Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.31, NO.3, Jun. 2021 ISSN 2288-2715(Online)
https://doi.org/10.13089/JKIISC.2021.31.3.411

진동 신호를 사용한 MEMS 센서 대상 신호오류 주입공격 탐지 방법*

조 현 수,[1†] 오 희 석,[2] 최 원 석[2‡]
[1]고려대학교 정보보호대학원 (대학원생), [2]한성대학교 (교수)

Vibration-Based Signal-Injection Attack Detection on MEMS Sensor*

Hyunsu Cho,[1†] Heeseok Oh,[2] Wonsuk Choi[2‡]
[1]School of Cybersecurity, Korea University (Graduate student),
[2]Hansung University (Professor)

요 약

무인이동체에 탑재되는 자율주행 시스템은 여러 센서를 통해 외부 환경을 인식하고 이를 통해 최적의 제어값을 도출한다. 무인이동체의 자율주행 시스템은 최근들어 사이버공격의 타겟이 되고 있다. 예를 들어, 무인이동체의 센서를 대상으로 신호오류 주입공격을 수행함으로써 센서 데이터를 악의적으로 조작하는 PHY 레벨 (Physical level) 공격과 관련한 연구 결과들이 발표되고 있다. PHY 레벨에서 수행되는 신호오류 주입공격은 주변 환경에 물리적 조작을 가하여 센서가 잘못된 데이터를 측정하게 하므로 소프트웨어 레벨에서 공격을 탐지하기 어렵다는 특징을 갖고 있다. 신호오류 주입공격을 탐지하기 위해서는 센서가 측정하는 데이터의 신뢰성을 검증하는 과정이 필요하다. 현재까지 자율주행 시스템에 탑재되는 센서들을 대상으로 PHY 레벨 공격을 시도하는 다양한 방법이 제시되었으나 이를 탐지하고 방어하는 연구는 아직까지는 부족한 상황이다. 본 논문에서는 무인이동체 환경에서 널리 쓰이고 있는 MEMS 방식의 센서를 대상으로 신호오류 주입공격을 재연하고, 이러한 공격을 탐지하는 방법을 제안한다. 제안하는 방법의 정확도를 분석하기 위해서 신호오류 주입 탐지 모델을 구축하였으며, 실험실 환경에서 유효성을 검증하였다.

ABSTRACT

The autonomous driving system mounted on the unmanned vehicle recognizes the external environment through several sensors and derives the optimum control value through it. Recently, studies on physical level attacks that maliciously manipulate sensor data by performing signal-injection attacks have been published. signal-injection attacks are performed at the physical level and are difficult to detect at the software level because the sensor measures erroneous data by applying physical manipulations to the surrounding environment. In order to detect a signal-injection attack, it is necessary to verify the dependability of the data measured by the sensor. As so far, various methods have been proposed to attempt physical level attacks against sensors mounted on autonomous driving systems. However, it is still insufficient that methods for defending and detecting the physical level attacks. In this paper, we demonstrate signal-injection attacks targeting MEMS sensors that are widely used in unmanned vehicles, and propose a method to detect the attack. We present a signal-injection detection model to analyze the accuracy of the proposed method, and verify its effectiveness in a laboratory environment.

Keywords: Vibration, Signal-Injection Attack, PHY-level Attack, MEMS Gyroscope

Received(05. 03. 2021), Modified(06. 02. 2021), Accepted(06. 02. 2021)

* 이 논문은 2021년도 정부(교육부)의 재원으로 한국연구재단의 지원을 받아 수행된 기초연구사업(No.NRF-2020R1C1C1007446) 지원과 2021년도 정부(과학기술정보통신부)의 재원으로 정보통신기획평가원의 지원을 받아 수행된 연구임 (No. 2020-0-00374, 무인이동체 공통핵심 보안기술 개발 연구)

† 주저자, hscho20@korea.ac.kr
‡ 교신저자, wonsuk@hansung.ac.kr(Corresponding author)

I. 서 론

최근 들어 스마트 자동차나 드론과 같이 자율주행 기능이 탑재되어 있는 시스템 개발에 대한 관심이 늘어나고 있고, 이러한 자율주행 시스템을 실제로 사용하는 사례도 쉽게 발견할 수 있다. 특히, AI (Artificial Intelligence) 기술의 발달은 자율주행 기능의 상용화를 가속화하고 있다. 자율주행 기능은 다수의 센서를 이용하여 물리 세계 정보를 습득하고 이를 분석한 결과를 바탕으로 엑추에이터를 통해 다시 물리 세계에 적용한다. 이처럼, 자율주행 시스템은 우리가 살아가는 물리 세계와 사이버 세계가 서로 융합하는 CPS(Cyber Physical Systems)의 대표적인 예라 할 수 있다. 자율주행 시스템과 더불어 CPS는 다양한 분야에 적용되어 안정성, 효율성, 신뢰성, 보안성에 혁신적인 변화를 가져올 것이라 예상된다.

따라서 무인이동체를 포함하여 CPS의 모든 분야에서는 주변 상황 및 환경 인지를 위해 센서 기술의 발달이 필수적으로 요구되고 있다. 예를 들어, 3축 자이로스코프(3-axis gyroscope) 센서는 비행하는 드론의 자세를 판단하기 위해 사용된다. 센서 기술은 매우 다양한 분야에서 사용되고 있으며 기술 개발을 통하여 앞으로 측정 정확도도 계속해서 향상될 것으로 기대되고 있다. 하지만 센서 기술의 활용도가 넓어짐에 따라 최근 센서를 대상으로 하는 악의적인 공격 방법들도 다양하게 등장하고 있다. 특히, PHY 레벨에서 신호오류 주입을 수행하는 공격 방법들이 소개되고 있다[1]. 신호오류 주입을 통하여 센서가 주변 상황을 제대로 인지하지 못하게 하여 결과적으로 특정 애플리케이션의 오동작을 유도한다. CPS 환경에서 애플리케이션의 오동작은 물리 세계로까지 영향이 확장되는 것을 의미하기 때문에, 사이버 세계에 국한되어 영향을 끼치는 사이버 공격과 달리 센서를 대상으로 하는 공격은 최악의 경우 인명피해까지 발생시킬 수 있는 파급력이 존재한다. 실제로, Son et al. 연구팀은 자이로스코프 센서가 탑재되어 있는 드론을 대상으로 의도적인 음향 노이즈를 생성 및 주입하여 해당 드론의 오동작을 유도하는 연구 결과를 발표하였다[7]. 이러한 연구는 신호오류 주입공격으로 인해 드론이 사람과 충돌까지 할 수 있고 결국에는 해당 사람이 사망까지 할 수 있음을 의미한다.

센서를 대상으로 하는 신호오류 주입공격은 PHY 레벨에서 수행되기 때문에, 전통적인 소프트웨어 기반의 보안기법으로는 탐지가 매우 어렵다는 특징이 있다. 또한, 소프트웨어 기반의 보안기법을 통해 센서값을 보정하더라도 CPS의 특성상 시스템의 실시간성에 악영향을 미쳐 결과적으로 서비스 중단에 이르는 상황까지 발생할 수 있다[16]. 이러한 이유로 기존 보안기법의 접근 방식으로는 신호오류 주입공격을 탐지하기 어려우며 새로운 방식의 보안기법 연구가 필요하다.

본 논문에서는 자율주행 기능이 탑재되어 있는 CPS 환경에서 가장 널리 사용되고 있는 MEMS(Micro ElectroMechanical Systems) 방식의 센서를 대상으로 신호오류 주입공격을 재연하고 이를 적절하게 탐지할 수 있는 기법을 제안 및 평가한다. Shoukry et al. 연구팀은 단일 센서 환경에서 신호오류 주입공격을 탐지할 수 있는 Pycra라 불리는 기법을 제안하였지만, Pycra는 초음파 센서와 같은 Active 센서에만 적용 가능한 기법으로, MEMS 센서와 같은 Passive 센서에는 적용이 불가능하다[2]. 우리는 Passive 단일 센서 환경에서 적용이 가능한 신호오류 주입공격 탐지 기법을 제안하고 이에 대한 평가 결과를 보여주도록 하겠다. 제안하는 기법에서는 마이크로컨트롤러가 랜덤하게 선택한 주파수 또는 신호 세기를 진동 모듈에 전달하여 진동을 발생시키고 이 진동을 MEMS 센서가 정확하게 측정하는지 여부를 판단하여 신호오류 주입공격을 탐지한다. 만약 마이크로컨트롤러가 선택한 주파수 또는 신호 세기에 해당하는 진동을 MEMS 센서가 측정하지 못한 경우에는 신호오류 주입공격으로부터 영향을 받았다고 간주할 수 있다.

II. 관련연구

이번 장에서는 센서를 대상으로 하는 신호오류 주입공격과 관련된 기존 연구에 대하여 소개한다. 설명에 앞서 신호오류 주입공격 방법에 대한 이해를 돕기 위해 센서가 측정하는 에너지의 소스에 따라 구분되는 Passive 센서와 Active 센서에 대하여 설명하겠다. Passive 센서는 주변에 존재하는 에너지를 측정하는 센서를 의미한다. 예를 들어, 온도나 습도는 Passive 센서에 의하여 측정된다. Active 센서의 경우에는 센서가 직접 에너지를 생성 및 방사하여 돌아오는 에너지를 다시 측정하는 센서를 의미한다. 다시 말해, 에너지의 소스가 센서 자신이 된다. Active 센서는 거리를 측정하기 위해 사용되는 초음파 센서가 대표적인 예이다. 본 논문에서 타겟으로 하는 MEMS 방식의

센서의 경우에는 Passive 센서로 분류된다. 최근에는 이러한 Passive 및 Active 센서를 대상으로 PHY 레벨에서 수행되는 신호오류 주입공격 방법이 연구되고 있으며, 공격에 사용하는 신호오류의 대역에 따라 In-band 신호오류 주입 공격과 Out-of-band 신호오류 주입 공격으로 분류할 수 있다. 우리는 이번 장에서 이 두 공격 방법에 대한 기존 연구들을 소개하도록 하겠다.

2.1 In-band 신호오류 주입 공격

In-band 신호오류 주입공격은 타겟 센서가 측정하는 신호유형과 동일한 대역의 신호를 외부에서 악의적으로 주입하는 공격 방법이다. Passive 센서에 대한 In-band 신호오류 주입공격은 센서 주변의 물리적 상황을 조작하여 센서가 측정하는 물리량에도 변화를 일으키는 방법으로 수행된다. Davidson et al. 연구팀은 드론에 장착되어 있는 비전센서를 대상으로 In-band 신호오류 주입공격을 수행하였다[3]. 비행 중인 드론은 지면에 대한 정보를 비전센서를 이용하여 광학흐름(optical flow)을 측정 및 분석하고 그 결과를 드론의 자세제어를 위해 활용한다. 예측한 방향과 실제 움직이는 방향의 차이만큼 드론을 조정하여 드론이 표류하지 않고 안정적인 비행이 가능하도록 보장한다. Davidson et al. 연구팀은 프로젝터와 레이저포인터를 이용하여 지면에 조작된 이미지를 투사하였고 그 결과 드론의 비전센서가 잘못된 이미지 정보를 수집하도록 하는 일종의 스푸핑 방법을 발표하였다. 이러한 공격 방법으로 인해 비행중인 드론은 안정적인 자세제어가 불가능해지고 표류하게 되는 결과를 보여주었다. Chen et al. 연구팀의 경우 음성인식(speech recognition) 시스템에 탑재되어 있는 음향 센서를 대상으로 In-band 신호오류 주입공격을 수행하였다[4]. 사람이 인지하기에는 어려운 음향 노이즈(perturbation)을 음향 센서에 주입하였고, 음성인식 시스템은 이를 사람의 음성 명령이라고 인지하였다.

Active 센서를 대상으로 하는 In-band 신호오류 주입공격의 경우에는 Active 센서에서 발생시키는 신호 자체를 스푸핑(spoofing)하여 해당 센서가 제대로 된 에너지양을 측정하지 못하도록 하는 공격 방법이다. Shin et al. 연구팀은 자율주행 자동차에 탑재되는 라이다 센서를 대상으로 스푸핑 공격을 수행하였다[5]. 스푸핑 공격을 통해 라이다 센서에 illusion 현상을 유도하여 자율주행 자동차가 존재하지 않는 장애물을 감지하게 하였다. Yan et al. 연구팀은 자율주행 자동차에 탑재되는 레이더 센서를 대상으로 In-band 신호오류 주입공격을 수행한 연구 결과를 발표하였다[6]. 테슬라 차량에 탑재되는 레이더 센서에 재밍 공격과 스푸핑 공격을 수행함으로써 전방의 장애물을 탐지하지 못하도록 하거나 장애물과의 거리를 변조시켜 정상적인 주행이 불가능하도록 하였다.

2.2 Out-of-band 신호오류 주입공격

Out-of-band 신호오류 주입공격은 센서가 측정하는 신호와 다른 대역의 신호를 주입하여 센서의 오동작을 유도하는 공격 방법이다. Out-of-band 신호오류 주입공격 같은 경우에는 모두 Passive 유형의 센서를 대상으로 하는 공격에 대한 연구가 진행되었으며, 센서의 공진주파수를 이용한 방법과 EMI(ElectroMagnetic Interference)를 이용한 방법으로 분류된다. Son et al. 연구팀은 드론에 탑재되어 있는 MEMS 방식의 자이로스코프 센서에 대하여 공진주파수와 일치하는 음향 노이즈를 주입함으로써 드론의 오동작을 유도하는 연구 결과를 발표하였다[7]. Trippel et al. 연구팀은 MEMS 방식의 가속도 센서를 대상으로 공진주파수와 일치하는 음향 신호를 주입하는 연구결과를 발표하였다[8]. 또한, Tu et al. 연구팀의 경우에는 MEMS 방식의 IMU(Inertial Measurement Unit) 센서를 대상으로 연구를 진행하여 발표하였다[9].

전자파 간섭을 활용한 Out-of-band 신호오류 주입공격의 경우에 ADC(Analog to Digital Converter)의 동작 원리를 이용하여 공격을 수행하였다. 센서는 물리 세계에서 측정한 물리량을 아날로그 신호로 표현한다. 그리고 이를 다시 ADC를 이용하여 디지털 신호로 변환한다. 전자파 간섭은 ADC의 입력이 되는 아날로그 신호에 영향을 미쳐 결과적으로 마이크로컨트롤러가 측정하는 센싱 값이 달라지게 한다. Selvaraj et al. 연구팀은 임베디드 시스템의 센서 및 액추에이터에 악의적 전자파 간섭 신호를 주입하여 시스템을 조작하는 공격 방법에 관한 내용을 발표하였다[10]. 공격자는 공격 대상 회로에 물리적으로 접근할 수 있지만, EMI 신호를 통해서만 상호작용할 수 있다. 이 연구에서는 아날로그 센서에 대한 공격, 디지털 센서에 대한 공격, 액추에이

터에 대한 공격으로 나누어 수행한 연구 결과를 제시하였다. Tu et al. 연구팀은 온도 감지 및 제어 시스템에 사용되는 아날로그 온도 센서를 대상으로 직접 EMI 신호를 주입하는 DPI(Direct Power Injection) 공격을 소개하고 분석 결과에 대해 발표하였다[11]. EMI 신호의 경우 벽과 창문 같은 일반적인 물리적 장벽을 통과하여 대상 시스템에 주입될 수 있으며, 신호의 주파수 및 진폭을 조정하는 등 공격의 정교화를 통해 시스템을 공격자가 원하는 상태로 동작시키는데 용이하다.

III. 공격자 모델

자율주행 자동차나 드론과 같이 자율주행 기능이 탑재되어 있는 시스템에서 사용하고 있는 센서를 대상으로 하는 신호오류 주입공격은 PHY 레벨에서 수행되기 때문에, 소프트웨어 레벨에서의 전통적인 보안기법으로는 탐지가 매우 어렵다. 이러한 사실을 악용하여, CPS를 대상으로 하는 사이버보안 공격 방법 중 하나로 신호오류 주입공격이 주목받고 있다. 이번 장에서는 CPS에 탑재되어 있는 센서를 대상으로 신호오류를 주입하는 공격자 모델을 설명하도록 하겠다. 공격자는 신호오류 주입공격을 통하여 CPS가 주변 상황을 제대로 인지하게 못하게 하여 결국에는 CPS의 오동작을 유도하는 것을 최종목표로 갖고 있다. CPS의 오동작은 사이버 세계뿐만 아니라 물리 세계에 그 영향을 미치기 때문에, 오동작의 파급력이 매우 크다고 말 할 수 있다.

본 논문에서는 주변 상황 인지를 위해 CPS 환경에서 가장 널리 사용되고 있는 MEMS 방식의 Passive 센서를 대상으로 외부에서 공진주파수를 주입하는 Out-of-band 신호오류 주입공격만을 고려하도록 하겠다. 센서 유형에 따라 신호오류 주입 방법의 차이가 조금씩 다르지만, 전체적인 방법론은 같다. 예를 들어, 센서들은 자신의 공진주파수가 각각 다르기 때문에 주입해야 하는 신호오류의 주파수 대역이 달라진다. MEMS 방식의 센서의 경우에는 가청 주파수 대역의 공진주파수를 갖고 있다. 그리고 신호오류 주입공격을 효과적으로 수행하기 위해 공격자는 타겟 센서의 공진주파수를 알아야 한다. 공진주파수를 모르는 경우라 하더라도, 모든 경우의 수를 검색하면서 찾아낼 수 있다. 하지만, 본 논문에서는 공격자는 타겟 센서의 공진주파수를 사전에 알고 있다고 가정한다. 타겟 센서의 제조사와 제품명이 알려

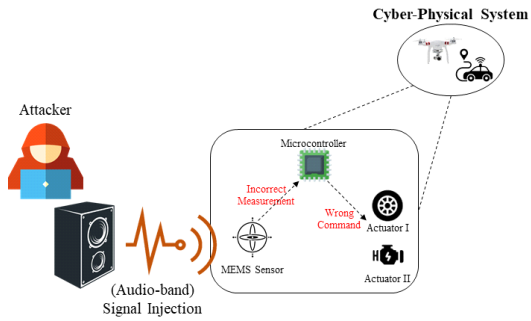

Fig. 1. Attack Model

져 있는 경우에는 모든 경우의 수를 전수조사하지 않더라도 공진주파수는 대부분 쉽게 알아낼 수 있다. 또한, 공격자가 신호오류 주입을 하기 위해서는 타겟 센서와 일정 거리 이내를 유지하여야 한다. 기본적으로 가청 주파수 대역의 신호의 경우에는 신호의 이동거리가 짧다. 신호의 세기를 크게 하여 이동거리를 확장 시킬 수 있기는 하지만, 본 논문의 주요 목적은 신호의 세기와 상관없이 신호오류 주입공격을 탐지하는 것이기 때문에 공격 재연의 간편함을 위해서 공격자가 타겟 센서와 일정 거리 이내에서 공격할 수 있다고 가정한다. "Fig.1."은 MEMS 방식의 센서를 대상으로 신호오류 주입공격을 수행하는 공격자 모델을 보여주고 있다.

IV. 신호오류 주입공격

이번 장에서 우리는 Active 및 Passive 센서를 대상으로 신호오류 주입공격을 재연한다. 이를 위해, 우리는 Active 센서로 HC-SR04 초음파 센서 그리고 Passive 센서로 MEMS 방식의 MPU6050 3축 자이로스코프 센서를 이용하였다[12, 13]. Active 센서를 대상으로 하는 신호오류 주입공격은 해당 센서가 측정하는 신호와 같은 대역의 신호를 미리 주입하거나 신호의 양을 증가함으로써 센서가 측정하는 정보를 왜곡하는 방법이다. 따라서 타겟 센서와 동일 대역의 신호를 주입하는 방법이기 때문에 Active 센서를 대상으로 하는 신호오류 주입은 In-band 신호오류 주입공격 방법으로 분류된다. Passive 센서를 대상으로 하는 신호오류 주입 공격은 해당 센서의 공진주파수와 같은 대역의 신호를 주입하여 공명 현상을 발생시켜 센서가 올바른 값을 측정하지 못하도록 하는 방법이다. 공명 현상을 발생시

기 위해서는 타겟 센서가 측정하는 신호와 다른 대역의 신호를 이용하기 때문에 Passive 센서를 대상으로 공진주파수를 주입하는 공격은 Out-of-band 신호오류 주입공격 방법으로 분류할 수 있다.

Passive 센서 대상 Out-of-band 신호오류 주입공격을 수행하는 방법을 이해하기 위해서는 공진주파수에 대한 개념에 대한 이해가 필요하기 때문에 신호오류 주입공격 재연에 앞서 공진주파수에 대하여 간단하게 설명하겠다.

4.1 공진주파수

자연 상태에서 모든 시스템과 물체는 정지해 있더라도, 아주 미세하게는 주기적인 흔들림이 존재하는 것으로 알려져 있다[14]. 이와 같은 물체의 흔들림은 각각 고유한 주기를 갖고 있고 이를 공진주파수라 한다. 그리고 특정 물체의 공진주파수와 같은 진동수로 외부에서 힘이 작용되어 진동이 강해지는 것을 공명 현상이라 한다. 예를 들어, 우리가 일상생활에서 흔하게 사용하는 전자레인지는 파장 12cm, 진폭 2,450MHz인 마이크로파를 방출하고 이 마이크로파에 의해 음식물 속의 물 분자가 공명 현상에 의해 진동하면서 열에너지를 만들어내는 원리이다.

센서의 경우에도 고유한 공진주파수를 가지고 있으며 공명 현상이 발생할 수 있다. 외부에서 센서의 공진주파수와 동일한 주파수의 신호가 주입되면 공명 현상으로 인해 측정값에 오류가 발생한다. 따라서, 이러한 현상을 악용하여 공격자는 의도적으로 공진주파수와 동일한 주파수의 신호를 생성 및 주입하여 해당 센서가 잘못된 운동량을 측정하게 만드는 신호오류 주입공격을 수행한다. 이는 결과적으로 해당 센서의 전체 시스템 오류를 발생시키게 된다.

4.2 타겟 센서 대상 신호오류 주입공격

우리는 Passive 센서 중 하나인 MEMS 방식의 자이로스코프 센서를 대상으로 하는 신호오류 주입공격 탐지 기법을 제안하기에 앞서, 신호오류 주입공격을 실제로 재연하여 보여주도록 하겠다. 우리가 제안하는 신호오류 주입공격 탐지의 경우에는 Passive 센서를 대상으로 하는 Out-of-band 신호오류 주입공격만을 고려하고 있지만, 본 장에서는 Active 센서를 대상으로 하는 In-band 신호오류 주입공격까지 재연하여 보여주도록 하겠다.

4.2.1 초음파 센서 대상 In-band 신호오류 주입공격

HC-SR04 초음파 센서는 40kHz의 주파수를 이용하여 초음파 신호를 전송하고 다시 반사되어 돌아오는 신호를 측정함으로써 대상과의 거리를 측정하는 Active 센서이다. 우리는 신호발생기를 사용하여 초음파 센서와 동일한 40kHz의 주파수 신호를 발생시켰다. 신호발생기로부터 생성된 신호를 전송시키기 위해 초음파 대역을 지원하는 스피커를 통해 음향 신호를 출력하였다.

"Fig.2."는 초음파 센서 대상 In-band 신호오류 주입공격을 수행하였을 때, 초음파 신호가 측정하는 거리를 보여주고 있다. 그림에서 x, y축은 각각 시간과 대상과의 측정 거리를 의미하며, 약 3,000ms ~ 4,800ms 구간에서 신호오류 주입공격을 수행하였다. 정상 상황에서는 측정 대상과의 거리를 약 7cm로 측정하였으나, 신호오류 주입공격 상황 동안에는 0cm로 측정하는 오류가 발생하였음을 알 수 있다.

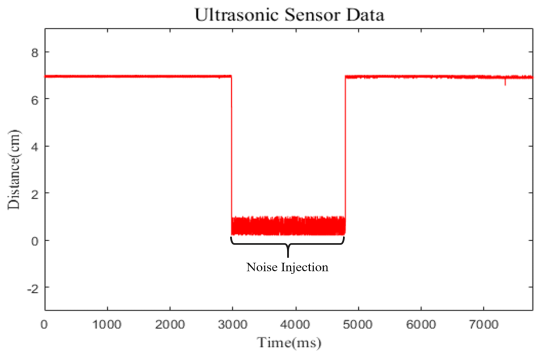

Fig. 2. Signal Spoofing Attack on HC-SR04

4.2.2 자이로스코프 센서 대상 Out-of-band 신호오류 주입공격

MEMS 방식의 자이로스코프 센서는 가청대역의 공진주파수를 가지고 있는 것으로 알려져 있다[15]. 따라서 스피커를 이용하여 MEMS 방식의 자이로스코프 센서를 대상으로 신호오류 주입공격을 수행할 수 있다. 우리는 먼저, 신호발생기를 사용하여 자이로스코프 센서의 공진주파수 대역인 27kHz의 신호를 발생시켰고, 증폭기와 스피커를 통해 음향 신호로 출력하였다. 출력되는 음향 신호는 자이로스코프 센서 쪽으로 향하여 주입되도록 하였다. "Fig.3."는 자

이로스코프 센서를 대상으로 Out-of-band 신호오류 주입공격을 수행한 결과를 보여주고 있다. 그래프의 x축은 시간을 의미하며, y축은 자이로스코프 센서의 3축에서 측정한 각속도를 의미한다. 자이로스코프 센서의 3축 신호는 각각 파랑, 검정, 빨강 색으로 표시되어 있으며, 주입한 음향 신호는 자이로스코프 센서의 z축 측정값에 영향을 미쳐 진폭에 큰 변화를 준 것을 확인할 수 있다.

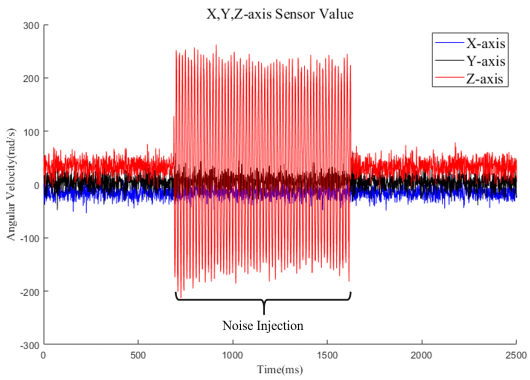

Fig. 3. Signal Injection Attack on MPU6050

V. 제안하는 기법

이번 장에서는 MEMS 방식의 자이로스코프 센서를 대상으로 하는 신호오류 주입공격 탐지 기법에 대해 제안한다. MEMS 방식의 자이로스코프 센서 대상 신호오류 주입공격을 탐지하기 위해 우리는 진동 모듈을 함께 사용한다. 진동 모듈을 이용하여 챌린지 신호를 생성하고 이를 자이로스코프 센서가 정확히 측정하였는지 여부를 바탕으로 신호오류 주입공격을 탐지한다. "Fig.4."는 우리가 제안하는 방법의 시스템 모델로써, 신호오류 주입공격을 탐지하기 위해 사용되는 마이크로컨트롤러, 진동 모듈, 자이로스코프 센서 3가지 구성요소를 보여주고 있다. 우리는 신호오류 주입공격 탐지 방법을 다음과 같이 3단계로 설명하도록 하겠다.

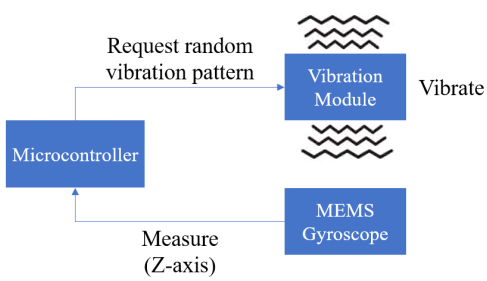

Fig. 4. System Model

5.1 신호 인코딩 및 디코딩

진동의 크기에 따라 자이로스코프 센서가 측정하는 신호의 진폭이 변화하는 사실을 이용하여, 자이로스코프 센서가 진동 모듈이 전송하는 1010 bit 시퀀스를 수신하는지 여부를 확인하고 이를 통해 신호오류 주입공격 여부를 탐지한다. 이를 위하여, ASK(Amplitude Shift Keying)를 이용하여 진동 신호를 인코딩 및 디코딩 한다. ASK를 사용하면 진폭의 존재 유무를 바탕으로 0 또는 1로 진동 신호를 표현할 수 있다. "Fig.5."는 ASK를 이용하여 1010 bit 시퀀스를 진동 신호로 인코딩하고 진동 신호를 다시 1010 bit 시퀀스로 디코딩하는 과정을 보여주고 있다. 신호오류 주입공격을 탐지하기 위해 우리가 제안하는 기법에서는 마이크로컨트롤러가 먼저 n-bit 랜덤 시퀀스를 선택하고, 이를 ASK를 이용하여 진동 모듈에 진동 신호를 발생할 것을 요청한다. 이렇게 진동 모듈에서 발생하는 진동은 자이로스코프 센서에 의하여 측정된다. 한 축에서 측정된 신호는 n-bit 랜덤 시퀀스가 인코딩된 신호를 의미한다. 그리고 마이크로컨트롤러는 요청한 진동 패턴과 자이로스코프 센서에서 측정한 진동 패턴이 일치하는지 확인하기 위해 측정값을 디코딩하여 n-bit 디지털 진동 패턴으로 복원한다.

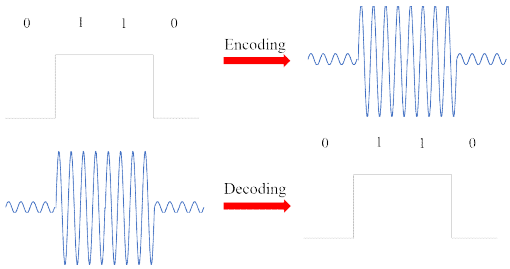

Fig. 5. ASK Encoding and Decoding

5.2 챌린지 신호 생성

우리는 마이크로컨트롤러가 요청하는 n-bit 랜덤 챌린지 신호를 4bit로 설정하였다. 따라서 0000부터 1111까지 16가지의 랜덤 시퀀스를 요청할 수 있

다. 각 bit를 표현하기 위해 4개의 타임 슬롯을 설정하였다. 각 타임 슬롯에서는 진동 발생 여부를 토대로 0 또는 1의 bit 정보를 포함하고 있으며, Bit 타임에 맞춰 진동 신호를 발생시킨다. 타임 슬롯의 Bit 타임은 80ms로 설정하였다. 진동의 특성상 잔여 진동이 다음 타임 슬롯에 영향을 끼칠 수 있기 때문에 Bit 타임을 적당한 시간으로 조정하는 것이 필요하였으며, 실험적으로 잔여 진동이 완전히 소멸하는 최소 시간을 측정하여 Bit 타임을 80ms로 설정하였다. "Fig.6."은 챌린지 진동 신호를 1010으로 요청하였을 때 자이로스코프 센서의 측정값을 보여주는 그림이다. 각 타임 슬롯에서 측정값의 평균이 임계값(threshold)을 넘지 못하는 경우 0, 임계값을 넘는 경우 1로 디코딩된다.

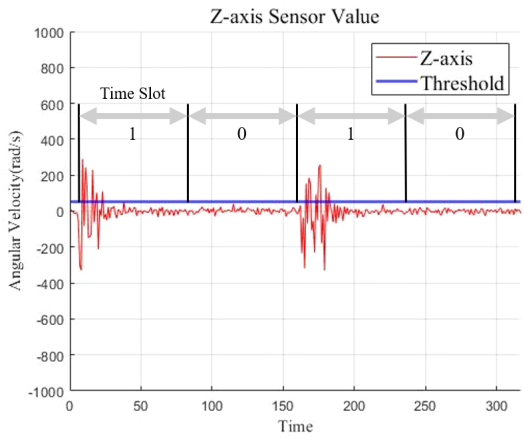

Fig. 6. '1010' Vibration Pattern

5.3 신호 측정 및 신호오류 공격 탐지

마이크로컨트롤러가 n-bit 랜덤 시퀀스 진동 패턴을 요청하면 자이로스코프 센서는 진동 모듈이 생성한 진동 신호를 측정한다. 마이크로컨트롤러는 이 측정값을 다시 ASK 기법을 이용하여 bit 시퀀스로 디코딩한다. 마이크로컨트롤러가 선택한 챌린지 진동 패턴과 자이로스코프 센서가 측정한 값을 비교하여 진동 패턴의 일치 여부를 확인하고 두 패턴이 일치하지 않는 것으로 판단되면 신호오류 주입공격이 발생하였다고 판단할 수 있다. 외부에서 자이로스코프 센서를 대상으로 신호오류 주입공격으로 인한 신호가 주입되면 센서값에 오류가 발생하여 자이로스코프 센서가 정확한 센서값을 측정하지 못하게 되고, 결과적으로 챌린지 진동 패턴과 다른 패턴으로 디코딩된다는 점을 이용하여 신호오류 주입공격을 탐지할 수 있다.

VI. 평 가

이번 장에서는 제안하는 기법의 신호오류 주입공격 탐지 정확도와 탐지 성능에 대하여 평가한다.

6.1 실험 환경

제안하는 기법을 평가하기 위한 실험 환경 구축을 위해, AC 진동 모듈과 DC 진동 모듈을 사용하였다. 진동 모듈을 제안하는 기법 상에서 마이크로컨트롤러 요청하는 n-bit 랜덤 챌린지 신호를 생성하기 위해 사용된다. 신호오류 주입공격 대상이 되는 타겟 센서는 MEMS 방식의 자이로스코프 센서인 MPU6050을 사용하였다. 신호발생기는 Keysight N9310A를 사용하였다. 마이크로컨트롤러로는 아두이노 UNO 보드를 사용하였다. 신호오류 주입을 위해 음향 신호를 스피커로 출력하여 자이로스코프 센서에 직접 주입하였다. 신호발생기를 통해 MPU6050의 공진주파수인 27kHz LF(Low Frequency) 신호를 발생시켰고, 이를 스피커로 출력하였다. 신호오류의 진폭은 1mV ~ 20mV까지 1mV씩 높여가며 실험을 진행하였다. MPU6050과 스피커는 10cm 떨어진 거리에 위치시켰으며, 진동이 발생함에 따라 움직이지 않도록 고정한 후 평가를 진행하였다. "Fig.7."은 제안하는 기법을 평가하기 위한 실험 환경을 보여주고 있다.

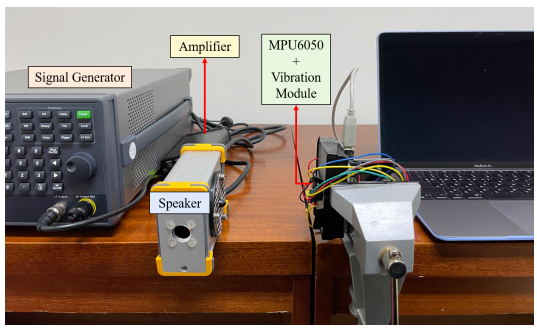

Fig. 7. Experimental Setup

6.2 정상 상황에서 False Alarm

신호오류 주입공격이 발생하지 않는 상황에서 탐지 모델은 False Alarm이 없거나 적게 발생해야 한다. 따라서 우리가 제안하는 신호오류 주입공격 탐지 방법이 정상 상황에서 False Alarm을 얼마나 발생시키는지 평가하였다. 정상 상황에서 False Alarm 발생빈도 측정을 위해 신호오류를 주입하지 않고 챌린지 진동만을 발생시켰다. 그 결과 일반적인 상황에서 자이로스코프 센서는 진동 모듈이 생성하는 챌린지 신호만을 측정할 뿐 다른 움직임은 없었다. 우리는 동일한 실험을 1,000회 반복하였으며, 모든 경우에서 마이크로컨트롤러가 생성한 진동 패턴을 정확히 디코딩하였음을 확인하였다. "Fig.8."은 정상 상황에서 False Alarm의 발생빈도를 나타내는 그래프이며, 정상 상황에서는 False Alarm이 전혀 발생하지 않았음을 알 수 있다.

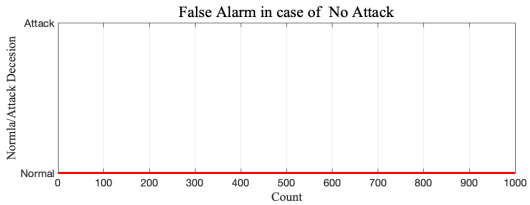

Fig. 8. False Alarm in case of No Attack

6.3 AC 진동 모듈을 사용한 신호오류 주입공격 탐지

AC 진동 모듈을 장착한 탐지 모델을 대상으로 신호오류 주입공격을 수행하고 우리가 제안하는 방법으로 신호오류 주입공격을 탐지하는 것을 보인다. AC 진동 모듈의 전원은 아두이노 UNO에서 PWM(Pulse Width Modulation)을 사용하여 공급하였다. 마이크로컨트롤러는 1010의 챌린지 진동 패턴을 2회 요청하고, 두 번째 챌린지 진동 패턴을 요청했을 때에만 신호오류를 주입하였다. 첫 번째 챌린지 진동 패턴을 요청한 시간 동안은 공격 신호를 주입하지 않는 정상 상황이며, 자이로스코프 센서에서 측정한 값이 1010으로 디코딩되어 정상 상황으로 판단하였다. 두 번째 1010 진동 패턴을 요청한 시간 동안은 진동이 발생하지 않은 타임 슬롯에서도 신호오류로 인해 1로 디코딩되었다. 따라서 요청한 진동 패턴과 일치하지 않는 진동 패턴으로 디코딩되어 마이크로컨트롤러는 이를 공격 상황으로 판단하는 결과를 보였다. "Fig.9."와 "Fig.10."은 AC 진동 모듈을 장착한 신호오류 주입공격 탐지 모델을 대상으로 각각 신호오류의 진폭이 15mV, 30mV인 신호오류 주입공격을 수행하고 우리가 제안하는 방법으로 신호오류 주입공격 탐지를 보여주는 그림이다.

신호오류의 진폭별 탐지율을 확인하기 위해 신호오류의 진폭을 1mV씩 높여가면서 신호오류 주입공격을 200회 반복 수행하였다. 200회 반복 수행한 결과를 바탕으로 신호오류 주입공격 상황을 정상 상황으로 판단하는 FNR(False Negative Rate)을 각 진폭별로 계산하였다. "Table 1."은 신호오류의 진폭을 1mV씩 높여가며 신호오류 주입공격을 수행한 결과를 나타내는 표이다. "Table 1."의 결과에서 공격 신호의 진폭이 12mV 이상인 경우 FNR이 0%로 측정되었으며, 이는 12mV 이상의 진폭을 가

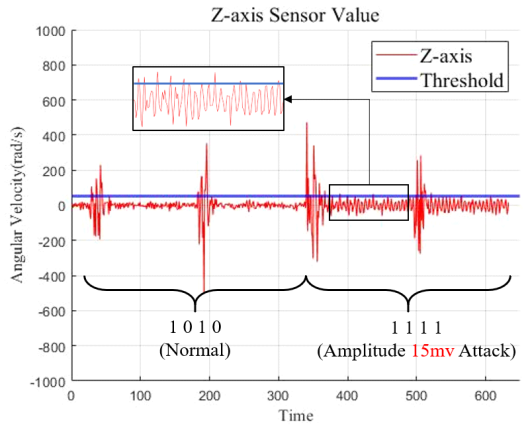

Fig. 9. 27kHz, Amplitude 15mV Attack Injection

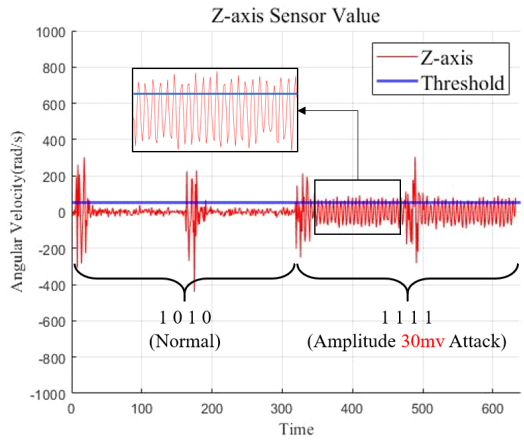

Fig. 10. 27kHz, Amplitude 30mV Attack Injection

Table 1. False Negative Rate with AC Vibration Module

Attack Signal Amplitude	Number of attacks	Attack	Normal	FNR
1mV	200	0	200	100%
2mV	200	0	200	100%
…	…	…	…	…
6mV	200	0	200	100%
7mV	200	1	199	99.5%
8mV	200	92	108	54%
9mV	200	146	54	27%
10mV	200	175	25	12.5%
11mV	200	199	1	0.5%
12mV	200	200	0	0%
13mV	200	200	0	0%

지는 신호오류 주입공격은 100% 탐지할 수 있음을 뜻한다. 미리 설정해둔 임계값을 낮출수록 FNR은 작아지는 결과를 보였지만 정상 상황을 신호오류 주입 공격 상황으로 판단하는 False Alarm은 증가하여 정상 상황에서의 탐지 모델 신뢰성이 떨어지게 된다.

6.4 DC 진동 모듈을 사용한 신호오류 주입공격 탐지

DC 진동 모듈을 사용한 탐지 모델 역시 AC 탐지 모델과 비슷한 결과를 보였다. DC 진동 모듈의 경우 진동의 세기가 더 세고 AC 진동 모듈과 달리 PWM을 사용하지 않더라도 진동 모듈에 전원을 공급할 수 있어 원하는 세기의 진동 신호를 생성하기 수월하다. AC 탐지 모델과 동일하게 신호오류의 진폭을 1mV씩 높여가며 진폭별로 200회씩 신호오류 주입공격을 수행하였다. "Table 2."는 DC 진동 모듈을 사용한 탐지 모델을 대상으로 신호오류의 진폭을 1mV씩 높여가며 신호오류 주입공격을 수행한 결과를 나타내는 표이다. "Table 2."의 결과는 공격 신호의 진폭이 11mV 이상일 때 FNR이 0%로 나타나 AC 탐지 모델에 비해 진폭이 1mV 더 작은 공격 신호도 탐지할 수 있음을 보여주고 있다. "Fig.11."은 탐지 모델의 신호오류 진폭별 탐지율을 나타내는 그래프이다. 그림에서 빨간색으로 표시되는 선은 AC 진동 모듈을 사용한 탐지 모델의 탐지율을 나타내며, 파란색으로 표시된 선은 DC 진동 모듈의 탐지율이다. 앞서 확인한 결과와 같이 공격 신호의 진폭이 12mV 이상일 때 신호오류 주입공격 상황임을 100% 탐지할 수 있었다.

Table 2. False Negative Rate with DC Vibration Module

Attack Signal Amplitude	Number of attacks	Attack	Normal	FNR
1mV	200	0	200	100%
2mV	200	0	200	100%
…	…	…	…	…
6mV	200	0	200	100%
7mV	200	4	196	98%
8mV	200	72	128	64%
9mV	200	130	70	35%
10mV	200	178	22	11%
11mV	200	200	0	0%
12mV	200	200	0	0%
13mV	200	200	0	0%

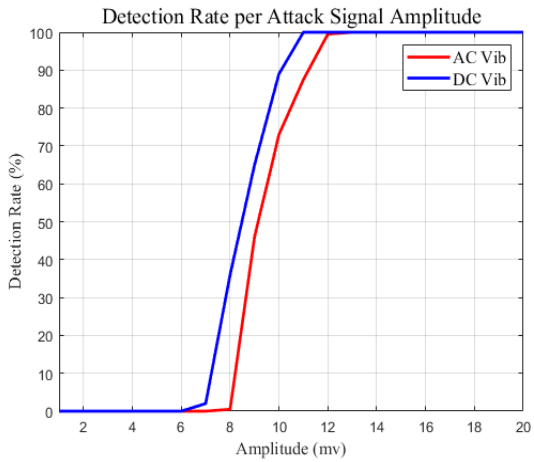

Fig. 11. Detection Rate per Attack Signal Amplitude

6.5 낮은 진폭의 신호오류 주입공격

우리가 제안하는 모델은 약 10mV 이하의 진폭을 가지는 신호오류 주입공격에 대해서는 탐지율이 떨어지는 문제가 있다. 그러나 실제로 자이로스코프 센서에 주입되는 10mV, 11mV 진폭의 공진주파수는 측정값에 유의미한 영향을 미치지 못한다는 것을 확인하는 것이 필요하였다. 우리는 실험 환경과 동일한 조건에서 5초간 10mV, 11mV 진폭을 가지는 공진주파수를 주입하였다. 정상 구간에서 자이로스코프 센서가 측정한 양(+)의 z축 각속도 값 평균은 약 11.3241rad/s이며, 신호오류가 주입되는 구간에서 양의 z축 각속도 값 평균은 약 14.1363rad/s로 측정되었다. 따라서 10mV, 11mV 진폭의 공진주파수는 자이로스코프 센서의 측정값에 약 2.8rad/s의

오류를 발생시키며, 이는 자이로스코프 센서가 탑재된 무인이동체의 오동작을 유발하기에는 어렵다는 것을 실험적으로 확인하였다. "Fig.12."와 "Fig.13."은 각각 10mV, 11mV 진폭의 신호오류를 자이로스코프 센서에 주입한 결과를 나타내는 그래프이며, 신호오류가 주입되더라도 유의미한 결과가 나타나지 않았음을 알 수 있다.

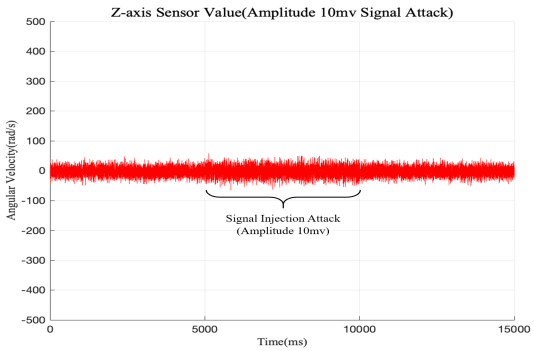

Fig. 12. 27kHz Amplitude 10mV Attack Injection

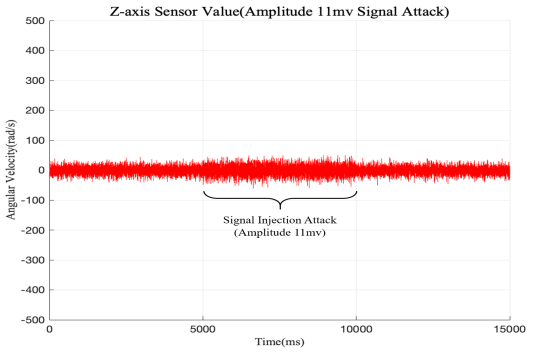

Fig. 13. 27kHz Amplitude 11mV Attack Injection

VII. 결 론

자율주행 시스템은 차량뿐만 아니라 선박 및 항공 등 다양한 분야에서 사용되고 있으며 이에 따른 보안 이슈도 함께 등장하고 있다. 본 논문에서 우리는 무인이동체 환경에서 널리 사용되고 있는 MEMS 방식의 Passive 센서를 대상으로 하는 Out-of-band 신호오류 주입공격을 탐지하는 방법에 대해 제안하였다. 두 종류의 진동 모듈을 사용한 탐지 모델을 구축하였고 이를 통해 센서가 측정하는 데이터의 신뢰성을 보장할 수 있었다. 또한, 공격 탐지에 소요되는 시간을 0.32초로 최소화하였으며, 이러한 이유로 무인이동체의 오동작을 유발할 수 있는 최소한의 시간 동안 주입되는 공격 신호 역시 탐지할 수 있을 것으로 기대된다.

References

[1] I. Giechaskiel and K. Rasmussen, "Taxonomy and Challenges of Out-of-Band Signal Injection Attacks and Defenses," IEEE Communications Surveys & Tutorials, vol. 22, no. 1, pp. 645-670, Firstquarter. 2020.

[2] Y. Shoukry, P. Martin, Y. Yona, S. Diggavi, and M. Srivastava, "PyCRA: Physical Challenge-Response Authentication For Active Sensors Under Spoofing Attacks," Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security, pp. 1004-1015, Oct. 2015.

[3] D. Davidson, H. Wu, and R. Jellinek, "Controlling UAVs with Sensor Input Spoofing Attacks," 10th {USENIX} Workshop on Offensive Technologies ({WOOT} 16), Aug. 2016.

[4] T. Chen, L. Shangguan, Z. Li, and K. Jamieson, "Metamorph: Injecting inaudible commands into over-the-air voice controlled systems," Proceedings of NDSS, Feb. 2020.

[5] H. Shin, D. Kim, Y. Kwon, and Y. Kim, "Illusion and Dazzle: Adversarial Optical Channel Exploits Against Lidars for Automotive Applications," In International Conference on Cryptographic Hardware and Embedded Systems, vol. 10529, pp. 445-467, 2017.

[6] C. Yan, W. Xu, and J. Liu, "Can you trust autonomous vehicles: Contactless attacks against sensors of self-driving vehicle," DEFCON, 2016.

[7] Y. Son, H. Shin, D. Kim, Y. Park, J.

Noh, K. Choi, J. Choi, and Y. Kim, "Rocking Drones with Intentional Sound Noise on Gyroscopic Sensors," In 24th {USENIX} Security Symposium, pp. 881-896, Aug. 2015.

[8] T. Trippel, O. Weisse, W. Xu, P. Honeyman, and K. Fu, "WALNUT: Waging doubt on the integrity of MEMS accelerometers with acoustic injection attacks," IEEE European Symposium on Security and Privacy (EuroS&P), pp. 3-18, April. 2017.

[9] Y. Tu, Z. Lin, I. Lee, and X. Hei, "Injected and Delivered: Fabricating Implicit Control over Actuation Systems by Spoofing Inertial Sensors," In 27th {USENIX} Security Symposium, pp. 1545-1562, Aug. 2018.

[10] J. Selvaraj, G.Y. Dayanıklı, N.P. Gaunkar, D. Ware, R.M. Gerdes, and M. Mina, "Electromagnetic Induction Attacks Against Embedded Systems," Proceedings of the 2018 on Asia Conference on Computer and Communications Security, pp. 499-510, May. 2018.

[11] Y. Tu, S. Rampazzi, B. Hao, A. Rodriguez, and K. Fu, "Trick or Heat?: Manipulating Critical Temperature-Based Control Systems Using Rectification Attacks," Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security, pp. 2301-2315, Nov. 2019.

[12] Google "MPU-6000 and MPU-6050 Product Specification Revision 3.4," https://invensense.tdk.com/wp-content/uploads/2015/02/MPU-6000-Datasheet1.pdf, May. 2021.

[13] Google "HC-SR04 module Datasheet," https://cdn.sparkfun.com/datasheets/Sensors/Proximity/HCSR04.pdf, May. 2021.

[14] R.E. Blake, "Basic Vibration Theory," Shock and Vibration Handbook, New York, NY, USA:McGraw Hill, 1988.

[15] R.N. Dean, G.T. Flowers, A.S. Hodel, G. Roth, S. Castro, R. Zhou, A. Moreira, A. Ahmed, R. Rifki, B.E. Grantham, D. Bittle, and J. Brunsch, "On the degradation of MEMS gyroscope performance in the presence of high power acoustic noise," IEEE International Symposium on Industrial Electronics, pp. 1435-1440, Jun. 2017.

[16] Y. Ashibani and Q.H. Mahmoud, "Cyber physical systems security: Analysis, challenges and solutions," Computers & Security, vol. 68, pp. 81-97, July. 2017.

〈저자소개〉

조 현 수 (Hyunsu Cho) 학생회원
2020년 8월: 고려대학교 전자및정보공학과 졸업
2020년 9월~현재: 고려대학교 정보보호대학원 정보보호학과 석사과정
〈관심분야〉 정보보호, 전자공학, 센서 보안

오 희 석 (Heeseok Oh) 정회원
2017년: 연세대학교 전기전자공학과 박사 졸업
2017년~2017년: 삼성전자 DMC연구소 책임연구원
2017년~2020년: 한국전자통신연구원 선임연구원
2020년~현재: 한성대학교 IT융합공학부 조교수
〈관심분야〉 영상처리, 컴퓨터비전, 혼합현실, 심층생성모델

최 원 석 (Wonsuk Choi) 종신회원
2008년 2월: 서울시립대 수학과 졸업
2013년 2월: 고려대학교 정보보호대학원 석사 졸업
2018년 8월: 고려대학교 정보보호대학원 박사졸업
2018년 9월~2020년 2월: 고려대학교 정보보호연구원 연구교수
2020년 3월~현재: 한성대학교 IT융합공학부 조교수
〈관심분야〉 센서 보안, 자동차 보안, 암호 프로토콜