Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.34, NO.2, Apr. 2024 ISSN 2288-2715(Online)
https://doi.org/10.13089/JKIISC.2024.34.2.217

차량용 LiDAR 센서 물리적 신호교란 공격 중심의 실험적 분석과 대응방안 제안*

황 지 웅,[1†] 윤 요 섭,[2] 오 인 수,[3] 임 강 빈[4‡]
[1,2,3,4]순천향대학교 (학생, 대학원생, 박사후 연구원, 교수)

Experimental Analysis of Physical Signal Jamming Attacks on Automotive LiDAR Sensors and Proposal of Countermeasures*

Ji-ung Hwang,[1†] Yo-seob Yoon,[2] In-su Oh,[3] Kang-bin Yim[4‡]
[1,2,3,4]Soonchunhyang University (Undergraduate student, Graduate student, Postdoc, Professor)

요 약

자율주행 자동차의 안전한 운행을 위해 카메라, RADAR(RAdio Detection And Ranging), 초음파 센서 중 중추적인 역할을 하는 LiDAR(Light Detection And Ranging) 센서는 360도에서 사물을 인식하고 탐지할 수 있다. 하지만 이러한 LiDAR 센서는 레이저를 통해서 거리를 측정하기 때문에 공격자에 노출되기 쉬우며 다양한 보안 위협에 직면해 있다. 따라서 본 논문에서는 LiDAR 센서를 대상으로 한 여러 가지 보안 위협인 Relay, Spoofing, Replay 공격을 살펴보고 물리적 신호교란(Jamming) 공격의 가능성과 그 영향을 분석하며, 이러한 공격이 자율주행 시스템의 안정성에 미치는 위험을 분석한다. 실험을 통해, 물리적 신호교란 공격이 LiDAR 센서의 거리 측정 능력에 오류를 유발할 수 있음을 보여준다. 개발이 진행 중인 차량 간 통신(Vehicle-to-Vehicle, V2V), 다중 센서 융합과 LiDAR 비정상 데이터 탐지를 통해 이러한 위협에 대한 대응방안과 자율주행 차량의 보안 강화를 위한 기초적인 방향을 제시하고 향후 연구에서 제안된 대응방안의 실제 적용 가능성과 효과를 검증하는 것을 목표로 한다.

ABSTRACT

LiDAR(Light Detection And Ranging) sensors, which play a pivotal role among cameras, RADAR(RAdio Detection And Ranging), and ultrasonic sensors for the safe operation of autonomous vehicles, can recognize and detect objects in 360 degrees. However, since LiDAR sensors use lasers to measure distance, they are vulnerable to attackers and face various security threats. In this paper, we examine several security threats against LiDAR sensors: relay, spoofing, and replay attacks, analyze the possibility and impact of physical jamming attacks, and analyze the risk these attacks pose to the reliability of autonomous driving systems. Through experiments, we show that jamming attacks can cause errors in the ranging ability of LiDAR sensors. With vehicle-to-vehicle (V2V) communication, multi-sensor fusion under development and LiDAR anomaly data detection, this work aims to provide a basic direction for countermeasures against these threats enhancing the security of autonomous vehicles, and verify the practical applicability and effectiveness of the proposed countermeasures in future research.

Keywords: LiDAR, Autonomous, Jamming, Security Threats

Received(01. 11. 2024), Modified(03. 14. 2024), Accepted(03. 14. 2024)

* 본 논문은 2023년도 한국정보보호학회 호남지부 학술대회에 발표한 우수논문을 개선 및 확장한 것임

* 본 연구는 정부(과학기술정보통신부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구임(2021R1A4A2001810)

* 본 연구는 2024년도 정부(과학기술정보통신부)의 재원으로 정보통신기획평가원의 지원을 받아 수행된 연구임(No. 2022-0-01197, 융합보안대학원(순천향대학교))

† 주저자, jiung5359@sch.ac.kr

‡ 교신저자, yim@sch.ac.kr(Corresponding author)

I. 서 론

자율주행 기술은 운전자의 직접적인 개입 없이 차량이 스스로 주행하는 혁신적인 기술로, 현대 자동차 산업에서 자율주행 기술은 주요 발전 분야 중 하나로 간주되며, 미국자동차공학회(Society of Automotive Engineers, SAE)에 의해 정의된 자율주행 단계는 두 가지 주요 부류로 구분된다. 초기 단계인 레벨 0부터 레벨 2는 운전자 보조 기능에 초점을 맞추며, 레벨 3부터 레벨 5까지는 완전한 자율주행 기능을 목표로 한다[1]. 자율주행의 고도화를 위해서는 첨단 센서 기술 및 인공지능(AI)의 결합이 필수적이며, 이를 위해 카메라, 초음파 RADAR (RAdio Detection And Ranging), LiDAR (Light Detection And Ranging) 등 다양한 센서가 활용된다. 이러한 센서들은 주변 환경을 정밀하게 인식하고 분석하여, 실시간 주행 의사결정을 위한 데이터를 제공한다.

여러 센서 중 카메라 센서는 주변 환경을 2차원 이미지로 포착하는 데 널리 사용된다. 하지만 조도, 음영, 악천후 등 외부 요인에 의한 영향을 많이 받는다. 반면, LiDAR 센서는 레이저 펄스를 사용하여 외부 조건에 덜 민감하다. 또한, 레이저 펄스로 주변 환경을 매핑하고, 주변 물체의 정확한 거리와 형태 정보를 캡처하는 중요한 이점을 제공한다[2]. 이러한 장점들을 바탕으로 LiDAR 센서는 정밀한 데이터 수집 및 실시간 환경 스캔 능력 덕분에 자율주행 차량의 핵심 센서 기술로 자리매김하고 있다.

국내외 차량 제조사(OEM: Original Equipment Manufacturer)들은 LiDAR 센서를 장착한 자율주행 자동차의 연구 및 개발에 주력하고 있으며, 이 기술의 중요성은 2023년 CES(Consumer Technology Show)에서 30개 이상의 기업이 LiDAR 기술을 선보임으로써 강조되었다[8]. 또한, ResearchInChina의 보고서에 따르면 지능형 운전이 발전함에 따라 차량에 LiDAR 센서를 탑재하는 비율이 증가하는 것을 볼 수 있다[9]. 본 논문은 LiDAR 센서의 필수성을 강조하고, LiDAR 센서의 사용 증가에 따른 보안 위협을 설명한다. 또한, 차량용 LiDAR 센서에 대한 물리적 신호교란 공격에 관한 실험적 연구를 제시하며, LiDAR 센서의 잠재적인 보안 위협에 대응하는 방안을 소개함으로써, 자율주행 기술의 안정성과 신뢰성을 높이는 방향을 제안한다.

II. 배 경

2.1 차량용 LiDAR 센서 동작 원리

LiDAR 센서의 기본 구성은 Fig. 1.과 같이 레이저 송신기(Transmitter)와 레이저 수신기(Receiver)로 구성된다. 레이저 송신기는 환경에 레이저 펄스를 방출하는 역할을 하며, 이 펄스는 주변 물체에 반사되어 다시 센서로 돌아온다. 레이저 수신기는 이러한 반사된 레이저 펄스를 감지하고 측정하는 기능을 수행한다. 두 구성 요소의 상호작용을 통해 LiDAR 시스템은 주변 환경에 대한 정밀한 3차원 데이터를 수집하고 분석한다. 이 데이터는 자율주행 차량의 주변 환경 인식 및 의사결정 과정에서 중요한 역할을 한다.

LiDAR 센서의 근본적인 작동 원리는 ToF (Time of Flight)에 기반을 두고 있다. ToF 메커니즘은 레이저 송신부에서 발사된 레이저가 측정 범위 내의 물체에 도달하고, 그 물체로부터 반사된 레이저가 광다이오드에 의해 수신되는 과정을 포함한다. 이때, 레이저가 송신부에서 물체에 닿은 후 다시 돌아오기까지 걸리는 시간을 측정하여 물체와의 거리를 계산한다[3]. 반사된 레이저 신호들은 수많은 점으로 구성되며, 이 점들이 집적되어 3차원 공간에 주변 환경을 상세하게 표현한다. 이러한 데이터 집합을 '3D 포인트 클라우드'라고 부른다. 포인트 클라우드의 해상도는 LiDAR 센서의 채널 수에 의해 결정되며, 채널 수가 많을수록 더 높은 해상도의 3D 환경 표현이 가능하다[4][5]. 이는 LiDAR 기술이 복잡한 환경에서도 정밀한 주변 정보를 제공할 수 있음을 의미하며, 이는 자율주행 차량의 안전성과 효율성을 크게 향상시키는 중요한 요소로 작용한다.

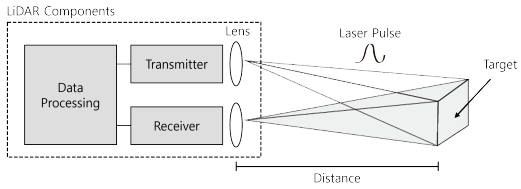

Fig. 1. Principle of Automotive LiDAR Sensor

2.2 차량용 LiDAR 센서 종류

LiDAR 센서 기술은 시야각(Field of View,

FOV) 확장을 목표로 지속해서 진화해 왔다. 본 절에서는 두 가지 주요 LiDAR 구조, 즉 기계식 LiDAR(Mechanical Scanning LiDAR)와 고정형 LiDAR(Solid-State LiDAR)에 관해 설명한다.

2.2.1 기계식 LiDAR

기계식 LIDAR 센서는 전기모터를 이용하여 구동부를 회전시켜, 전체 360도 시야각을 제공한다[3][5]. 이 구조는 주변 환경의 모든 객체를 탐지하고, 그 거리 및 방향 정보를 정확히 측정할 수 있게 한다. 기계식 LiDAR의 주요 특징 중 하나는 수직 방향으로 송수신되는 레이저의 개수에 따라 다양한 채널 수를 가지는 것이며, 이는 4채널부터 128채널까지 다양하다. 채널 수가 많아질수록 해상도는 높아지지만, 이는 동시에 센서의 구성이 복잡해지고 가격이 상승하는 단점을 가져온다. 또한, 회전 메커니즘의 물리적 구조로 인해 크기가 크며, 물리적 충격과 같은 외부 요인에 의한 영향을 받아 제품의 수명이 상대적으로 짧다는 단점도 있다[6][7].

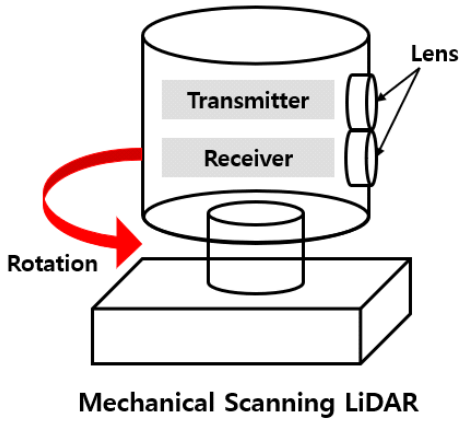

Fig. 2. Mechanical Scanning LiDAR

2.2.2 고정형 LiDAR

고정형 LiDAR 센서는 MEMS(Micro-Electro-Mechanical Systems) 기반 거울을 이용하여 주변 환경을 스캔하거나 광학 위상 배열 (Optical Phased Array, OPA)을 사용하는 방법이 일반적이다[5][7].

회전하는 구동부가 없이 반도체 소자를 활용하여 구성이 단순하며 일반적으로 간소화 및 내구성이 향상되어, 회전형 LiDAR에 비해 빠른 데이터 획득 속도를 제공한다는 점에서 회전형 LiDAR 센서의 단점을 보완한다. 하지만 회전하는 기계식 구동부를 제거하여, 회전형 LiDAR보다 시야각이 줄어든다. 줄어든 시야각 때문에 시야각을 넘으면 물체 탐지가 불가능하지만, 이는 여러 개의 고정형 LiDAR를 사용하여 보완할 수 있다[3].

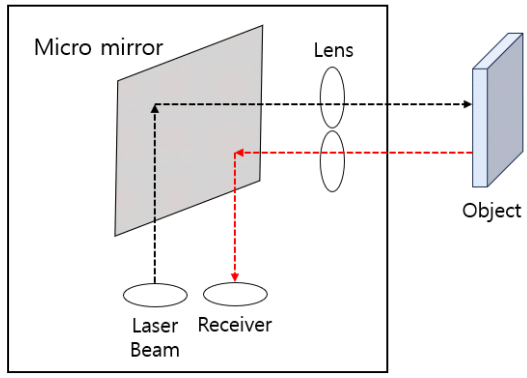

Fig. 3. Solid-State LiDAR

III. 차량용 LiDAR 대상 기존 공격 관련 연구

최근 연구는 LiDAR 기반 자율주행 아키텍처를 통해 장애물에 대한 오인식을 유도하여 자율주행 차량의 물체 감지 모델의 신뢰성을 약화하는 데 초점을 맞추고 있다. 자율주행차의 핵심 구성 요소 중 하나인 자율주행 시스템은 차량에 장착된 센서에서 수입한 데이터를 기반으로 주행 결정을 내린다. 이 논문에서는 적응형 주행 제어(ACC), 충돌 방지 시스템(CAS), 주변 차량, 보행자 및 기타 물체의 감지 및 인식에 필수적인 LiDAR 센서의 중요한 역할에 대해 중점적으로 설명한다. LiDAR 센서는 자율주행의 '눈'으로서 중요한 역할을 한다. 이러한 맥락에서 3장에서는 센서 기능이 손상되거나 악의적으로 조작될 경우 치명적인 사고로 이어질 수 있다는 점을 강조하면서 LiDAR 센서의 보안 측면에 초점을 맞춘 연구를 소개한다. LiDAR 센서를 노리는 주요 공격 유형에는 Relay 공격, Spoofing 공격, Replay 공격이 있다. 이 장에서는 이러한 공격 방법론을 자세히 살펴보고 잠재적인 위협을 소개한다.

Table 1. LiDAR sensor attack methods

Type	Method	Attack Result
Relay Attack	The attacker uses two transceivers to relay the LiDAR signal delay the signal and then attack the LiDAR	An obstacle was detected further away than the actual distance
Spoofing Attack	The attacker injects a fake laser pulse reflected from an object from a different location	A self-driving car traveling in a simulation detects a fake obstacle created by an attacker and stops abruptly
Replay Attack	The attacker duplicates the LiDAR sensor's datagram, stores it in a buffer and plays it back	The attack caused nearby vehicles traveling in the same direction to appear to be traveling in reverse

3.1 Relay Attack

자율주행 차량의 LiDAR 시스템을 노리는 Relay 공격에 대한 자세한 분석을 제시한다. Relay 공격은 LiDAR 센서에서 방출된 원래 레이저 신호를 중간 단계에서 가로채서 미리 정의된 시간 간격 동안 지연시킨 다음 조작된 레이저 신호를 다시 LiDAR 센서로 전송하는 공격이다.

Fig. 4.는 LiDAR 센서를 이용한 릴레이 공격의 개념을 시각화한 것으로, 실제 실험 결과가 아닌 개념적 이해를 돕기 위한 도식이다. 그림은 피해 차량 V1의 LiDAR 시스템이 공격 차량 V2를 실제보다 더 멀리 있는 것으로 잘못 인식하도록 하는 공격 메커니즘을 나타낸다. t0의 시점에서 V1은 V2에 신호를 보내지만, V2는 공격을 위해 설계된 장치를 통해 이 신호를 지연시킨 후, 지정된 시간 t1에 신호를 반환한다. 이러한 릴레이 공격의 결과로 V1의 LiDAR는 V2를 실제 위치보다 멀리 감지하게 되며, 이는 자율주행 시스템의 안전성과 결정에 영향을 미칠 수 있다.

이 공격의 주요 목표는 실제 물체를 실제 위치보다 더 멀리 보이게 만드는 것이다. 다른 연구팀은 두 개의 레이저 트랜시버를 사용하여 LiDAR 센서에서 방출되는 레이저 신호를 중계하는 구체적인 실험을 통해 이러한 공격의 효과를 입증했다[10]. 이 트랜시버는 LiDAR에서 약 1m 떨어진 곳에 배치되었지만, 각각 20m와 50m 떨어진 것처럼 보이도록 조작되었다. 이 실험의 결과는 장애물이 실제 위치와 다른 위치에서 감지되어 자율주행 차량의 정확한 주행 결정 능력에 상당한 영향을 미칠 수 있음을 보여준다.

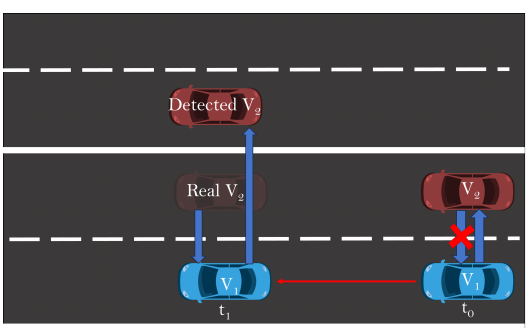

Fig. 4. Diagram of Relay Attack on V1

3.2 Spoofing Attack

Spoofing 공격은 가짜 장애물을 만들어 특정 위치에 주입하는 것이다. 참고 논문에서 수행된 실험에는 LiDAR 센서, 트랜시버 1개, 제어 로직 2개가 사용되었다. 제어 로직을 통해 원래 레이저 신호의 특성을 모방한 위조 레이저 신호가 생성되었다. 이 신호는 트랜시버를 통해 LiDAR 센서로 전송되어 실제로 1m 떨어진 장애물을 50m 떨어진 것처럼 보이게 한다[10]. 이러한 공격은 차량 운행의 안전에 직접적인 위협이 될 수 있다. 또한, 다른 연구팀의 시뮬레이션 결과에서는 43km/h로 주행 중인 차량이 Spoofing 공격으로 인해 갑자기 정지하는 시나리오를 보여 운전자와 승객의 안전에 심각한 위협을 가하고 잠재적으로 후방 차량의 충돌이나 교통 혼잡을 유발할 수 있는 상황을 연출했다[11].

다른 실험에서는 레이저 기반 스푸핑 기술을 활용하여 자동차의 인식 시스템에 입력되기 전 센서 수준에서 실제 장애물의 LiDAR 포인트 클라우드 데이터를 선택적으로 지우는 방식을 통해 공격하는 방안을 제안한다. 물리적인 제거 공격 방법론이라는 새로운 방법론을 사용해 실제 장애물을 자율주행 프레임워크가 인식하지 못하도록 한다. 연구 결과는 다양한

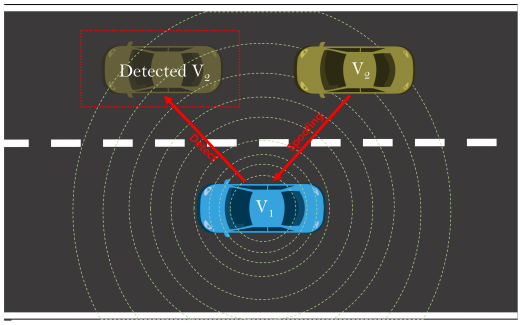

Fig. 5. Diagram of Spoofing Attack

조건으로 공격의 효과성을 입증하며, 장애물 포인트 클라우드를 성공적으로 제거하는 높은 성공률을 달성했다. 또한, 이러한 공격에 대항하기 위한 대책으로 가짜 그림자 감지 및 방위 기반 감지 같은 방법을 제안하며, 스푸핑된 포인트 클라우드 데이터를 식별하고 필터링하는 데 그 효과를 입증한다[12]. 또한, 클라우드 데이터 내에 특정 패턴이나 객체를 조작, 삽입하여 인식 시스템의 결정 과정을 왜곡하는 방법도 존재한다[13]. 이러한 공격들에 취약한 것을 방어하기 위해서 새로운 방어 메커니즘을 제안한 연구도 존재한다.

한 연구에서는 CARLO 메커니즘이라는 LiDAR에 대한 방어기법을 통해 공격을 감지, 방어하는 과정을 소개한다. 이는 특징적으로 탐지된 경계 상자 내의 자유공간과 해당 경계 상자에 대응하는 점들의 위치를 분석한다. 이를 통해 물리적 불변성을 마련하여 공격자가 파괴하기 어려운 메커니즘을 설계한다[14].

3.3 Relay Attack

역재생 공격(Replay Attack)은 다른 센서 기반의 공격과 달리 물리적 센서 공격이 아니라 사이버 위협모델에 기반을 둔다. 본 연구는 자율주행 시스템에서 LiDAR 센서의 데이터가 네트워크 통신을 통해 이루어지는 점에 주목한다.

공격 방법론은 Fig. 6.과 같다. 공격자는 LiDAR 센서에서 생성된 데이터 그램을 복제하여 복사본을 버퍼에 저장한다. 이 데이터 그램에는 주변 환경 및 장애물에 관한 정보가 포함되어 있다. 이후 공격자는 저장된 버퍼를 재생하며, 버퍼의 내용을 끝부터 전송한다. 실험 결과, 이러한 공격으로 인해 같은 방향으로 주행 중이던 주변 차량이 역방향으로 주행하는 것

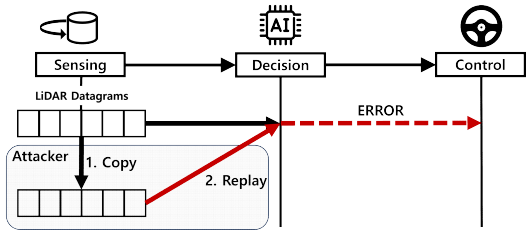

Fig. 6. Scenario of Replay Attack on LiDAR Sensors

처럼 인식되었다[15]. 이는 자율주행 시스템이 실제로 존재하지 않는 상황에 근거하여 잘못된 주행 결정을 내릴 수 있음을 의미하며, 이로 인해 시스템의 오작동이 발생하고 심각한 사고를 유발할 가능성이 있다.

IV. 차량용 LiDAR 물리적 신호교란 공격 시나리오

물리적 신호교란 공격은 센서의 성능 저하를 초래하거나, 센서가 정확한 정보를 수집하고 전송하는 과정에 방해를 주는 현상으로, 외부 신호나 잡음의 영향을 받는 것을 의미한다. 특히, LiDAR 센서에 대한 물리적 신호교란 공격은 LiDAR 시스템이 환경을 감지하고 매핑하는 데 필수적인 레이저 신호의 방해 또는 조작을 목표로 한다. 이러한 공격은 LiDAR 센서가 사용하는 것과 같은 파장의 레이저를 집중적으로 사용하여 LiDAR 센서가 올바른 정보를 수집하지 못하게 방해하는 것을 목적으로 한다. 결과적으로, 이 공격은 LiDAR 센서가 주변 환경을 정확하게 인식하고 분석하는 능력을 저해하며, 이는 자율주행 차량의 안전 운행에 직접적인 위험을 초래한다. 본 장에서는 공격자의 관점에서 다른 공격 기법들과 달리 공격 환경 구현이 쉬워, 실제 상황에서 빈번하게 발생 가능한 LiDAR 센서의 물리적 신호교란 공격 실험을 소개한다.

4.1 실험 환경 구축

본 논문에서 수행한 물리적 신호교란 공격 실험은 자율주행 차량에 탑재되는 LiDAR 센서를 대상으로 하였다. 실험 환경은 Fig. 7.과 같이 구성했으며, 공격의 주 대상이 된 LiDAR는 Velodyne 사의 VLP-16이다. 이는 16개의 레이저 채널을 갖추고 있으며, 360도 전 방위로 주변 환경을 스캔할 수 있

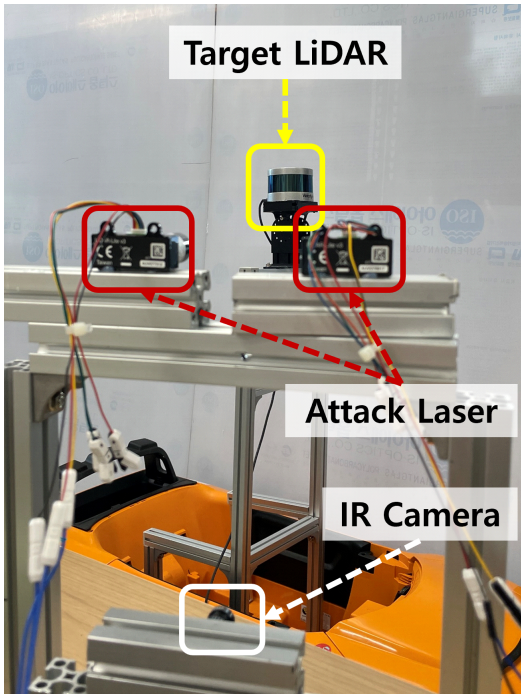

Fig. 7. LiDAR Jamming Attack Experimental Environment

는 능력을 갖추고 있다. 이를 통해 전방, 측면, 후방의 장애물을 탐지하고 그 위치를 정확히 파악할 수 있으며, 최대 100m까지의 탐지 범위를 제공한다.

이러한 특성은 넓은 지역을 대상으로 하는 자율주행 및 환경 감지 애플리케이션에 이상적으로 적합하다[17]. 본 실험에서 사용된 Velodyne의 LiDAR는 GM의 자율주행 자동차 Cruise[17], Motional 및 현대자동차의 아이오닉 자율주행 자동차[17][19], 그리고 Google의 Waymo[18]와 같이 실제 자율주행 차량에 탑재되어 사용되는 센서이다.

공격에 사용된 레이저는 타겟 LiDAR와 같은 905nm 파장을 가지는 공격용 레이저 모듈을 사용하였다. 정밀한 공격 수행을 위해, 라즈베리파이에 연결된 적외선 카메라 모듈을 사용하여 타겟 LiDAR에 공격 레이저를 정확하게 조준하였다. LiDAR는 인체에 해가 없는 적외선 영역의 빛을 이용하여 물체와의 거리를 측정하는 기술을 바탕으로 하며, 이 빛은 적외선 카메라를 통해 시각화할 수 있다. 또한, 실험 과정에서 수집된 데이터의 실시간 시각화 및 분석을 위해, VeloView 시각화 소프트웨어를 사용하였다[18]. 이 소프트웨어는 센서 데이터의 실시간 시각화 및 분석에 있어 핵심적인 도구로, 공격 시나리오 하에서 LiDAR 센서의 반응 및 영향을 명확히 파악하는 데 중요한 역할을 하였다.

4.2 실험 내용

본 연구에서 진행한 물리적 신호교란 공격 실험은 세 가지 다른 시나리오를 통해 수행되었다. 각 시나리오는 LiDAR 센서에 대한 공격 레이저의 영향을 평가하기 위해 설계되었다. 이를 통해, 공격 레이저의 존재 및 수량이 LiDAR 센서의 성능에 미치는 영향을 구체적으로 분석할 수 있었다. Fig. 8.은 실험을 간단하게 설명한 개요도이다.

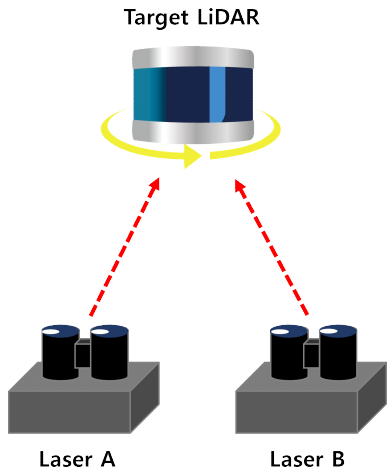

Fig. 8. Schematic Diagram of the Experiment

4.2.1 첫 번째 시나리오: LiDAR 정상 작동 상황

첫 번째 시나리오에서는 공격 레이저 없이 타겟 LiDAR만을 작동시켜 정상적인 작동 상태에서의 센서 데이터를 수집하였다. 이를 통해, 타겟 LiDAR의 기준 성능 및 데이터 프로필을 확립할 수 있었으며, 이후 공격 시나리오와의 비교 분석 기준점으로 활용되었다.

4.2.2 두 번째 시나리오: 단일 레이저 공격

두 번째 시나리오에서는 하나의 공격 레이저를 사용하여 타겟 LiDAR에 물리적 신호교란 공격을 시행하였다. 공격 레이저는 LiDAR 센서가 정상적인 환경 데이터를 수집하는 데 방해를 주기 위해 설계되

었다. 이 시나리오를 통해, 단일 공격 레이저가 LiDAR 센서의 데이터 수집 및 처리 능력에 미치는 영향을 관찰하였다.

4.2.3 세 번째 시나리오: 다중 레이저 공격

마지막 시나리오에서는 두 개의 공격 레이저를 모두 작동시켜 타겟 LiDAR에 대한 공격 강도를 높였다. 이를 통해, 다수의 공격 소스가 동시에 작동할 때 LiDAR 센서의 성능 및 데이터 정확도에 미치는 영향을 평가할 수 있었다.

각 시나리오에서는 Veloview 소프트웨어를 사용하여 1분 동안의 LiDAR 센서 데이터를 수집하였다. 이 데이터는 후속 분석을 위해 기록되었으며, 공격 시나리오가 LiDAR 센서의 성능 및 데이터 정확도에 미치는 영향을 정량적으로 평가하는 데 중요한 역할을 하였다. 이러한 실험적 접근은 자율주행 시스템에 대한 보안 위협을 식별하고 이해하는 데 필수적이며, 더 강력하고 안전한 자율주행 시스템 개발을 위한 중요한 기초 자료를 제공한다.

V. 차량용 LiDAR 물리적 신호교란 공격 실험 결과

본 장에서는 LiDAR 센서 데이터의 정상 상태와 변조 상태를 비교 분석하였다. 이를 통해 LiDAR 시스템의 보안 취약점을 평가하고, 잠재적 공격 시나리오에 대응하는 전략을 개발하는 데 중요한 기초 자료를 제공한다.

5.1 첫 번째 시나리오: LiDAR 정상 작동 상황

본 실험에서는 VLP-16 LiDAR 장비를 활용하여 실험 공간의 3차원 구조를 파악하였다. LiDAR 장비의 단독 작동 시나리오 하에서, 공간 내 물리적 구조물의 포인트 클라우드 데이터를 수집하였다.

Fig. 9.는 LiDAR 장비에서 수집된 포인트 클라우드 데이터를 시각화한 것으로, 장비의 위치로부터 최대 14.9m 거리의 공간 구조를 성공적으로 기록하였음을 보여준다. 수집된 데이터는 LiDAR 장비로부터 각각의 포인트까지의 거리를 기준으로 정량적 분석을 수행하였으며, 이를 통해 얻은 결과는 균일한 분포를 나타냈다.

Fig. 10.은 LiDAR 센서가 정상적으로 작동할 때 수집한 데이터 포인트의 거리를 Laser ID 별로 시각화한 산점도이다. 데이터는 모든 Laser ID에 대해 일관되고 균일한 거리 분포를 보이며, 대부분의 데이터 포인트가 0-15m 범위 내에 위치한다. 이는 LiDAR 센서가 실제 환경을 정확하게 감지하고 있다는 것을 나타낸다.

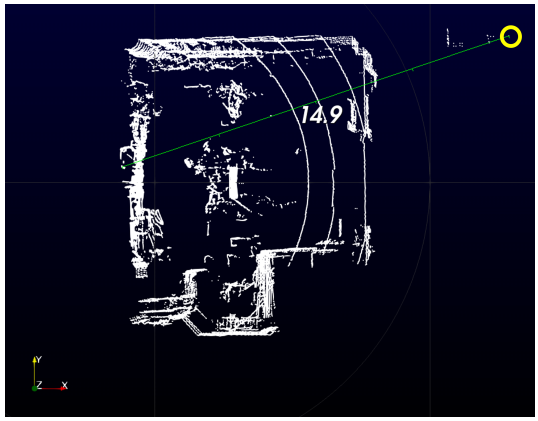

Fig. 9. Point cloud when only the target LiDAR is activated

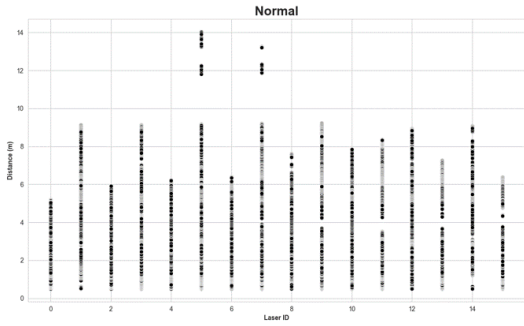

Fig. 10. A graph of the distance of points collected when only the target LiDAR is activated

5.2 두 번째 시나리오: 단일 레이저 공격

실험에 사용된 VLP-16 LiDAR의 명시된 최대 탐지 거리는 100m임에도 불구하고, 이 시나리오에서는 Fig. 11.과 같이 123m라는 비현실적인 거리가 측정되었다. 실험 환경의 실제 크기를 훨씬 초과하는 이 거리는 LiDAR 시스템이 실존하지 않는 장애물을 인식하게 만드는 공격으로 인한 결과로 해석될 수 있다. 이러한 결과는 LiDAR 시스템이 잠재적인 보안 위협에 취약할 수 있음을 시사한다. 특히,

공격자가 LiDAR 시스템에 조작된 데이터를 주입함으로써, 실제로는 존재하지 않는 장애물을 생성하고 매핑하는 과정에 영향을 미칠 수 있다는 점이 주목할 만하다. 또한, 이와 같은 조작은 시스템이 의존하는 데이터의 신뢰성을 저하시키며, 이는 특히 자율주행 차량과 같은 안전-민감 시스템에서 심각한 결과를 초래할 수 있다.

조작된 데이터 포인트들은 정상 상태에서 관찰되지 않는 거리에 분포되어 있으며, 이는 시나리오 1에서 얻어진 데이터와 비교했을 때 명확한 차이를 보인다. 이러한 분포는 데이터의 일관성 및 정확성을 판단하는 중요한 지표가 될 수 있다.

Fig. 12.는 공격자가 LiDAR 시스템에 대한 공격을 시도하여 하나의 레이저만을 작동시킨 상태에서의 데이터 포인트 거리 분포를 보여준다. 이 시나리오에서는 특정 Laser ID에서 비정상적으로 높은 거릿값을 관찰할 수 있다. 이는 공격 레이저가 다른 정상적인 LiDAR 센서들의 동작에 영향을 주어 거리 측정에 오류를 유발한 결과로 해석될 수 있다.

5.3 세 번째 시나리오: 다중 레이저 공격

Fig. 13.은 두 개의 공격 레이저를 동시에 작동시킨 상태에서의 LiDAR 포인트 클라우드를 나타낸다. Fig. 11.을 보면 단일 공격 레이저를 사용했을 때, 특정 방향으로 LiDAR 센서를 조작하여 거리 측정에 오류를 유발한 것으로 보인다. 그러나 이 경우에는 LiDAR 시스템의 나머지 부분이 정상적인 거릿값을 보여줘, 공격의 영향이 상대적으로 제한적이었다. 반면에, Fig. 13, 14.에서와 같이 다중 공격 레이저를 사용했을 때, LiDAR 센서가 수집한 데이터 포인트들은 더 넓은 범위에서 비정상적인 거릿값을 나타냈다. 이는 단일 공격 시나리오보다 데이터 조작의 범위와 강도가 증가했음을 시사한다. 두 공격 레이저의 사용은 LiDAR 시스템이 수집하는 데이터 포인트들 사이의 거리가 더욱 다양해지고, 실존하지 않는 여러 장애물을 인식하게 만드는 결과를 초래했다.

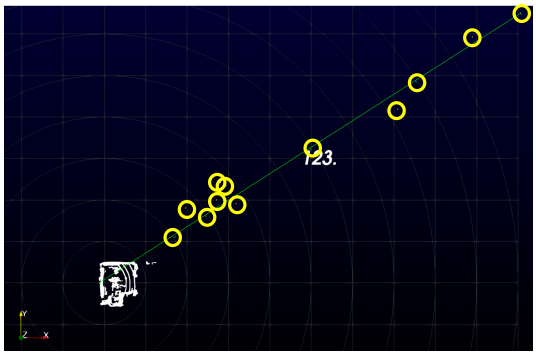

Fig. 11. Point cloud when one attack laser is activated

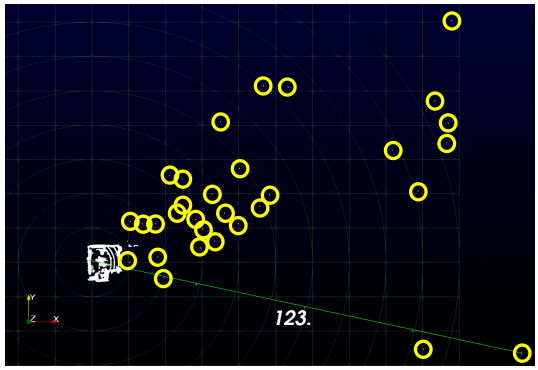

Fig. 13. Point cloud when two attack lasers are activated

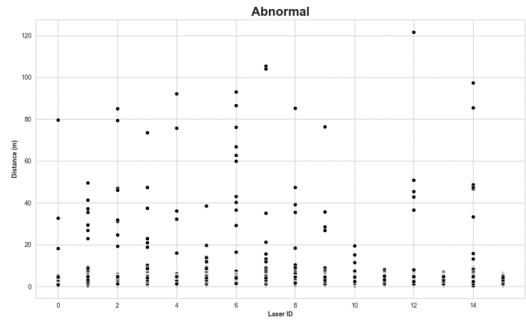

Fig. 12. A graph of the distance of points collected when triggering a single attack laser

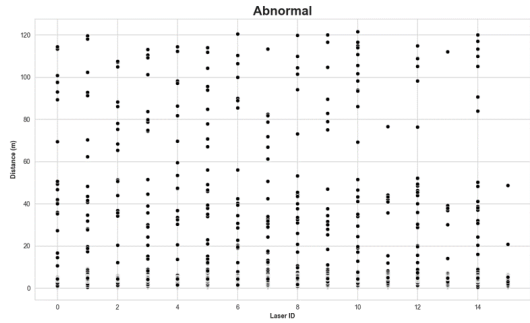

Fig. 14. A graph of the distance of points collected when triggering two attack lasers

이러한 비교 분석은 LiDAR 시스템에 대한 공격이 얼마나 복잡하고 광범위하게 이루어질 수 있는지를 시사한다. 단일 공격 레이저는 제한적인 조작을 유발하는 반면, 다중 공격 레이저는 LiDAR 시스템 전체에 영향을 미쳐 더욱 심각한 데이터 왜곡을 초래할 수 있다. 이러한 결과는 LiDAR 시스템의 보안 측면을 강화하고, 데이터 조작을 탐지하며 신뢰할 수 있는 센서 데이터를 보장하기 위한 추가적인 방어 메커니즘이 필요함을 강조한다.

VI. 차량용 LiDAR 센서의 물리적 신호교란 공격 보안 위협 대응방안

차량용 LiDAR 센서가 직면한 물리적 신호교란 공격은 자율주행 기술의 신뢰성을 해치는 주요 위협 중 하나로 인식되고 있다. 이러한 위협에 대응하기 위해, 차량 간 통신(Vehicle-to-Vehicle, V2V)을 활용한 센서 데이터 공유는 주변 환경 정보의 정확도를 향상시키고 시스템의 안정성을 높이는 유력한 방법으로 간주한다. 주변 차량으로부터의 추가적인 데이터는 각 차량의 센서 데이터 중복성을 증가시키며, 이를 통해 장애물 인식 데이터에 대한 불일치를 감지하고 LiDAR 센서에 대한 공격 성공률을 감소시키는 데 기여할 수 있다[10].

센서 데이터 중복성을 증가시키는 다른 방법은 다중 센서 융합이다. 이는 카메라, 초음파, RADAR 및 LiDAR와 같은 다양한 센서들을 통합하여 장애물 인식 데이터의 신뢰도를 더욱 높이는 전략이다. 각 센서로부터 얻어진 데이터를 종합함으로써, 하나의 센서가 공격을 받거나 오류를 보일 때 다른 센서들이 이를 보완할 수 있다[19]. 또는 LiDAR 센서를 추가하여 공격에 대응할 수 있다. 그러나, 다수의 LiDAR 센서를 추가하는 방안은 비용 증가를 초래하고 새로운 취약점을 일으킬 수 있어, 이러한 방안을 선택할 때는 비용 대비 이점을 신중하게 평가해야 한다.

또한, 본 연구에서 수행된 실험 데이터는 LiDAR 데이터가 비정상적으로 변화할 경우를 감지할 수 있는 행동 기반 분석의 적용 가능성을 보여준다. 이는 기계학습 기법을 통해 LiDAR 센서 데이터의 시간적 변화를 분석하고, 물리적 신호교란 공격과 같은 비정상적인 패턴을 감지하는 데 사용될 수 있다.

이러한 대응 전략은 물리적 신호교란 공격에 대한 효과적인 방어를 구축하고 LiDAR 센서의 정확성을 개선하는 데 기여할 것으로 예상한다. 그런데도, 이들 방법이 LiDAR 센서의 생산 비용을 증가시킬 가능성을 고려하여, 각 전략을 채택하기 전에 장기적인 비용 대비 효과 분석이 요구된다.

VII. 결 론

본 논문에서는 자율주행 자동차의 핵심 구성 요소인 LiDAR 센서의 보안 측면을 심도 있게 분석하였다. 자동차의 '눈' 역할을 하는 LiDAR 센서는 기술 발전에 따라 증가하는 보안 위협에 직면해 있다. 본 연구를 통해, LiDAR 센서를 대상으로 한 물리적 신호교란 공격이 자율주행 시스템의 안전성과 신뢰성을 심각하게 저해할 수 있는 주요 위협임을 확인하였다. 이러한 공격은 자율주행 기술의 발전을 저해하고, 차량의 안전한 운행을 위협하는 중대한 보안 취약점으로 작용한다. 따라서, 자율주행 시스템의 안정성을 확보하기 위해서는 보안 강화와 적극적인 방어 기술의 개발이 필요하다. 이는 차량 간 통신, 다중 센서 융합, 기계학습을 활용한 이상 탐지 등 다각적인 접근 방식을 포함한다.

향후 연구에서는 본 연구에서 제안된 대응방안들의 실행 가능성과 효과성을 더욱 개선하고, 실제 도로 환경에서의 적용을 평가해야 할 것이다. 자율주행 기술이 지속해서 발전함에 따라, 이와 관련된 보안 문제에 관한 연구와 혁신 역시 매우 중요하다. 본 논문의 결과는 이 분야의 연구자들과 기술자들에게 자율주행 차량의 안전한 미래를 위한 기초를 제공할 것으로 기대된다.

References

[1] SAE, "Taxonomy and Definitions for Terms Related to Driving Automation Systems for On-Road Motor Vehicles," J3016_202104, Apr. 2024

[2] Jiseong Jeong, Junhwan Jang, and Jaekwon Lee, "Trends in the Lidar Sensor Technology for Autonomous Vehicles," AUTO JOURNAL : Journal of the Korean Society of Automotive Engineers, vol. 45, no. 4, pp. 22-26, 2023

[3] Khader, Motaz, and Samir Cherian.

"An introduction to automotive lidar," Texas Instruments, 2020.
〔4〕 Eunbin Na, "Autonomous vehicles and LiDAR," The Magazine of the IEEE, vol. 50, no. 1, pp. 44-49, 2023
〔5〕 LUMISOL, "Types of Lidar Sensors Based on Operation," http://www.lumisol.co.kr/sub/reference/lidar.asp?mode=view&bid=4&s_type=&s_keyword=&s_cate=&idx=162&page=1, Nov. 2020
〔6〕 G.D Choi, M.H Han, M.H Song, H.S Seo, C. Kim, S. Hong, and B. Mheen, "Development Trends and Expectations of Three-Dimensional Imager based on LIDAR Technology for Autonomous Smart Car Navigation," ETRI Electronics and Telecommunications Trends, vol. 31, no. 4, pp. 0-0, 2016.
〔7〕 Y. Li and J. Ibanez-Guzman, "Lidar for Autonomous Driving: The Principles, Challenges, and Trends for Automotive Lidar and Perception Systems," in IEEE Signal Processing Magazine, vol. 37, no. 4, pp. 50-61, July 2020
〔8〕 Chris Clonts, "LIdar vs. Everybody in the Onboard Sensor Race," SAE ADAS&Autonomous Vehicle Engineering, pp. 10-15, Apr. 2023
〔9〕 ResearchInChina, "Automotive LiDAR Industry Report, 2023," BXM153, Research In China, Oct. 2023
〔10〕 Petit. J, Stottelaar. B, Feiri. M, and Kargl. F, "Remote Attacks on Automated Vehicles Sensors: Experiments on Camera and LiDAR," Black Hat Europe, vol. 11, no. 2015, pp. 995, 2015
〔11〕 Cao, Yulong, et al. "Adversarial sensor attack on lidar-based perception in autonomous driving," Proceedings of the 2019 ACM SIGSAC conference on computer and communications security, pp. 2267-2281, Aug. 2019
〔12〕 Cao, Yulong and Bhupathiraju, S Hrushikesh and Naghavi, Pirouz and Sugawara, Takeshi, and Mao, Z Morley and Rampazzi, Sara, "You Can't See Me: Physical Removal Attacks on LiDAR-based Autonomous Vehicles Driving Frameworks," 32nd USENIX Security Symposium (USENIX Security 23), pp. 2993-3010, 2023
〔13〕 Yang, Kaichen, Tzungyu Tsai, Honggang Yu, Max Panoff, Tsung-Yi Ho, and Yier Jin. "Robust roadside physical adversarial attack against deep learning in lidar perception modules," In Proceedings of the 2021 ACM Asia Conference on Computer and Communications Security, pp. 349-362, 2021
〔14〕 Sun, Jiachen, Yulong Cao, Qi Alfred Chen, and Z. Morley Mao. "Towards robust {LiDAR-based} perception in autonomous driving: General black-box adversarial sensor attack and countermeasures." In 29th USENIX Security Symposium (USENIX Security 20), pp. 877-894, 2020
〔15〕 Hallyburton, R Spencer and Pajic, Miroslav, "Securing Autonomous Vehicles Under Partial-Information Cyber Attacks on LiDAR Data," arXiv e-prints, pp. arXiv-2303, Mar. 2023
〔16〕 Shin, Hocheol Kim, Dohyun, Kwon, Yujin, and Kim, Yongdae, "Illusion and Dazzle: Adversarial Optical Channel Exploits against Lidars for Automotive Applications," Cryptographic Hardware and Embedded Systems--CHES 2017: 19th International Conference, Taipei, Taiwan,

September 25-28, 2017, Proceedings, pp. 445-467, 2017
〔17〕 Velodyne, "VLP-16 user manual" https://velodynelidar.com/wp-content/uploads/2019/12/63-9243-Rev-E-VLP-16-User-Manual.pdf, 20th. Dec. 2023
〔18〕 ParaVeiw, "VeloView" https://www.paraview.org/veloview/, 20th. Dec. 2023
〔19〕 Ren, Kui, Wang, Qian, Wang, Cong, Qin, Zhan, and Lin, Xiaodong, "The Security of Autonomous Driving: Threats, Defenses, and Future Directions," Proceedings of the IEEE, vol. 108, no. 2, pp. 357-372, Feb. 2020
〔20〕 Pierrick Boulay, "LiDAR industry report:Hesai wins top rankings in the global market," Yole Group, Aug. 2022
〔21〕 RON AMADEO, "Google's Waymo invests in LiDAR technology, cuts costs by 90 percent," ars TECHNICA, Jan. 2017
〔22〕 HYUNDAI, "ioniq5 robotaxi" https://www.hyundai.com/worldwide/ko/brand-journal/mobility-solution/ioniq-5-based-robotaxi, 27th. Dec. 2023

〈저자소개〉

황 지 웅 (Ji-ung Hwang) 학생회원
2023년 3월~현재: 순천향대학교 정보보호학과 학사과정
〈관심분야〉 정보보호, 자동차보안

윤 요 섭 (Yo-seob Yoon) 학생회원
2024년 2월: 순천향대학교 정보보호학과 졸업
2024년 3월~현재: 순천향대학교 모빌리티융합보안학과 석사과정
〈관심분야〉 정보보호, 바이너리분석

오 인 수 (In-su Oh) 정회원
2018년 2월: 순천향대학교 정보보호학과 졸업
2020년 2월: 순천향대학교 정보보호학과 석사
2023년 8월: 순천향대학교 정보보호학과 박사
2023년 9월~현재: 순천향대학교 정보보호학과 박사후연구원
〈관심분야〉 정보보호, 모바일보안, 자율주행차보안

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