Rocking Drones with Intentional Sound Noise on Gyroscopic Sensors

Yunmok Son, Hocheol Shin, Dongkwan Kim, Youngseok Park, Juhwan Noh, Kibum Choi, Jungwoo Choi, and Yongdae Kim, *Korea Advanced Institute of Science and Technology (KAIST)*

Rocking Drones with Intentional Sound Noise on Gyroscopic Sensors

Yunmok Son, Hocheol Shin, Dongkwan Kim, Youngseok Park, Juhwan Noh, Kibum Choi,
Jungwoo Choi, and Yongdae Kim
Korea Advanced Institute of Science and Technology (KAIST),
Daejeon, Republic of Korea
{*yunmok00, h.c.shin, dkay, raccoon7, juhwan, kibumchoi, khepera, yongdaek*}@*kaist.ac.kr*

Abstract

Sensing and actuation systems contain sensors to observe the environment and actuators to influence it. However, these sensors can be tricked by maliciously fabricated physical properties. In this paper, we investigated whether an adversary could incapacitate drones equipped with Micro-Electro-Mechanical Systems (MEMS) gyroscopes using intentional sound noise. While MEMS gyroscopes are known to have resonant frequencies that degrade their accuracy, it is not known whether this property can be exploited maliciously to disrupt the operation of drones.

We first tested 15 kinds of MEMS gyroscopes against sound noise and discovered the resonant frequencies of seven MEMS gyroscopes by scanning the frequencies under 30 kHz using a consumer-grade speaker. The standard deviation of the resonant output from those gyroscopes was dozens of times larger than that of the normal output. After analyzing a target drone's flight control system, we performed real-world experiments and a software simulation to verify the effect of the crafted gyroscope output. Our real-world experiments showed that in all 20 trials, one of two target drones equipped with vulnerable gyroscopes lost control and crashed shortly after we started our attack. A few interesting applications and countermeasures are discussed at the conclusion of this paper.

1 Introduction

Sensors are devices that detect physical properties in nature and convert them to quantitative values for actuators and control systems. In many sensing and actuation systems, actuations are determined on the basis of information from sensors. However, these systems can malfunction because of physical quantities that sensors fail to measure or measure insensitively. Furthermore, most sensors cannot distinguish between normal and abnormal physical properties. Therefore, sensors can measure malicious inputs that are intentionally crafted by an attacker in addition to the physical stimuli that the sensors should detect. Because providing detection capabilities for attacks against sensors increases production costs, most commercial devices with sensors are not equipped with any ability to detect or protect against such attacks.

Recently, many sensor-equipped devices, such as smartphones, wearable healthcare devices, and drones, have been released to make the devices easier and more convenient to use. In particular, commercial and open-source drones have been widely used for aerial photography, distribution delivery [2, 3], and private hobbies. These drones have multiple sensors, such as gyroscopes, accelerometers, and barometers. A gyroscope measures changes in tilt, orientation, and rotation based on angular momentum. It is thus a core sensor for flight attitude control and position balancing.

To make the flight control modules of drones small, lightweight, and inexpensive, Micro-Electro-Mechanical Systems (MEMS) gyroscopes are used. MEMS gyroscopes are designed as Integrated Circuit (IC) packages. Each design has a unique mechanical structure in the IC package. Depending on the structure of the MEMS gyroscope, resonance occurs as a result of sound noise at resonant frequencies [37, 38, 39, 49]. This resonance causes performance degradation of the gyroscope.

The resonant frequencies of MEMS gyroscopes are usually designed to be higher than the audible frequency band to prevent malfunctioning of the sensing and actuation systems. However, in our experiments, we discovered that some MEMS gyroscopes that are popularly used in commercial drones resonate at audible frequencies as well as ultrasonic frequencies. Our experiments were designed and conducted to analyze how drones are affected by this phenomenon from an adversary point of view. The flight control software of our target drone was also analyzed to examine the propagation of this phenomenon through the whole system. The results of our

real-world experiments and a software simulation show that this phenomenon could be exploited to launch incapacitating attacks against commercial drones.

The contributions of this research to the field can be summarized as follows:

- We found, using a consumer-grade speaker, that the resonant frequencies of several popular MEMS gyroscopes are not only in the ultrasonic frequency band but also in the audible frequency band, and we analyzed their resonant output.

- We investigated the effect of the resonant output of MEMS gyroscopes on the flight control of drones via software analysis and simulations.

- We developed a novel approach to attacking drones equipped with vulnerable MEMS gyroscopes using intentional sound noise, and we demonstrated the consequences of our attack in real-world experiments [1]

This paper is organized as follows: Section 2 outlines security research to date on sensor systems. Section 3 provides background information on drone systems and MEMS gyroscopes. Section 4 describes the analyses and experiments conducted in this study to investigate the effects of sound noise on MEMS gyroscopes. Analysis of the flight control software, real-world experiments, and simulations for attacking drones are described in Section 5. A discussion of the results and conclusion drawn from the results are presented in Sections 6 and 7, respectively.

2   Related Work

The security of sensors recently started to draw attention with the introduction of consumer-grade sensing and actuation systems. As this study was focused on input spoofing attacks on gyroscopes, we review in this section previous researches on 1) privacy issues related to gyroscopes, 2) resonant frequencies of gyroscopes, 3) security analyses of commercial drones, and 4) input spoofing attacks on sensing circuitry.

Privacy Issues Related to Gyroscopes: Embedded devices can be used to record the private information of users without their recognition. Because a gyroscope can be used to measure changes in tilt, orientation, and rotation, it can be used to steal a smartphone user's keystroke information, such as unlock passwords, banking passwords, and credit card numbers [36, 47]. By exploiting

the capability of the gyroscopes of smartphones to measure acoustic vibrations at a low frequency band, a new attack was proposed to eavesdrop speech [59]. The focus of these studies differed from that of this paper in that they examined the use of gyroscopes to extract private information, without affecting actuation.

Resonant Frequencies of Gyroscopes: Resonant frequency has been identified as a problem that causes the performance degradation of MEMS gyroscopes. In general, the vibrating structures of MEMS gyroscopes have resonant frequencies. Resonance can occur as a result of sound noise [37, 38, 39]. Some mechanisms for mitigating interference from sound have been proposed. Roth suggested a simple and cheap defense technique that involves surrounding the gyroscope with foam [49]. Soobramaney proposed the use of an additional structure in a gyroscope that responds only to the resonant frequency to cancel out the resonant output from the gyroscope [52]. Using an additional feedback capacitor connected to the sensing electrode, the resonant frequency and the magnitude of the resonance effect can be tuned [35, 43]. It is widely believed that most consumer-grade MEMS gyroscopes have resonant frequencies. However, these resonant frequencies are often considered to be commercial secrets or are designed to be just higher than the audible frequency range.

Security Analysis of Commercial Drones: There were a couple of works on hacking commercial drones. Samland et. al. showed that *AR.Drone* [5] was vulnerable to network attacks due to unencrypted Wireless LAN (WLAN) communication and the lack of authentication for Telnet and FTP [50]. Kamkar showed that a drone can be hijacked by another drone using similar vulnerabilities [44]. Attacks such as these are focused on hijacking network connections or system privileges.

Input Spoofing Attacks on Sensing Circuitry: All sensing and actuation systems have sensing circuitry that is composed of the sensor itself and a wire that connects the sensor to other components of the system. Kune et. al. showed that an adversary can inject an Electro Magnetic Interference (EMI) signal into the wire connecting an analog sensor and Analog-to-Digital Converter (ADC) to fake a sensing signal [45]. By injecting fake waveforms, the researchers were able to inhibit pacing or induce defibrillation shocks in Cardiac Implantable Electrical Devices (CIEDs). Without affecting the sensor itself, they were able to spoof the sensing signal by injecting an EMI signal into the sensing circuitry.

It is also possible to affect the sensor itself. For example, biometric imaging sensors have frequently been targeted in sensor spoofing attacks. Tsutomu et al. showed that a verification rate of more than 68 % could be achieved against 11 different fingerprint systems using artificial fingers [46]. Galbally et al. fabricated fake

---

[1]A demo video of our attack against the target drone in the real world is available at https://sites.google.com/site/rockingdrone/.
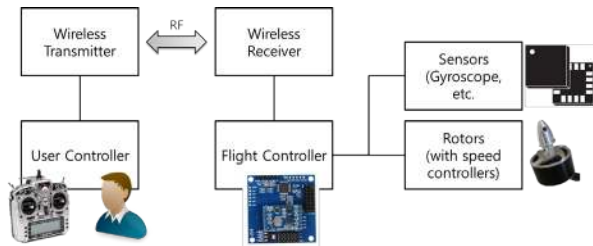
Figure 1: Block diagram of a typical drone system

fingerprints from standard minutiae templates, and more than 70 % of the fake fingerprints were accepted by the system tested [42]. In addition, a method for bypassing the user authentication of facial cognitive biometric systems was proposed as an example of sensor input spoofing against the imaging sensor systems of commercial laptops [40].

We were able to find only one notable and relevant study not related to biometric image sensors. Shoukry et al. injected magnetic fields to spoof the wheel speed of vehicles by placing a magnetic actuator near the Antilock Braking System (ABS) wheel speed sensor of which is also a magnetic sensor also [51]. In other words, the researchers used the same physical property as that intended to be sensed through the sensing channel of the target sensor for their spoofing attack. This work is similar to ours in that it explored intentional interference with sensors to cause malfunctioning of actuators However, we investigated whether intentional sound noise at the resonant frequency of a gyroscope can incapacitate a drone. This means that our attack is an interference attack through a channel other than the sensing channel that has to be insensitive for the gyroscope. Note that a MEMS gyroscope is *the most basic sensor used in maintaining a drone in an upright position* without any external torque.

3 Background

In this section, we explain the operation and characteristics of the drone considered in this study, its flight control system and a MEMS gyroscope.

3.1 Drone (Multicopter)

A drone is a kind of Unmanned Aerial Vehicle (UAV). Drones are used not only for military purposes but also for various non-military purposes such as delivery services, aerial photography, search and rescue (S&R), crop-dusting, and hobbies. Because of accessibility reasons, military drones were not considered in this paper. Many commercial drones have been released in recent

years as the non-military drone market has grown [2, 3]. Both finished drones and DIY drones with open-source drone projects for the flight control software are commercially available. *AR.Drone* [5] is a popular commercial finished drone product. *Multiwii* [24] and *ArduPilot* [7] are open-source flight control software used widely with both DIY and commercial drones. These drones are also known as multicopters (quadcoptors if they have four rotors) because they usually have multiple rotors.

Typically, a drone system consists of multiple rotors, one flight controller, one wireless receiver, and one wireless transmitter (remote controller). Figure 1 shows a block diagram of a drone system. The flight controller receives control signals from the wireless transmitter through the receiver, and manipulates the speed of the rotors in accordance with the user's control supported by the flight controller.

3.2 Flight Attitude Control

It is very important for the drone flight controller to adjust each rotor's speed for horizontally leveling off in the air, because multiple rotors are not always exactly the same and the center of mass cannot always be ensured. To stabilize a drone's balance automatically, a flight attitude control system is implemented in the flight control software. This flight attitude control system computes the proper control signal for multiple rotors with algorithms based on the data from Inertial Measurement Units (IMUs), including gyroscopes.

IMUs, which consist of sets of sensors, are fundamental components of flight control systems for aircraft, spacecraft, and UAVs, including drones. An IMU measures the orientation, rotation, and acceleration of a drone, using a combination of a gyroscope and an accelerometer, and in some cases also a magnetometer and a Global Positioning System (GPS) [55]. MEMS gyroscopes are thus necessary components of drones and must be robust to control drones successfully.

In the case of open-source flight control software [7, 24], the most common algorithm for flight attitude control is Proportional-Integral-Derivative (PID) control. The PID control algorithm is a control loop feedback mechanism that minimizes the difference between the desired control and the current status. It is made up of three terms: the proportional, the integral, and the derivative terms, denoted by *P*, *I*, and *D*, respectively. The *P* term applies control to the system in proportion to the difference (error) between the current state and the desired state to the system. The *I* term is used to reduce the steady-state error through proportional control of the accumulation of past errors. The *D* term is used to reduce overshoot and increase stability through proportional control of the changing rate of errors. Each

term has a gain (G_P, G_I, and G_D) for tuning the control system, and users can change each gain for stability and sensitivity of drones of various types, sizes, and weights.

3.3 MEMS Gyroscope

3.3.1 Operation

The principle underlying the MEMS gyroscope [1, 9] is the law of physics known as the Coriolis effect or Coriolis force. The Coriolis effect is the deflection of a moving object in a rotating reference frame. This effect appears only to an observer in the same rotating reference frame. In the observer's view, the path of the moving object is observed to be bent by a fictitious force, i.e. the Coriolis force. In other words, when an object is moving in a rotating container or package, the path of the moving object is bent in a direction different from the moving direction. Therefore, the observer on the container or package can sense this bending. Figure 2 illustrates the concept of a MEMS gyroscope structure for one axis. To sense motion with respect to one axis such as Z-axis rotation, there is a mechanical structure called a sensing mass in a MEMS gyroscope. While a sensing mass is continuously vibrating at a certain frequency with respect to the X-axis, the Coriolis force is applied in the Y-axis direction as a result of the Z-axis rotation. The amount of rotation is proportional to the amount of bending.

Figure 3 shows an example of a MEMS gyroscope structure with three axes. This gyroscope is manufactured by *STMicroelectronics* [10]. In Figure 3, M1 through M4 correspond to continuous vibrations of the sensing masses. Bending occurs in the direction orthogonal to both the vibrating axis and the rotating axis when this structure rotates with respect to each axis [10].

MEMS gyroscopes support digital interfaces such as Inter-Integrated Circuits (I^{2}Cs) and Serial Peripheral Interfaces (SPIs) that communicate with the processors of application systems. By reading registers of the gyroscopes that contain the sensed values, a system's processor can calculate the amount of rotation that occurs. The maximum sampling frequency for reading the registers of the MEMS gyroscopes varies from a few hundred to a few thousand samples per second. This means that gyroscopes cannot sense and recover correctly from fast changes in rotation over a few kHz without additional signal processing, according to the sampling theorem. The sampling theorem defines the minimum sampling frequency as a frequency higher than $2 \times B$ Hz when the given signal contains no frequency components higher than B Hz. If this condition is not satisfied, distortion occurs in the frequency response. This is referred to as aliasing. Because of the aliasing problem, a frequency analysis of the gyroscope output is not very useful.
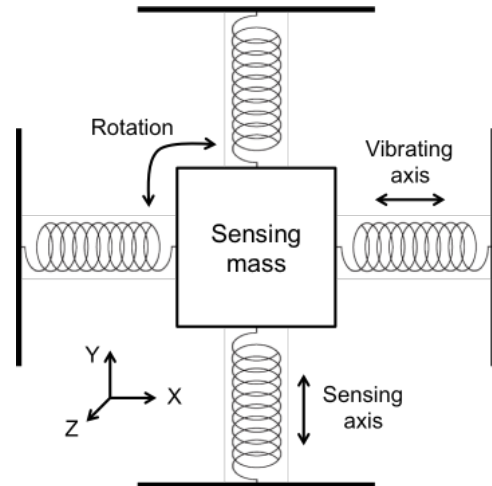

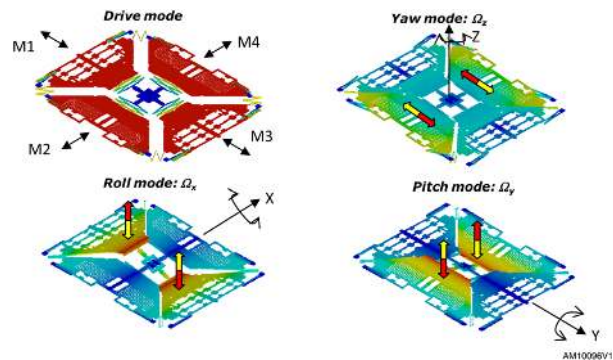Figure 2: Concept of MEMS gyroscope structure for one axis

Figure 3: Operation of a three-axis MEMS gyroscope [10] (the X-, Y-, and Z-axes are defined as the pitch, roll, and yaw, respectively.)

3.3.2 Acoustic Noise Effect

The accuracy degradation of MEMS gyroscopes by harsh acoustic noise is well known to researchers who have studied the performance of MEMS sensors [37, 38, 39, 49]. A MEMS gyroscope has a resonant frequency that is related to the physical characteristics of its structure, and high-amplitude acoustic noise at the resonant frequency can produce resonance in the MEMS structure. As a result of this resonance, the MEMS gyroscope generates an unexpected output that may cause the related systems to malfunction. To minimize the resonance effect of acoustic noise in daily life, MEMS gyroscopes are typically designed with resonant frequencies above the audible frequency limit (i.e., above 20 kHz).

However, we found that some MEMS gyroscopes have resonant frequencies in both the audible and ultrasonic frequency ranges, and these sensors generate ghost outputs with injected sound noise by an attacker. In addi-
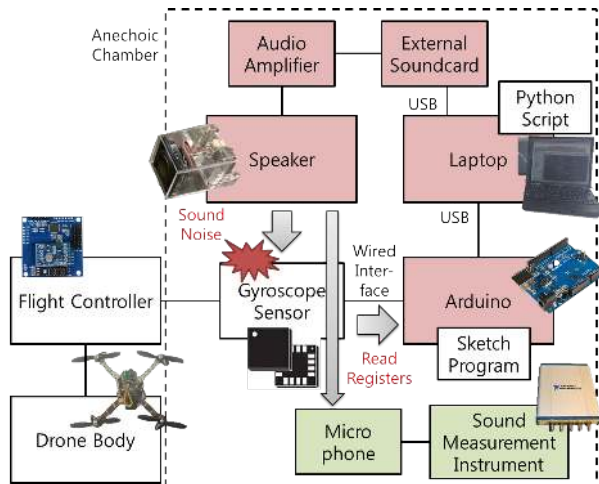
Figure 4: Overview of our experiment

Figure 5: SPL and THD+N measurement using sound measurement instrument (National Instruments USB-4431)

tion, these MEMS gyroscopes are widely used in drone flight controllers and smartphones. The accuracy degradation problem of MEMS gyroscopes has only been considered in the context of performance issues, but this phenomenon can be used as a new attack vector. Therefore, it is important to study this phenomenon as a vulnerability that can cause critical loss of control of MEMS gyroscope application systems, such as drones.

4 Analysis of Sound Noise Effects

To explore the effects of sound noise on drones, it is necessary to identify the resonant frequencies of MEMS gyroscopes used for drones precisely. However, the datasheets of some MEMS gyroscopes do not include information on their exact resonant frequencies, and the resonant frequencies are even classified in some cases. A simple and reliable way to find the resonant frequency of a MEMS gyroscope is exhaustive search, i.e., scanning with pure single-tone sound over a chosen frequency band. In this section, the measurement and analysis of the effect of sound noise on MEMS gyroscopes are described.

4.1 Overview

An overview of our experiment is shown in Figure 4. Python scripts to generate sound noise with a single frequency and to collect data from the target gyroscopes are run on a laptop computer. A consumer-grade speaker connected to the laptop is used as the noise source and is set 10 cm above the top of the target gyroscope. We used Arduino [6], a programmable microprocessor board, to read and write registers of the target sensors. A single-tone sound noise scanning the sound frequency range
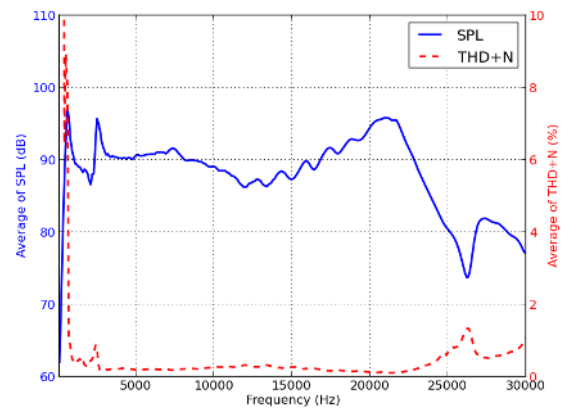
was maintained until 1,000 samples had been collected from the target gyroscopes. We generated single-tone noises at frequencies from 100 Hz to 30 kHz at intervals of 100 Hz. In other words, this experiment was performed using not only audible noise (below 20 kHz) but also ultrasonic noise (above 20 kHz).

We evaluated 15 kinds of MEMS gyroscopes manufactured by four vendors, which are readily available on online websites. Most of the target gyroscopes were from *STMicroelectronics* and *InvenSense*, two leading vendors of MEMS gyroscopes [22]. Each kind of gyroscope requires a different application circuit and register configuration for proper operation. We therefore implemented simple application circuits and Arduino codes for the target gyroscopes by referring to their datasheets. The effects produced on each gyroscope by sound noise were measured in an anechoic chamber (indicated by the dotted line box in Figure 4).

4.2 Sound Source

We considered the loudness and linearity of the sound source to select a sound source for further analysis.

A common noise measurement unit for the loudness of sound is the Sound Pressure Level (SPL), because sound is a pressure wave in a medium such as air or water. To show the noise level generated by our sound source [12], a consumer-grade speaker, SPL values were measured with no weighting using a professional sound measurement instrument [26] and a microphone [8]. The speaker was placed 10 cm from the microphone, and single-tone noises were generated from 100 Hz to 30 kHz at intervals of 100 Hz. We used an audio amplifier to make the sound noise sufficiently loud. In addition, we set the sampling

Table 1: Summary of experiment results (investigation of the resonant frequencies of MEMS gyroscopes using intentional sound noise)

Sensor	Vender∗	Axis	Interface	Resonant freq. in the datasheet (axis)	Resonant freq. in the experiment (axis)
L3G4200D†	STM	X, Y, Z	Digital	no information	7,900 ∼ 8,300 Hz (X, Y, Z)
L3GD20†	STM	X, Y, Z	Digital	no information	19,700 ∼ 20,400Hz (X, Y, Z)
LSM330	STM	X, Y, Z	Digital	no information	19,900 ∼ 20,000 Hz (X, Y, Z)
LPR5150AL	STM	X, Y	Analog	no information	not found in our experiments
LPY503AL	STM	X, Z	Analog	no information	not found in our experiments
MPU3050	IS	X, Y, Z	Digital	33 ± 3 kHz (X)	not found in our experiments
MPU6000†	IS	X, Y, Z	Digital	30 ± 3 kHz (Y)	26,200 ∼ 27,400 Hz (Z)
MPU6050	IS	X, Y, Z	Digital	27 ± 3 kHz (Z)	25,800 ∼ 27,700 Hz (Z)
MPU6500	IS	X, Y, Z	Digital	27 ± 2 kHz (X, Y, Z)	26,500 ∼ 27,900 Hz (X, Y, Z)
MPU9150	IS	X, Y, Z	Digital	33 ± 3 kHz (X)	27,400 ∼ 28,600 Hz (Z)
IMU3000	IS	X, Y, Z	Digital	30 ± 3 kHz (Y)	not found in our experiments
ITG3200	IS	X, Y, Z	Digital	27 ± 3 kHz (Z)	not found in our experiments
IXZ650	IS	X, Z	Analog	24 ± 4 kHz (X), 30 ± 4 kHz (Z)	not found in our experiments
ADXRS610	AD	Z	Analog	14.5 ± 2.5 kHz	not found in our experiments
ENC-03MB	Murata	X	Analog	no information	not found in our experiments

∗ *STM: STMicroelectronics, IS: InvenSense, AD: Analog Devices*
† *12 sample chips for experiments (2 sample chips for others)*

Table 2: Effect of sound noise (standard deviations and their ratios for vulnerable gyroscopes, averaged for all sample chips)

Sensor	Without noise			With noise			Ratio		
	$\sigma_{X_{wo}}$	$\sigma_{Y_{wo}}$	$\sigma_{Z_{wo}}$	σ_{X_w}	σ_{Y_w}	σ_{Z_w}	$\sigma_{X_w}/\sigma_{X_{wo}}$	$\sigma_{Y_w}/\sigma_{Y_{wo}}$	$\sigma_{Z_w}/\sigma_{Z_{wo}}$
L3G4200D	3.15	2.69	2.88	12.1	22.04	4.45	**3.84**	**8.21**	**1.55**
L3GD20	2.92	2.47	2.3	62.03	76.67	3.09	**21.21**	**31.04**	**1.35**
LSM330	13.09	16.03	21.45	177.71	114.34	30.44	**13.57**	**7.13**	**1.42**
MPU6000	11.79	13.92	12.8	12.48	14.74	111.21	1.06	1.06	**8.69**
MPU6050	13.21	12.32	11.17	13.8	12.55	58.17	1.04	1.02	**5.21**
MPU6500	17.34	19.63	18.21	363.21	71.04	56.15	**20.95**	**3.62**	**3.08**
MPU9150	10.69	11.47	10.71	10.98	11.97	58.59	1.03	1.04	**5.47**

rate of the sound source to 96 kHz rather than 48 kHz to remove aliasing of the generating sound signal.

Another important property of a sound source is Total Harmonic Distortion plus Noise (THD+N), which is the ratio of the power of the harmonics and noise components to that of a fundamental component, expressed as a percentage. Every speaker has a nonlinear characteristic to its frequency response. This nonlinearity leads to harmonic distortions and noise of output sound at frequencies that are different from a fundamental frequency. If the power of these harmonics and noise is high (i.e., high THD+N), it is hard to regard the identified response as the effect from a single frequency. However, it is not necessary for low THD+N of the sound source to attack.

Figure 5 shows the average values of both the SPL and THD+N for all of the experiments. In most fre-quency bands, the SPL values were above 80 dB and the THD+N values were less than 2 %. Because the sound source we used was a tweeter that is usually used for high-frequency sound, the performance was not good in the low-frequency region (below 1 kHz). It is usually difficult to hear sound noise at frequencies above approximately 15 kHz, although we set the maximum volume at those frequencies. The measured SPL in our experiment was equivalent to the noise level (around 90 dB SPL) of a hand drill, hair dryer, heavy city traffic, noisy factory, and subway in the real world.
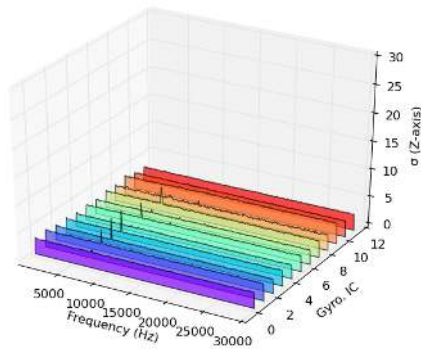
4.3 Effect of Sound Noise

Raw data samples from the registers of the target gyroscopes were collected for use in this analysis. The target gyroscopes were fixed on a stable frame in an ane-
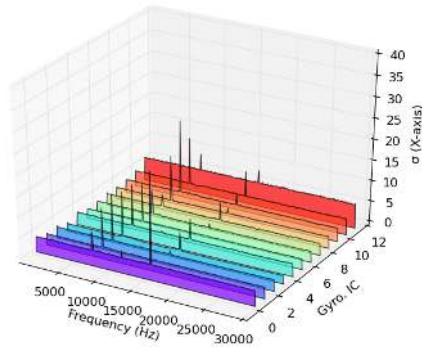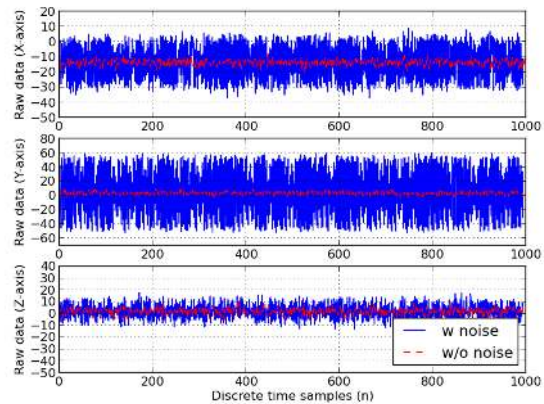
(a) Standard deviation of raw data samples for 12 identical L3G4200D chips (X-axis)
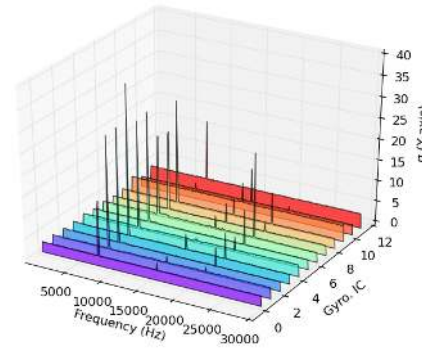
(b) Standard deviation of raw data samples for 12 identical L3G4200D chips (Y-axis)

(c) Standard deviation of raw data samples for 12 identical L3G4200D chips (Z-axis)

(d) Raw data samples of one L3G4200D chip with the single tone sound noise at 8,000Hz

Figure 6: Sound noise effect on L3G4200D gyroscopes (all samples were collected as raw data stored in the gyroscope's register)

choic chamber, with and without sound noise. Because the standard deviation of the raw data samples should ideally be zero without sound noise when the target gyroscopes are on the frame, we consider the difference in the standard deviations with and without sound noise as a criterion for the resonance of the target gyroscopes.

The results of the experiment are summarized in Table 1. The third and fourth columns indicate the degrees of freedom and the interface type of each gyroscope, respectively. The resonant frequencies [2] and axes from the datasheets [4, 13, 14, 15, 16, 17, 18, 19, 25, 28, 29, 30, 31, 32] are listed in the fifth column, and the resonant frequencies identified in our experiment are listed in the last column.

Our results show that seven of these gyroscopes (i.e., vulnerable gyroscopes) resonated at their own resonant frequencies in response to sound noise. Three of the vulnerable gyroscopes were manufactured by *STMicroelectronics*, and the others were manufactured by *InverSense*. No documentation on the resonant frequencies of the tested gyroscopes was available from vendors other than *InvenSense* and *Analog Devices*. We figured out that the gyroscopes manufactured by *STMicroelectronics* had resonant frequencies in the audible range (almost below 20 kHz), and that they were affected considerably more along the X-axis and Y-axis than along the Z-axis. In contrast, the gyroscopes manufactured by *InvenSense* resonated in the ultrasound range (above 20 kHz) and were affected in the Z-axis direction only.

Both keeping resonant frequencies secret and raising them to the higher-frequency region are good ways to

---

[2]These are described as mechanical frequencies in the datasheets for the *InvenSense* gyroscopes.
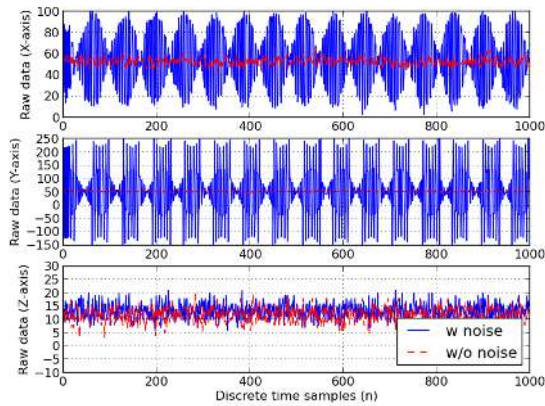
(a) Raw data samples of one L3GD20 chip with a single-tone sound noise at 20,100Hz
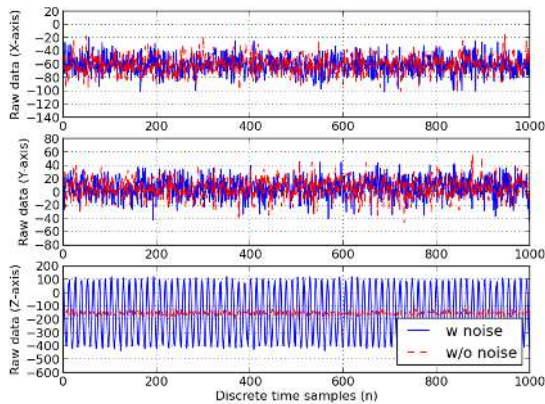
(b) Raw data samples of one MPU6000 chip with a single-tone sound noise at 26,800Hz

Figure 7: Sound noise effects on two vulnerable MEMS gyroscopes (all samples were collected as raw data stored in the gyroscope's register)

reduce resonance due to sound noise. However, as our results show, resonance can be induced by a malicious attacker, as long as resonant frequencies exist in gyroscopes. Additionally, the standard deviations of the output data from these gyroscopes are largely increased without any rotation or tilt when the resonance occurs as a result of intentional sound noise. This abnormal output can potentially make gyroscope application systems malfunction.

We did not detect resonance effects for the other eight gyroscopes evaluated in our experiments. Particularly, for five of these gyroscopes, no resonant frequencies were observed, even though their resonant frequencies are described in their datasheets. We obtained additional measurements with the frequency resolution enhanced by a factor of two (50 Hz), but resonant frequencies were

not found. It might be possible that the frequency intervals (100 Hz and 50 Hz) used in our tests were not sufficiently narrow. The fact that resonant frequencies were not detected in our experiments does not necessarily mean that they do not exist in the frequency range below 30 kHz.

A comparison between the standard deviations (σ_{axis}) with and without sound noise for the seven vulnerable gyroscopes is presented in Table 2. To validate our attack method, 12 individual gyroscope chips were tested for L3G4200D, L3GD20, and MPU6000, whereas only two chips were tested for the others. All of the values shown in Table 2 are average for all outputs from the same kind of vulnerable gyroscopes. The standard deviations of the gyroscope outputs with sound noise at the resonant frequencies are relatively large. The ratios of the standard deviations with sound noise to those without sound noise are summarized in the last three columns. The standard deviations changed by factors up to dozens, with the greatest change being by a factor of 31.04 (for the Y-axis of L3GD20).

Figures 6(a), 6(b), and 6(c) show the standard deviations of the raw data samples for each axis from the 12 individual L3G4200D chips. The different L3G4200D chips have different output characteristics because of manufacturing variances. However, every L3G4200D chip has a peak in the range of 7,900 to 8,300 Hz. To investigate what happens at these frequencies in more detail, the raw data samples for one L3G4200D gyroscope with and without sound noise at 8,000 Hz were compared, as shown in Figure 6(d). This graph clearly shows that resonances occur for all axes, and the amplitudes are dozens of times larger than the normal output. These amplitudes are equivalent to the output produced by sudden and fast shaking of the gyroscope or the target drone's body by hands or rapidly changing winds. Raw data samples of two other vulnerable gyroscopes, L3GD20 and MPU6000, are shown in Figure 7. L3G4200D and MPU6000, two of the vulnerable gyroscopes in our experiments, were used in the target drones described in the next section.

It should be noted that a speaker generates sound from a vibrating membrane fixed to the enclosure of the speaker, and thus vibration from the enclosure itself was unavoidable in the experiments. However, our experimental results indicate that vibration had very little effect on the identification of the resonant frequencies of the target gyroscopes. Because we tested all of the gyroscopes in the same environment, there should have been consistent resonance frequencies for all of the gyroscopes if any enclosure vibration had influenced the motion of the gyroscopes. In addition, some of the gyroscopes listed in Table 1 exhibited no resonance (i.e., almost constant standard deviation), which would not have
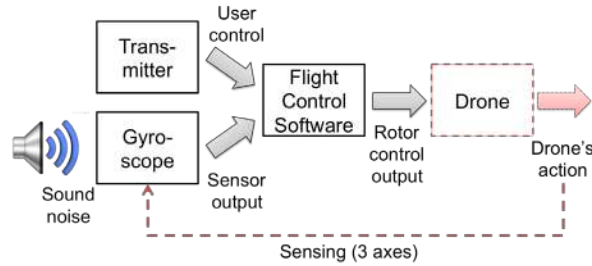
Figure 8: Propagation of the effect of sound noise

been possible if there had been a strong vibration due to vibration of the enclosure.

5 Attacking Drone

As described in the previous section, the outputs of MEMS gyroscopes fluctuate with the sound noise at the gyroscopes' own resonant frequencies. This section describes the impact of this fluctuation on the control of a drone. To understand this, we first need to understand how the user input from a remote controller and the input from the gyroscope propagate to the operation of a drone. Figure 8 shows each step in this propagation. The flight control software calculates each control signal for four rotors based on the user input and gyroscope output. This control signal mechanically controls the speed of each rotor, which determines the tilt, orientation, and rotation of the drone in turn. This section describes the analysis of how sound noise at the resonant frequency of a gyroscope affects control of target drones.

We took the following three steps. 1) To understand the reaction of the target drones as actuators to the fluctuation of the gyroscope output as abnormal sensing, the flight control software was analyzed statically. 2) We then launched our attack on two target drones under real-world conditions to assess the effect of the maximum sound noise against them. 3) To identify cost-efficient parameters for our attack, we performed software simulations with gyroscope outputs varying from 1% to 100 % of the maximum noise.

5.1 Target Drones

For this experiment, two DIY drones were built for use as the target drones, and they were equipped with L3G4200D and MPU6000 respectively, two of the vulnerable gyroscopes. This approach was taken because the gyroscopes on most finished drones are not user selectable, and it was necessary to evaluate the effect of sound noise in the sensing and actuation systems. The main specifications of the two target drones are given in Table 3. All DIY drones require calibration for stable

operation. Following the instructions in the manual for the flight control software, we calibrated the IMU sensors and four rotor controllers, and we adjusted the PID gains (see Section 3.2) for stable flight.

5.2 Software Analysis

Target drone A's flight control software, *Multiwii* [24], supports various gyroscopes. However, the main routine of this software is essentially the same for all gyroscopes except with respect to the way the sensors are prepared and the way the raw data are accessed. The main processor reads the raw data from the gyroscope's registers through an I^2C interface, along with the raw data from the transmitter controlled by the user. Each raw data sample for each axis was stored in two 8-bit registers. These raw data were the main inputs to the flight control software, and the outputs were the rotor control data calculated by the PID control algorithm. The PID controller seeks to minimize the difference between the measured control and the desired control for the control systems. While PID controller implementation and PID gains vary depending on their application and the gyroscope used, the fundamental algorithm remains the same.

Algorithm 1 describes a high-level implementation of the default PID control algorithm in this flight control software. The details of the software are omitted for simplicity. Conceptually, the P, I, and D terms influence the target drone's control as follows:

- *P* is proportional to the present output of the gyroscope, and if the present output value (*gyro*[*axis*]) of the gyroscope is abnormally large, the desired control from the transmitter (*txCtrl*[*axis*]) can be ignored (line 7).

- *I* is proportional to the accumulated error between the output from the transmitter and the gyroscope (line 10), which can be ignored, because the default value of the I term gain (G_I) for the target drone is very small.

Table 3: Specifications of two target drones for the real world attacking experiment

Spec.	Target Drone A	Target Drone B
Processor	STM32F103CBT6	ATMEGA2560
Gyroscope	L3G4200D	MPU6000
Flight Ctrl. Software	Multiwii [24]	ArduPilot [7]
Diagonal Frame Size	45 cm	55 cm
Propeller Size	10×4.5	10×4.5

Algorithm 1: Simplified PID algorithm of *Multiwii* flight controller (calculating the rotor control data according to the output of the gyroscope)

Input: The sensed data from the MEMS gyroscope
Input: The received data from the transmitter
Output: The data to control the rotor

1   initialization;
2   G_P, G_I, and G_D: pre-configured P, I, and D gain by user (configured as the default values);
3   **while** *True* **do**
4   read data from the gyroscope for 3 axes;
5   receive data from the transmitter for 4 channels (3 axes and throttle);
6   **for** *axis* **do**
7       $P = txCtrl[axis] - gyro[axis] \times G_P[axis]$;
8       $error = txCtrl[axis]/G_P[axis] - gyro[axis]$;
9       $error_{accumulated} = error_{accumulated} + error$;
10      $I = error_{accumulated} \times G_I[axis]$;
11      $delta = gyro[axis] - gyro_{last}[axis]$;
12      $delta_{sum}$ = sum of the last three delta values;
13      $D = delta_{sum} \times G_D[axis]$;
14      $PIDCtrl[axis] = P + I - D$;
15   **end**
16   **for** *rotor* **do**
17   **for** *axis* **do**
18        $rotorCtrl[rotor] = txCtrl[throttle] + PIDCtrl[axis]$;
19   **end**
20   limit *rotorCtrl[rotor]* within the pre-defined MIN (1,150) and MAX (1,850) values;
21   **end**
22   actuate rotors;
23   **end**

- *D* is proportional to the changes ($delta_{sum}$) between the previous and present output values of the gyroscope (line 13).

These three terms directly affect the PID control values ($PIDCtrl[axis]$) for each axis (line 14). If the values of *P* and *D* are abnormally large, the PID control values will also increase abnormally. The desired throttle control ($txCtrl[throttle]$) can thus be ignored (line 18). In the end, all rotor control values are constrained by the pre-defined minimum and maximum values (line 20). Throughout the process, the raw data from the gyroscope were not checked, filtered, or verified. In other words, the target drone system fully trusted the integrity of the gyroscope output in its sensing and actuation. Therefore, the control of the target drone could be directly affected by our attack.

We also analyzed the flight control software of

ArduPilot [7] for target drone B. A manual software analysis shows that the PID algorithm used in *ArduPilot* is essentially the same as that used with target drone A. The only difference between two algorithms is in slight changes of the gains that are multiplied to each of the *P*, *I*, and *D* terms. This can be considered a discrepancy in the configuration values of the sensors.

5.3   Real-World Experiment

While the software analysis described in the previous section led us to believe that the *PIDCtrl[axis]* values would fluctuate when the gyroscope outputs fluctuated, this information was not sufficient to answer the following questions: 1) Given user inputs *txCtrl[throttle]* and fluctuating *PIDCtrl[axis]*, how much does *rotorCtrl[rotor]* change? 2) How does a change in *rotorCtrl[rotor]* affect the behavior of the drone? To answer these questions, we decided to launch our attack in the real world with sound noise causing the fluctuation.

Attack Setup: In this experiment, we attached a small Bluetooth speaker above the target system's gyroscope at a distance of 10 cm to serve as an attacking sound source. The SPL of the fundamental frequency component was 113 dB with the maximum volume of the speaker. Low THD+N was not a consideration for the sound source used in the attack. The sound noise was turned on while the target drones were stably maintained in the air. To observe the status of the target drones before, during, and after the attack, sound noise at the resonant frequency was turned off, turned on (attack), and turned off again for every 10 seconds.

Attack Results: The results of our attack experiment are summarized on two target drones (A and B) in Table 4. Our attacks successfully disrupted control of target drone A, but it did not affect target drone B. The reason of attack failure on target drone B is that the gyroscope of target drone B resonated only along the Z-axis. The Z-axis of target drone B corresponds to the horizontal orientation that is also sensed by the magnetometer on the board.
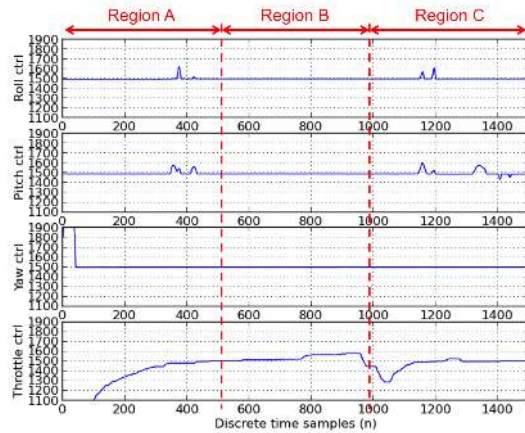
We also attached a sonar device to gauge the altitude

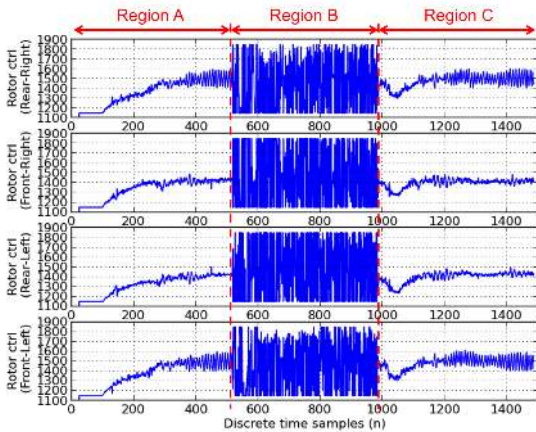Table 4: Result of attacking two target drones

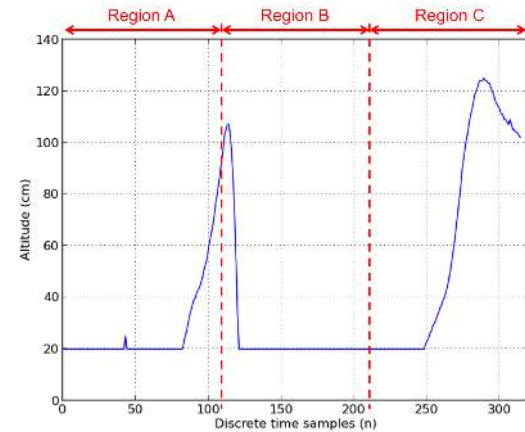| Item	Target Drone A	Target Drone B
Resonant Freq. (Gyroscope)	8,200 Hz (L3G4200D)	26,200 Hz (MPU6000)
SPL at Resonant Freq.	97 dB	95 dB
Affected Axes	X, Y, Z	Z
Attack Result	Fall down	Not affected
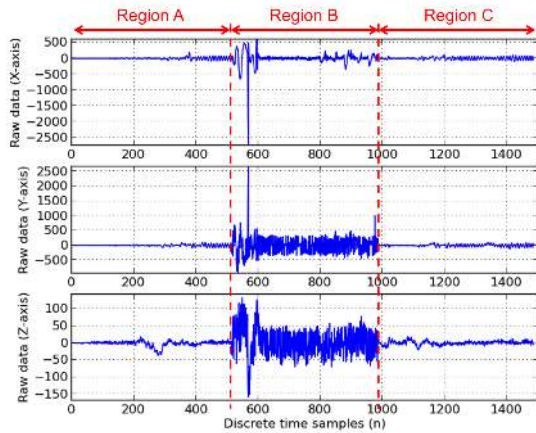
(a) Raw data samples of the gyroscope

(b) Received data samples from the transmitter

(c) Rotor control data samples (from the flight control software)

(d) Altitude data samples from sonar

Figure 9: The results of our attack against target drone A in a real-world experiment (sound noise turned off, on, and off every 10 seconds; note that the sonar's sampling rate was different from that for the data in other figures)

and two Bluetooth-to-UART (Universal Asynchronous Receiver/Transmitter) modules to collect real-time data from target drone A. The Bluetooth-to-UART modules were connected to a UART interface on target drone A's flight controller board and the sonar module. Using this UART interface, we were able to communicate with a computer for configuration purpose. We were also able to monitor the status of target drone A, including the raw data from the sensors and the rotor control data, using the *Multiwii* [24] Graphical User Interface (GUI) program. By analyzing the *Multiwii* source code, we were able to understand the protocol used for the UART communication. Each request or response message consists of a 3-bytes fixed header, 1 byte for the data length (n), a 1-byte command, n bytes of data, and a 1-byte checksum. Using this protocol and the Bluetooth-to-UART modules, we were able to record the resonant outputs of the gyroscope, the control data from the transmitter, the rotor

control data of the flight control software, and the altitude data from target drone A in the air. Note that the altitude data were sampled at a different rate than the other data because of a technical limitation of the sonar module, and the minimum sensing distance of the sonar was 20 cm.

Figure 9 shows the detailed results of the attack against target drone A in the real-world experiment. Region A in Figure 9 corresponds to the period before the attack. The user gradually raised the throttle (Figure 9(b)), and the speeds of the four rotors were increased correspondingly (Figure 9(c)). In response, target drone A rose over 100 cm in the air (Figure 9(d)). When the attack was started (Region B), the output of the gyroscope fluctuated because of the sound noise at the resonant frequency (Figure 9(a)). According to the resonant output of the gyroscope, the rotor control data fluctuate between the maximum and minimum values (Region B in Figure 9(c)).
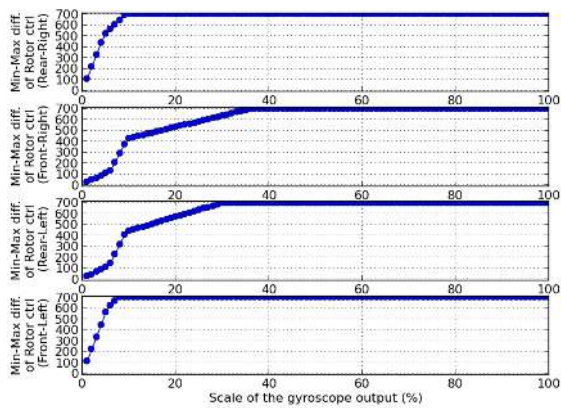
Figure 10: Rotor control outputs from our software simulation (the maximum change of the rotor control output was 700)
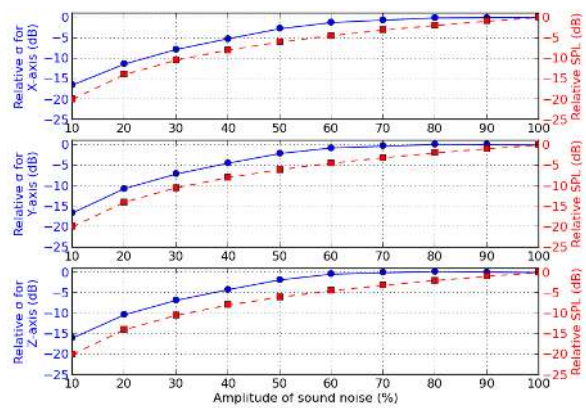

Figure 11: Sound noise effect on one L3G4200D gyroscope versus sound noise amplitude with theoretical relative SPL (data averaged for ten identical experiments and 1,000 raw data samples collected per experiment)

When the attack started, target drone A dropped instantaneously. During the attack, target drone A could not ascend or recover its control, even though throttle control was maintained to allow it to ascend slowly (Figure 9(b)). After the attack was stopped (Region C), target drone A ascended normally again and recovered its control. We attacked target drone A 20 times in the real-world experiments, and it lost control and crashed shortly after our attack in every test.

To assess the effectiveness and practicality of our attack, more real-world attack experiments are required. However, there are obstacles such as the damage to the target drone (e.g., broken arms) and the repetitive recalibration required after each crash, because the unpredictable changes in the drone's balancing are fed back into the gyroscope by our attack (see the dotted line and box in Figure 8).

5.4   Attack Distance

Our real-world experiments showed that an acoustic attack can completely incapacitate a target drone equipped with a gyroscope vulnerable to X-axis and Y-axis resonance due to sound incidence. We also want to determine the conditions or bounds of a cost-effective attack. For example, we need to find out possible attack distance or sound level of a sound source required to destabilizing a target drone in the air.

We may try to conduct tests at various distances to discover either the approximate minimum distance or the sound level required to incapacitate target drone A in the air. However, it would disrupt the stability of the target drone to attach a longer structure with the sound source on the target drone. It is also difficult to take aim at

the target drone with sound noise from outside during its flight without attaching any structure to it.

Therefore, to minimize the number of trials and overcome the practical limitations mentioned above, we first ran a simulation using the functions of Algorithm 1, which were extracted from the source code for target drone A. Based on the results of this simulation, we found out the effective fluctuation (i.e., standard deviation) of the gyroscope output with a few real-world tests. Then, we measured the standard deviations of target drone A on a desk exposed to sounds of various amplitudes. By combining the results of this simulation and our measurements, we were able to identify an approximate range of sound amplitude for testing the target drone in the air. We then derived the feasible attack distance theoretically using the SPL value that we had measured in our attack with the effective amplitude of the sound noise.

Simulation: For the software simulation, the recorded gyroscope output and the control data from the transmitter in the real-world attack experiments were used as the inputs. The recorded gyroscope output was linearly scaled from 1 % to 100 % in increments of 1 %, and the control data from the transmitter were the same as in the real-world experiment. Figure 10 shows the results of the simulation. Because the rotor control output was bounded between 1,150 and 1,850 in Algorithm 1, the maximum change of the rotor control output was 700. The minimum scale of the gyroscope output that could achieve the maximum change in all rotor controls was 37 % in our simulation (Figure 10).

Indoor Measurements: The standard deviation of the gyroscope output with respect to the sound noise am-

plitude was measured for the L3G4200D gyroscope of target drone A on a desk. Figure 11 shows the relative standard deviation of the gyroscope output measured at a 10 cm distance, which decreases logarithmically as the sound level decreases. Theoretically, the relationship between the sound amplitude and SPL is described by Equation 1 [27]. At the point of the reference SPL (SPL_{ref}), the amplitude of the sound noise signal is A_{ref}.

$$SPL = SPL_{ref} + 20 \log \left(\frac{A}{A_{ref}} \right) \qquad (1)$$

The relative SPL obtained by changing the amplitude is the second term in Equation 1, and it is illustrated in Figure 11, along with the measured relative standard deviations. The decreasing trend in our measurements is similar to that for the theoretical relative SPLs, but the amount of decrease in our measurements was smaller than that for the theoretical relative SPLs from the amplitude range over 70 %. This mismatch is the typical output characteristic of consumer-grade speakers at high amplitude levels, which is caused by the nonlinear distortion that also leads to the leakage of sound energy into harmonic and subharmonic frequencies.

Distance Analysis: The amplitude of the sound noise corresponding to 37 % (-8.64 dB) of the standard deviation in Figure 11 is approximately 27 %, because the standard deviation of the gyroscope output is proportional to the scale of the gyroscope output. Accordingly, the sound noise greater than 27 % in amplitude can induce the maximum changes in all rotor controls for target drone A, if the drone is tested at the same environment as that of our real-world attack.

In the real-world experiments, we changed the amplitude of the sound noise in the same environment and observed that around 30 % sound amplitude is the lower bound for making target drone A crash. The SPL measured at this 30 % sound amplitude was 108.5 dB. Using the following relationship between the distance and SPL [58], we can derive a possible attack distance of a remotely located sound source, where the reference distance (d_{ref}) and SPL (SPL_{ref}) are those measured from the real-world attack experiments.

$$SPL = SPL_{ref} - 20 \log \left(\frac{d}{d_{ref}} \right) \qquad (2)$$

According to this prediction, the possible attack distance is approximately 16.78 cm using the same sound source that we used for the real-world attack with the maximum volume (113 dB). This attack distance range might not be sufficient for a malicious attacker. However, attackers can overcome this distance limitation by using a more powerful and directional source (e.g., a loudspeaker array) than the single speaker used in our experiments. For instance, *SB-3F* [23] from *Meyersound*

can generate sound of 120 dB at 100 m, and *450XL* [21] from *LRAD* and *HyperShield* [33] from *UltraElectronics* can produce 140 dB at 1 m, which is equivalent to 108.5 dB at 37.58 m. Therefore, the possible attack distance is 37.58 m, if an attacker uses a sound source that can generate 140 dB of SPL at 1 m.

6 Discussion

In this section, we present a discussion of potential attack scenarios and countermeasures.

6.1 Potential Attack Scenarios

The attack model used in this paper seems to be too strong in two ways: 1) Use of audible sound can be easily detected, and 2) the speaker is close to the drone body. However, the more practical attack can be designed to weaken this attack model from the analysis result of this study.

First, several gyroscopes listed in Table 1 have resonant frequencies in the inaudible band (i.e., above 20 kHz). If the resonant frequency is above 20 kHz, a successful attack is possible using an ultrasonic sound generator and transducer. In addition, sound at frequencies higher than 15 kHz is difficult for humans to hear.

Second, the distance analysis shows that various remote attacks are also possible using different types of sound generators. Some of promising ways for the remote attack are described below.

Compromising the Sound Source: It is not hard to imagine drones with speakers (consider police and military operations or search-and-rescue operations). If one can compromise the source of the sound from the speaker, the effect will be the same as that of our original attack model. For example, insecurity of the Hybrid Broadcast-Broadband Television (HbbTV) standard and implementation would allow an adversary to control the TV stream [48].

Drone to Drone Attack: In 2013, Kamkar demonstrated the 'SkyJack' attack, in which an adversary drone hijacks a victim drone using a wireless denial-of-service attack [44]. A similar attack could involve following and taking a picture of a moving object, which could become a popular drone application. An adversary drone equipped with a speaker could steer itself toward a victim drone and generate a sound with the resonant frequency of the victim's gyroscope to drag it down. Of course, in this case, the resonant frequency of the adversary's gyroscope has to be different from that of the victim.

Long Range Acoustic Device: Long Range Acoustic Device (LRAD) [56] could be used as a sonic weapon [57] or Acoustic Hailing Device (AHD) [54]. Sonic weapons can cause damages to human organs

by inducing intense sound waves at certain frequencies, even if the sound source is not in contact with opponents [41, 53]. AHDs are specially designed loudspeakers that communicate over longer distances than normal loudspeakers [21, 23, 33]. In both cases, the most important requirement is a high SPL in a specific frequency band. Obviously, these technologies could be used to increase the range of our attack.

Sonic Wall/Zone: Because drones can be made small, they can be difficult to detect using radar. Therefore, it might be desirable to enforce no-fly zones for drones, as illustrated by recent drone incidents [11, 34]. One might consider building a sonic wall or a zone that radiates continuous sound noise (at various frequencies) in a specific area to enforce the no-fly zone.

6.2 Countermeasures

Several researches that have been conducted to improve the performance of MEMS gyroscopes in harsh acoustic environments are discussed below.

Physical Isolation: The simplest way to mitigate our attack is to provide physical isolation from the sound noise. This is the same concept as shielding against Electro Magnetic Interference (EMI). For example, the iPhone 5S, which is equipped with an L3G4200D gyroscope [20], would not be affected by our attack, because of the compact casing of the hardware circuit. Surrounding the gyroscope with foam would also be a simple and inexpensive countermeasure. Foam that is 1 inch thick has approximately 120 dB insertion loss in SPL [49].

Figure 12 shows the result of physical isolation experiments conducted using four different materials: a paper box, an acrylic panel, an aluminum plate, and foam. We put these materials between the sound source and the target gyroscope. The isolation performances of the different materials were not very different. Using these materials, the effect of the sound noise on one L3G4200D gyroscope was decreased to 23.78%, 16.25%, and 60.49% for the three axes.

Differential Comparator: While physical isolation is a passive approach to mitigation, use of a differential comparator is an active approach to mitigation. Using an additional gyroscope with a special structure that responds only to the resonant frequency, the application systems can cancel out the resonant output from the main gyroscope [52]. The concept of this countermeasure was introduced by Kune et al. [45] to detect and cancel out analog sensor input spoofing against CIEDs.

Resonance Tuning: In the operation of MEMS gyroscopes, the bending mentioned in Section 3.3.1 changes the capacitance between the sensing mass and the sensing electrode, and this capacitance change is sensed as the output of the gyroscope. By using an additional feed-
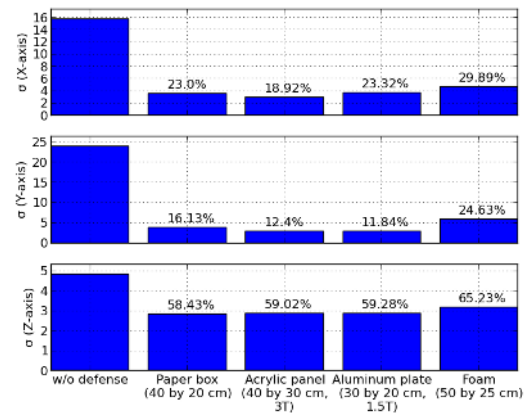

Figure 12: Physical isolation test for one L3G4200D gyroscope with four different materials (data averaged for ten identical experiments and 1,000 raw data samples collected per experiment)

back capacitor connected to the sensing electrode, the resonant frequency and the magnitude of the resonance effect can be tuned [35, 43].

These countermeasures may be used to mitigate our attack. However, physically surrounding the gyroscope sensor with certain materials could cause several problems, such as affecting other sensors or components and raising the temperature of the board. These problems may cause malfunctions of the drone control systems. In addition, use of a differential comparator with another gyroscope implies an additional cost. The resonance tuning countermeasure also has the limitation that the resonant frequency does not disappear as a result of tuning. Because the resonant frequency still exists, an attack at that frequency remains possible.

7 Conclusions and Future Work

Many sensing and actuation systems trust their measurements, and actuate according to them. Unfortunately, this trust can lead to security vulnerabilities that cause critically unintended actuations. We found that the sound channel can be used as a side channel for MEMS gyroscopes from a security point of view. In our experiment, we tested 15 kinds of MEMS gyroscopes, and seven of them were found to be vulnerable to disruption using intentional sound noise. The output of the vulnerable MEMS gyroscopes was found using a consumer-grade spaeker to fluctuate up to dozens of times as a result of sound noise.

To demonstrate the effects of this vulnerability, we implemented an attack against two target drones equipped with different kinds of vulnerable MEMS gyroscopes.

As a result of a firmware analysis of the target drones and a simulation of the flight control software output, the control signals of four rotors were found to fluctuate up to the maximum value and down to the minimum value by the injected gyroscope output. One of the target drones, which was equipped with with a small speaker, lost control and crashed in all 20 real-world attack experiments. We found in these experiments that an attacker with only 30% of the amplitude of the maximum sound noise could achieve almost the same effect at the same distance.

The countermeasures that are mentioned in the last subsection have limitations and require hardware modifications and additional materials. Because these mitigations would increase the production costs, it is necessary to develop a low-cost, software-based defense mechanism against sensor attacks for various types of embedded devices.

Some MEMS gyroscopes are integrated with accelerometers in the same IC package. In our experiments, we found that some accelerometers are also affected by high-power sound noise at certain frequencies. It would be interesting to further investigate this finding.

Acknowledgements

References

[1] A Critical Review of MEMS Gyroscopes Technology and Commercialization Status. http://invensense.com/mems/gyro/documents/whitepapers/MEMSGyroComp.pdf.

[2] Alibaba begins drone delivery trials in China. http://www.bbc.com/news/technology-31129804.

[3] Amazon Prime Air (Amazon.com, Inc.). http://www.amazon.com/b?node=8037720011.

[4] Analog Devices ADXRS610 datasheet. http://www.analog.com/media/en/technical-documentation/data-sheets/ADXRS610.pdf.

[5] AR.Drone (Parrot, Inc). http://ardrone2.parrot.com/.

[6] Arduino UNO. http://arduino.cc/.

[7] ArduPilot (open-source drone project). https://github.com/diydrones/ardupilot.

[8] Brüel & Kjær Microphone Unit Type 4189-A-021. http://www.bksv.com/Products/transducers/acoustic/microphones/microphone-cartridges/4189.

[9] Design and Analysis of MEMS Gyroscopes (Tutorial at IEEE Sensor 2013). http://ieee-sensors2013.org/sites/ieee-sensors2013.org/files/Serrano_Slides_Gyros2.pdf.

[10] Everything about STMicroelectronics' 3-axis digital MEMS gyroscopes. http://www.st.com/web/en/resource/technical/document/technical_article/DM00034730.pdf.

[11] German pirate party uses drone to crash angela merkel event. http://www.slate.com/blogs/future_tense/2013/09/18/german_pirate_party_uses_drone_to_crash_event_with_chancellor_angela_merkel.html.

[12] Hi-Vi B1S Full Range Loudspeaker. https://www.madisoundspeakerstore.com/approx-1-fullrange/hi-vi-b1s-full-range/.

[13] InvenSense IMU3000 datasheet. http://www.invensense.com/mems/gyro/documents/PS-IMU-3000A.pdf.

[14] InvenSense ITG3200 datasheet. http://www.invensense.com/mems/gyro/documents/EB-ITG-3200-00-01.1.pdf.

[15] InvenSense IXZ650 datasheet. http://invensense.com/mems/gyro/documents/PS-IXZ-0650B-00-01.pdf.

[16] InvenSense MPU3050 datasheet. http://www.invensense.com/mems/gyro/documents/PS-MPU-3000A.pdf.

[17] InvenSense MPU6000/6050 datasheet. http://www.invensense.com/mems/gyro/documents/PS-MPU-6000A-00v3.4.pdf.

[18] InvenSense MPU6500 datasheet. http://www.invensense.com/mems/gyro/documents/PS-MPU-6500A-01.pdf.

[19] InvenSense MPU9150 datasheet. http://dlnmh9ip6v2uc.cloudfront.net/datasheets/Sensors/IMU/PS-MPU-9150A.pdf.

[20] iPhone 5s Teardown. https://www.ifixit.com/Teardown/iPhone+5s+Teardown/17383.

[21] LRAD 450XL datasheet. http://www.lradx.com/wp-content/uploads/2015/05/LRAD_Datasheet_450XL.pdf.

[22] Market share information of MEMS gyroscope in 2013 (page 17). http://www.semiconwest.org/sites/semiconwest.org/files/data14/docs/SW2014_JCEloy_YoleDeveloppement_0.pdf.

[23] Meyersound SB-3F datasheet. http://www.meyersound.com/sites/default/files/sb-3f_ppi.pdf.

[24] Multiwii (open-source drone project). https://github.com/multiwii/baseflight and https://code.google.com/p/multiwii/.

[25] Murata ENC-03MB datasheet. http://www.mouser.com/catalog/specsheets/ENC-03M_ref.pdf.

[26] National Instruments USB-4431, Sound and Vibration Data Acquisition Instrument. http://www.ni.com/pdf/products/us/cat_usb4431.pdf.

[27] Relative Sound Pressure according to Amplitude. http://www.indiana.edu/~emusic/acoustics/amplitude.htm.

[28] STMicroelectronics L3G4200D datasheet. http://www.st.com/web/en/resource/technical/document/datasheet/CD00265057.pdf.

[29] STMicroelectronics L3GD20 datasheet. http://www.st.com/st-web-ui/static/active/en/resource/technical/document/datasheet/DM00036465.pdf.

[30] STMicroelectronics LPR5150AL datasheet. http://www.st.com/web/en/resource/technical/document/datasheet/CD00237211.pdf.

[31] STMicroelectronics LPY503AL datasheet. http://www.st.com/web/en/resource/technical/document/datasheet/CD00237199.pdf.

[32] STMicroelectronics LSM330 datasheet. http://www.st.com/web/en/resource/technical/document/datasheet/DM00059856.pdf.

[33] UltraElectronics HyperShield datasheet. `http://www.ultra-hyperspike.com/Data/Pages/26fa8e2abe074313d60fe15a9af35440-HyperShield_Dat_Sheet.pdf`.

[34] White house drone crash described as a u.s. workers drunken lark. `http://www.nytimes.com/2015/01/28/us/white-house-drone.html`.

[35] ADAMS, S., BERTSCH, F., SHAW, K., HARTWELL, P., MAC-DONALD, N. C., AND MOON, F. Capacitance Based Tunable Micromechanical Resonators. In *International Conference on Solid-State Sensors and Actuators* (1995).

[36] CAI, L., AND CHEN, H. On the practicality of motion based keystroke inference attack. In *Trust and Trustworthy Computing*. Springer Berlin Heidelberg, 2012.

[37] CASTRO, S., DEAN, R., ROTH, G., FLOWERS, G. T., AND GRANTHAM, B. Influence of acoustic noise on the dynamic performance of MEMS gyroscopes. In *International Mechanical Engineering Congress and Exposition* (2007), American Society of Mechanical Engineers.

[38] DEAN, R. N., CASTRO, S. T., FLOWERS, G. T., ROTH, G., AHMED, A., HODEL, A. S., GRANTHAM, B. E., BITTLE, D. A., AND BRUNSCH, J. P. A characterization of the performance of a MEMS gyroscope in acoustically harsh environments. *IEEE Transactions on Industrial Electronics 58* (2011).

[39] DEAN, R. N., FLOWERS, G. T., HODEL, A. S., ROTH, G., CASTRO, S., ZHOU, R., MOREIRA, A., AHMED, A., RIFKI, R., GRANTHAM, B. E., ET AL. On the degradation of MEMS gyroscope performance in the presence of high power acoustic noise. In *IEEE International Symposium on Industrial Electronics* (2007).

[40] DUC, N. M., AND MINH, B. Q. Your face is not your password face authentication bypassing Lenovo–Asus–Toshiba. *Black Hat Briefings* (2009).

[41] FOWLKES, J. B., AND HOLLAND, C. K. Section 4: Bioeffects in tissues with gas bodies. *Journal of ultrasound in medicine 19* (2000).

[42] GALBALLY, J., CAPPELLI, R., LUMINI, A., MALTONI, D., AND FIERREZ, J. Fake fingertip generation from a minutiae template. In *International Conference on Pattern Recognition* (2008).

[43] JEONG, C., SEOK, S., LEE, B., KIM, H., AND CHUN, K. A study on resonant frequency and Q factor tunings for MEMS vibratory gyroscopes. *Journal of Micromechanics and Microengineering 14* (2004).

[44] KAMKAR, S. SkyJack. `http://samy.pl/skyjack/`, 2013.

[45] KUNE, D. F., BACKES, J., CLARK, S. S., KRAMER, D., REYNOLDS, M., FU, K., KIM, Y., AND XU, W. Ghost talk: mitigating EMI signal injection attacks against analog sensors. In *IEEE Symposium on Security and Privacy* (2013).

[46] MATSUMOTO, T., MATSUMOTO, H., YAMADA, K., AND HOSHINO, S. Impact of artificial gummy fingers on fingerprint systems. In *Electronic Imaging* (2002), International Society for Optics and Photonics.

[47] MILUZZO, E., VARSHAVSKY, A., BALAKRISHNAN, S., AND CHOUDHURY, R. R. Tapprints: your finger taps have fingerprints. In *Proceedings of the ACM international conference on Mobile Systems, Applications, and Services* (2012).

[48] OREN, Y., AND KEROMYTIS, A. D. From the aether to the ethernet–attacking the internet using broadcast digital television. In *Proceedings of the USENIX Security Symposium* (2014).

[49] ROTH, G. Simulation of the Effects of Acoustic Noise on MEMS Gyroscopes. Master's thesis, Auburn University, 2009.

[50] SAMLAND, F., FRUTH, J., HILDEBRANDT, M., HOPPE, T., AND DITTMANN, J. AR.Drone: security threat analysis and exemplary attack to track persons. In *Society of Photo-Optical Instrumentation Engineers Conference Series* (2012).

[51] SHOUKRY, Y., MARTIN, P., TABUADA, P., AND SRIVASTAVA, M. Non-invasive spoofing attacks for anti-lock braking systems. In *Cryptographic Hardware and Embedded Systems*. Springer, 2013.

[52] SOOBRAMANEY, P. *Mitigation of the Effects of High Levels of High-Frequency Noise on MEMS Gyroscopes.* PhD thesis, Auburn University, 2013.

[53] TANDY, V., AND LAWRENCE, T. R. The ghost in the machine. *Journal of the Society for Psychical Research 62* (1998).

[54] WIKIPEDIA. Acoustic hailing device — wikipedia, the free encyclopedia, 2015. [Online; accessed 17-June-2015].

[55] WIKIPEDIA. Inertial measurement unit — wikipedia, the free encyclopedia, 2015. [Online; accessed 17-June-2015].

[56] WIKIPEDIA. Long range acoustic device — wikipedia, the free encyclopedia, 2015. [Online; accessed 17-June-2015].

[57] WIKIPEDIA. Sonic weapon — wikipedia, the free encyclopedia, 2015. [Online; accessed 17-June-2015].

[58] WIKIPEDIA. Sound pressure — wikipedia, the free encyclopedia, 2015. [Online; accessed 17-June-2015].

[59] YAN MICHALEVSKY AND DAN BONEH AND GABI NAKIBLY. Gyrophone: Recognizing speech from gyroscope signals. In *Proceedings of the USENIX Security Symposium* (2014).