`False Reality`: Uncovering Sensor-induced Human-VR Interaction Vulnerability

Yancheng Jiang
Zhejiang University
jiangyancheng@zju.edu.cn

Yan Jiang
Zhejiang University
yj98@zju.edu.cn

Ruochen Zhou
Hong Kong University of Science and Technology
zrccc@ust.hk

Yi-Chao Chen
Shanghai Jiao Tong University
yichao@sjtu.edu.cn

Xiaoyu Ji
Zhejiang University
xji@zju.edu.cn

Wenyuan Xu
Zhejiang University
wyxu@zju.edu.cn

Abstract—**Virtual Reality (VR) techniques, serving as the bridge between the real and virtual worlds, have boomed and are widely used in manufacturing, remote healthcare, gaming, etc. Specifically, VR systems offer users immersive experiences that include both perceptions and actions. Various studies have demonstrated that attackers can manipulate VR software to influence users' interactions, including perception and actions. However, such attacks typically require strong access and specialized expertise. In this paper, we are the first to present a systematic analysis of physical attacks against VR systems and introduce `False Reality`, a new attack threat to VR devices without requiring access to or modification of their software. `False Reality` disturbs VR system services by tampering with sensor measurements, and further spoofing users' perception even inducing harmful actions, e.g., inducing dizziness or causing users to crash into obstacles, by exploiting perceptual and psychological effects. We formalize these threats through an attack pathway framework and validate three representative pathways via physical experiments and user studies on five commercial VR devices. Finally, we further propose a defense prototype to mitigate such threats. Our findings shall provide valuable insights for enhancing the security and resilience of future VR systems.**

I. INTRODUCTION

Virtual Reality (VR) technology is seeing widespread adoption across a variety of domains, including immersive gaming [1], medical simulation [2], and industrial teleoperation [3]. The global VR market is projected to reach \$18 billion by 2025 [4, 5], with a user base exceeding 8.58 million worldwide [6]. As inherently human-in-the-loop systems, modern VR platforms integrate various sensors and system services to deliver immersive experiences and enable user interaction. Since user perception and behavior are driven by system outputs, ensuring the security and reliability of VR system components is essential for enabling trustworthy user interaction in immersive environments.

Prior studies [7–11] have shown that malicious VR applications or compromised software components can lead users to misperceive virtual environments, resulting in unintended behaviors such as stepping into walls or colliding with physical objects. However, these efforts primarily focus on software-level threats, often relying on privileged software access, firmware modifications, or detailed knowledge of the system internals. In contrast, sensor-level vulnerabilities remain underexplored, despite sensors forming the core interface between the physical and virtual worlds. This raises a key question: *can the integrity of sensor outputs influence the correctness of user interaction?* Given that VR responses are tightly driven by sensor data, even minor perturbations may propagate through the system pipeline and influence what users perceive and how they act.

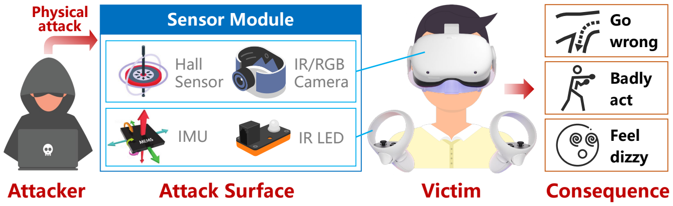


Figure 1. Illustration of `False Reality` by spoofing VR built-in sensors. Malicious signals can be injected into the VR sensors to manipulate user perception and action such that the users may feel dizzy, or go the wrong way.

In this paper, we present the first systematic exploration of sensor-induced attacks on VR systems, triggered by external physical signals. We propose a security analysis framework, `False Reality`, which demonstrates how physical signals, without requiring access to software or firmware, can propagate through sensor-service pipelines and ultimately disrupt human-VR interaction, affecting both user perception and behavior. `False Reality` models the end-to-end pathway from physical signal injection to user response, revealing how sensor-level perturbations are processed by VR system services, how immersive experiences may amplify users' psychological susceptibility, and how these factors together manifest in altered user actions. We identify and address two key challenges in realizing `False Reality`:

(1) How can physical signals disrupt VR system services? VR services are continuous, sensor-driven functions that support core operations, such as head-mounted display (HMD) localization and controller tracking, which are essential for user movement and interaction in virtual environments. While modern systems employ protections like sensor fusion and error correction, our analysis shows that carefully crafted phys-

ical signal perturbations can still bypass these mechanisms and interfere with service execution. To address this, we develop a framework that maps sensor-to-service pathways and identifies attack vectors. We focus on key sensors supporting critical services and design signals that spoof measurements and disrupt functionality. For example, we examine inertial sensors through theoretical modeling and fuzz testing, and identify specific acoustic signals that may bypass sensor filtering and interfere with measurement outputs. These signals are then refined to reliably disrupt target services.

(2) How to spoof users' perception or induce false actions? The ultimate goal of `False Reality` is to manipulate the victim's perception or induce false actions, which is challenging since users continuously interact with the virtual environment and are highly sensitive to inconsistencies in sensory feedback. To address this, we explore human perceptual and psychological effects to guide the design of attack signals. By leveraging known cognitive biases and sensory processing mechanisms, we identify disturbances that can subtly distort perception or inadvertently trigger incorrect user responses. For example, to manipulate a user's walking trajectory, an attacker can exploit the path integration deficit [12] by modulating signal intensity to remain imperceptible. To induce motion sickness, an attacker can introduce image jitter to create visual–vestibular conflict [13], provoking discomfort and behavioral disengagement.

We evaluate the effectiveness of `False Reality` through three real-world case studies across representative VR application scenarios. We design and deploy physical-signal attacks on five commercial VR systems, including two Meta Quest 2 [14] with different system versions (v60 and v50), a PICO 4 Pro [15], a Meta Quest 3 [16], and a Google Cardboard [17]. As shown in Figure 1, these attacks target user-level effects, resulting in trajectory manipulation, avatar distortion, and induced dizziness, which we evaluate through a user study involving 20 participants, capturing both system responses and user feedback. The results suggest that `False Reality` enables a new class of sensor-induced attacks, introducing a novel physical-layer threat vector that challenges existing VR security assumptions and highlights the need for broader protection strategies at the sensor level.

Our contributions are summarized as follows:

- We present the first security analysis framework for VR systems from the physical-signal-triggered attacks perspective, modeling how external signals propagate through sensors and services to influence user perception and behavior.
- We demonstrate sensor-level human-VR interaction attacks using physical signals on five commercial VR devices, revealing real-world vulnerabilities in both sensing pipelines and user perception.
- We develop a lightweight countermeasure prototype that leverages the mapping between sensor inputs and user perception, and show that multimodal feedback can enhance system robustness against physical-layer interference.

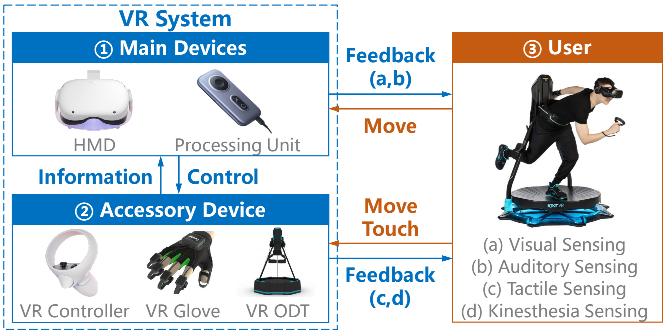


Figure 2. Illustration of a VR system. It consists of main devices (such as the HMD), accessory devices (such as the controller). The user interacts with virtual environments.

II. BACKGROUND

Virtual Reality System. As shown in Figure 2, VR system comprises two main components: main devices and accessory devices. There are numerous sensors and corresponding algorithms on the main devices and accessory devices such as shown in Figure 3.

Main devices are used for providing an immersive virtual environment for users, typically including a Head-Mounted Display (HMD) and a processing unit, e.g., a PC. An HMD generally features a 6 Degrees of Freedom (6 DoF) perception, which is enabled by the Visual-Inertial Simultaneous Localization and Mapping (VI-SLAM) algorithm, helping users stay within a safe zone to avoid collisions. To provide an immersive and comfortable experience for the users, HMDs often is equipped with an automatic interpupillary distance (IPD) adjustment system, which can optimize the alignment of the VR display with the user's eyes by moving a stepper motor [18]. The processing unit is used to render immersive virtual environments in real time.

Accessory devices are used to enhance the overall experience by providing more immersive, interactive, and comfortable interactions within environments, such as VR controllers, haptic feedback gloves, and omnidirectional treadmills (ODTs). The most common accessory device is the VR controller, which is a handheld device used to interact with the virtual world and typically includes buttons and often features motion tracking to detect the user's hand movements. To calibrate the IMU data drift of the controller, the designer often uses an IR camera on the HDM to locate the IR LEDs that are arranged in specific patterns on the controller.

Virtual Reality Sickness. VR Sickness refers to a cluster of adverse symptoms, including nausea, disorientation, and oculomotor fatigue, experienced by users during or after exposure to virtual environments [19]. VR Sickness arises from sensory conflicts between visual, vestibular, and proprioceptive systems, exacerbated by hardware limitations (e.g., latency, flicker) and content design flaws (e.g., excessive optic flow, unmatched field-of-view ratios). Although several technologies have been proposed to mitigate VR sickness, malicious attackers could still exploit these vulnerabilities by manipulating system parameters [7] or content dynamics [8] to amplify sensory incongruities, intentionally inducing or aggravating VR sickness.

Human Perceptual Threshold. Perceptual threshold refers to the minimum intensity of a stimulus that a human can detect, and it can be classified into two types:

1) Absolute threshold. This is the minimum intensity of a stimulus that can be detected 50% of the time [20]. For example, in a very quiet environment, the faintest sound you can hear represents the absolute threshold for hearing.
2) Differential threshold. Also known as the just noticeable difference (JND), it refers to the minimum change in stimulus intensity that can be perceived as different [21]. For instance, when two objects have very slight weight differences, the minimum weight difference that you can just notice is the difference threshold.

III. THREAT MODEL

Attack Goals. In this paper, an attacker aims to spoof the victim's perception in the virtual world or trigger false actions by conducting physical attacks. Specifically, we classify the attack goals into two categories as follows.

Perception Manipulation. The attacker's goal is to manipulate the victim's perception (cognitive appraisal) by conducting physical attacks and interfering with VR system services. For example, an attacker can manipulate the hall sensor's measurement to disrupt the IPD-adjustment service, causing frame shakes and thereby inducing the victim's dizziness.

Action Manipulation. It refers to an attacker inducing the victim to perform false actions by spoofing his sensory input. For example, an attacker can utilize the false visual perception to induce the victim beyond the safe boundary, potentially resulting in severe consequences such as hitting obstacles.

Attacker. We present assumptions for attackers as follows.

Attacker's Capability. Unlike traditional software-based attacks, we assume the attacker cannot modify the firmware of VR devices and cannot gain access to the software of VR. The attacker can only launch *physical signal attacks* to interfere with the VR system without accessing to the VR device.

Attacker's Knowledge. The attacker is able to know information about the victim's device, e.g., internal sensor models and the logic of VR system services. This assumption is practical as the attacker can examine detailed information online through datasheets. Furthermore, we assume the attacker can do a pre-analysis on a VR device, identical to the victim's model, before conducting attacks.

Victim. We focus on analyzing the security threats posed by the immersive experiences of VR devices. Therefore, we do not consider mixed reality (MR) devices like Microsoft Hololens, which merge virtual elements with the real world. For VR devices, a pass-through video stream would not be fed to the user when the victim remains within the VR safety boundaries. Therefore, we assume the victim is immersed in the virtual world and cannot observe the real-world scenes.

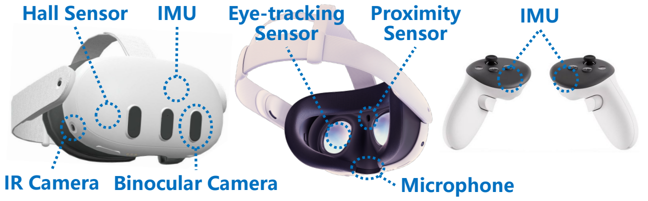


Figure 3. Illustration of embedded sensors in Meta Quest 3 VR headset and hand controllers.

IV. SYSTEMATIC SECURITY ANALYSIS

In this section, we present the security analysis framework for VR systems and first analyze the vulnerability of VR systems from sensors to human perception and actions. We illustrate a complete attack pathway as: *physical signals* → *sensor measurements* → *VR system services* → *human perception and actions*. Each subpathway will be introduced in the following sections.

A. *Physical signals→Sensor measurements* (❶)

1) *Overview.*

Sensors are essential for VR devices to perceive the environment and user status. For example, binocular cameras capture surroundings, and IMUs detect users' gestures and motions. However, these sensors are vulnerable to malicious physical signals, such as acoustic waves and laser beams. In this work, we aim to spoof the measurements of critical sensors to disrupt the integrity of the VR system's operation. Thus, the first step of `False Reality` is to highlight the threats posed by physical signals to sensor measurements.

2) *Analysis of Sensor Manipulation*

Various physical signal attacks against sensor measurements [22–25] have been studied, such as using magnetic field to manipulate hall sensors. However, these studies cannot directly be launched to this work as VR devices are highly integrated and compact packaging of multiple sensors. To interfere with sensor measurements, we need to identify the physical effects resulting from the principles of the sensor. By design, sensors are sensitive to certain physical stimuli, even if such stimuli are not intended for measurement. These stimuli are converted into measurable voltage signals through physical effects such as the photoelectric effect, the Hall effect, and resonance effects, among others. These effects ensure that at least one type of physical signal can influence the sensor. Consequently, physical signals can be maliciously exploited to manipulate the sensor's output. Types of malicious physical signals include but are not limited to, visual light, infrared light, acoustic signals, ultrasonic waves, laser light, and electromagnetic interference (EMI).

3) *Specific VR Sensor Manipulation.*

Camera. The internal circuitry of a camera can be coupled and interfered with by Intentional Electromagnetic Interference (IEMI), leading to the introduction of colored stripes [26]. Besides, adversarial infrared patches can disrupt infrared-based object detection via IR camera [27].

Hall Sensor. The feasibility of manipulating Hall sensors in solar inverters [23] and anti-lock braking systems (ABS)

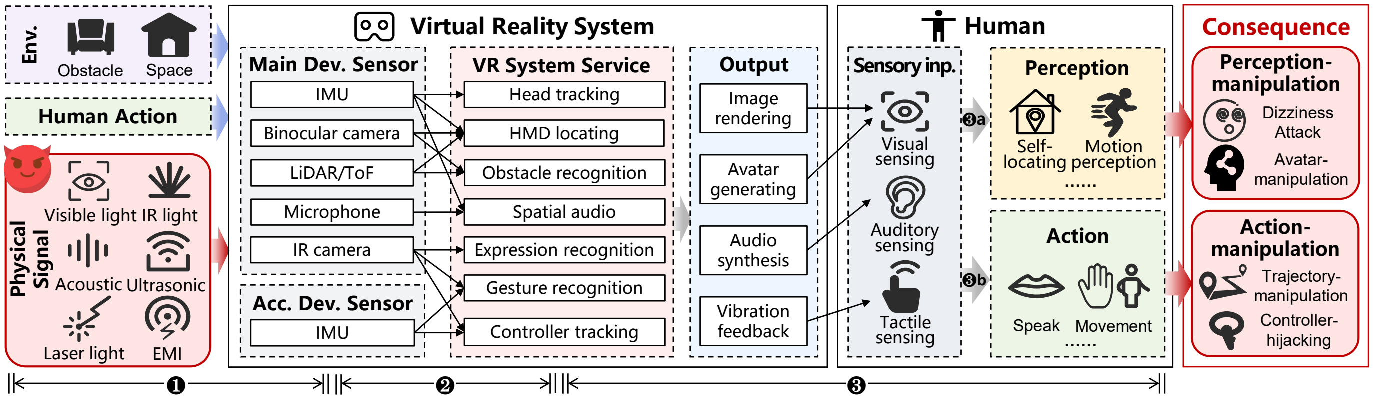


Figure 4. Illustration of security analysis framework for VR systems. Specifically, we explore a new attack pathway: Physical signals → Sensor measurements → VR system services → Human perception and actions. In practice, an attacker first injects an attack signal to spoof the sensor measurements of the VR system. Next, these false data influence critical algorithms, resulting in disturbing VR system services, e.g., HMD locating. By exploiting human perceptual and psychological effects, an attacker can manipulate the victim user's perception, e.g., inducing dizziness, and even inducing false actions, e.g., crashing into an obstacle or wall, compromising the security of users. *Note: Main Dev. Sensor* means *Sensors on main devices*. *Acc. Dev. Sensor* means *Sensors on accessory devices*.

[28] has also been demonstrated, which takes advantage of the influence of magnetic fields on the Hall effect.

IMU. Attackers can inject false data into IMUs using IEMI via electric field coupling effect [29] or ultrasonic waves via resonance effect [22, 30].

Microphone. Voice commands can be injected into microphones using light via photoelectric effect [25] or ultrasonic signals via nonlinear demodulation effect [24].

B. *Sensor measurements→VR services* (❷)

1) *Overview.*

The second stage involves disrupting VR services by exploiting false sensor measurements. Processing modules use sensor measurements to create a spatial map of the user's environment and movements, supporting services like HMD-locating and avatar-generating. Incorrect sensor data can mislead VR services. For instance, in VI-SLAM, which updates a digital map and tracks the user's position and orientation, a wrong IMU measurement can corrupt the VI-SLAM outputs, leading to inaccurate virtual representations and compromised user interactions.

2) *Analysis of VR Services Disruption.*

To disturb VR system services, we analyze the algorithms used in VR system services and identify the sensors they rely on. According to this, VR services can be classified into:

Single-sensor-based service. This type of service is typically straightforward, relying primarily on data from a single sensor. For instance, the hall sensor's output is directly sent to the IPD system. Understanding the mathematical foundations of the algorithm in service allows for the theoretical deduction of signal types that could manipulate its output. This involves analyzing the equations and logic of the algorithm and identifying potential vulnerabilities [22, 31].

Multi-sensor-correction-based service. This type of service typically involves obtaining the same data from multiple sensors and performing mutual calibration among them. For example, controller tracking obtains pose data for the controller separately through an IMU and an IR camera, and then performs mutual calibration using a Kalman filter algorithm. In such cases, an attack signal must be crafted to bypass validation mechanisms, requiring a deep understanding of how different sensor inputs interact and influence the algorithm's output. It enables building a simulation model of the algorithm. Fuzzy testing can be conducted based on this simulation model. This process involves inputting various signals to observe their effects, helping to identify which signals can successfully achieve the desired manipulation [32, 33].

Multi-sensor-fusion based service. This type of service typically involves acquiring multimodal data from multiple sensors, which are then fused using algorithms. For example, obstacle recognition acquires visual information from a camera and depth information from a ToF sensor, and the final obstacle identification is performed using a machine learning model. In such cases, gradient-based optimization methods can be employed to generate effective attack inputs. By defining the attack objective, these methods can iteratively adjust the input signals to optimize the attack's effectiveness. This approach leverages the algorithm's gradients to converge on an optimal attack signal efficiently.

3) *Specific Cases.*

HMD locating. HMD locating monitors users' head movement to adjust the virtual environment in real-time. It belongs to single-sensor-based service. IMUs help detect head movements and orientation to adjust the virtual environment. If an attacker wants to disturb head tracking service, he can target on these IMU sensors as shown in the pathway in Figure 4.

Expression recognition. Expression recognition captures the user's facial expressions and translates them into virtual avatars for more expressive interactions in VR. It belongs to single-sensor-based service. IR cameras detect facial movements and micro expressions.

Gesture recognition. Gesture recognition tracks the user's body movements to interpret gestures for intuitive interaction within the virtual environment. It belongs to multi-sensor-

Table I. Overview of `False Reality` with 3 representative cases on 5 commercial VR devices. √ indicates we can successfully launch attacks, and / means the VR device is not equipped with corresponding sensors or functions. Device i is Meta Quest 2(v60). Device ii is Meta Quest 2(v50). Device iii is PICO 4 Pro. Device iv is Meta Quest 3. Device v is Google Cardboard.

#	Cases	Signal	Sensor	VR system services	Psychological Effects	Outcome	VR devices				
							i	ii	iii	iv	v
1	Trajectory manipulation	Ultrasound	IMU	HMD location	Path integration deficit	Walk path misleading	√	√	√	√	/
2	Avatar manipulation	Ultrasound	IMU	Avatar generation	Visual dominance	Robotic arm misoperation	√	√	√	√	/
3	Dizziness attack	EMI	Hall	IPD adjustment	Visual-vestibular conflict	Motion sickness	√	√	√	√	√

fusion-based service. Cameras and IMUs on wearables track the user's body movements to interpret gestures.

Controller tracking. Controller tracking detects the position and movement of VR controllers, allowing users to interact with the virtual world through buttons and gestures. It belongs to multi-sensor-correction-based service. IMU and IR cameras track the movement and position of VR controllers.

C. VR services→Human perceptions and actions (❸)

1) Overview.

The final stage involves manipulating human perceptions and actions by disrupting VR system services. VR system services adapt the virtual environment to align with the user's actions, like updating the view based on head movements. By compromising the alignment between the virtual and real world, attackers can confuse users and induce false actions through perceptual and psychological effects.

2) Analysis of Human Perception (❸a) and Action (❸b) Spoofing.

Certain psychological effects can influence human perception. For instance, the visual-vestibular conflict effect may cause dizziness; the visual masking effect makes individuals less sensitive to the movement of objects in the environment during blinking or motion; and the auditory masking effect, where a strong pure tone can obscure weaker tones near its frequency [34]. To spoof a victim's perception, an attacker can partially modify VR service to affect sensory input and exploit human perceptual psychology effects to craft attack signals. Some psychological effects can even influence human actions, as individuals typically rely on their sensory perceptions to guide their behavior. Blind trust in sensory input may cause individuals to subconsciously make incorrect actions. This effect can be exploited by attackers. Therefore, in addition to manipulating user perception, another objective is to covertly mislead human actions, causing the victim to unknowingly perform attacker-predefined operations. For example, the visual dominance effect may lead individuals to misestimate their posture, resulting in incorrect actions, while the path integration deficit effect may cause errors in estimating their position, prompting reorientation during walking.

D. From Analysis to Case Studies

Building on the theoretical analysis of the physical-signal-driven attack pathways, we next validate our findings through real-world case studies. To this end, we select three representative VR scenarios—locomotion interactions [35], robot teleoperation [36], and immersive viewing [37]—and implement end-to-end attacks on 5 commercial VR systems. As summarized in Table I, each attack is launched by injecting crafted physical signals targeting specific sensors and associated system services, resulting in three distinct types of user-impacting effects, i.e., trajectory manipulation, avatar manipulation, and induced dizziness. Notably, all five tested VR devices exhibit varying levels of susceptibility to these attacks, indicating a class of vulnerabilities that warrants further attention from both the research community and VR system designers.

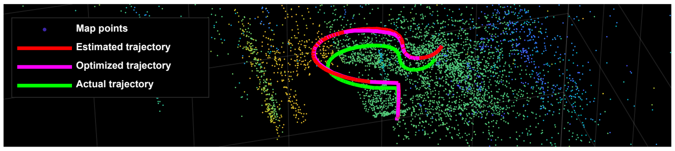


Figure 5. Simulation results of ORB-SLAM by manipulating the IMU sensor measurements. The actual trajectory (green) is deviated from the estimated and optimized trajectories.

To assess the perceptual and behavioral impact of these attacks, we further conduct a user study involving 20 participants aged 18 to 35, including 15 individuals with prior VR experience, of whom 5 self-identified as experienced users. We follow the principle of a blind testing [38], where participants are unaware of the security-related nature of the scenarios. Each participant is randomly assigned to interact with one or more of the three cases. We record system behavior and collect user feedback to evaluate the effectiveness and perceptibility of the attacks. Detailed implementation and results of each case are presented in the following sections.

V. CASE 1: TAMPERING USER'S TRAJECTORY

HMD localization is crucial for accurate and responsive rendering of the virtual world. Therefore, the first case study examines how spoofing the HMD localization service can manipulate the user's trajectory in reality while they navigate within the VR world. We summarize the attack pathway for this case as: *IMU on main device → HMD localization service → visual sensing → trajectory manipulation.*

A. Disturb HMD-locating Service (❶ + ❷)

1) Design.

VI-SLAM is a critical algorithm for VR systems to perceive the external environment, achieve virtual-real alignment, and realize HMD locating by integrating data from cameras and IMUs [39]. To prevent users from physical collisions with real-world objects, VR system designs a safe boundary based on the VI-SLAM. When a user approaches the boundary, the system would trigger a warning. Therefore, accurate sensor measurements and location are crucial for users' safety. In this work, we disclose that attackers can spoof the location by interfering with the IMU measurement. Specifically, in a VI-SLAM system, the IMU data is used to provide motion constraints between adjacent key frames and iteratively update the system's state:

$$R_j, v_j, p_j = f(R_i, v_i, p_i, \omega, a) \tag{1}$$

where R is the rotation matrix, v is the velocity, p is the displacement, ω is the angular velocity measured by the IMU, and a is the acceleration measured by the IMU. The specific iteration formula can be found in the Appendix (Equation 14) [40]. The iterative formula for R is as follows:

$$\begin{aligned} R_j &= R_i \exp\Big(\sum_{k=i}^{j-1}(\omega_k - \omega_{bias})\Delta t\Big) \\ &\approx R_i \exp(\theta_T - \omega_{bias} T) \end{aligned} \tag{2}$$

where θ_T represents the orientation angle deviation measured by the IMU at time T. According to equations 1 and 2, the variation in θ_T will affect the estimation of p.

To achieve the perturbation of the orientation angle data, recent studies have shown that IMUs are susceptible to resonant acoustic interference [22, 30]. However, a constant frequency and amplitude ultrasonic signal like Figure 7a only causes fluctuations in the IMU's ω measurement. It has minimal impact on the computed orientation angle θ_T due to data integration. To overcome this challenge, we propose a signal construction method, gradually weakening sound wave signal as shown in Figure 7b:

$$x = \left(-\frac{c}{T}t + c\right)\sin(2\pi f_b t) \tag{3}$$

where c is the maximum amplitude of the sound that the attack device can emit. T is the time for the sound to decay to zero. f_b is the resonance frequency of the IMU. The angular velocity ω caused by this ultrasonic wave is given by:

$$\omega = k\left(-\frac{c}{T}t + c\right)\sin(2\pi f_b t) \tag{4}$$

where k is the conversion factor. Subject to IMU sampling and aliasing effects, the angular velocity value observed ω_o is:

$$\begin{aligned} \omega_o &= k\left(-\frac{c}{T}t + c\right)\sin(2\pi f_o t) \\ &= k\left(-\frac{c}{T}t + c\right)\sin(2\pi |f_b - n f_s| t) \end{aligned} \tag{5}$$

where $f_o = |f_b - n f_s|$, f_s is the sampling frequency of the IMU, typically ranging from 80 to 100 Hz. n is the integer closest to f_b/f_s such that $f_o \leq f_s/2$. Integrating the angular velocity ω yields the orientation angle θ_T:

$$\begin{aligned} \theta_T &= \int_0^T \omega \mathrm{d}t = \int_0^T k\left(-\frac{c}{T}t + c\right)\sin(2\pi f_o t)\mathrm{d}t \\ &= \frac{ck}{4\pi^2 {f_o}^2 T}\sin(2\pi f_o T) - \frac{ck}{\pi f_o}\cos(2\pi f_o T) + \frac{ck}{2\pi f_o} \end{aligned} \tag{6}$$

This means that every time T elapses, the attacker can introduce a bias θ_T to the orientation angle, thereby affecting the estimation of the displacement p. Moreover, θ_T tends to increase as f_o decreases and c increases, which is shown in Figure 6.

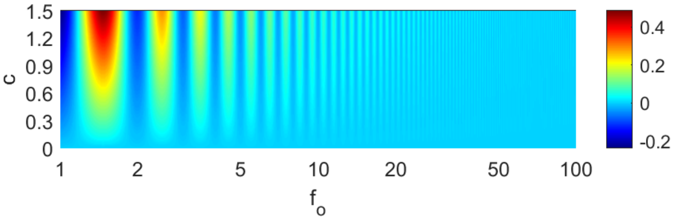
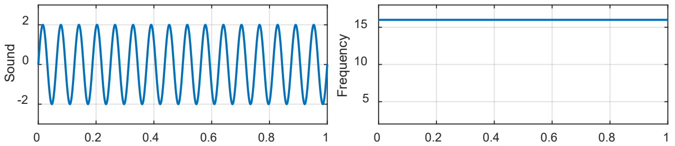
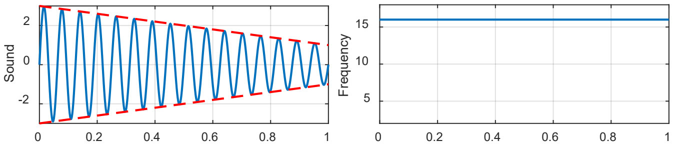


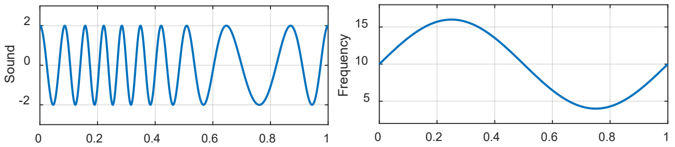
Figure 6. The relationship of θ_T with respect to f_o (Hz) and c (rad/s) as Equation 6 where $k = 1$. Warmer colors indicate higher values of θ_T.



(a) Single frequency sound



(b) The sound intensity decreases gradually



(c) Frequency of sound fluctuation

Figure 7. Illustration of attack signal for disturbing specific sensor measurements and VR system services, including interfering with IMU's measurements, changing the HMD-locating, and inducing false gestures for avatars.

2) Simulated Evaluation.

Although various VI-SLAM algorithms [39] are used in existing VR devices, the core method for locating and processing IMU data remains consistent across them, typically estimating the pose based on IMU data [41].

In this case, we assessed the attack's feasibility by conducting simulation experiments on the classic VI-SLAM algorithm (ORB-SLAM [42], VINS-Mono, Kimera-VIO), using a series of samples from the BlackBird [43] and Euroc dataset. We introduced a fluctuation noise signal defined as Equation 6 to the IMU measurement data.

The results showed that this faulty orientation angle data can cause false localization. For example, a trajectory deviation of ORB-SLAM is shown in Figure 5. for example, In the absence of attacks, the algorithm's positioning Mean Absolute Error(MAE) and Root Mean Squared Error(RMSE) are $0.149m$ and $0.110m$, respectively. However, under attack, the positioning AME and RMSE increase to $0.404m$ and $0.324m$, representing a rise of 171.14% and 194.55%, respectively.

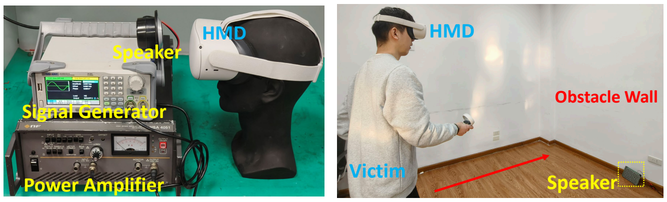
The results of a larger-scale experiment are presented in Table II. As the aliased fluctuation frequency of the IMU data decreases, the adverse effects on the accuracy of VI-SLAM algorithms become more pronounced. This observation aligns with theoretical predictions. For instance, when the IMU data fluctuation intensity is held constant, the Mean Absolute Error (MAE) and Root Mean Square Error (RMSE) values for all three algorithms exhibit a significant increase as the fluctuation frequency drops from 75Hz to 5Hz. Notably, at

Table II. Performance of the VI-SLAM algorithm under different IMU measurement fluctuations. f_s means the sampling frequency of IMU. f_o means the fluctuation frequency of measurement observed by IMU after aliasing. ω_o means the fluctuation intensity of measurement observed by IMU.

Algorithm	Dataset	f_s	f_o	5Hz		20Hz		40Hz		75Hz	
			ω_o	MAE(m)	RMSE(m)	MAE(m)	RMSE(m)	MAE(m)	RMSE(m)	MAE(m)	RMSE(m)
ORB-SLAM	BlackBird	100Hz	0 rad/s	0.149	0.110	0.149	0.110	0.149	0.110	0.149	0.110
			0.2 rad/s	**0.404**	**0.324**	0.160	0.121	0.172	0.109	0.159	0.122
			0.4 rad/s	0.369	0.296	0.156	0.119	0.154	0.117	0.169	0.128
			0.6 rad/s	0.385	0.304	0.152	0.116	0.165	0.124	0.165	0.126
			0.8 rad/s	0.341	0.270	0.158	0.122	0.170	0.127	0.167	0.128
			1.0 rad/s	0.300	0.237	0.154	0.119	0.171	0.128	0.168	0.129
VINS-Mono	BlackBird	100Hz	0 rad/s	0.168	0.190	0.168	0.190	0.168	0.190	0.168	0.190
			0.2 rad/s	0.517	0.376	0.277	0.202	0.278	0.203	0.271	0.196
			0.4 rad/s	0.620	0.453	0.277	0.202	0.280	0.205	0.274	0.200
			0.6 rad/s	0.687	0.494	0.278	0.202	0.282	0.207	0.279	0.204
			0.8 rad/s	0.699	0.515	0.279	0.203	0.284	0.208	0.284	0.208
			1.0 rad/s	**0.831**	**0.613**	0.279	0.204	0.286	0.210	0.288	0.213
Kimera-VIO	Euroc	200Hz	0 rad/s	0.161	0.103	0.161	0.103	0.161	0.103	0.161	0.103
			0.2 rad/s	0.175	0.118	0.136	0.0892	0.0938	0.0591	0.181	0.129
			0.4 rad/s	0.211	0.148	0.140	0.0871	0.217	0.153	0.1227	0.0815
			0.6 rad/s	0.223	0.181	0.119	0.0754	0.190	0.133	0.1852	0.1341
			0.8 rad/s	0.313	0.246	0.163	0.106	0.119	0.0804	0.1069	0.0714
			1.0 rad/s	**0.418**	**0.305**	0.387	0.292	0.186	0.135	0.1223	0.0793

the lowest frequency of 5Hz, the MAE and RMSE values are substantially higher compared to those at higher frequencies, indicating a greater degradation in algorithmic performance. Furthermore, the data underscores the sensitivity of different VI-SLAM algorithms to these fluctuations. VINS-Mono appears to be particularly susceptible, showing the most dramatic increases in error metrics across all fluctuation intensities and frequencies.

In summary, this empirical evidence supports the hypothesis that lower aliased fluctuation frequencies of IMU data, induced by sound wave attacks, can severely compromise the accuracy of VI-SLAM algorithms.



(a) Ultrasonic transmitter system (b) Attack scene

Figure 8. Illustration of experiment setup and attack scene. (a) Setup of sound-based trajectory-tempering attack. (b) Attack scene of trajectory-tempering.

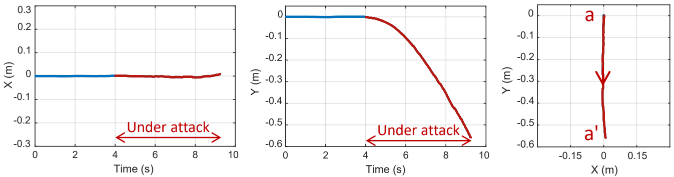
3) *Physical Evaluation.*

We also verify our analysis via physical experiments.

Setup. As shown in Figure 8a, the ultrasonic transmitter system consists of an arbitrary waveform generator (SDG6032X [44]), a power amplifier (NFHSA4051 [45]) and an ultrasonic speaker (Fostex FT17H [46], bandwidth $5kHz \sim 30kHz$) as shown in Figure 8a. The waveform generator emits the attack signal, which is amplified by the power amplifier and converted into ultrasonic waves by the speaker. The ultrasonic speaker targets on the IMU on Meta Quest 2 [14] HMD, which is mounted on a mannequin head. We utilize pyOpenvr [47] to get position data from the HMD.

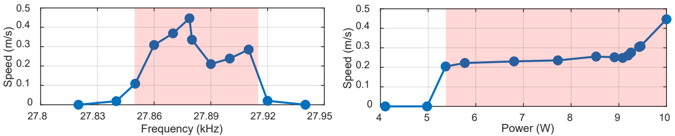
Results. Experimental results show that the ultrasonic signal (Equation 3) causes a positional retreat at a velocity of v. In addition, we evaluate how attack signal parameters—specifically frequency and amplitude—affect the attack's effectiveness, and analyze the maximum effective attack distance and average attack success rate.

- **Frequency**. Figure 10a demonstrates that the frequency of acoustic waves selectively influences the retreat velocity v (at the energy of $9.0W$). However, effective attack frequencies consistently fall within the resonance frequency range of the IMU ($f_b = 27.85kHz \sim 27.91kHz$). Attackers can manipulate the retreat velocity by adjusting the frequency of the acoustic waves used in the attack.
- **Energy**. Figure 10b illustrates that when the ultrasonic power is between $5.5W$ and $9.0W$ (at the frequency of $27.8787kHz$), the retreat velocity v is approximately $0.25m/s$, which is an appropriate velocity. As the power exceeds $9W$, the retreat velocity v begins to increase. This indicates that attackers can achieve the attack without emitting high-power signals.
- **Distance**. Furthermore, the placement and mounting method of the IMU inside the HMD determines the attacker's capability to launch attacks from different angles. Figure 11a demonstrates that launching an attack from a position 45° to the left side of the HMD is the most feasible. The attack distance can reach up to $2.2m$. In contrast, launching an attack from directly below the HMD results in a shorter attack distance of only $1.0m$.
- **Success rate**. We tested the success rate of attacks on multiple VR devices under the optimal attack parameters, as shown in Table III. The average success rate was 85%.



(a) X-axis coordinate (b) Y-axis coordinate (c) Location

Figure 9. Illustration of IMU's measurements and locating results in the virtual environment. The attack can effectively induce errors for VI-SLAM, leading to an offset along y-axis (a → a').



(a) Ultrasonic frequency (b) Ultrasonic power

Figure 10. Illustration of the frequency and intensity response of the ultrasound to the movement speed. (a) The frequency response shows the frequency near the IMU's resonant frequency can induce significant movement in the VR environment. (b) When the ultrasound energy is over $5.5W$, an attacker can effectively induce false speed.

B. *Misleading Move Action: Redirect Walking* (❸)

1) *Design.*

People can accurately estimate their instantaneous state of motion but are much poorer at perceiving their overall motion path. Therefore, users tend to compensate for small inconsistencies while walking unconsciously [12], which is called path-integration-deficit effect. Attackers can manipulate the visual motion path, causing victims to subconsciously adjust their movements. For instance, shortening the visual feedback of walking distance may lead victims to walk farther to correct the perceived inconsistency. When the user's movement speed in the virtual environment decreases by 10%, the user's speed in the real space will unconsciously increase by 10% to compensate for this reduction. This means that when the user walks forward, the distance traveled in the real space will be 110% of that in the virtual environment. This results in significant discrepancies between the virtual and real worlds, which may lead to the user colliding with obstacles or walls in real worlds.

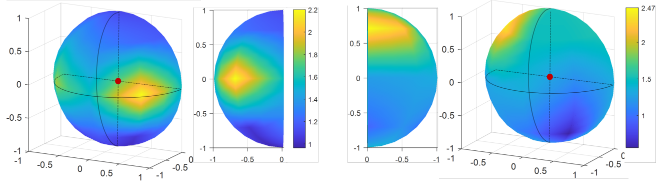
2) *Evaluation.*

In this evaluation, we aim to create a mismatch between the virtual and real worlds and spoof the victim to step out of the safety boundary [48], which is used to ensure the user stays within a safe zone as shown in Figure 27.

Setup. As shown in Figure 8b, a victim is playing with a VR device while a malicious speaker is hiding nearby. We do not need to keep the attack device continuously aimed at the victim's HMD. It only needs to be aimed for a short period. Because once a locating bias is created during that time, the bias will persist. As a result, the victim may unknowingly crash his head into an obstacle wall due to the position bias. Note that the attacker can extend the attack range by increasing the power of the speaker. To ensure safety, we experimented in a flat area, marking a safe zone ($2.25m \times 0.40m$) and a dangerous zone ($0.65m \times 0.40m$) to simulate obstacles. During the attack, the virtual environment moves forward relative to the user, shifting the VR system's safety boundary. Participants started at a designated point and were instructed to walk quickly to reach a virtual target point near the safety boundary's edge as shown in Figure 28. We conduct experiments based on the setup described above with 15 person-times. Their additional walking distance, compared to the normal distance (2.25m), was recorded.

Table III. Success rate of disturbing VR services on several devices. / means the VR device is not equipped with this service. (i) Meta Quest 2 (v60), (ii) Meta Quest 2 (v50), (iii) PICO 4 Pro, (iv) Meta Quest 3, (v) Google Cardboard.

Case	Disturbed Service	i	ii	iii	iv	v
1	HMD-locating	19/20	18/20	16/20	15/20	/
2	Avatar-generating	18/20	15/20	20/20	17/20	/
3	Display	20/20	20/20	19/20	19/20	20/20



(a) HMD (b) Right controller

Figure 11. Illustration of maximum attack distances in multi-directions. The red dots represent the location of test devices. Yellow represents a greater distance, while blue indicates a shorter distance. Unit: meter. (a) We can interfere with HMD up to $2.2m$. (b) We can interfere with the right controller up to $2.47m$.

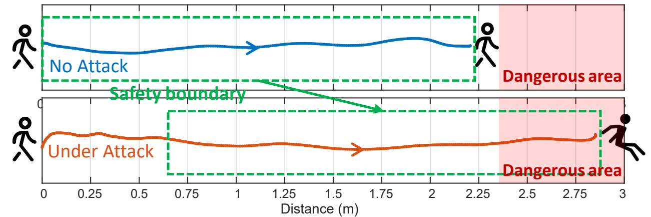
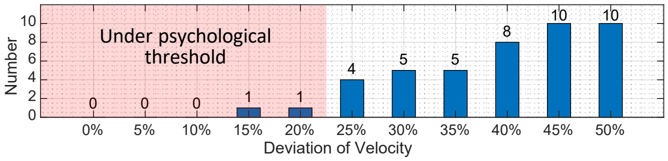


Figure 12. Walking trajectory of the victim normally (blue wave) and under the trajectory-tempering attack (orange wave). Results show that the attack can successfully shift the virtual VR safety boundary (green dashed box), causing the victim to step outside the actual safe zone in the real world with an additional.

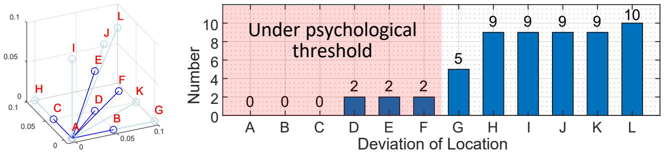
Results. The average distance they walked beyond the safety boundary was $0.597m$. This occurs because, when fully immersed in the virtual environment, users fail to notice subtle shifts in the relative positioning of the virtual space and safety boundary. Furthermore, the false safety boundary fails the warning systems of VR devices. One of the recorded walking trajectories of participants w/o attacks is shown as solid lines in Figure 12, where green dashed boxes represent the safety boundaries of VR systems. The below figure of Figure 12 demonstrates that `False Reality` causes a shift of the safety boundary and induces participants to move into dangerous areas, like hitting the wall, as shown in Figure 8b.

3) *Stealthiness Discussion.*

Although the attacker can change the victim's position in the virtual world, the movement speed must not be too fast, or the victim will easily notice. If the user's actual forward speed is v_t and the attack causes a backward speed of v_a,



(a) Simulation evaluation on Redirected Walking



(b) Simulation evaluation on Relocated Hand-moving

Figure 13. Results of the simulation evaluation on (a) Redirected Walking and (b) Relocated Hand-moving. When the deviation is within the psychological thresholds (the pink zone), users are generally unaware of the attack. *Note*: *Number* means *the number of users who are aware of attacks*.

the perceived visual speed will be $v_t - v_a$. We would like to determine the range of v_a within which it is difficult for the victim to detect.

Setup. We developed a Unity-based VR software called "TrajOffset", which includes a VR virtual room. We applied a bias to the self-locating results using the Unity VR API. For example, if the correct self-locating result is (x, y, z), we modify it to (kx, ky, z), where $k \in [0, 1]$. k can be dynamically adjusted by the researchers. Before starting, participants were informed that our study focused on perception and performance in virtual reality. It was emphasized that it was crucial for us to know if they noticed any anomalies in the VR experience. They were instructed to report any unusual occurrences immediately. We provided them with three examples of events they might report: dizziness, issues with the VR display, or feeling that their position in the virtual environment seemed incorrect. The researchers gradually decreased k from 1, as shown in Figure 13a, until the participants reported feeling that their position in the virtual environment was incorrect. Finally, we recorded the number of participants who detected anomalies at each level of offset. We recruited 10 volunteers who were familiar with VR to carry out the experiment.

Results. As shown in Figure 13a, when the virtual speed was only 80% of the actual speed, i.e., $k = 0.8$, only 1 participant detected the anomaly. It means that the attack will be unnoticeable in most cases if $\frac{v_a}{v_t} < 0.2$. A normal walking speed for humans is about $1.35m/s$ [49], which means v_a should be kept below $0.27m/s$. Our attack capability can meet this requirement.

VI. CASE 2: ALTERING AVATAR-BASED ROBOTIC OPERATION

The second representative case is altering the avatar-based robot's operation. Unlike Case 1 in Section V, which targets vulnerabilities in the main device, this case explores vulnerabilities of accessory devices. The attack pathway of this case is identified as: *IMU on the accessory device* → *avatar-generating service* → *visual sensing* → *avatar manipulation*.

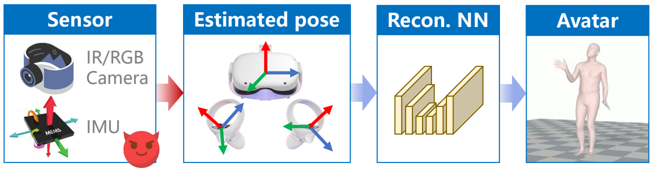


Figure 14. Illustration of the pipeline of avatar-generating service. Sensor measurement is used to estimate pose and then reconstructed to avatar by neural network. *Note*: *Recon.* means *reconstruct*.

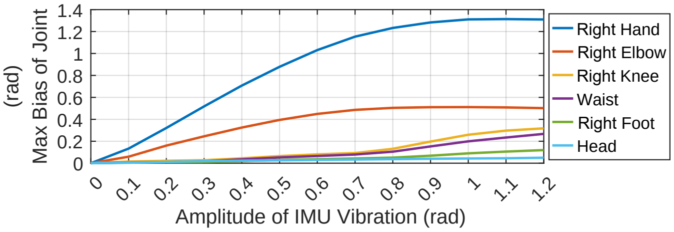


Figure 15. Evaluation of the relationship between the interference on IMU of the right controller and the position offset of joints of avatars in VR systems. The results show that the attacker can interfere with the IMU sensor of the controller to change the avatar's gesture.

To further demonstrate the attack's feasibility, we achieved an extended attack range of up to $2.47m$.

A. Disturb Avatar-generating Service (❶ + ❷)

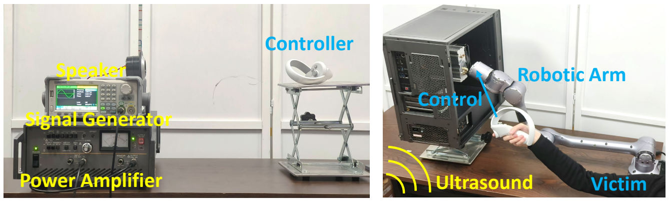
Avatars, digital representations of users in a virtual environment, serve as a bridge between the physical user and the virtual world. By leveraging sensors to capture body, hand, and head movements, VR systems enable avatars to replicate these actions in real time, extending their functionality to control physical humanoid robots or robotic arms for tasks such as maintenance and production in the manufacturing industry [3, 50], remote surgeries [51]. Thus, precise control signals to avatars are critical to physical downstream systems being controlled.

1) Design.

Avatars are typically reconstructed in real-time using motion data from VR sensors (e.g., IMUs, cameras) processed by deep neural networks as shown in Figure 14, such as the open-source *AvatarJLM* model by *ByteDance, PICO* [52]. *AvatarJLM* first estimates arm and head pose using sensor data from HMD and controllers, then reconstructs the avatar with a neural network. Thus, sensor errors can impair the avatar's reconstruction accuracy.

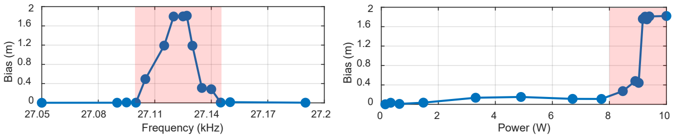
To explore effective attack signals, we first conduct fuzz testing in the digital domain to evaluate the effect of erroneous input arm pose data on model reconstruction. Since human posture is determined by various joint angles [53], we use joint angle changes, e.g., hand, elbow, and wrist, to assess the posture deviation. In practice, we feed arm pose data overlaid with crafted sinusoidal wave to the avatar reconstruction model. The results in Figure 15 demonstrate that: 1) Faulty pose data can impact the avatar's joint angles; 2) Increasing attack amplitude leads to greater changes in joint angles.

The next step is injecting noises into the arm pose data by conducting physical attacks. To achieve this, we exploit the ultrasonic resonance effect of IMU sensors [22, 30] to inject



(a) Sound-based attack setup (b) Attack scene

Figure 16. Illustration of experiment setup and attack scene. (a) Setup of sound-based avatar-manipulation attack. (b) Attack scene.



(a) Ultrasonic frequency (b) Ultrasonic power

Figure 17. Evaluation of the impact of ultrasound frequency and energy on controller's pose changes. The results show that when the frequency is near the resonant frequency of the IMU and the power of the ultrasound signal is above $9.5W$, the attacker can induce significant displacement.

false measurements. Typically, the estimation of arm pose does not rely solely on IMU data. For example, in the PICO 4 Pro [15], the Error-State Kalman Filter (ESKF) algorithm [54] fuses both IMU data (sampling rate $f_{IMU} = 500Hz$) and infrared vision locating data (sampling rate $f_{camera} = 30Hz$). The error state measurement updating can be represented by Equation 7 which fuses infrared vision positioning data.

$$\begin{aligned} \delta\hat{\mathrm{X}}_{\mathrm{k+1}} &= \mathrm{K}\left(\mathrm{Y}_{\mathrm{k+1}} - \mathrm{h}\left(\hat{\mathrm{X}}_{\mathrm{t,k+1}}\right)\right) \\ \mathrm{X}_{\mathrm{k+1}} &= \hat{\mathrm{X}}_{\mathrm{k+1}} + \delta\hat{\mathrm{X}}_{\mathrm{k+1}} \end{aligned} \tag{7}$$

where $\delta\hat{\mathrm{X}}_{\mathrm{k+1}}$ represents the estimation of error, K is the Kalman gain, $\mathrm{Y}_{\mathrm{k+1}}$ is the infrared vision locating data, $\mathrm{h}(\hat{\mathrm{X}}_{\mathrm{t,k+1}})$ is the IMU measurement data, $\hat{\mathrm{X}}_{\mathrm{k+1}}$ is the estimated value of the nominal state, and $\mathrm{X}_{\mathrm{k+1}}$ is the final output measurement value.

To bypass the correction for IMU measurement by infrared vision locating, attackers should carefully select the ultrasound frequency. We first identify the IMU's resonant frequency f_r and bandwidth f_w. Ultrasound with frequencies of $[f_r - \frac{1}{2}f_w, f_r + \frac{1}{2}f_w]$ can interfere with the IMU. The attacker chooses a frequency $f_a = 500m + 30n$ within this range, where $n \leq 16$ and m, n are positive integers. Given that $f_a \mod f_{IMU} = 30n$, the IMU will output a sinusoidal wave at $30n$ due to aliasing. Since $30n \mod f_{camera} = 0$, the IMU's sinusoidal wave phase will align with each measurement updating, allowing for fine-tuning of the phase to ensure alignment with zero during each update. Thus, the sinusoidal signal is sampled to values nearly identical to the IR locating data, producing minimal error. After multiple updates, the system's trust in future measurements decreases (lowering K), leading to greater reliance on IMU data. Thus, when the ultrasound induces resonance in the IMU, it can bypass fusion with visual data, enabling manipulation of arm pose.

2) Evaluation.

Setup. We use the attack setup as introduced in Section V-A, but replace the HMD with the right controller of PICO 4 Pro. We focus on the pose changes of the avatar's right hand reconstructed by the model in PICO 4 Pro. Because this is crucial for the injection of hand movements.

Results. We employ a scanning strategy to evaluate the overall performance from signal injection to the final output. Our objective is to determine the optimal frequency and angle for the attack, as well as to identify the minimum power and maximum distance required for the attack to be effective.

- **Frequency.** An ultrasonic signal with a power of 10W and bandwidth of $20kHz \sim 30kHz$ is injected into the IMU. As shown in Figure 17a, the frequency range of $27.10kHz$ to $27.15kHz$ is suitable for the attack frequency, with the optimal frequency being $27.125kHz$.
- **Energy.** We varied the energy of the ultrasonic signal within the range of $0W$ to $10W$ and recorded the responses. Figure 17b indicates that the stronger the ultrasonic signal, the greater its ability to change pose.
- **Angle.** Figure 11b indicates that it is the most effective to launch attack from the upper right at a 45° angle on the right controller. The attack distance can reach up to $2.47m$. In contrast, the attack launched from the lower left at a 45° angle has an attack distance of only $0.55m$. This is because the IMU is installed in the upper right of the controller.
- **Success rate**. We tested the success rate of attacks on multiple VR devices under the optimal attack parameters, as shown in Table III. The average success rate was 87.5%.

B. Spoof Human Perception: Relocate Hand Movement (❸)

1) Design.

There is a discrepancy between human visual and proprioceptive senses. When identifying the position of one's own hand, the weight of reliance on visual information is higher than on proprioceptive information. When there is a discrepancy between the two, people instinctively trust visual signals over vestibular signals [55]. It is called Visual-dominance effect. In the context of controlling a robotic arm via VR devices, the accuracy of the end-effector's motion trajectory is particularly critical. An incorrect trajectory of the end-effector could result in the failure of medical procedures or industrial production accidents. Therefore, in this subsection, we aim to control the avatar-based robotic arm. To achieve this, we explore humans' insensitivity to differences between visual and proprioceptive inputs to launch the attack. As shown in Figure 17a, we can adjust the attack frequency to control the trajectory offset. For instance, when the attack frequency is $27.102kHz$, the offset distance is approximately $0.09m$. Additionally, it is better to ensure the offset to be increased gradually than abruptly in practice, since abrupt visual onsets are particularly effective in capturing human attention [56]. To achieve this, we sweep the attack signal from the inflection frequency $f_0 = 27.100kHz$ to the target attack frequency $f_a = 27.102kHz$ over a larger period $T = 1s$ as shown in Figure 7c. The mathematical expression for this signal is

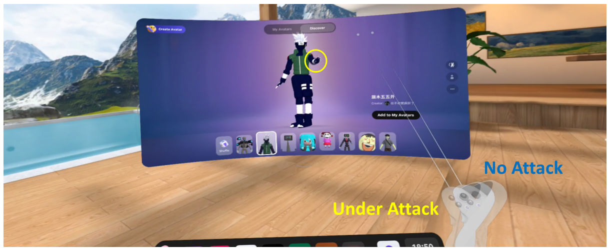


Figure 18. Results of manipulating avatar on PICO 4 Pro. An offset is induced for the avatar by emitting ultrasound.

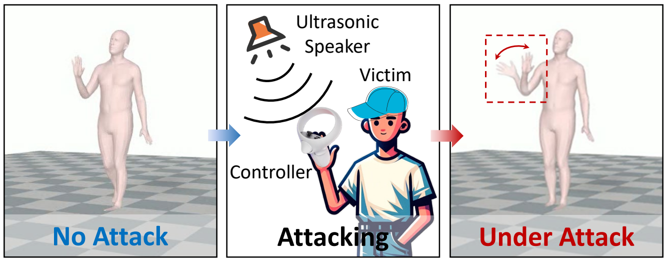


Figure 19. Simulated evaluation of Case 2 on *AvatarJLM* model. Specifically, we alter the IMU data of the right controller with false data, inducing false gestures for the avatar in the VR systems.

expressed as:

$$\begin{aligned} x &= A\cos(2\pi F(t))A = \cos(2\pi \int_0^t f(t)) \\ f(t) &= (f_a - f_0)\,\frac{\sin\left(\frac{2\pi}{T}t\right)+1}{2} + f_0 \end{aligned} \tag{8}$$

2) Simulated Evaluation.

We use *AvatarJLM* model as the test subject and selected 50 data samples from AMASS [57] dataset for digital verification. We then superimposed sinusoidal vibrations onto the y-axis and z-axis IMU data. The experimental result for one of the data samples is shown in Figure 19, where the virtual hand of the avatar begins to sway left and right after being reconstructed by the *AvatarJLM* model. The results indicate that 100% of the data samples exhibited reconstruction errors under attack.

3) Physical Evaluation.

The setup is shown in Figure 16b. The pose data collected by the PICO 4 Pro is sent to a processing computer that converts the data into the coordinate system of the robotic arm. Using the inverse kinematics of the robotic arm (Unitree Z1 [58]), it calculates the rotation angles for each motor. The processing computer then sends these angle commands to the robotic arm, which moves to the specified position accordingly. During the experiments, volunteers are instructed to wear a PICO 4 and hold the VR controller. Then, they are required to operate an arm motion such as a fencing motion, i.e., moving in a straight line from point A to point B. Then, the robotic arm will move back to front according to the motion changes of the VR controller. The attacker places the ultrasonic speaker approximately $50cm$ from the user's controller to initiate the attack at critical moments, such as during chip welding or surgical organ removal. We conducted an experiment with 15 trials using the setup described above and recorded the trajectory of the robotic arm to determine whether it was successfully hijacked.

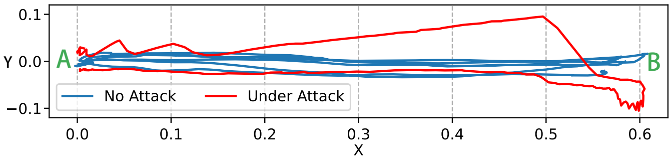


Figure 20. The volunteer was instructed to hold the VR controller, move as quickly as possible from point A to point B directly ahead, and repeat this movement multiple times. The blue line represents the motion trajectory without attack, approximately following a straight line. The red line represents the motion trajectory under attack, where a deviation is observed along the Y-axis (left-right direction).

Results. The gesture and trajectory outcomes of the tested avatar arm are illustrated in Figure 18 and Figure 20. A clear deviation along the Y-axis (left–right direction) is observed in the trajectory, indicating that the attacker successfully hijacked the avatar's pose data, thereby spoofing the robotic arm's movements. Imagine if this robotic arm were used in remote surgery—even a slight deviation could lead to a fatal accident. Additionally, the attacker successfully introduced a bias to the robotic arm's end effector with an average displacement distance of $0.626m$ and an attack success rate of 100%.

4) Stealthiness Discussion.

Although an attacker can alter the position of the controller in the virtual environment, the displacement cannot be too large, as this would make it easily detectable by the victim. We aim to determine the range of displacement that is less likely to be noticed by the victim.

Setup. We introduced a displacement in the displayed position of the controller by *Unity SDK*. Specifically, we developed a Unity-based VR software called "CtrOffset", which includes a VR virtual room. We applied an offset to the controller's locating results through the Unity VR API. For example, if the correct controller position is (x, y, z), we modified it to $(x+\alpha, y+\beta, z+\gamma)$. α, β, γ can be dynamically adjusted by the researchers. Each participant wore a Meta Quest 2 HMD and held the controllers in both hands. The HMD presented a virtual room where the positions of the controllers were rendered as virtual hands. Participants were instructed to freely move around in this virtual space, including walking and waving the controllers. Before starting, participants were informed that our study focused on perception and performance in virtual reality. It was emphasized that it was crucial for us to know if they noticed any anomalies in the VR experience. They were instructed to report any unusual occurrences immediately. We provided them with three examples of events they might report: dizziness, issues with the VR display, or the virtual hand appearing to deviate from the actual position of their hand. Researchers gradually increased the offset of the virtual hand (including both distance and direction) from 0, as shown in Figure 13b, until participants reported that the virtual hand appeared to deviate from the position of their actual hand. Finally, we recorded the number of participants who detected anomalies at each level of offset. We recruited 10 volunteers who were familiar with VR to experiment.

Results As shown in Figure 13b, when the displacement

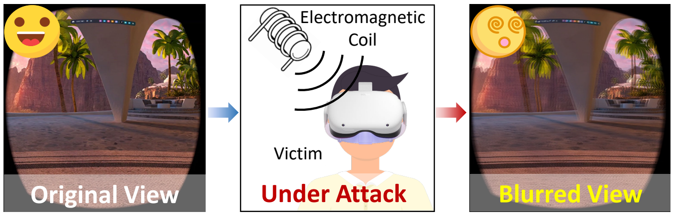
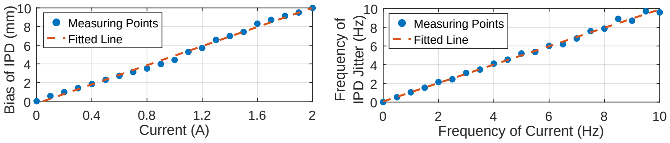


Figure 21. Illustration of dizziness attack. The results show that electromagnet-based attacks can effectively blur images in the VR systems, making users feel dizzy.



(a) Current Intensity (b) Current Frequency

Figure 22. The impact of (a) current intensity and the (b) current frequency of the electromagnet on the interpupillary distance (IPD) offset of HMD. The results show the IPD offset is proportional to the current intensity and frequency.

was less than $0.09m$, only 2 participants detected the anomaly. This indicates that an attacker only needs to ensure the displacement is less than $0.09m$ to maintain stealth.

VII. CASE 3: INDUCING DIZZINESS FOR USERS

The third case targets human perception by inducing dizziness in users. The identified attack pathway is: *Hall sensor on the main device → Display service → visual sensing → dizziness*. This case is presented in two steps: disrupting display service and causing dizziness for users.

A. Disturb Display Service (❶ + ❷)

1) Design.

Vision is the most critical sensory modality for an immersive experience in VR [59]. Users continuously focus on the HMD screen, making any display anomalies likely to cause discomfort. To enhance the user experience, VR HMDs automatically adjust the distance between the left and right displays using a stepper motor, based on the user's interpupillary distance (IPD). A Hall sensor detects the display's position and then feeds the distance between the two displays back to the system to adjust the display image. To explore effective attack signals, recent research suggests that Hall sensor outputs can be manipulated by injecting a specifically designed magnetic field [23, 28], such as a time-varying sinusoidal magnetic field produced by an electromagnet. This will result in changes of position to the HMD display image.

2) Evaluation.

Setup. As shown in Figure 21, we use the magnetic transmitter system as the attack device, which consists of an arbitrary waveform generator (SDG6032X [44]), a power amplifier (NFHSA4051 [45]) and a 1000-turn coil with a core. The power amplifier applies an AC voltage to the coil, generating a magnetic field proportional to the current intensity. The coil is placed near the HMD, and a specific current is used to produce the desired magnetic field.

Results. We evaluated the IPD deviation under different current intensities, and the results are shown in Figure 22a. The IPD bias is roughly proportional to the excitation current. At an excitation current of $2A$, the IPD bias peaks at $10mm$, reducing the IPD from $68mm$ to $58mm$—the maximum and minimum settings of the Meta Quest 2, respectively.

B. Spoof Human Perception: Causing Dizziness (❸)

1) Design.

The motion sickness [13] is caused by the perceptual conflicts between human visual and vestibular inputs. Thus, an attacker can induce motion sickness by interfering with the IPD auto-adjustment system, leading to dizziness, nausea, and headaches [60, 61]. Since the bias of IPD is proportional to the instantaneous current intensity, a low-frequency alternating current can be used to generate a low-frequency alternating magnetic field, causing low-frequency jitter in the IPD.

$$\left.\begin{aligned} bias_{IPD} &= kI_{coil} \\ I_{coil} &= A\sin(2\pi f_I t) \end{aligned}\right\} \Rightarrow bias_{IPD} = kA\sin(2\pi f_I t) \tag{9}$$

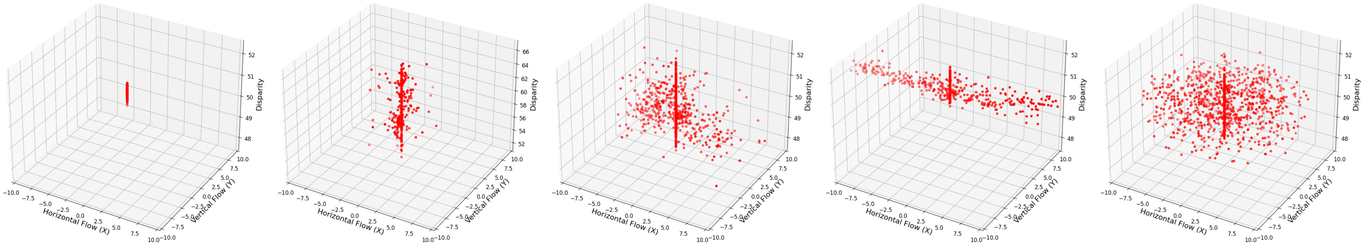
Moreover, the frequency of the IPD jitter is approximately equal to the current frequency as shown in Figure 22b. An attacker can control the frequency of the current to maintain the image jitter frequency that easily induces dizziness like $0.5Hz$ [62, 63]. By applying a dynamically changing sinusoidal magnetic field to the central part of the VR headset, specifically where the Hall sensor is located, we continuously alter the IPD. This manipulation leads to persistent screen jitter as illustrated in Figure 21.

2) Simulated Evaluation.

Existing research indicates that several factors contribute to the onset of VR sickness, including horizontal optical flow speed, vertical optical flow speed, and disparity [64]. Regarding horizontal flow speed, higher speeds are associated with an increased risk of motion sickness. As for vertical flow speed, while it may exacerbate VR sickness, its impact depends on the specific context. In terms of disparity, motion in the distant background (small disparity) is more likely to induce sickness compared to motion in the foreground (large disparity). Among these factors, horizontal flow speed is the most direct and significant contributor.

Setup. We used Android Debug Bridge (ADB) [65] and scrcpy [66] tools to capture binocular footage from the Quest 2 in five different scenarios. The average horizontal optical flow speed, vertical optical flow speed, and disparity for each frame were computed using OpenCV [67], and these values were plotted on a three-dimensional coordinate system, as shown in Figure 23. Based on the aforementioned findings, the greater the dispersion of the coordinate points in the cloud, the higher the likelihood of inducing dizziness, particularly along the x-axis (horizontal flow speed) direction.

Results. Figure 23a shows that when the user remains stationary, horizontal and vertical flow speeds are zero, resulting in a minimal risk of dizziness. Figure 23b illustrates that when the user appreciates virtual scenery (with small head movements), horizontal and vertical flow speeds remain within a small range, making dizziness unlikely. Figure 23c



(a) Keep Still (b) Appreciate Scene (c) Play Game (d) Magnetometric Attack (e) Ultrasonic Attack

Figure 23. The distribution maps of the three-dimensional indicators *(horizontal flow, vertical flow, disparity)* in different scenarios (Case 3). A larger absolute value of flow and a smaller disparity are associated with a higher risk of dizziness. Scenarios with more dispersed point clouds are more likely to induce dizziness. (a) The user remains stationary. (b) The user is immersed in the appreciation of the virtual scenery. (c) The user is engaging in the roller-coaster game, which is prone to inducing motion sickness. (d) Malicious magnetic signals cause fluctuations in the IPD. (e) Malicious ultrasonic waves cause drifting of the VR display.

demonstrates that when the user engages in games that are prone to inducing dizziness (such as roller-coaster games), both horizontal and vertical flow speeds may reach higher values. Figure 23e shows that when we initiate a Magnetometric Dizziness Attack, the horizontal flow speed increases significantly, even surpassing that of the roller-coaster game, which elevates the risk of dizziness.

3) Physical Evaluation.

We recruited 15 participants for the experiment, each wearing a Meta Quest 2 HMD. During the attack, the display exhibited shaking due to the injected physical signals. Participants rated their discomfort on a four-point dizziness scale: 3 (severe dizziness), 2 (moderate dizziness), 1 (mild discomfort), and 0 (no discomfort). The average reported dizziness level was 1.67, suggesting that the physical-signal attack induces a noticeable degree of visual discomfort.

VIII. DISCUSSION

A. Countermeasures

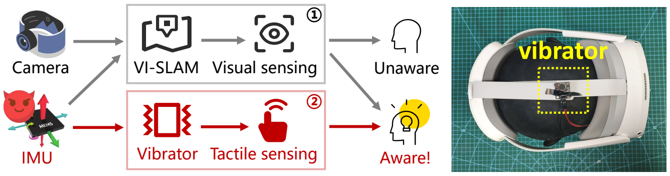
`False Reality` poses a significant risk to mainstream VR devices, enabling attackers to bypass security boundaries and execute malicious operations. To address this threat, we propose potential countermeasures focused on abnormal signal detection and perceptual fusion.

1) Abnormal Signal Detection.

We propose a software-based detection method that leverages the characteristic changes in sensor values to distinguish between normal and attack signals. Attack signals often follow specific patterns due to the constraints of attack conditions. For example, ultrasound-injected IMU data typically exhibits sinusoidal waveforms. Additionally, one sensor's data can often be correlated with another sensor's data in VR systems [68]. For instance, IMU angular data from the HMD should correlate positively with camera-captured optical flow changes. Based on these observations, we suggest training a classifier network to detect tampered sensor data.

2) Human Perceptual Fusion.

Principle. We propose a potential countermeasure based on human perceptual fusion. We observed that a critical factor enabling `False Reality` attack is the VR system's reliance on a single sensory modality. For example, in HMD-locating service, VR systems typically deliver visual information to the user solely through the display as shown in path① of Figure 24a. It is easy for attackers to exploit vulnerabilities in human visual perception. We propose that integrating multimodal feedback can significantly increase the difficulty for attackers. Exploiting multiple sensory modalities simultaneously is challenging for attackers, as their ability to inject manipulative signals across different senses is limited.



(a) Principle (b) Setup

Figure 24. Prototype of the human-perceptual-fusion-based countermeasure. (a) Principle: The system padditionally rovides vibration sensing (b) Setup: A cheap vibrator is added to receive the IMU's measurements in practice.

Table IV. Performance of *Human Perceptual Fusion*.

Volunteer	Without Vibration		With Vibration	
	Immersion	Defense	Immersion	Defense
Mean	2.8	1.8	**2.6**	**3.2** ↑

Note: *Immersion Scoring*: 4-Highly immersive, almost like reality. 3-Good immersion, but with some differences. 2-Average immersion, no noticeable issues (e.g., vibrations). 1-No immersion. *Defense Scoring*: 4-Excellent defense, abnormalities reported $< 10s$. 3-Good defense, abnormalities reported $< 60s$. 2-Average defense, abnormalities reported $< 300s$. 1-Poor defense, no abnormalities reported.

Prototype. As shown in Figure 24b, we integrated a vibration module into the HMD-locating service, which vibrates in sync with the IMU data. This provides the user with tactile feedback as shown in path② of Figure 24a. The vibration intensity increases with the z-axis velocity of IMU, which can be calculated using the following equation.

$$V = (1 - e^{-|v_z|})V_{max} \tag{10}$$

where, V represents the vibration amplitude of the module, v_{max} is the maximum vibration amplitude, and v_z is the z-axis velocity detected by the IMU. This approach involves adding a low-cost vibration module (around \$1) and a simple algorithm with minimal computational overhead. Under normal VR use, the user's head movement along the z-axis is minimal, so the vibration module remains largely inactive. However, when under ultrasonic attack, significant fluctuations of velocity in the z-axis cause the module to vibrate intensely. Since this intense vibration doesn't match the user's actual movements, it alerts the user to an anomaly, potentially indicating an attack.

Evaluation. We conduct a user-participatory evaluation to assess the effectiveness and usability of the proposed approach. Specifically, we recruited five volunteers who were familiar with VR devices but had never worn one. They were first asked to wear a headset without vibration feedback, followed by one with vibration feedback. In both attack and non-attack conditions, they were asked to evaluate the immersive experience of the headset and determine whether they could perceive the attack. The headset used in the experiment was the PICO 4 Pro, and the parameters of the ultrasonic attack signal were $26.8612kHz$ and $10W$. The experimental results are shown in Table IV. The results indicate that the decrease in immersion due to vibration feedback is minimal, while it significantly enhances the defensive capability.

B. Future Work

Assessing more VR devices. To validate the effectiveness and transferability of `False Reality` attack, we conducted experiments on 5 high-market-share device models, two Meta Quest 2 [14] with different system versions (v60 and v50), a PICO 4 Pro [15], a Meta Quest 3 [16], and a Google Cardboard [17] paired with IQOO NEO 5 SE as shown in Table I. The results demonstrate multiple VR devices are susceptible to `False Reality` even though they vary in models. The underlying reasons are the core principle of critical services and sensor usage remains consistent. For instance, cameras, IMUs, and other sensors are still employed to perceive the 3D environment. Besides, in this paper, we do not consider Apple Vision Pro since they are in a small market share yet (less than 100k sales [69] compared to 7650k [70] of the total market). In the future, we will keep exploring the security of new VR systems when they use new sensors.

Exploring more attack paths. In this work, we presented detailed 3 attack pathways due to page limitations. Besides, we have conducted preliminary validation for other attack paths, e.g., modifying the avatar's action by spoofing IR cameras and inducing display jitter by interfering with IMU (Figure 23e). In the future, we will thoroughly analyze and keep exploring alternative attack pathways.

IX. RELATED WORK

Systematization of VR Security. [71] and [72] address the heightened security and privacy risks in VR compared to traditional systems. [73] reviews current VR security threats across five areas: input, data access, output, interactivity, and device integrity. [74] classifies VR security research into four dimensions: attack surface, security property, impact, and damage, noting that HMDs may obscure users' awareness of cyberattacks affecting their physical environment, such as mismatches between virtual and real worlds, altered safety boundaries, or induced VR sickness. [75] categorizes 15 types of attacks based on their difficulty, consequences, and risk levels. Unlike these papers, we focuses on analyzing sensors as the attack surface. We examine how sensor attacks could potentially impact VR systems and cause harm to users.

Perceptual Manipulation Attack in VR System. [10] suggests that attackers can manipulate users' multisensory perceptions (e.g., visual, auditory, tactile) through mixed reality (MR) content, potentially leading to physical collisions or dizziness. [9] describes how malicious applications, disguised as benign ones, can hijack and manipulate user interactions within VR environments. [7] shows that attackers can deceive users into altering their physical positions by modifying virtual environment settings through VR system configuration files. [76] illustrates how visual illusions can be exploited to distort users' depth perception of the environment or objects. However, most of these works initiate attacks from the software layer, requiring attackers to access the victim's VR device software, which lacks stealth and feasibility. In contrast, our method enables remote and covert attacks without needing prior access to the victim's device.

Sensor Spoofing Attack. Over the past decades, substantial research focus on sensor spoofing attacks. For instance, attackers can blur camera images using acoustic waves [77] or introduce colored stripes via Intentional Electromagnetic Interference (IEMI) [26]. Adversarial infrared patches have been suggested to disrupt infrared-based object detection [27]. The feasibility of manipulating Hall sensors in solar inverters [23] and anti-lock braking systems (ABS) [28] has also been demonstrated. Additionally, attackers can inject false data into IMUs using IEMI [29] or ultrasonic waves [22, 30]. Voice commands can be injected into microphones using light [25] or ultrasonic signals [24], and sensor data can be controlled by manipulating power supply voltage [78]. Despite extensive research, sensor attacks within VR systems remain underexplored and warrant attention due to their potential risks.

X. CONCLUSION

This paper presents the first security analysis framework for VR systems from the perspective of physical-signal-based attacks. We propose `False Reality`, a framework that uncovers the underlying relationships among sensors, VR services, and human responses, and systematically maps out attack pathways that spoof human perception and induce false actions through physical signals. By incorporating human perceptual and psychological factors, `False Reality` offers practical insights into real-world vulnerabilities. Finally, we validate `False Reality` through three case studies across five commercial VR systems and propose potential countermeasures.

REFERENCES

[1] Chris Mays. *A whole new world: the virtual reality experience made accessible*. https://userway.org/blog/virtual-reality-experience/. 2025.

[2] ScienceSoft. *Virtual Reality for Surgery: Key Aspects*. https://www.scnsoft.com/healthcare/virtual-reality/surgery. 2024.

[3] Robotics@MIT. *Teleoperating robots with virtual reality*. https://robotics.mit.edu/teleoperating-robots-virtual-reality. 2019.

[4] J Jauhiainen. *VR, AR and XR enterprises and related demand and supply in Finland*. 2021.

[5] Statista. *Virtual reality (VR) - statistics & facts*. https://www.statista.com/topics/2532/virtual-reality-vr/. 2024.

[6] Yongzhong Yang et al. "Research on the Perceived Quality of Virtual Reality Headsets in Human–Computer Interaction". In: *Sensors* 23.15 (2023), p. 6824.

[7] Peter Casey, Ibrahim Baggili, and Ananya Yarramreddy. "Immersive virtual reality attacks and the human joystick". In: *IEEE Transactions on Dependable and Secure Computing* 18.2 (2019), pp. 550–562.

[8] Wen-Jie Tseng et al. "The dark side of perceptual manipulations in virtual reality". In: *Proceedings of the 2022 CHI Conference on Human Factors in Computing Systems*. 2022, pp. 1–15.

[9] Zhuolin Yang et al. "Inception Attacks: Immersive Hijacking in Virtual Reality Systems". In: *arXiv preprint arXiv:2403.05721* (2024).

[10] Kaiming Cheng et al. "Exploring user reactions and mental models towards perceptual manipulation attacks in mixed reality". In: *32nd USENIX Security Symposium (USENIX Security 23)*. 2023, pp. 911–928.

[11] Daniel Medeiros et al. "The benefits of passive haptics and perceptual manipulation for extended reality interactions in constrained passenger spaces". In: *Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems*. 2023, pp. 1–19.

[12] Frank Steinicke et al. "Estimation of detection thresholds for redirected walking techniques". In: *IEEE transactions on visualization and computer graphics* 16.1 (2009), pp. 17–27.

[13] Omar Merhi et al. "Motion Sickness, Console Video Games, and Head-Mounted Displays". In: *Human Factors* 49.5 (2007), pp. 920–934.

[14] Meta. *Meta Quest 2*. https://www.meta.com/tw/quest/products/quest-2/. 2024.

[15] PICO. *PICO 4 Pro*. https://www.picoxr.com/cn/products/pico4-pro. 2024.

[16] Meta. *Meta Quest 3*. https://www.meta.com/quest/quest-3/. 2024.

[17] Google. *Google Cardboard*. https://arvr.google.com/cardboard/. 2020.

[18] Varjo. *Control interpupillary distance (IPD)*. https://developer.varjo.com/docs/unity-xr-sdk/ipd-control-with-varjo-xr-plugin. 2024.

[19] Eunhee Chang, Hyun Taek Kim, and Byounghyun Yoo. "Virtual reality sickness: a review of causes and measurements". In: *International Journal of Human–Computer Interaction* 36.17 (2020), pp. 1658–1682.

[20] Ray Meddis and Wendy Lecluyse. "The psychophysics of absolute threshold and signal duration: a probabilistic approach". In: *The Journal of the Acoustical Society of America* 129.5 (2011), pp. 3153–3165.

[21] Harry T Lawless et al. "Measurement of sensory thresholds". In: *Sensory evaluation of food: principles and practices* (1999), pp. 173–207.

[22] Timothy Trippel et al. "WALNUT: Waging doubt on the integrity of MEMS accelerometers with acoustic injection attacks". In: *2017 IEEE European symposium on security and privacy (EuroS&P)*. IEEE. 2017, pp. 3–18.

[23] Anomadarshi Barua and Mohammad Abdullah Al Faruque. "Hall Spoofing: A Non-Invasive DoS Attack on Grid-Tied Solar Inverter". In: *29th USENIX Security Symposium (USENIX Security 20)*. 2020, pp. 1273–1290.

[24] Guoming Zhang et al. "Dolphinattack: Inaudible voice commands". In: *ACM SIGSAC conference on computer and communications security*. 2017, pp. 103–117.

[25] Takeshi Sugawara et al. "Light commands:Laser-Based audio injection attacks on Voice-Controllable systems". In: *29th USENIX Security Symposium (USENIX Security 20)*. 2020, pp. 2631–2648.

[26] Qinhong Jiang et al. "GlitchHiker: Uncovering Vulnerabilities of Image Signal Transmission with IEMI". In: *USENIX Security*. Vol. 23. 2023.

[27] Xingxing Wei, Jie Yu, and Yao Huang. "Physically adversarial infrared patches with learnable shapes and locations". In: *Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition*. 2023, pp. 12334–12342.

[28] Yasser Shoukry et al. "Non-invasive spoofing attacks for anti-lock braking systems". In: *Cryptographic Hardware and Embedded Systems-CHES 2013: 15th International Workshop, Santa Barbara, CA, USA, August 20-23, 2013. Proceedings 15*. Springer. 2013, pp. 55–72.

[29] Joon-Ha Jang et al. "Paralyzing Drones via EMI Signal Injection on Sensory Communication Channels." In: *The Network and Distributed System Security Symposium (NDSS)*. 2023.

[30] Yazhou Tu et al. "Injected and delivered: Fabricating implicit control over actuation systems by spoofing inertial sensors". In: *27th USENIX security symposium (USENIX Security 18)*. 2018, pp. 1545–1562.

[31] Gökçen Yılmaz Dayanıklı et al. "Physical-Layer attacks against pulse width Modulation-Controlled actuators". In: *31st USENIX Security Symposium (USENIX Security 22)*. 2022, pp. 953–970.

[32] Wanyou Lv et al. "A deep convolution generative adversarial networks based fuzzing framework for industry control protocols". In: *Journal of Intelligent Manufacturing* 32 (2021), pp. 441–457.

[33] Zhihui Li et al. "An Intelligent Fuzzing Data Generation Method Based on Deep Adversarial Learning". In: *IEEE Access* 7 (2019), pp. 49327–49340.

[34] Eberhard Zwicker and Hugo Fastl. "Information Processing in the Auditory System". In: *Psychoacoustics: Facts and Models*. Berlin, Heidelberg: Springer Berlin Heidelberg, 1999, pp. 23–60.

[35] Meta Horizon. *Locomotion Interactions*. https://developers.meta.com/horizon/documentation/unity/unity-isdk-locomotion-interactions/. 2024.

[36] Robotics of MIT. *Teleoperating robots with virtual reality*. https://robotics.mit.edu/teleoperating-robots-virtual-reality/. 2024.

[37] Vivestia. *Immersive View Meaning: What you need to know*. https://thevivestia.com/immersive-view-meaning/. 2023.

[38] Wikipedia. *Blinded experiment*. https://en.wikipedia.org/wiki/Blinded_experiment. 2025.

[39] Basheer Al-Tawil et al. "A review of visual SLAM for robotics: evolution, properties, and future applications". In: *Frontiers in Robotics and AI* 11 (2024), p. 1347985.

[40] Axel Barrau and Silvere Bonnabel. "A mathematical framework for IMU error propagation with applications to preintegration". In: *2020 IEEE International Conference on Robotics and Automation (ICRA)*. IEEE. 2020, pp. 5732–5738.

[41] Zheng Huai and Guoquan Huang. "A Consistent Parallel Estimation Framework for Visual-Inertial SLAM". In: *IEEE Transactions on Robotics* 40 (2024), pp. 3734–3755. DOI: 10.1109/TRO.2024.3433868.

[42] Carlos Campos et al. "ORB-SLAM3: An Accurate Open-Source Library for Visual, Visual–Inertial, and Multimap SLAM". In: *IEEE Transactions on Robotics* 37.6 (2021), pp. 1874–1890. DOI: 10.1109/TRO.2021.3075644.

[43] Amado Antonini et al. "The Blackbird Dataset: A large-scale dataset for UAV perception in aggressive flight". In: *2018 International Symposium on Experimental Robotics (ISER)*. 2018. DOI: 10.1007/978-3-030-33950-0_12. URL: https://doi.org/10.1007/978-3-030-33950-0_12.

[44] SIGLENT. *SDG6032X*. https://siglentna.com/product/sdg6032x/. 2021.

[45] Micronix. *NF HSA4051*. https://eshop.micronix.eu/measurement-equipment/electrical-quantities/nf-corporation-instruments/high-speed-bipolar-amplifiers/hsa-4051.html. 2013.

[46] Fostex. *Fostex FT17H*. https://www.fostex.jp/products/FT17H/. 2024.

[47] Pyopenvr. *Pyopenvr*. https://github.com/cmbruns/pyopenvr. 2023.

[48] Microsoft. *Boundary system overview — MRTK2*. https://learn.microsoft.com/en-us/windows/mixed-reality/mrtk-unity/mrtk2/features/boundary/boundary-system-getting-started?view=mrtkunity-2022-05. 2024.

[49] Jeannette Montufar et al. "Pedestrians' normal walking speed and speed when crossing a street". In: *Transportation research record* 2002.1 (2007), pp. 90–97.

[50] Y. H. Su et al. "Development of an Effective 3D VR-Based Manipulation System for Industrial Robot Manipulators". In: *2019 12th Asian Control Conference (ASCC)*. 2019, pp. 1–6.

[51] Grace Kay. *These tech startups enable surgeons to train and supervise operations remotely during the pandemic.* https://www.businessinsider.com/hospitals-surgeons-startups-operate-from-home-2021-2. 2021.

[52] Xiaozheng Zheng et al. "Realistic Full-Body Tracking from Sparse Observations via Joint-Level Modeling". In: *Proceedings of the IEEE/CVF International Conference on Computer Vision*. 2023, pp. 14678–14688.

[53] Arthur D Kuo and Felix E Zajac. "Human standing posture: multi-joint movement strategies based on biomechanical constraints". In: *Progress in brain research* 97 (1993), pp. 349–358.

[54] Joan Sola. "Quaternion kinematics for the error-state Kalman filter". In: *arXiv preprint arXiv:1711.02508* (2017).

[55] E. Burns et al. "The hand is slower than the eye: a quantitative exploration of visual dominance over proprioception". In: *IEEE Proceedings. VR 2005. Virtual Reality, 2005.* 2005, pp. 3–10.

[56] Steven Yantis and John Jonides. "Abrupt visual onsets and selective attention: evidence from visual search." In: *Journal of Experimental Psychology: Human perception and performance* 10.5 (1984), p. 601.

[57] Naureen Mahmood et al. "AMASS: Archive of Motion Capture as Surface Shapes". In: *International Conference on Computer Vision*. Oct. 2019, pp. 5442–5451.

[58] Unitree Robotics. *Unitree Z1*. https://www.unitree.com/z1/. 2024.

[59] Emily C Crofton et al. "Potential applications for virtual and augmented reality technologies in sensory science". In: *Innovative Food Science & Emerging Technologies* 56 (2019), p. 102178.

[60] Afsaneh Koohestani et al. "A knowledge discovery in motion sickness: a comprehensive literature review". In: *IEEE access* 7 (2019), pp. 85755–85770.

[61] Jan-Philipp Stauffert, Florian Niebling, and Marc Erich Latoschik. "Latency and cybersickness: Impact, causes, and measures. A review". In: *Frontiers in Virtual Reality* 1 (2020), p. 582204.

[62] Cyriel Diels and Peter A Howarth. "Frequency characteristics of visually induced motion sickness". In: *Human factors* 55.3 (2013), pp. 595–604.

[63] Jinzhao Chen. "Frequency responses of visually induced motion sickness: isolating effects of velocity and

amplitude of visual stimuli". PhD thesis. Hong Kong University of Science and Technology, 2014.

[64] Nitish Padmanaban et al. "Towards a machine-learning approach for sickness prediction in 360 stereoscopic videos". In: *IEEE transactions on visualization and computer graphics* 24.4 (2018), pp. 1594–1603.

[65] Google. *Android ADB*. https://source.android.google.cn/docs/setup/build/adb?. 2024.

[66] *scrcpy*. https://github.com/Genymobile/scrcpy.

[67] *OpenCV*. https://opencv.org/.

[68] Lin Chai, William A Hoff, and Tyrone Vincent. "Three-dimensional motion and structure estimation using inertial sensors and computer vision for augmented reality". In: *Presence* 11.5 (2002), pp. 474–492.

[69] Bloomberg. *Apple's Vision Pro Won't Cross 500,000 Sales This Year, IDC Says*. https://www.bloomberg.com/news/articles/2024-07-11/apple-s-vision-pro-wont-cross-500-000-sales-this-year-idc-says. 2024.

[70] International Data Corporation (IDC). *Worldwide Virtual Reality Headset Market Shares, 2023: Sony Erodes Meta's Leadership*. https://www.idc.com/getdoc.jsp?containerId=US52031824&pageType=PRINTFRIENDLY. 2024.

[71] Franziska Roesner, Tadayoshi Kohno, and David Molnar. "Security and privacy for augmented reality systems". In: *Communications of the ACM* 57.4 (2014), pp. 88–96.

[72] Tao Ni. "Sensor Security in Virtual Reality: Exploration and Mitigation". In: *Proceedings of the 22nd Annual International Conference on Mobile Systems, Applications and Services*. MOBISYS '24. New York, NY, USA: Association for Computing Machinery, 2024, 758–759. ISBN: 9798400705816.

[73] Jaybie A De Guzman, Kanchana Thilakarathna, and Aruna Seneviratne. "Security and privacy approaches in mixed reality: A literature survey". In: *ACM Computing Surveys (CSUR)* 52.6 (2019), pp. 1–37.

[74] Blessing Odeleye et al. "Virtually secure: A taxonomic assessment of cybersecurity challenges in virtual reality environments". In: *Computers & Security* 124 (2023), p. 102951.

[75] Tânia Silva et al. "A survey and risk assessment on virtual and augmented reality cyberattacks". In: *2023 30th international conference on systems, signals and image processing (IWSSIP)*. IEEE. 2023, pp. 1–5.

[76] Susanne Schmidt, Gerd Bruder, and Frank Steinicke. "Depth perception and manipulation in projection-based spatial augmented reality". In: *PRESENCE: Virtual and Augmented Reality* 27.2 (2018), pp. 242–256.

[77] Xiaoyu Ji et al. "Poltergeist: Acoustic adversarial machine learning against cameras and computer vision". In: *2021 IEEE Symposium on Security and Privacy (SP)*. IEEE. 2021, pp. 160–175.

[78] Kai Wang et al. "Volttack: Control IoT Devices by Manipulating Power Supply Voltage". In: *2023 IEEE Symposium on Security and Privacy (SP)*. IEEE Computer Society. 2023, pp. 1771–1788.

[79] Farzaneh Ahmadi et al. "Bio-effects and safety of low-intensity, low-frequency ultrasonic exposure". In: *Progress in biophysics and molecular biology* 108.3 (2012), pp. 119–138.

[80] David Baeza Moyano, Daniel Arranz Paraiso, and Roberto Alonso González-Lezcano. "Possible effects on health of ultrasound exposure, risk factors in the work environment and occupational safety review". In: *Healthcare*. Vol. 10. 3. MDPI. 2022, p. 423.

[81] Elliott Wen et al. "VR. net: A real-world dataset for virtual reality motion sickness research". In: *IEEE Transactions on Visualization and Computer Graphics* (2024).

APPENDIX

A. Ethics Considerations

IRB Approval. We have got IRB approval from Institutional Review Boards before the user study.

Manikin instead of Human. In the attack capability assessment and validation experiments, we used a manikin for wearing the tested VR devices and used the ADB tool [65] and python interface of OpenVR (pyopenvr [47]) to collect the experiment data remotely.

Volunteer Protection. In the psychological experiments and end-to-end attack scenarios, we made the following efforts to protect participants' security and informed the participants that they could terminate the trial at any time.

- *Software-based experiments*: In the psychological experiments, we utilized software to simulate the disturbed VR system services, eliminating the impact of the attack signals on participants.
- *Limit attack signal energy*: We strictly limited the transmission power of the attack signals within a safe range. For example, we set the ultrasonic waves below 90 dB, which is far lower than the safe range (120dB) [79, 80].
- *Shielding attack signals*: Participants are required to wear the specific shielding devices (an electromagnetic shielding suit, 3M ear-muffs, and Infrared goggles) to shield attack signals (electromagnetic signals, ultrasound, and IR beams).

Responsible disclosure. We have disclosed the vulnerabilities presented in this paper to the respective product security teams. Our reports included the affected products, a brief description of the vulnerability, and a proof-of-concept demonstration. We also provided suggestions for expected correct behavior and potential workarounds. As of the submission date, we have not yet received response from the vendors.

B. Attack Flow Model

To clarify how the attack signals take effect, we build a transfer function model to analyze the attack flow paths. As shown in Figure 25, the input of VR consist of environmental signals, human signals and attack signals. Captured and processed by the VR devices, the input is converted into the output by the transfer functions $F_s(s)$, $F_p(s)$ and $F_a(s)$. Users perceive the output of the VR devices through their senses ($H_s(s)$) and act accordingly ($H_a(s)$). The user's action generates the human signal, which creates positive feedback. Suppose that the attack signal is $attack(x)$ and the user's perception is $sense(x)$. The transfer function $G(s)$ is a linear mapping of the Laplace transform of $sense(x)$ to the Laplace transform of $attack(x)$. $G(s)$ can be calculated as:

$$G(s) = \frac{sense(s)}{attack(s)} = \frac{F_s(s)F_p(s)F_a(s)H_s(s)}{1 - F_s(s)F_p(s)F_a(s)H_s(s)H_a(s)} \tag{11}$$

In fact, the processing of the VR system does some substitutions. For example, real environments are replaced with virtual ones, real hands are replaced with animated ones and real positions are replaced with virtual ones. Therefore, the key information (e.g., positional relationship between objects, movement of limbs) remains unchanged. That means $F_p(s) \approx 1$. Moreover, the actuators in the VR system are similar. They simply visualize the virtual data to the user. For example, the HMD displays a binocular screen and speakers play audio. This process may introduce non-ideal noise, but the signal remains roughly constant. That means $F_a(s) \approx 1$.

Therefore, $G(s)$ can be simplified as

$$G(s) = \frac{sense(s)}{attack(s)} \approx \frac{F_s(s)H_s(s)}{1 - F_s(s)H_s(s)H_a(s)} \tag{12}$$

The transfer function $P(s)$ is defined as a linear mapping of the Laplace transform of $action(x)$ to the Laplace transform of $attack(x)$. $P(s)$ can be calculated as:

$$P(s) = \frac{action(s)}{attack(s)} = G(s)H_a(s) \approx \frac{F_s(s)H_s(s)H_a(s)}{1 - F_s(s)H_s(s)H_a(s)} \tag{13}$$

According to Equations 12 and 13, the impact of the attack signal on the user (i.e. the consequences of `False Reality` Attack) depends mainly on the sensitivity of the user's senses and the degree of amplification of the attack signal by the sensor. Everyone has a different level of sensory sensitivity. Maybe some people are more sensitive and others are not. This is something the attacker can't change. But according to [81], some of people are prone to discomfort when wearing VR devices, i.e. they are more sensitive. Therefore, if the attacker wants to maximize the effect of the attack, he must find the attack signals that are most sensitive to the sensors. Additionally, to ensure the stealthiness of the attack, the sensory sensitivity of the victim must also be taken into account. These will be discussed in detail in Section IV.

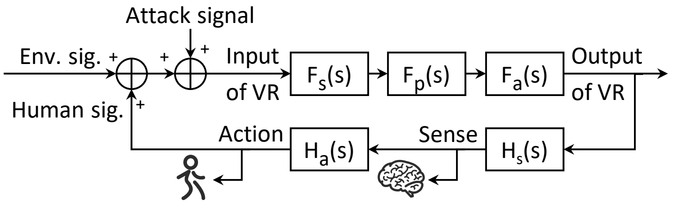


Figure 25. Block diagram of the transfer function of the VR system. Attack signals eventually affect the user's perception and actions through multiple transfer functions. *Note:* Env. sig. means environmental signal. Human sig. means the signal from the user. $F_s(s)$ presents the transfer function of sensors. $F_p(s)$ presents the transfer function of processing program in VR. $F_a(s)$ presents the transfer function of actuators. $H_s(s)$ presents the transfer function of human senses. $H_a(s)$ presents the transfer function of human muscle.

C. Attack Flow of attackers

(a) The attack flow of the attacker is shown in Figure 26. There is a feedback loop for the attacker to dynamically adjust the attack signal.

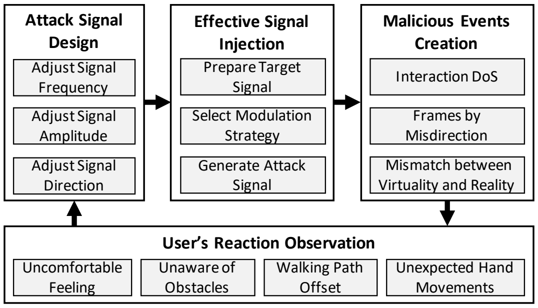


Figure 26. Illustration of `False Reality` attack flow. We first design an attack signal for effective injection. Then we inject an attack signal to VR system in order to create malicious events. As feedback, we observe the victim user's reaction to dynamically adjust the attack signals. In this loop, we can continuously deceive and manipulate the victim.

D. Equations

$$
\begin{aligned}
R_j &= R_i \prod_{k=i}^{j-1} \exp((\omega_k - \omega_{bias})\Delta t) \\
v_j &= v_i + g\Delta t_{ij} + \sum_{k=i}^{j-1} R_k(a_k - a_{bias})\Delta t \\
p_j &= p_i + \sum_{k=i}^{j-1} v_k \Delta t + \frac{1}{2} g \Delta t_{ij}^2 + \frac{1}{2}\sum_{k=i}^{j-1} R_k(a_k - a_{bias})\Delta t^2
\end{aligned}
\tag{14}
$$

where R is the rotation matrix, v is the velocity, p is the displacement, ω is the angular velocity measured by the IMU, a is the acceleration measured by the IMU, ω_{bias} and a_{bias} represent the bias components of ω and a, and g denotes the gravitational acceleration. Specifically, the iterative formula for *R* can be transformed as follows:

$$
\begin{aligned}
R_j &= R_i \prod_{k=i}^{j-1} \exp((\omega_k - \omega_{bias})\Delta t) \\
&= R_i \exp(\sum_{k=i}^{j-1} (\omega_k - \omega_{bias})\Delta t) \\
&\approx R_i \exp(\int_0^T (\omega_k - \omega_{bias}) dt) \\
&= R_i \exp(\theta_T - \omega_{bias} T)
\end{aligned}
\tag{15}
$$

E. Supplementary Materials of Evaluation

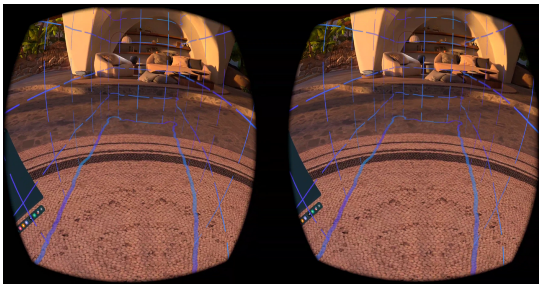


Figure 27. Safety boundary of Meta Quest 2.

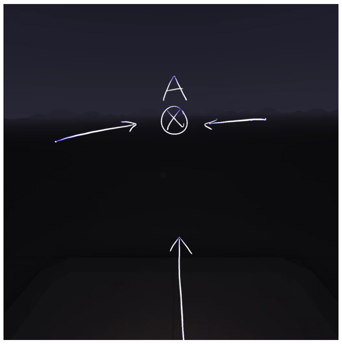


Figure 28. Setup of virtual environment in Case 1.

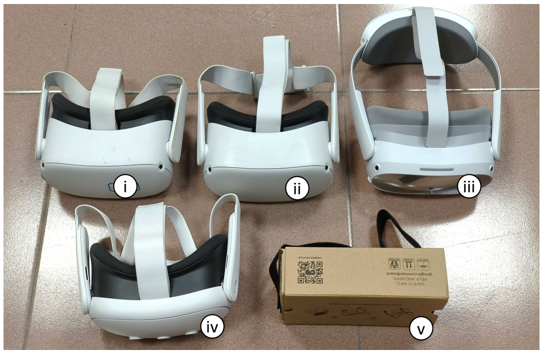


Figure 29. The 5 commercial VR devices tested in the evaluation: (i) Meta Quest 2 (v60), (ii) Meta Quest 2(v50), (iii) PICO 4 Pro, (iv) Meta Quest 3, (v) Google Cardboard.

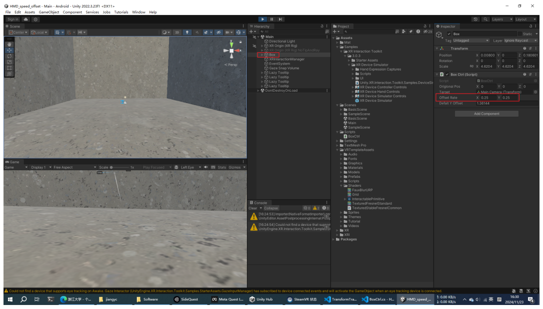


Figure 30. Unity-based VR APP "TrajOffset".

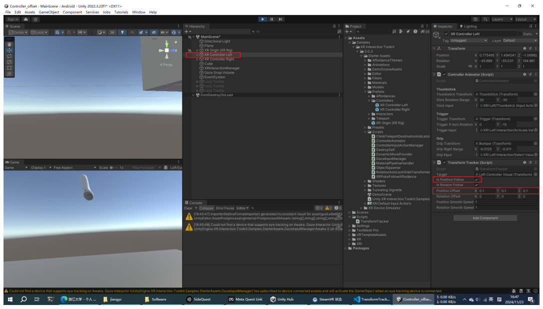


Figure 31. Unity-based VR APP "CtrOffset".