 구축하고 물리적인 오류 주입을 통해 초음파 센서가 사용하는 LIN 프로토콜에 주입한 공격이 차량 내부 네트워크에 어떠한 영향을 미치는지 분석하고 평가한다.

V. LIN-CAN 통합 분석 테스트베드 구현

본 장에서는 LIN과 CAN의 데이터를 동시에 수집하고 확인할 수 있는 통합 분석 테스트베드를 구현한다. 또한, 거리별로 장애물을 위치시켜 테스트할 수 있는 테스트베드용 지그(jig)를 개발한다. 구현한 테스트베드에서는 실제 초음파 센서 동작에 따라 LIN 프레임 신호를 확인할 수 있고 CAN 메시지가 생성되는 것을 확인할 수 있다.

5.1 LIN-CAN 통합 분석 테스트베드

차량에 탑재되어 있는 초음파 센서 모듈과 초음파 센서를 구동시키는 ECU를 직접 제어하기에는 ECU가 차량 내부 깊이 탑재되어 있거나 차량 전방 범퍼 하드웨어를 분해해야 하는 물리적인 문제가 있다. 또한, 차량의 오류 주입을 통해 실제 차량이 오작동을 발생할 가능성이 있기 때문에 실제 차량을 통해 직접 구동시키기에는 어려움이 존재한다. 따라서, 실제 차량을 기반으로 초음파 센서 교란을 위한 차량용 초음파 센서 모듈을 활용하여 Fig.3.과 같이 테스트베드를 설계하고 구축하여 실험 환경을 구성하였다.

실제 차량을 기반으로 초음파 센서를 구동하여 차량 내부에서 사용되는 프로토콜인 LIN 데이터를 수집하기 위해서는 ECU(Electronic Control Unit) 끼리의 연결이 필수적이기 때문에 Fig. 4.와 같이 회로도를 설계하여 작동할 수 있도록 연결하였다.

초음파 센서와 통신하는 대표적인 ECU로 ICU(Integrated Control Unit), IBU(Integrated Body Control Unit), 운전자 주차 보조 제어기를 사용하여 연결하였으며 각각의

Fig. 3. Test-bed for LIN-CAN frames co-analysis

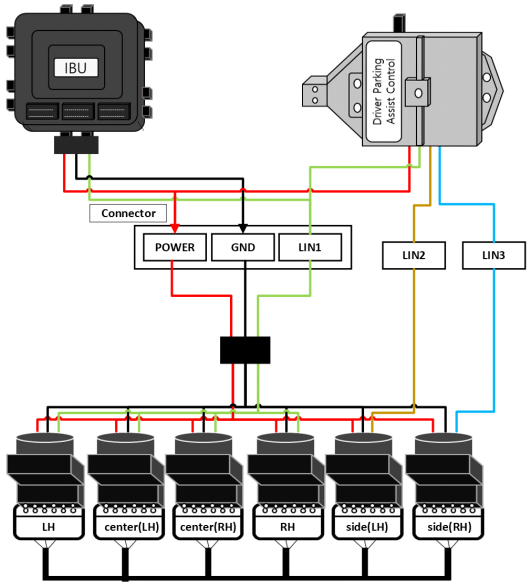

Fig. 4. Ultrasonic sensor connection circuit diagram

ECU와 초음파 센서에 전원을 공급하고 차량 측면부에 탑재되는 초음파 센서는 운전자 주차 보조 제어기와 연결되며 차량 전면부 및 후면부 센터에 장착되는 초음파 센서는 IBU와 연결하였다.

전방과 후방에 탑재된 초음파 센서는 장애물의 위치에 따라 Fig. 5.와 Fig. 6.과 같이 총 1, 2, 3단계의 경고로 구분하며 1, 2단계의 경보는 주의 경보, 3단계는 연속적인 경보와 시각적인 정보로 운전자에게 주의를 제공한다. 또한, 차량의 전진 및 후진 속도가 10km/h 이하일 경우에 작동한다. 따라서, 본 논문에서는 초음파 센서 앞에 장애물이 설치되는 위치에 따라 데이터가 다를 수 있음을 가정하여 장애

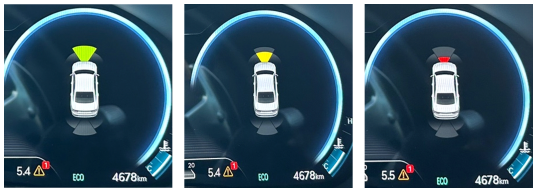

Fig. 5. CAN data collection under front ultrasonic sensor operation

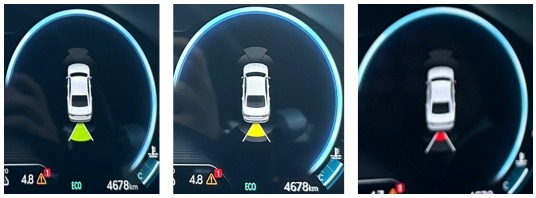

Fig. 6. CAN data collection under rear ultrasonic sensor operation

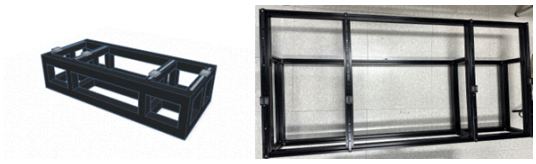

Fig. 7. Ultrasonic sensor error injection zig for physical error injection analysis

물을 고정해 전후로 움직일 수 있도록 Fig. 7.과 같이 테스트 지그를 설계하였고 구축된 테스트베드는 초음파 센서의 특성인 직진성을 고려하여 사물의 위치를 전면부 중앙과 후반부 중앙에 초음파 센서와 일직선으로 일치할 수 있도록 설치하였다.

또한, 테스트베드에서 실제 상황을 재현하고 LIN 프로토콜 데이터를 분석하기 위해 실제 차량에서 발생할 수 있는 총 14개의 초음파 센서 작동 상황별 시나리오를 설계하여 초음파 센서와 관련 있는 내부 네트워크 메시지인 B-CAN(Body CAN) 데이터를 수집하였다. 테스트베드에 B-CAN 데이터를 주입하면 수집 당시 상황에서의 LIN 데이터를 오실로스코프로 측정해본 결과 초음파 센서 관련 LIN 신호가 표준에 명시된 프레임과 동일한 신호로 Fig. 8.과 같이 정상적으로 수집되는 것을 확인하였다.

Table 2.와 같이 실제 차량에서 초음파 센서가 동작하기 위한 조건인 10km/h 속도의 전진(D)과 후진(R) 상태에서 전방과 후방 초음파 센서의 14개의 시나리오에 따른 CAN 데이터셋을 수집하였다. LIN 프레임이 발생하기 위한 내부 B-CAN 데이터셋을 기반으로 분석에 활용하기 위해 각각 1분씩 수집하였다.

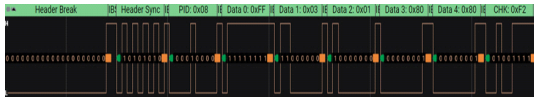

Fig. 8. LIN Logic signal frame

Table 2. 14 ultrasonic sensor run scenarios

No	Situation	Content
1	Front Center	Step 1 Alarm
2		Step 2 Alarm
3		Step 3 Alarm
4	Front Side(RH)	Step 2 Alarm
5		Step 3 Alarm
6	Front Side(LH)	Step 2 Alarm
7		Step 3 Alarm
8	Rear Center	Step 1 Alarm
9		Step 2 Alarm
10		Step 3 Alarm
11	Rear Side(RH)	Step 2 Alarm
12		Step 3 Alarm
13	Rear Side(LH)	Step 2 Alarm
14		Step 3 Alarm

VI. 초음파 센서 기반 LIN-CAN 패킷 연계분석

6.1 실차 기반 LIN 데이터 수집 방법

LIN 데이터 수집을 위해 PEAK사에서 개발한 PCAN-LIN 수집기를 활용하였다. LIN 데이터를 수집하기 위해서는 PEAK사에서 개발한 LIN 하드웨어 수집기인 PLIN-USB의 핀맵(pin-map)과 일치하도록 연결해야 한다. 실제 LIN 버스와 연결되는 4번 핀, 그라운드 선과 연결되는 5번, 6번 핀(LIN-GND), 마지막으로 6~28V 범위의 외부 DC 전원 공급을 위한 9번 핀(Vbat-LIN)의 4가지 선으로 구성되어 있다.

PLIN-USB와 연결이 완료되었으면 Fig.10.와 같이 구축한 테스트베드에 설치된 ECU의 LIN 버스와 연결하여 PLIN-view PRO 프로그램을 통해 포트를 설정하고 LIN 데이터 프레임 수집을 진행하였다.

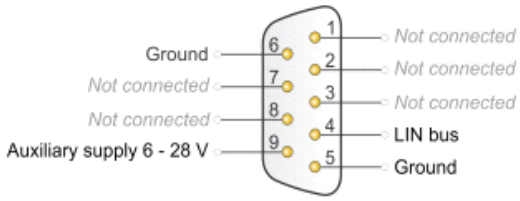

Fig. 9. PCAN-LIN Hardware accessory Pin-map[13]

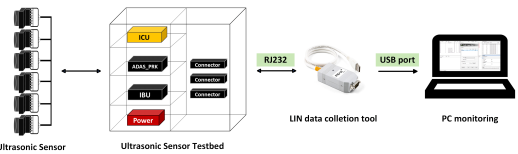

Fig. 10. Schematic diagram for collecting LIN data from vehicle ultrasonic sensors testbed

6.2 LIN 데이터 주입 방법

LIN 프로토콜 특성상 마스터가 명령을 보내고 슬레이브가 응답하는 구조로 형성되어 있다. PLIN view PRO 프로그램 또한 마스터, 슬레이브 기능이 구분되어 있으며 PLIN-USB 수집기를 2개 사용하여 각각 마스터, 슬레이브로 환경 설정할 수 있다.

프로그램 내에서는 데이터를 송신하는 publisher와 데이터를 수신하는 subscriber의 용도를 구분하여 사용하고 있다. 연결된 수집기 2개 중 하나는 마스터 역할을 하여 주입하고자 하는 ID에 데이터 바이트를 입력하여 publish를 하게 되면 슬레이브 역할을 하고 있는 다른 하나의 수집기에 전달되어 마스터에서 보낸 ID와 데이터를 수신할 수 있다. Fig. 11.과 같이 마스터 창에서 ID가 0x05이며 0x00, 0x00, 0xC0, 0x20, 0x7A, 0xFF의 LIN 데이터

ID	Symbol	L...	Data	Count	Direction	CST
05h		6	00 00 C0 20 7A FF	113	Publisher	Enhanced
05h		6	00 00 C0 82 7A 49	12	Publisher	Enhanced
05h		6	B3 72 FC 82 7A 4B	28	Publisher	Enhanced

Fig. 11. Master mode

ID	Symbol	L...	Data	P...	Count	Direction	CST	Ch...
06h		6	29 64 EE 02 7A 89	100	1750	Subscriber Automa...	Enha...	77h
08h		5	FF 03 01 20 70	90	3494	Subscriber Automa...	Enha...	63h
05h		6	00 00 C0 20 7A FF	63	1845	Subscriber Automa...	Enha...	1Fh
07h		6	29 98 FB 80 BB 55	180	1747	Subscriber Automa...	Enha...	69h
04h		6	29 78 F8 82 BB 55	220	1744	Subscriber Automa...	Enha...	0Dh
20h		2	7A FF	2374	10	Subscriber Automa...	Auto...	1Fh
15h		0			1	Subscriber Automa...	Auto...	00h

Fig. 12. Slave mode

가 Fig. 12.와 같이 슬레이브 창에 주입되는 것을 확인할 수 있다.

6.3 CAN 프로토콜과 LIN 프로토콜의 연관성

초음파 센서는 이러한 LIN 프로토콜의 특성을 활용하여 초음파 센서의 마스터인 IBU에서 차량 전방에 물체를 감지할 시 거리를 계산하는 명령을 보낸다. 초음파 센서는 주변 장애물을 탐지하고 전파를 송출하여 되돌아오는 전파 신호를 기반으로 수집된 데이터를 LIN 프로토콜을 통해 IBU로 전송한다. 그런 다음, CAN 프로토콜로 변환되어 차량 내부 네트워크에 전달되어 계기판에 경고를 표출하여 운전자에게 주의를 시킨다.

앞 절에서 언급한 상황별 시나리오에서 수집한 B-CAN 데이터를 테스트베드에 주입하였을 때 나온 LIN 데이터는 Fig. 13.과 같다. 해당 테스트는 중앙에 있는 전방 초음파센서 4개를 대상으로 진행하였으며 아래 표와 같이 전방 초음파센서는 60~100cm까지 1단계 경보, 30~60cm까지는 2단계 경보, 30cm 이하에서는 3단계로 버저를 구동한다.

전방 초음파 센서를 작동시킨 데이터를 주입하였을 때 LIN ID가 0x06, 0x07인 데이터가 생성되었으며 각각의 PID는 0x85, 0x06이었다. 설치된 초음파 센서 앞에서 장애물을 거리별로 위치하여 측정해본 결과 LIN 데이터값이 지속적으로 변화하는 것을 확인할 수 있었다. 또한, 테스트한 초음파 센서는 4개지만 LIN 버스 상에서는 2개의 LIN ID만 활성화되었으며 동시에 CAN 데이터를 통해 확인해본 결과 CAN ID가 0x3E5의 데이터값이 변화하는 것을 확인하였다.

Table 3. Obstacle sensing alarm by distance

Step	Direction
1	60~100cm
2	30~60cm
3	30cm or lower

ID	Symbol	Length	Data	Period	Count	Direction	CST	Checksum	Errors
07h		6	29 4C EA 80 BB 54	180	28	Subscriber ...	Enhanced	C7h	
08h		5	FF 03 01 40 E0	110	56	Subscriber ...	Enhanced	D2h	
06h		6	00 00 C0 20 7A 98	300	28	Subscriber ...	Enhanced	06h	
05h		6	43 40 DC 80 7A 4F	300	28	Subscriber ...	Enhanced	CFh	
04h		6	9E 68 D7 00 BB 65	180	28	Subscriber ...	Enhanced	3Bh	

Fig. 13. LIN protocol data extracted from the front ultrasonic sensor after injecting CAN dataset into testbed

3E0h	8	66 20 01 00 54 03 00 00	200.0	561
3E1h	8	E8 60 00 00 00 00 00 00	200.0	561
3E2h	8	BF 20 00 00 10 02 00 00	200.0	561
3E5h	8	A9 60 02 01 00 18 1B 00	200.0	655
3E6h	8	10 20 00 00 00 00 00 00	200.0	561
410h	8	64 10 FF FF FF FF FF FF	200.0	560
411h	8	07 11 00 00 10 04 44 04	200.0	560

Fig. 14. CAN data on physical error injection

또한, 테스트베드 지그를 통해 장애물을 초음파 센서와 일정한 거리를 두고 측정해본 결과 3번째 바이트, 4번째 바이트에서는 0x02, 0x01의 데이터 값, 6번째 바이트, 7번째 바이트에서는 각각 0x18, 0x1B의 데이터 값으로 대칭을 이루어 일정하게 변화하고 있었다.

초음파 센서 테스트베트 검증을 위해서 Fig. 14와 같이 실제 차량에서 0x3E5인 CAN ID를 사용하여 장애물 위치별로 변화한 데이터 중에서 3번째 바이트와 4번째 바이트에 0x02와 0x01, 데이터의 6번째, 7번째 바이트에 0x18과 0x1B로 바뀐 0xA9, 0x60, 0x02, 0x01, 0x00, 0x18, 0x1B, 0x00의 데이터로 주입해본 결과 실제로 2단계 수준의 초음파 센서 버저음이 구동되었다.

따라서, 본 논문에서 구현한 초음파 센서용 테스트베드는 LIN 데이터와 CAN 데이터를 동시에 확보할 수 있으며 비교 분석이 가능하다.

VII. 결 론

운전자의 편의성과 안전성에 초점을 맞추어 현대 차량의 발전이 지속함에 따라 차량의 눈이 되어 주행이나 주차를 보조하는 역할인 차량 외부에 장착되는 센서의 수도 증가하고 있다. 그 중에서도 차량용 초음파 센서는 현대 차량에 기본으로 탑재되며 운전자가 주로 사용하는 기능이다. 차량용 초음파 센서는 LIN 프로토콜을 사용하지만, LIN 프로토콜 특성으로 인한 보안 문제점이 발생할 수 있다. 이러한 초음파 센서에 대해 악의적으로 접근하여 물리적인 오류를 주입할 시에 차량 오작동이 발생하여 사고를 유발할 수 있다.

따라서, 본 논문에서는 초음파 센서를 사용하여 간이 테스트베드를 구축하였고 장애물을 위치별로 테스트하기 위해 테스트베드용 지그를 개발하였다. 또한, 구현한 간이 테스트베드의 검증을 위해 테스트베드에서 수집하였던 데이터를 실제 차량에 주입해보며 초음파 센서 버저가 작동하는 결과를 보여주었다.

향후 단계에서는 차량용 초음파 센서 간이 테스트베드를 사용하여 LIN 데이터를 분석하고 더 나아가 소프트웨어 V모델을 기준으로 삼아 해당 차량이 합리적인 구조로 설계가 되었는지를 테스트하기 위한 시나리오를 작성하여 테스트할 수 있을 것으로 사료된다. 또한, 이를 기반으로 테스트 지그의 구동을 모터 구동으로 전자화하여 자동차 전체에서의 LIN-CAN 연동 분석을 위한 통합 자동화 패킷 수집 분석 프레임워크로 발전시키고자 한다.

References

[1] Seo, Hwajeong, Kwon YongBeen, Kwon HyeokDong and An Kyuhwang, “Security trends for automonous driving vehicle,” Review of KIISC, 28(5), pp. 9-14, Oct. 2018.

[2] Jin San Kwon, Tae Ho Hwang and Hyun Moon Park, “A development of effective object detection system using multi-device LiDAR sensor in vehicle driving environment,” KIECS, 13(2), pp. 313-320, Apr. 2018.

[3] Si Hyeon Lee and Yeonsik Kang, “Segmentation of driving areas for autonomous vehicle based on deep learning method using automotive camera sensor,” Journal of institute of Control, Robotics and Systems, 26(6), pp. 452-461, May. 2020.

[4] Si-woong Jang and Dong-hun Jung, “Design and implementation of a distance measurement system using radar sensor,” Journal of the Korea Institute of Information and Communication Engineering, 22(7), pp. 1009-1014, July, 2018.

[5] W. Xu, C. Yan, W. Jia, X. Ji and J. Liu, “Analyzing and enhancing the security of ultrasonic sensors for autonomous vehicles,” IEEE Internet of Things Journal, vol. 5, no. 6, pp. 5015-5029, Aug. 2018.

[6] ISO SC31, ″Road vehicles-local interconnect network (LIN)-Part 1: General information and use case

definition", ISO 17987, Aug. 2016.
[7] LIN Steering Group, "LIN Specification Package, Revision 2.2A," LIN Consortium, Dec. 2010.
[8] Yeji Koh, Yoonji Kim, Seoyeon Kim, Insu Oh and Kangbin Yim, "Efficient CAN dataset collection method for accurate security threat analysis on vehicle internal network," International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing. Springer, pp.137-146, Oct. 2022.
[9] Jong-Bae Lee and Seongsoo Lee. "Design and verification of automotive LIN Controller," Journal of IKEEE, 20(3), pp. 333-336. Sep. 2016.
[10] J. M. Ernst and A. J. Michaels, "LIN bus security analysis," IECON 2018 - 44th Annual Conference of the IEEE Industrial Electronics Society, pp. 2085-2090, Oct. 2018.
[11] B. S. Lim, S. L. Keoh and V. L. L. Thing, "Autonomous vehicle ultrasonic sensor vulnerability and impact assessment," 2018 IEEE 4th World Forum on Internet of Things (WF-IoT), pp. 231-236, May. 2018.
[12] Yan Chen, Wenyuan Xu, and Jianhao Liu. "Can you trust autonomous vehicles: Contactless attacks against sensors of self-driving vehicle," Def Con, Vol.24, Aug. 2016.
[13] PEAK System, "PLIN-View Pro", https://www.peak-system.com/PLIN-USB.485.0.html?&L=1, Dec. 2023.

〈저자소개〉

김 윤 지 (Yoon-ji Kim) 학생회원
2023년 2월: 순천향대학교 정보보호학과 졸업
2023년 3월~현재: 순천향대학교 모빌리티융합보안학과 석사과정
〈관심분야〉 정보보호, 자동차보안

고 예 지 (Ye-Ji Koh) 학생회원
2022년 2월: 순천향대학교 정보보호학과 졸업
2022년 3월~현재: 순천향대학교 모빌리티융합보안학과 석사과정
〈관심분야〉 정보보호, 자동차보안

오 인 수 (In-su Oh) 학생회원
2018년 2월: 순천향대학교 정보보호학과 졸업
2020년 2월: 순천향대학교 정보보호학과 석사
2022년 8월: 순천향대학교 정보보호학과 박사 수료
2022년 9월~현재: 순천향대학교 정보보호학과 박사 수료후 연구원
〈관심분야〉 정보보호, 모바일보안, 자동차보안

임 강 빈 (Kang-bin Yim) 종신회원
1992년 2월: 아주대학교 전자공학과 졸업
1994년 2월: 아주대학교 전자공학과 석사
2001년 2월: 아주대학교 전자공학과 박사
2003년 3월~현재: 순천향대학교 정보보호학과 교수
〈관심분야〉 정보보호, 취약점분석, 자동차보안