정 보 보 호 학 회 지
제 31 권 제1호, 2021. 2

MEMS 센서대상 오류주입 공격 및 대응방법

조 현 수*, 이 선 우*, 최 원 석**

요 약

자율주행 시스템이 탑재되어 있는 무인이동체는 운용환경에 따라 공중, 해상, 육상 무인이동체로 분류할 수 있고 모든 분야에서 관련 기술 개발이 활발히 진행되고 있다. 무인이동체는 자율주행 시스템이 탑재되어 외부 환경을 스스로 인식해 상황을 판단하는 특징을 갖고 있다. 따라서, 무인이동체는 센서로부터 수집되는 데이터를 이용하여 주변 환경을 인식해야 한다. 이러한 이유로 보안 (Security) 분야에서는 무인이동체에 탑재되는 센서를 대상으로 신호 오류주입을 수행하여 해당 무인이동체의 오동작을 유발하는 연구결과들이 최근 발표되고 있다. 신호 오류주입공격은 물리레벨 (PHY-level) 에서 수행되기 때문에, 공격 수행 여부를 소프트웨어 레벨에서 탐지하는 것은 매우 어렵다는 특징을 갖고 있다. 현재까지 신호 오류주입 공격을 탐지할 수 있는 방법은 다수의 센서를 이용하는 센서퓨전 (Sensor Fusion)을 기반으로 하는 방법이 있다. 하지만, 현실적으로 하나의 무인이동체에 동일한 기능을 하는 센서 여러 개를 중복해서 탑재하는 것은 어려움이 있다. 그리고 단일 센서만을 이용하여 신호 오류주입 공격을 탐지하는 방법에 대해서는 아직까지 연구가 진행되고 있지 않다. 본 논문에서는 무인이동체 환경에서 가장 널리 사용되고 있는 MEMS 센서를 대상으로 신호 오류주입 공격을 재연하고, 단일 센서 환경에서 해당 공격을 탐지할 수 있는 방법에 대하여 제안한다.

Ⅰ. 서 론

인공지능 (AI) 기술의 발달로 인해 스스로 인지하고 판단하여 동작하는 자율시스템이 탑재된 무인이동체가 등장하고 있다. 무인이동체는 외부 환경을 인식해 스스로 상황을 판단하여 이동하고, 필요한 작업을 수행하는 이동체로 정의된다. 무인이동체는 운용환경에 따라 공중, 해상, 육상무인이동체로 분류할 수 있다. 이러한 무인이동체는 상황판단을 위한 인공지능 기술뿐만 아니라, 주변 환경을 인지하기 위해 센서 기술이 필수적으로 요구된다. 예를 들어, 3축 자이로스코프 (3-aixs Gyroscope) 센서를 이용하여, 비행하고 있는 드론의 자세를 판단하고 유지할 수 있도록 한다. 하지만, 최근 센서를 대상으로 신호 오류주입 공격이 등장하였고, 이러한 공격은 결과적으로 무인이동체의 오동작을 유도한다 [1,2,3,4]. 이러한 센서를 대상으로 하는 오류주입 공격은 무인이동체의 핵심 공통기술 중 하나인 탐지 및 인식 과정에서 치명적인 오류를 발생시킬 수 있으며, 이로 인해 인명 피해나 경제적 피해가 발생할 수 있다. 실제로 Son et al. 연구팀은 자이로스코프가 탑재되어 있는 드론을 대상으로 의도적인 음향 노이즈를 생성 및 주입하여 해당 드론을 오동작 하는 연구 결과를 발표하였다 [1].

본 논문에서는 인공지능 시스템이 탑재되어 있는 무인이동체들 중 가장 널리 사용되고 있는 미세전자기계시스템 (Microelectromechanical systems, MEMS) 방식의 센서를 대상으로 오류주입 공격을 재연하고 이에 대한 대응방법을 제안하고 평가결과를 보여준다. 단일 센서 환경에서는 초음파 센서와 같이 Challenge-Response 구조로 동작하는 센서에서만 신호오류주입 공격 탐지가 가능한 방법만이 제안되었고, Challenge-Response 구조가 아닌 MEMS 센서 환경에서 신호주입 공격을 탐지하는 방법은 아직까지 연구되지 않았다. 또한, 우리는 본 논문에서 실험실 환경에서 신호오류주입 공격을 재연하고 제안하는 방법을 평가한다.

Ⅱ. 관련연구

이번 장에서는 센서를 대상으로 하는 신호 오류주입 공격과 그에 대한 대응 방법과 관련하여 수행된 연구

본 연구는 2020년도 정부(과학기술정보통신부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구임(NRF-2020R1C1C1007446)
* 고려대학교 정보보호대학원 (대학원생, jhsuper@korea.ac.kr; 대학원생, lswoo92@gmail.com)
** 한성대학교 IT융합공학부 (교수, wonsuk@hansung.ac.kr)

내용에 대하여 설명하도록 하겠다.

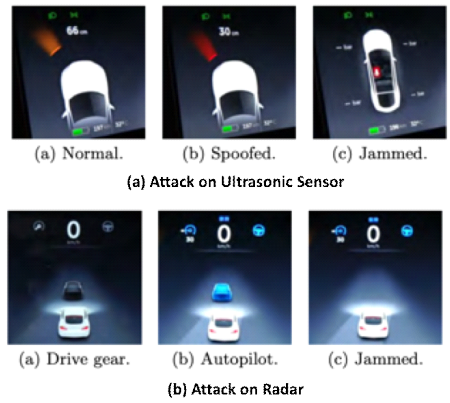
2.1. 센서 대상 신호 오류주입 공격

자동차에 탑재된 센서에 악성 오류를 주입하여 정상적으로 센서가 작동하지 못하게 하는 연구가 수행되어 왔다. Petit et al. 연구팀은 자동차에 탑재된 카메라 센서에 레이저를 주입하여 블라인드 공격을 수행하기 위하여 LiDAR 센서에 재밍, 리플레이, 릴레이 및 스푸핑 공격을 수행하였다 [6]. Shin et al. 연구팀은 LiDAR 센서에 대해 악성 신호를 주입함으로써 착시 현상을 유발하거나 물체의 실제 위치보다 더 가깝게 보이도록 하는 스푸핑 공격을 수행하였으며 [8], Cao et al. 연구팀 또한 LiDAR 센서에 대해 악의적인 신호를 주입함으로써 물체 인식 알고리즘을 스푸핑하는 공격을 수행하였다 [9]. Yan et al. 연구팀은 자동차에 탑재된 초음파 센서, 레이더 (Radar) 센서 및 카메라 센서에 대해 신호 오류주입공격을 수행하였다 [7]. [그림 1]은 각각 초음파 센서 및 레이더 센서에 악의적인 신호를 주입하여 실제로 차량 주변에 있는 장애물의 거리를 제대로 판단하지 못하는 결과를 보여주고 있다.

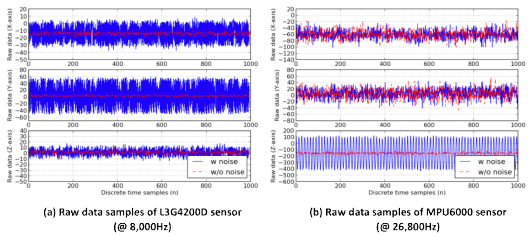
카메라 센서에 대한 신호 오류주입공격은 Petit et al. 연구팀 [6]과 Chen et al. 연구팀 [7]과 같이 단순히 레이저를 주입하는 것이 아닌, 카메라가 촬영하는 물체를 조작함으로써 물체를 잘못 인식하게 하는 연구가 수행되어왔다. Davidson et al. 연구팀은 드론에 탑재된 카메라 센서를 대상으로 신호 오류주입공격을 수행하였다 [4]. 프로젝터를 사용하여 악성 이미지를 지면에 비추거나 레이저를 이용하여 특정 격자 패턴을 지면에 비춤으로써 카메라 센서가 정상적인 물체 인식을 하지 못하도록 공격을 수행하였다.

최근에는 MEMS 센서의 공진주파수와 일치하는 주파수를 가진 음향 신호를 센서에 주입함으로써 센서가 정상적인 작동을 하지 못하도록 하는 공격이 연구되어 왔다. 공명은 특정 주파수에서 큰 진폭으로 진동하는 현상을 말하며, 이때 특정 주파수를 공명주파수라고 한다. 공명주파수에서는 작은 힘의 작용에도 큰 진폭 및 에너지를 전달할 수 있으므로 이러한 신호 오류주입공격을 수행할 경우 센서의 정상 작동을 방해 할 수 있다. Son et al. 연구팀은 20개의 MEMS Gyroscope 센서의 공진주파수를 분석하고 해당 주파수를 가지는 음향신호를 주입함으로써 신호 오류주입공격을 수행하였다 [1]. [그림 2]는 Gyroscope 센서인 L3G4200D와 MPU6050에 각각 8,000Hz 및 26,800Hz의 주파수인 가청대역의 신호를 주입한 후의 센서 값을 나타낸다. 신호 오류주입공격에 대해 L3G4200D 센서는 X,Y축이 영향을 받았으며, MPU6050 센서는 Z축만 영향을 받은 것을 알 수 있다. 또한 실제 L3G4200D를 탑재한 드론은 신호 오류주입공격을 수행한 결과 추락하였다.

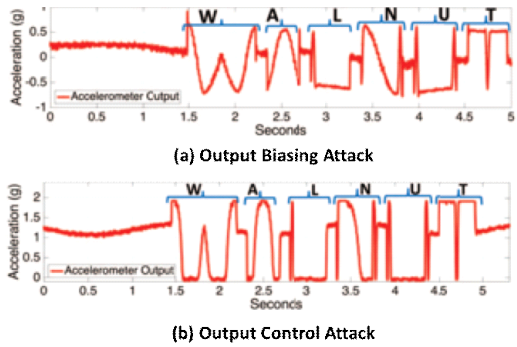
Trippel et al. 연구팀은 20개의 MEMS



〔그림 1〕 신호 오류주입공격 결과 〔7〕



〔그림 2〕 MEMS 센서에 대한 신호 오류주입공격 결과 〔1〕



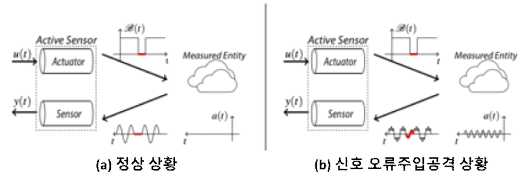
〔그림 3〕 MEMD Accelerometer 센서에 대한 신호 오류주입공격 결과 〔2〕

Accelerometer 센서의 공진주파수를 분석하고 회로상의 결함을 이용하여 두 가지의 신호 오류주입공격을 수행하였다 [2]. 출력 바이어스 공격은 센서의 ADC의 샘플링 결함을 이용한 공격이며, 출력 제어 공격은 센서의 안전하지 않은 증폭기를 이용한 공격이다. [그림 3]은 센서에 출력 바이어스 공격 및 출력 제어 공격을 수행하여 센서 값을 “WALNUT”으로 스푸핑한 결과를 보여주고 있다. 또한 스마트폰 스피커에서 악성 음향신호를 재생함으로써 온보드 MEMS Accelerometer 센서를 제어하여 RC 자동차를 악의적으로 조종하였다.

2.2. 센서 대상 신호 오류주입 공격에 대한 대응 방법

최근 센서 신호의 Challenge-response 방식을 이용하여 신호 오류주입 공격에 대한 대응방법이 연구되어 왔다. Shoukry et al. 연구진은 PyCRA라는 신호 오류주입공격에 대한 탐지 알고리즘을 제안하였다 [5]. PyCRA는 랜덤으로 프로브 신호(i.e., Challenge)를 전송하고 이에 대한 응답 신호(i.e., Response)를 검증함으로써 공격 여부를 탐지한다. [그림 4]는 정상 및 공격상황에서의 PyCRA의 탐지 매커니즘을 나타낸다. [그림 4]-(a)와 같이 정상 상황인 경우, 랜덤으로 특정 구간에 센서의 신호를 전송하지 않도록 하였을 때 이에 대한 반응 신호 또한 해당 특정 구간에서 아무런 신호가 탐지가 되지 않는다. 이에 반해 신호 오류주입 공격이 발생하는 경우, [그림 4]-(b)와 같이 응답 신호의 특정 구간에서 신호가 발생한 것을 알 수 있으며, 이를 통해 공격을 탐지할 수 있다.

또한 Challenge-response 방법을 기반으로 초음파 센서에 대한 신호 오류주입 공격을 탐지하는 연구도 되어왔다. Lee et al. 연구진은 단일 초음파 센서에서 송수신되는 신호의 관계를 기반으로 랜덤 초음파 신호(i.e., Challenge)를 전송하고 이에 대한 에코 응답신호를 (i.e., Response)를 검증함으로써 공격을 탐지한다 [10]. 이외에도 MEMS 센서를 대상으로한 신호 오류주입 공격에 대한 대응 방법으로 물리적 차폐, 추가 센서 도입, 센서의 설계 보완 [1]을 하거나, 랜덤 샘플링 방법 등을 제시하였다 [2].

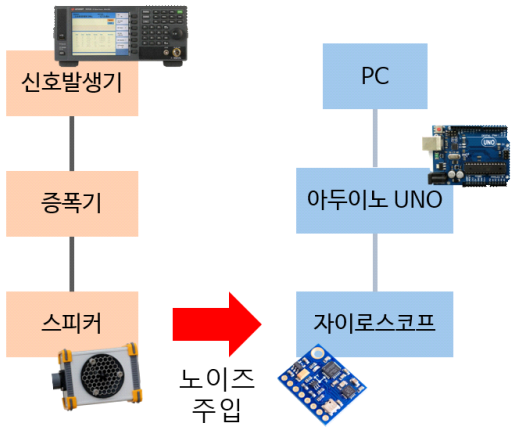


〔그림 4〕 PyCRA의 공격탐지 매커니즘 〔5〕

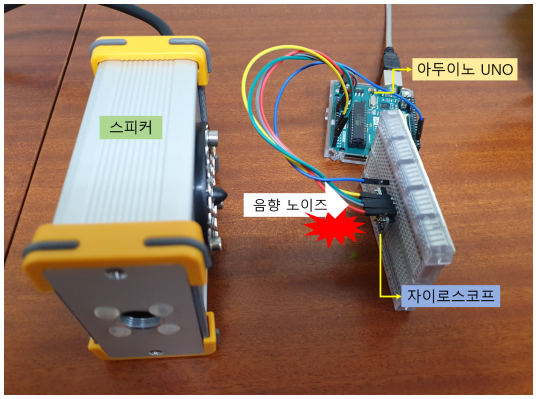
Ⅲ. 오류주입 공격

미세전자기계시스템 방식의 MEMS 센서는 특정 운동량을 측정하여 해당 값 만큼 전기신호로 변화하게 된다. 이렇게 만들어진 MEMS는 마이크로미터 수준의 크기에서 과거 기계방식의 센서와 같은 구동 방식을 제공함으로써 다양한 애플리케이션 분야에서 새로운 기능과 역할을 해 내고 있다. 하지만, MEMS 방식의 센서는 음향신호에 매우 민감하게 반응하여 노이즈 생겨나는 문제점을 갖고 있다고 알려져 있다. 따라서, 공격자가 의도적으로 음향 주파수 대역의 신호를 MEMS 센서에 주입을 하게되면 해당 센서는 잘못된 운동량을 측정하게 되고 결과적으로 센서가 탑재되어 있는 애플리케이션이 영향을 받게 된다.

우리는 본 논문에서 MEMS 방식의 3축 자이스코프(Gyroscope) 센서인 MPU6060을 대상으로 신호 오류주입 공격을 재연한다. [그림 6]은 신호 오류주입 공격을 위한 신호발생기 및 스피커를 포함한 실험 환경을 보여주고 있다. 가장 먼저, 우리는 타겟 센서의 공진주파수 (Reasont Frequency)를 찾기 위해 신호발생기를 이용하여 가청 대역과 초음파 대역의 신호를 주입해 보았다. 결과적으로 타겟 센서는 주파수 27kHz와 진폭 500mV의 LF (Low Frequency) 대역의 신호를 발생시켰을 때, 오동작을 하는 것을 찾아내었다. [그림 5]는 신호발생기와 스피커를 이용하여 앞서 설명한 주

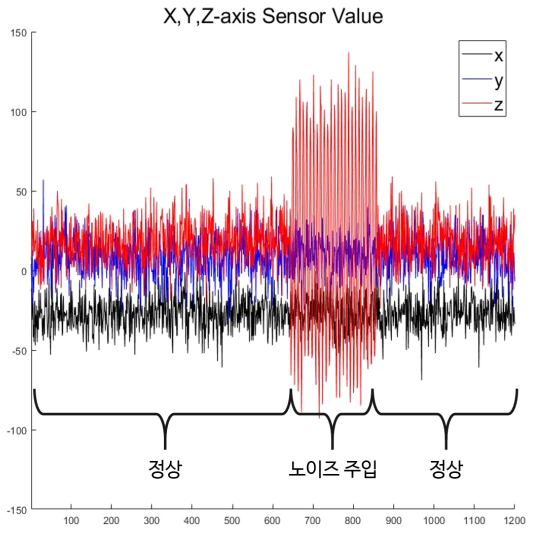


〔그림 5〕 타겟 센서 대상 오류주입 공격 절차



〔그림 6〕 타겟 센서 대상 오류주입 공격 모습

파수와 진폭의 신호를 타겟 센서에 오류를 주입하는 일련의 과정을 보여주고 있다. [그림 6]은 스피커를 이용하여 타겟 센서에 실제 오류를 주입하는 모습을 보여주고 있다. 우리는 타겟 센서를 아두이노 보드에 연결 하였고, 아두이노 보드를 다시 PC에 연결하였다. 그리고 아두이노 스케치를 이용하여 아두이노 보드에서 타겟 센서의 3축 신호를 실시간으로 읽어오는 프로그램을 작성하였다. [그림 7]은 우리가 작성한 프로그램을 이용하여 자이로스코프인 타겟 센서로부터 3축 신호를 읽은 결과를 보여주고 있다. 타겟 센서의 Z축 신호를 빨간색으로 나타내고 있으며, 실제로 우리가 오류를 주입하였을 때 빨간색 신호 값이 심하게 움직이

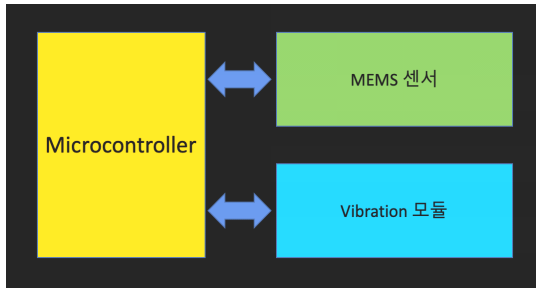


〔그림 7〕 오류주입을 수행하였을 때, 타겟 센서의 3축 신호 값

는 것을 확인할 수 있다. 또한, 우리가 오류주입을 멈췄을 때 다시 정상적인 신호 값을 보여주고 있다. 반면에 검정색, 파란색 선으로 각각 표시되는 X, Y축 센서 값에는 우리가 오류주입을 수행하였을 때 신호 값의 변화가 없음을 확인하였따. 이는 각 축별로 공진 주파수가 다르기 때문에, 우리가 찾은 27kHz 대역의 주파수는 타겟 센서의 Z축의 공진 주파수를 의미하기 때문이다. 마지막으로, 우리는 신호의 세기를 달리하여 오류주입을 수행하였다. 예상대로 신호의 세기가 클수록 타겟 센서의 신호 값이 크게 달라지는 것을 확인하였다.

Ⅳ. 오류주입 공격 탐지 방법

이번 장에서는 MEMS 센서를 대상으로 하는 오류주입 공격을 탐지하기 위한 방법을 설명한다. 우리는 오류주입 공격을 탐지하기 위한 방법으로 진동모듈을 사용한다. [그림 8]은 진동모듈을 포함하여 우리가 제안하는 방법의 시스템 모델을 보여주고 있다. 마이크로컨트롤러에서 특정 세기 또는 특정 주파수로 진동모듈에게 진동을 요청하고, 이 때 마이크로컨트롤러는 MEMS 센서가 측정할 값을 예측한다. 그리고 MEMS 센서가 실제로 측정한 값과 마이크로컨트롤러가 예측한 값의 유사도를 계산하여 기준보다 유사도가 낮은 경우 오류주입 공격으로 판단한다. 우리가 제안하는 오류주입 공격 탐지 방법에 대하여 자세히 설명하기 위하여, 3단계로 구분하여 설명하도록 하겠다.



〔그림 8〕 시스템 모델

4.1. 진동 요청 및 신호 예측

마이크로컨트롤러는 1에서 n까지의 값으로 다른 세기 또는 주파수 진동을 요청 할 수 있다. 따라서, 1부터 n까지의 숫자 중 하나를 랜덤하게 선택하여 진동모

듈에게 진동 발생을 요청한다. 그리고 마이크로컨트롤러는 MEMS 센서가 측정하게 될 신호를 미리 예측한다. 측정되는 신호를 예측하기 위해서 오류주입 공격이 없는 정상상황에서 각 세기별 진동에 대하여 사전에 여러 번 측정하여 평균 값으로 학습을 해둔다.

4.2. 진동 생성 및 신호 측정

마이크로컨트롤러로부터 진동 생성 요청을 받은 진동 모듈은 진동을 생성한다. 이 때, 마이크로컨트롤러가 1부터 n까지의 숫자 중 하나의 값을 랜덤하게 선택하여 요청하기 때문에 그 숫자에 맞는 진동 세기와 진동 주파수로 진동을 생성한다. 마이크로컨트롤러는 이 때 MEMS 센서에게 동작을 요청하여 MEMS 센서가 진동모듈이 생성하는 진동을 측정한다.

4.3. 유사도 비교 및 공격 탐지

마이크로컨트롤러가 예측하는 진동신호를 $X=(x_0,x_1,...,x_n)$라 하고 MEMS 센서가 실제로 측정한 진동신호를 $Y=(y_0,y_1,...,y_n)$라고 하였을 때, 마이크로컨트롤러가 두 신호의 유사도 d를 계산하기 위하여, 교차상관 관계 (Cross Correlation)을 이용한다. 교차상관 관계의 경우 시간 축에 대하여 정렬되지 않은 두 신호의 유사도를 계산하는데 효과적이다. 교차상관 관계를 이용하여 두 신호의 유사도를 계산하는 방법은 아래 수식과 같다.

$$XCorr_{X,Y}[l] = \sum_{m=0}^{n-1}(x_m \bullet y_{m-l}) \quad (1)$$

여기서, $l \in [0, n-1]$을 의미한다. 또한, 이렇게 계산된 교차상관 관계를 다음과 같이 정규화 (Normalization) 한다.

$$XCorr'_{X,Y}[l] = \frac{XCorr_{X,Y}[l]}{\sqrt{XCorr_{X,X}[0] \bullet XCorr_{Y,Y}[0]}} \quad (2)$$

여기서, $XCorr_{X,X}[0]$는 자기상관 관계 (Autocorrelation)을 의미한다. 마지막으로 교차상관 관계를 이용한 두 신호의 유사도는 아래 식과 같이 계산한다.

$$d = \arg\max_{l}(|XCorr'_{X,Y}[l]|) \quad (3)$$

두 신호의 유사도 계산 결과 값인 d가 임계값 (threshold)를 넘지 못하는 경우 두 신호는 유사하지 않게 되는 것이고 두 신호가 유사하지 않은 이유로 오류주입 공격으로 간주한다. 따라서, 임계값을 넘지 못하는 경우에는 오류주입 공격이 수행되고 있다고 판단한다.

Ⅴ. 실험 및 평가

5.1. 실험환경

우리는 제안하는 오류주입 공격 탐지 방법을 평가하기 위하여, [그림 9]와 같이 신호발생기를 포함한 실험환경을 구축하였다. MEMS 방식의 타겟 센서는 아두이노 보드와 연결을 하여 동작시켰으며, 아두이노 보드는 PC와의 시리얼 통신을 이용하여 조작하였다. [표 1]은 우리의 실험환경에서 사용된 각 구성요소에 대한

〔표 1〕 실험환경을 위한 구성요소

장비	용도
신호발생기 (Keysight N9310A)	공격에 적합한 주파수와 진폭을 가진 신호를 생성
진동 모듈 (ELB060416)	타겟 센서에 임의의 크기의 진동을 가하여 Challenge - Response 방식의 탐지 모델 구현
MEMS 자이스코프 센서 (MPU6050)	타겟 센서
스피커 (Avisoft Bioacoustics Ultrasonic Speaker Vifa)	공격 음향 신호를 출력
증폭기 (Avisoft Bioacoustics Portable Ultrasonic Power Amplifier)	생성된 LF 신호의 진폭을 조절하여 스피커에 입력

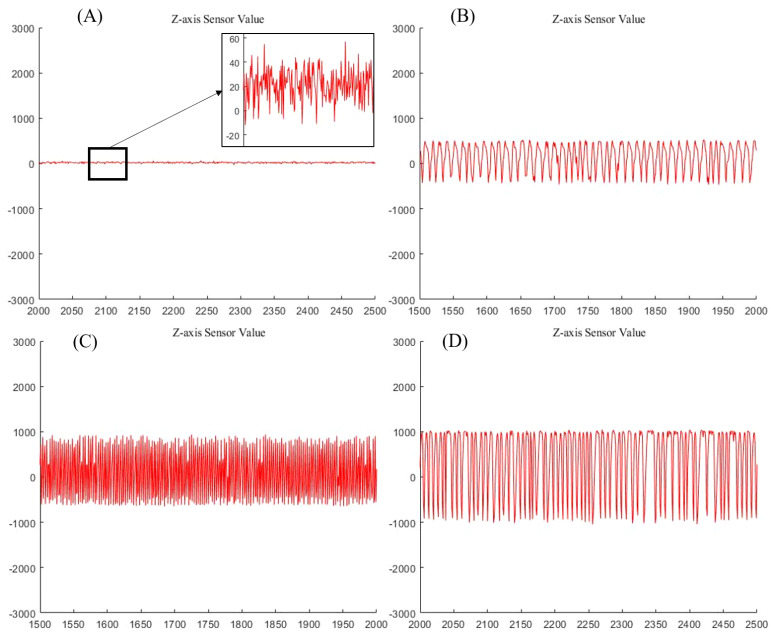
〔그림 9〕 실험 환경

자세한 설명을 보여주고 있다. 그리고 우리가 3장에서 재연한 오류주입 공격에서는 타겟 센서의 Z축에만 오류를 주입할 수 있었고, 나머지 X,Y축에는 오류를 주입하지 못하였다. 이는 각 축의 공진주파수가 서로 다르기 때문이었다. 우리는 이번 장에서 타겟센서의 Z축을 대상으로만 실험 및 평가를 진행한다.

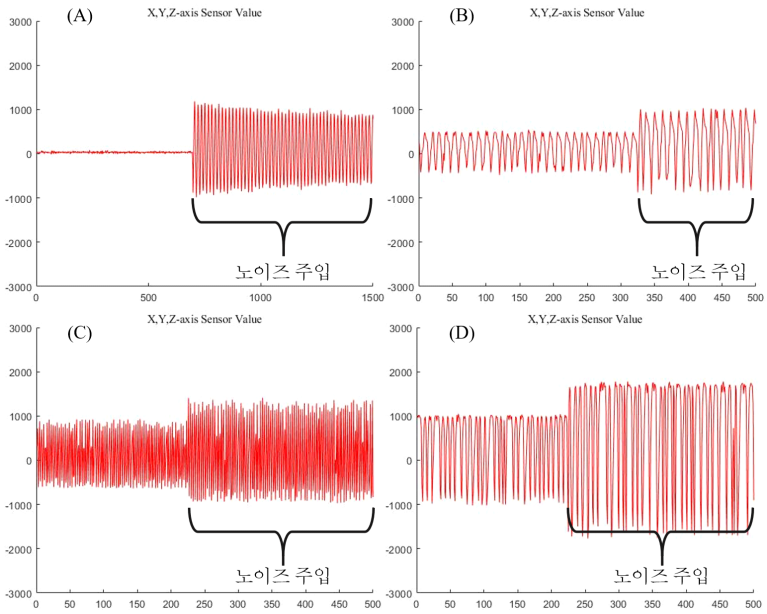
5.2. 센서 데이터 학습

우리가 제안하는 신호 오류주입 공격 탐지 방법은 진동 세기별 자이로스코프가 탐지하는 신호 값을 예측하기 위해, 이를 사전에 학습해 두어야 한다. 우리 실험환경에서 아두이노 보드와 진동모듈을 활용하여 진동세기를 0~255까지로 설정할 수 있다. 따라서, 우리는 각 진동 세기별로 자이로스코프가 측정하는 신호 값을 사전에 학습해두기 위해 각 세기별로 진동을 100번 발생하였고, 이 때 자이스코프 센서로부터 측정되는 신호 값을 측정하였다. 100개의 신호에 대한 평균 값을 계산 하기 위하여, 우리는 가장 먼저 교차 상관관계 수의 값이 최대가 될 때 래그 (lag) 값을 이용하여 각 신호를 정렬 (Alignment)하였다. 그리고 100개의 신호 값의 평균 값을 계산하여 이를 학습된 결과 즉, 각 진동 세기별 예측 신호 값으로 사용한다.

[그림 10]은 진동세기를 각기 달리 하였을 때 자이로스코프 센서의 측정값도 달라지는 모습을 보여주고 있다. 우리는 이러한 사실을 활용하여 진동 세기 값을 랜덤으로 선택하여 실제로 자이로스코프 센서가 오류주입 공격과 진동 모듈이 생성한 진동을 구분할 수 있는지 평가할 것이다.



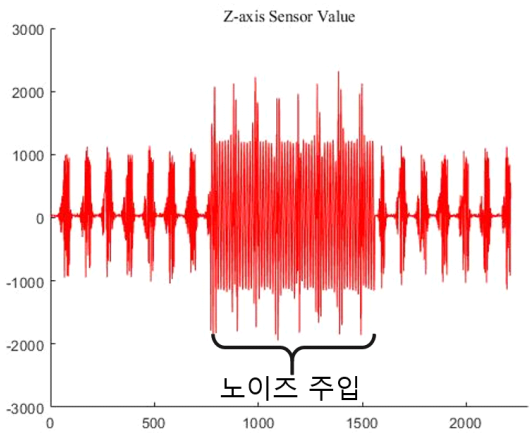
〔그림 10〕 (A) 진동 세기가 0일 때, (B) 진동 세기가 70일 때, (C) 진동 세기가 80일 때, (D) 진동 세기가 100일 때, 타겟 센서의 3축 신호 값



〔그림 11〕 (A) 진동 세기가 0일 때, (B) 진동 세기가 70일 때, (C) 진동 세기가 80일 때, (D) 진동 세기가 100일 때, 오류주입 공격을 수행한 타겟 센서의 신호 값

5.3. 오류주입 공격 탐지

오류주입공격 탐지를 위하여, 우리는 앞서 설명한 것처럼 진동 세기를 랜덤하게 선택하고 해당 세기로 진동 생성을 하였다. 이 때, 다시 신호 오류주입 공격을 수행하였다. [그림 11]은 랜덤하게 선택된 진동세기로 진동을 생성하고 오류주입 공격을 수행하였을 때, 자이로스코프 센서가 측정한 신호 값을 보여주고 있다. 오류주입 공격이 수행되지 않았던 [그림 10]과 비교하여, 오류주입 공격이 수행되었을 때 확연하게 신호의 값이 커지는 것을 알 수 있다. 이처럼, 우리가 예상하는 자이로스코프 센서의 신호 값과 다른 신호가 측정되는 경우 이를 오류주입 공격으로 탐지하게 된다. 실제로 이렇게 오류주입 공격이 수행된 신호와 우리가 예상하는 신호의 교차상관 관계를 계산해보면 뚜렷한 차이가 있음을 알 수 있다.



〔그림 12〕 진동세기를 변화하면서 오류주입 공격 타임

마지막으로, 우리는 랜덤하게 선택되는 진동 세기를 공격자가 예상하여 오류 주입의 세기 또한 알맞게 조절하는 공격자를 고려하였다. 우리의 실험 환경에서는 오류주입을 할 때 신호의 세기를 조절할 수는 없지만, 신호세기를 조절할 수 있는 공격자가 고려될 필요가 있다고 생각하였다. 이러한 경우에는 [그림 12]와 같이 진동 모듈에 생성되는 진동의 세기를 동적으로 변경하도록 요청하였다. 이러한 경우에는 신호의 세기를 조절할 수 있는 공격자라 할지라도 동적으로 신호세기가 변경되는 진동을 모두 유추할 수 없기 때문에 우리의 오류주입 공격 탐지 방법을 우회할 수 없다.

Ⅵ. 결 론

본 고에서 우리는 MEMS 센서를 대상으로 하는 신호 오류주입 공격과 이를 탐지할 수 있는 방법에 대하

여 알아보았다. 무인이동체와 같이 다수의 센서를 이용한 자율주행 시스템이 계속해서 개발되고 있기 때문에, 이에 따른 보안 이슈가 함께 등장하고 있다. 특히, PHY 레벨에서 수행되는 신호 오류주입 공격은 기존 소프트웨어 기반의 보안기법으로는 적절한 대응이 어렵다는 문제점이 있다. 본 고를 통하여 우리는 신호 오류주입 공격에 대한 지속적인 연구가 가능한 환경구축을 완료하였고, 기초적인 탐지 알고리즘에 대하여 제안 및 평가를 진행하였다. 향후 탐지 알고리즘 개선을 위한 추가 연구를 진행하여 신호 오류주입 공격을 보다 완벽하게 탐지할 수 있도록 할 계획이다.

참 고 문 헌

[1] Son, Yunmok, et al. "Rocking drones with intentional sound noise on gyroscopic sensors." 24th {USENIX} Security Symposium ({USENIX} Security 15). 2015.

[2] Trippel, Timothy, et al. "WALNUT: Waging doubt on the integrity of MEMS accelerometers with acoustic injection attacks." 2017 IEEE European symposium on security and privacy (EuroS&P). IEEE, 2017.

[3] Roy, Nirupam, et al. "Inaudible voice commands: The long-range attack and defense." 15th {USENIX} Symposium on Networked Systems Design and Implementation ({NSDI} 18). 2018.

[4] Davidson, Drew, et al. "Controlling UAVs with sensor input spoofing attacks." 10th {USENIX} Workshop on Offensive Technologies ({WOOT} 16). 2016.

[5] Shoukry, Yasser, et al. "Pycra: Physical challenge-response authentication foractive sensors under spoofing attacks." Proceedings of the 22nd ACMSIGSAC Conference on Computer and Communications Security. 2015.

[6] Petit, Jonathan, et al. "Remote attacks on automated vehicles sensors: Experiments on camera and lidar." Black Hat Europe 11 (2015):2015.

[7] Chen Yan et.al, “Can You Trust Autonomous Vehicles: Contactless Attacks against Sensorsof Self-driving Vehicle”, DEF CON 2016

[8] Shin, Hocheol, et al. "Illusion and dazzle: Adversarial optical channel exploits against lidars for automotive applications." International Conference on Cryptographic Hardware and Embedded Systems. Springer, Cham, 2017

[9] 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. 2019.

[10] Lee, Sunwoo, Wonsuk Choi, and Dong Hoon Lee. "Securing Ultrasonic Sensors Against Signal Injection Attacks Based on a Mathematical Model." IEEE Access 7 (2019): 107716-107729.

〈저 자 소 개〉

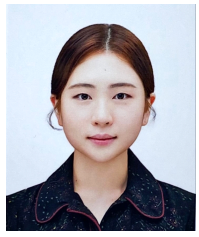
조 현 수 (Hyunsu Cho)

학생회원

2020년 8월 : 고려대학교 전자및정보공학과 졸업

2020년 9월~현재 : 고려대학교 정보보호대학원 정보보호학과 석사과정

<관심분야> 자동차 보안, 센서 보안



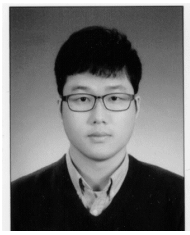
이 선 우 (Sunwoo Lee)

학생회원

2015년 2월 : 서강대학교 수학과 졸업

2015년 9월~현재 : 고려대학교 정보보호대학원 정보보호학과 박사과정

<관심분야> 센서 보안, 생체인증



최 원 석 (Wonsuk Choi)

정회원

2008년 2월 : 서울시립대학교 수학과 졸업

2013년 2월 : 고려대학교 정보보호대학원 정보보호학과 석사

2018년 8월 : 고려대학교 정보보호대학원 정보보호학과 박사

2018년 9월~2020년 2월 : 고려대학교 정보보호연구원 연구교수

2020년 3월~현재 : 한성대학교 IT융합공학부 조교수

<관심분야> 자동차 보안, IoT 보안, 암호학