Impacts of Latency Perception Manipulation in Virtual Reality: Effectiveness and User Perceptibility

1st Evan Anspach
Computer Science
Colorado State University
Fort Collins, United States of America
pidge.anspach@colostate.edu

2nd Evan Luebbert
Computer Science
Colorado State University
Fort Collins, United States of America
luebbertevan@gmail.com

3rd Matthew Sturgeon
Computer Science
Colorado State University
Fort Collins, United States of America
msturgeo@colostate.edu

4th Jessica Bahny
Computer Science
Colorado State University
Fort Collins, United States of America
jessica.bahny@colostate.edu

***Abstract*—Virtual reality devices have become increasingly useful for applications and purposes across different disciplines, in doing so they have also become a larger target for cyberattacks that wish to reduce the usefulness of said devices. Perception manipulation has become an increasing threat against these devices but their impact on the user or how noticeable to the user the attacks are has not yet been fully examined by prior research.**

We use a latency simulation approach in a Gridshot style shooting range simulation to measure the effect of added latency on the accuracy of the user and the amount of latency that is applied in which the user notices there is a change. Our study found no significant difference in user accuracy for added latencies from 0-80ms and found no significant difference in the noticability of the added latency to the user.

***Index Terms*—human computer interaction, virtual reality, VR security, perception, just noticeable difference, latency, cybersecurity**

I. Introduction

Virtual Reality (VR) was first envisioned as a way to obtain the "Ultimate Display" by Ivan Sutherland, a way of displaying information that feels real to the senses [24], [41]. The goal of a virtual environment is to provide an engaging and realistic experience that immerses the user into an emulated reality. Since then, the amount of authenticity that is felt in virtual reality has been defined as presence, and is one of the most important factors in the success of a virtual system. As such, one of the major goals of these systems has been to maximize both presence and overall immersion in order to create systems that promote task performance and efficiency. Virtual reality has been adopted by, and integrated into many fields and continues to be an avenue of innovation in a variety of well defined industries. Virtual reality applications are utilized for a plethora of diverse operations, such as sports training [1], stress mitigation [2], and construction management [3]. As virtual reality systems become increasingly more useful the influence of these applications develops alongside and virtual reality becomes ingrained within critical operations in many industries. The significance of virtual reality systems is precisely what makes it such an appealing target to attackers who aim to disrupt utility and reduce functionality. A potential approach to orchestrate an attack on a virtual reality application is to target an attribute shown to be a significant factor in usability, enjoyment and presence: latency.

User behavior and perception has become a major attack vector for adversaries who want to target virtual reality systems. An attacker who has gained access to a virtual reality device can exploit it to perform Perception Manipulation attacks by influencing how the user experiences and interprets the virtual environment. Latency heavily influences a users interpretation of virtual environments, because it degrades the illusory stability of the environment, lowing overall presence and immersion [35]. Latency can be induced on the headset using a variety of different approaches ranging from network based Denial of Service attacks, to maliciously designed applications, to vulnerabilities in application engines such as graphics rendering or physics engines. Manipulating perception within a Head Mounted Display (HMD) can cause physical harm, physiological harm, a reduction in effectiveness, or a complete denial of functionality. Due to the immersive nature of virtual reality devices and their ability to establish presence, users are especially susceptible to these kind of manipulation attacks. These attacks present specific complications since their occurrence is not transparent; perception manipulation on the HMD is difficult for a user to recognize by design, where as malicious behaviour on computer or network systems has precedent and thus is defensible to more recognizable behavior.

Previous research has focused on what exploits are pos-

sible on VR systems. However, there is a significant gap in current research when considering the investigation into the effectiveness of latency perception manipulation attacks. Our study addresses this gap and focuses on identifying when users are able to detect manipulation attacks that are focused on latency throttling in VR systems. Our research identifies the point in which an average user would be able to detect a latency perception manipulation attack as well as the amount an attacker would gain in terms of user performance degradation. The budding field of VR cyber-security is enhanced by our conclusions which inform whether or not latency is an effective attack vector on virtual reality systems. We attempt to determine how much an attacker stands to gain from conducting this type of attack and the necessary amount of latency required to degrade a users performance while also being difficult for users to recognize. Our results give a valuable insight on the degree of influence an attacker possesses by successfully manipulating users' perception. Our findings inform the approach of future studies related to VR cyber-security measures targeted at protecting users from latency based perception manipulation.

II. Related Works

A. Vulnerabilities and Attack Surfaces in VR Devices

1) Attack Classification: There are several major attacks vectors targeting VR devices and their operations or use that can be relevant to applying perception manipulation attacks to headsets. Many of these attacks have been categorized by Valluripally et al. and stored in an Attack Fault Tree [20]. There is a broad range of threats to security that contains many different types of attacks. One of which is a form of privilege escalation attack where a valid user is impersonated by an attacker to gain their privileges in the system. Breaches due to these attacks can lead to unauthorized disclosure of user information breaching user confidentiality. Denial of Service (DOS) attacks are also a major threat to VR applications, according to Roman et al. [22]. DOS attacks can target not only the network infrastructure and network resources of the provider, but also presents a major threat to the internals of the VR system via attacks that obtain degrees of control over the infrastructure of the headset.

2) Data Privacy: The Data privacy of VR devices is also a major concern, information such as bio-metric data, user credentials or other sources of sensitive or personal information can be leaked from the collection done by the headset, or compromised due to improper deletion and removal of such information as detailed by Gulhane et al. in their study of the use of attack tree formalism in VR security [21]. Packet Tampering and Packet sniffing is another of the major concerns for VR security, outgoing network packets on the device can be read and interpreted as to their nature to reveal private information, or the packets can be changed to affect the performance of the VR device or application or to cause unintended behavior. These attack surfaces show how a user may gain access to a VR device or application through either privilege escalation through malware or gaining credentials using one of confidentiality breach techniques. Credentials may allow the attacker to access features and permissions of the device that should only be available directly to the user or the user's account. Once an attacker has the needed access they would be able to perform different perception manipulation attacks against the user of the system or application such as the latency manipulation used in this work.

B. Attention And Perception Manipulation in VR

Virtual reality is vulnerable to several different techniques for changing the user's perception of a given task. Virtual object scaling, velocity, and position can be altered in order to influence how the user observes operations related to those objects such as conducting tasks or solving problems [1]. When manipulation is applied, users may view the task as easier or more difficult based on the changes applied, regardless of the true difficulty of the task. In cases of performance degradation the user's confidence in their ability regarding the task is likely to be lowered [19]. Our study builds off the directive of manipulating an applications latency during a task in order to affect user perception of the task difficulty, and their perception of their performance at task completion.

1) Distraction and Attention: Distraction and attention manipulation in VR has also been researched by several studies; Casey et al. identified overlay attacks as a major vulnerability in Virtual Reality [10]. Overlay attacks are when an attacker exploits either the headset architecture or a vulnerability within an application to create pop up overlays within the view of the user obstructing parts or all of their vision. They were able to successfully implement an overlay attack that would be introduced by a malicious application. The user would not be able to force close the created overlay without shutting down the device and restarting it. This would allow an attacker to introduce some type of distraction inside one of these overlays to change the attention of the user from their task to the overlay, possibly decreasing performance and user trust in the VR system. Casey et al. additionally comments on how overlay attacks can be used to cause emotional distress and psychological harm to a user by presenting disturbing and disgusting imagery on the overlay, forcing the user to observe it. Latency attacks may also disrupt users' abilities to engage with VR content and systems. Taylor et al. found that as latency in a system or other similar delays increased, expected user task completion and engagement dropped accordingly [33]. Attacks implemented similarly to the introduction of latency in Taylor et al.'s study may be used by an attacker to reduce the amount that users engage with an application over time which can have several targeted consequences such as negatively impacting the user's view of the application or damaging the reputation of both the product and owners of the application.

C. Latency and other VR stimuli

1) Latency: Latency effects the way that all stimuli is perceived by a user in a VR. Changes in stimuli introduced into

virtual environments can have adverse effects on the performance of the user in that space as well as the effectiveness of that environment. Audio changes in an environment, especially increases in auditory stimuli, can reduce the user's ability to notice visual cues and other related visual tasks [5]. Due to these factors, visual and auditory stimuli are targets for attackers that wish to change a user's perception of the environment. Latency in these systems is of exceptional import as motor performance of users immersed in the system is degraded in correlation with increased delays [4]. Meehan et al. also suggested that user presence is degraded by increasing latency [39]. They found that users in lower latency environments had significantly higher presence than those who were in a higher latency virtual environment. Louis et al. also found increased latency to be detrimental to user performance and presence [42]. This can reduce the effectiveness of training systems and other systems in virtual reality that use physical motor performance of a user or that rely on immersion or presence in the environment. Higher Latency can also affect both the perceived agency of the user and ownership of action taken within the system. User's ability to detect changes in latency has been examined by Roth et al., Addelstein et al., Ellis et al. and Mania et al. they found that the maximum Just Noticeable Differences (JND) in increases of latency was around 24.5ms [36]–[38], [40]. Our work builds off of this to determine not only when the attack is detected, but also how much the effectiveness of the user task had been compromised in that time.

2) Cybersickness: Latency has also been linked to motion sickness and cybersickness in virtual systems by a number of different works [16]–[18]. Cybersickness in VR systems has also been explored by several studies and has had its effects quantified in a number of ways. Gavgani et al. compared cybersickness to traditional motion sickness by examining the symptomatology of both conditions, and found that in advanced stages, cybersickness and traditional motion sickness are clinically identical [30]. Attackers can exploit these relationships to diminish the effectiveness of the device by attacking the physiological state of the user by inducing latency through network attacks or vulnerabilities in VR applications and hardware. Kourtesis et al. proposed a 7 point questionnaire for determining and quantifying the effects and severity of cybersickness in a VR system [32]. Our work will apply this questionnaire to quantify any possible cybersickness that would result from latency induction through a manipulation attack in our VR shooting range. This quantification will allow us to determine if an attacker through the latency attack vector would likely be able to induce cybersickness on the user, possibly compromising trust in or usefulness of the VR application.

D. Physical Harm from Manipulation

Several earlier studies have explored the effects of Perception Manipulation Attacks on the behavior of users within virtual environments and how they can be leveraged to cause harm to the user. Several of these studies have focused on how the movement of users can be changed without them noticing while immersed in a virtual reality system [8]. This is often done through a technique known as redirected walking [13], where the user is steered to a new location by imperceptibly rotating the virtual scene [14], [15]. This technique is applied to desynchronize the user's physical location from where they believe their location is in relation to the virtual space. This desynchronization technique can be used in conjunction with attacks that modify the bounding space of the virtual environment, causing the user to move to locations that may be designated as unsafe such as into walls or objects [8], [10]. There is also an attack known as the Human Joystick Attack. This attack forcibly guides the player over the bounding box of the virtual space–called the Chaperone–towards some sort of obstacle, object, or physical location that would be advantageous to the attacker [10]. This attack has been shown to be effective at moving the user to locations within the room without them noticing the change in location or the change between the mapping of their virtual location and the physical one [10]. Our work differs from these studies due to our focus on performance degradation in the system due to latency being maliciously induced rather then changing the user's physical location. However, these works do show ways that the user's virtual environment can be covertly manipulated by an attacker and the possible harms that can arise from similar attacks.

E. Privacy Loss from Manipulation

Significant privacy concerns have been explored and identified by previous works. The immersive nature of these virtual spaces provides users a heightened sense of intimacy and trust as virtual spaces may give an illusion of privacy akin the feeling of a real, physical room. However, with use of security vulnerabilities in either the Virtual Reality platform or the virtual environment, an attacker could gain access to the room and eavesdrop on the conversation, hearing and seeing everything that is occurring within the virtual private space while disabling safeguards built into applications that may inform the user of privacy breaches as identified by Vondráček et al. [11]. This allows the user's perception of their own privacy within the space to be manipulated by an attacker; a user would likely be more likely to reveal sensitive information if they believe they are in a private space than if they know an attacker can see and hear them. This can cause a substantial difference between the expected privacy for the virtual space and the actual privacy of the space. Privacy can also be compromised through physical eavesdropping on the user while they believe themselves to be in a private virtual environment. One of these methods of eavesdropping is a side channel attack where the VR participant is watched closely or filmed by the attacker as they input information into a keyboard in the virtual space. This attack was studied by Ling et al. where they studied the distance from the user needed and the amount of time needed to determine or infer sensitive information such as passwords and usernames, as well as how the attack could be perpetrated by the attacker using information about the headset or application keyboard

layouts to map the physical movement of the user to the virtual keyboard model [23]. Our work does not explore the user perception of privacy, however similar methods to the attack demonstrated by Vondráček et al. could be used to bypass systems built into applications to inform the user about the amount of latency in the VR system, compromising indicators meant to help the user identify unusual changes in latency.

III. Methods

A. Participants

A total of 12 subjects participated in our study, an amount chosen because it allows for enough data to analyse substantial results and determine a meaningful conclusion while also being realistic for our given constraints. Our experiment includes 8 iterations of our simulation. The first 3 trails operate as a training rounds with a firing latency of 0ms to acclimate users to the VR environment. 3 was chosen as the number of trial rounds because it was deemed an appropriate amount of rounds to emulate an application training period and eliminate learning bias which has the potential to cause vast changes in skill and performance between trials. Since our experiment aims to measure performance degradation it was paramount to eliminate learning bias as much as was feasible using this control period method. The remaining 5 trails consisted of the manipulation of the independent variable and observation as the firing latency was adjusted; because 8 rounds were required for a single subject, running the experiment required a significant allocation of time. This time cost was another factor which informed our decision to use the number of 12 participants due to the amount of resources that were available.

All participants volunteered to participate and did not receive compensation in any form, monetary or otherwise. Participants were recruited from local gaming communities at the university as well as from students participating in a virtual worlds course at the university. The demographic data collected shows that the pool of accessible subjects had a uneven spread of experience with VR which could potentially introduce a confounding condition influencing the resulting data because the performance will most likely be increased significantly. Additional factors that might have influenced the results of our experiment were many of the participants being female or participants mostly being 21 and 22 due to many of them being found through the university. The age range could tie into the fact that this age range has had more experiences with VR as mentioned above.

These subject conditions and demographic data must be taken into consideration an the results interpreted with these aspects in mind. The data and analysis of results must be discussed and applied only to the scope of the demographics that participated and results may not necessarily apply to other groups such as children, elderly adults, different education levels or other unrepresented groups.

B. Apparatus

1) Hardware and Software: Our experiment was designed to intentionally eliminate confounding variables that may be present in virtual reality to isolate the results to our specific research measures: performance and user perception. As such, we omitted many cosmetic features and distracting characteristics that can be available in many VR applications like menu options and settings, atmospheric flourishes and aesthetic characteristics. Participants were presented with a limited VR environment with a clear FOV. While inside the environment participants viewed a simplistic Virtual scene, a single empty white room that contained only the participant equipped with a firing tool and a display of targets positioned at a distance from the participant. Targets were presented in two stacked rows of five and spaced evenly apart. Targets were designed as squares with a simplistic three circle bullseye texture. Participants were informed of a successful hit with the target disappearing for a set time and reappear in the preprogrammed pattern. A simplistic firearm was used as the firing tool. Both the firing tool and the target were designed with qualities likely to be recognized by participants and associated with their intended function.

The environment was developed and experimental trials run on a Predator PH315-53 Laptop with an NVIDIA GeForce RTX 2060 GPU and a Intel i7-10750H CPU with 16GB of ram on 64-bit Windows 10. Unity3D was used to create and run the environment. The Meta Quest 2 was used as the Head Mounted Display to administer the experiment to participants. All Unity3D scripts were written in C#. All created assets were modeled in blender and imported into Unity3D. No 3rd party software or assets were included in the application. The hardware used was capable of running the software without complications or technical difficulties.

2) Latency Introduction: Latency is generally avoided in VR applications, as such there is no native support for features that can be used to artificially and deliberately add latency onto the headset. We worked around this limitation by creating timed delays within the application from when user input is applied to when the action is actually performed in the virtual space. However, this procedure of adding delay was only applied to the firing mechanism is triggered by the participant in the simulation, it fires after the pre-programmed delay has passed. This allows us to emulate input delay and latency without fully introducing latency into the entire system through performing something like a network DOS attack or similar attack vectors. This method was appealing because it introduces a large amount of control over the delay that the user faces in the application. It is important to note that this is dissimilar to natural latency and network delay. Our latency implementation only applies to a single feature of the application rather than being completely universal over all features such as view movement or target destruction. The application of this type of latency may or may not be realistic to certain scenarios. We made this design choice to isolate the effects one particular latent instance to simplify the manipulated variables and achieve more accurate and correlatable results. This type of experimental design would be most applicable to a perception manipulation attack targeting a specific mechanism of an application. An attacker may be

motivated to use this approach since it limits the attack's perceptibility and focuses on disrupting one particular aspect of functionality. In this type of attack a user would be less likely to recognize the introduction of latency since it is applied to a limited scope and not the application in it's entirety. This type of attack would maximize performance degradation and minimize latency recognition and therefore result in the most influence for the longest time. We chose to simulate this scenario since our experiment is focused towards this type of attack approach.

C. Procedure

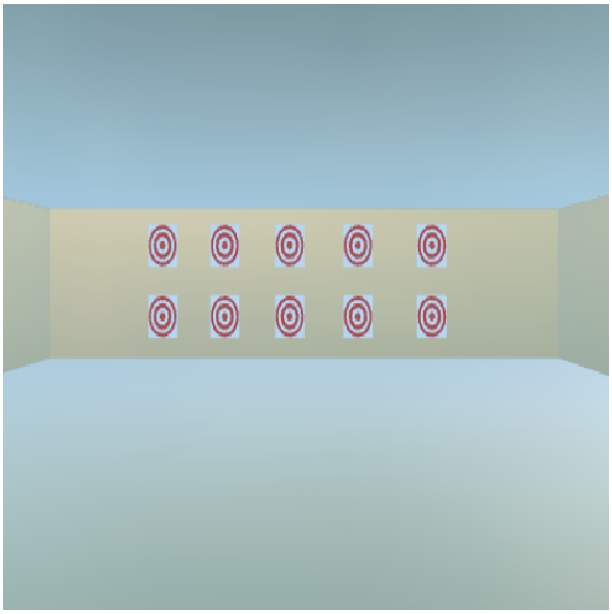

Fig. 1. Screenshot of the VE used for this experiment

The experimental process began with a brief participant initiation. First, participants were briefed on the experiment and the general requirements that would be asked of them. Participants were informed that they would be participating in a VR experiment as well as warned of potential risks involving motion sickness and cybersickness that could result from the study. Participants were invited to cease participation at any time for any reason if they chose to. A consent form was provided to the participants. Subjects were then asked to fill out a demographics survey that asked for information such as age, gender, VR experience level, history of cybersickness, expertise, and experience with fps.

Latency was defined and explained to the subjects prior to the experiment. Administrators also explained the nature of the experiment and what measurements where being recorded to inform if they would notice latency changes. Next the participants were guided through the process of putting on the VR Meta Quest 2 headset and properly holding the controllers. Additional explanations of how the controllers and VR experience operates was given as needed by administrators based on level of VR experience so that all participants were knowledgeable of the base functions. Additionally, participants were free to ask questions during the training rounds as is appropriate for a training period emulation.

The task the participants were asked to complete was a shooting range simulation and to shoot as many targets as they could within the time frame of 10 seconds. For each trial, participants were asked to shoot each target as fast as they could as the targets appear. Targets would be presented to the participant in the virtual space at a constant distance from the participant. The participant would have to shoot the targets as fast as possible with task success and accuracy being measured by the ratio of targets that were successfully hit by the participant and the number of shots fired. Timing was measured in milliseconds. If the participant missed their initial attempt to hit the target they would be able to continue shooting until the target was hit or the overall time of the trial was expended.

$$\begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 5 & 1 & 4 \\ 3 & 5 & 4 & 2 & 1 \\ 4 & 1 & 2 & 5 & 3 \\ 5 & 4 & 1 & 3 & 2 \end{bmatrix}$$

Fig. 2. Latin Square used for randomization

The task was presented in five rounds, the order of which was randomized for each participant using a Latin square which can be seen in figure 2. The duration of each round was 10 seconds. This duration was chosen based on earlier experimentation because it allows for enough time to get a reasonable portion of data and allows for some adjustment to latency but not so much time that participants became too familiar with the specific latency alteration. Targets would appear within the time frame on a pattern that was kept constant for each round. Each round had a different amount of controlled firing latency introduced into the system which ranged from 0ms to 80ms. Each round was an increment of 20ms. One round had no extra introduced latency to act as a control for comparison. The latency was only introduced onto the firing mechanism of the application, with a timed delay from user input to the actual firing taking place. Average

performance of the user for each round was collected and compared to other rounds within each participant as well as across participants. Between each round, participants were asked to fill out a survey based upon the Simulator Sickness Questionnaire described by Robert et al. [43]. The purpose of the questionnaire was to detect increased presence of cybersickness on an increasing severity scale of 0 - 3. We also asked the user to answer these questions at the end of each round. Additionally during the period between rounds participants were given a survey to measure their perception of latency in the last round.

1) Was there added latency present in the round?
2) If there was latency present, What severity on a scale of 0-10 was the latency.

Participants then were asked to take a one minute break before the beginning of the each subsequent round. This was done as an attempt to mitigate the user being influenced by the previous trial's latency delay as Roth et al. suggested from their work. They suggested that participants latency detection threshold could be influenced if the latency had increased or decreased relative to the latency of the previous trial [36]. This break allows for minor distraction from the previous trial to mitigate some bias of comparison to the last result. It also prevents participants from being able to see abrupt changes in the latency as rounds change.

D. Design

The experiment consisted of a within groups design. The independent variable manipulated was latency which was adjusted at intervals of 20ms particular to the Latin square orderings. Latency variation orderings determined by the Latin square were evenly spread and assigned at random for each participant for their particular 5 test trials. Dependent measures were the latency JND (ms) measured using a post experiment survey on an interval scale from 1 to 10, number of targets hit and number of shots fired. The ratio of shots to hits was used to determine a participants performance during a trial and performance was compared to the control round baseline established for each participant. A control condition of the experiment were the standardized protocols for conducting the experiment which included scripts for the initiation briefing and debriefing and the strict practice of equal participant treatment in which administrators of the experiment gave no special treatment, aid, or intervention to any participants consistent over the entire course of the study. Our chosen design ensures as much reliability and validity possible since confounding variables were controlled for as much as was reasonable. Additional confounding variables that were unreasonable to control for and remain uncontrolled in the experiment were participants gender, age, cultural background, physical health, mental health, cognitive abilities, level of stress, amount of sleep, academic history, previous level of experience in VR, and previous level of experience in first person shooters. These confounding factors have a possibility of influencing the results of the study but were not the focus of the experiment. Uncontrolled variables were either reasonably negligible or otherwise acknowledged and factored into the analysis of the results.

IV. Results

Summary of Accuracy Data					
Latency	0 ms	20 ms	40 ms	60 ms	80 ms
N	12	12	12	12	12
Mean	78.2954	77.5713	82.6251	78.4858	80.9627
Std.Dev.	17.532	19.9531	23.1188	18.6374	16.8635

Fig. 3. Overall Accuracy Summary

Accuracy ANOVA Results					
Source	*SS*	*df*	*MS*	*F*	*P*
Within-groups	20588.7615	55	374.3411	0.14479	0.964553

Fig. 4. Accuracy ANOVA Details

Summary of Perception Data					
Latency	0 ms	20 ms	40 ms	60 ms	80 ms
N	12	12	12	12	12
Mean	1.4167	1.6667	1.6667	1.3333	1.3333
Std.Dev.	2.1088	2.1462	2.2697	1.9228	1.3707

Fig. 5. Overall Perception Summary

Perception ANOVA Results					
Source	*SS*	*df*	*MS*	*F*	*P*
Within-groups	217.5833	55	3.9561	0.08847	0.985686

Fig. 6. Perception ANOVA Details

Simulator Sickness Questionnaire [43]				
Subject	Nausea	Oculomotor	Disorientation	Total Score
1	0	0	0	0
2	9.45	15.16	0	92.04
3	0	0	0	0
4	0	7.58	13.92	80.41
5	0	7.58	0	28.35
6	9.54	22.74	0	120.73
7	0	0	0	0
8	9.54	7.58	0	64.03
9	9.54	0	0	35.67
10	0	7.58	13.92	59.64
11	0	7.58	13.92	67.22
12	0	7.58	0	28.35
Mean	3.1725	6.94833	3.48	48.0367

Fig. 7. Simulator Sickness Questionnaire results [43]

The experimental portion of the study was conducted over several days. Subjects participated one at a time and all demographic data was successfully documented. Researchers encountered a technical obstacle during the experiment administration. There were certain hardware limitations which prevented researchers from porting the prototype application software onto the Meta Quest 2 VR headset. To solve this issue the prototype application software was run live on a Predator PH315-53 Laptop and the display information passed to the headset. This issue caused some unexpected consequences to the operation of the application during the experiment administration. The data transfer to the headset slowed down the processing speed from constant memory transmission. The transfer delay resulted in the introduction of some extraneous latency, a confounding condition that must be considered and will be further examined in the discussion of the results. There were no other issues during the experiment administration and all data was collected and recorded successfully from the surveys and the application. Researchers encoded data into respective measurement scales. An accuracy score was determined for each trail and was calculated as a ratio of shots fired and shots hit. After each trial a post round survey was given to participants to collect the latency perception and cybersickness data. A ratio based perceived latency score was documented as the response to the survey which asked the participant to answer on a scale of 0 - 10 how much latency they believed was present during the previous round. The cybersickness data was obtained from survey answers as ratio data on a scale of 0 - 3 of how sick they felt and specific cybersickness symptoms were also recorded based on the Simulator Sickness Questionnaire described by Robert et al. [43].

A. Descriptive Statistics

Some descriptive statistics of importance are as follows; the means given in the summary of accuracy data (fig. 3) show the average percentage of shots hit within each round with the given amount of latency. This value stays very consistent throughout all of the rounds which shows no correlation between latency and the accuracy. Another statistic which stood out was the means from the summary of perception data (fig. 5). These values are the amount of latency perceived by the user on a scale from 0-10, 0 being no latency at all. The users had been informed before hand that there may or may not be latency within each of the trials. The averages from each of the trials also stayed very similar indicating that the latency was equally as noticeable to the user from each trial to the next.

One notable participant had very accurate guesses of latency levels within the rounds. This participant reported they noticed no latency only within the single round in which there was no latency. Then in the subsequent rounds they noticed the latency, assigning both the 20 and 40 ms rounds a 1 out of 10 and the 60 and 80 ms rounds a 2 out of 10. One other unique attribute that made this participant notable is that they hit a larger total number of shots on target than many of the other subjects. They ranged from 19 to 30 shots hit averaging at 25.6 while the other participants ranged from 10 to 27 and averaged at 17.7. It is possible that the faster pace of moving between the different targets at different positions allowed them to notice the latency much more accurately than other participants.

B. One-Way Analysis of Variance

Our study collected parametric data from a within-groups design using the ratio scale of measurement. Based on the characteristic of our data, the one-way Analysis of Variance (ANOVA) statistical formula was selected as the most suitable means of analysis to compare the data across participants. A significance value of $p < 0.5$ was used to determine the statistical significance of results within groups. An ANOVA was run to determine the statistical significance between latency and performance as an accuracy score. The resulting p-value of .9646 suggests that there is no significant correlation between a change in latency and a participant's performance in this experiment (fig. 4). Another ANOVA was run to determine the significance of a participants perception regarding the amount of occurring latency and the actual present latency. A p-value of .9857 signifies that there is no statistical bases to support a connection between perceived latency and actual latency in our study (fig. 6). To summarize, the results of the ANOVAs indicate that there is not a connection between the independent variable, latency, and the dependant variables, performance and perceived latency.

V. Discussion

When examining the data an observation of note is that the JND values captured in our results have no significant correlation with the changes in latency between rounds. This is not consistent with the findings of previous works as they found the maximum JND for latency in VR systems was 24.5ms [36]–[38]. This difference could be due to our specific implementation of latency within the environment being less noticeable than how these studies applied latency to the HMD. All of these previous studies not only applied latency to functions inside the application but also to the movement and navigation functions within the headset. Our design only applied latency to the firing mechanism which is a much smaller component of the overall experiment. This did not seem to significantly decrease their accuracy as it may not stand out as much as the larger changes made in the previous works. Our findings are also not consistent with the work of Louis et al. which found that 60ms of latency was detrimental ($p = 0.043$) to presence within VR systems and that effect was noticed and reported by their participants as "minorly negative" [42]. They applied latency to the animation that would play on the sphere making it overall less responsive and a larger effect to the apparatus. Similar to the deviation from the earlier works mentioned, a possible cause of this dissimilarity is the smaller, less impact-full application of latency onto only the firing mechanism.

During the experiment cybersickness data was collected from the participants based on the Simulator Sickness Questionnaire described by Robert et al. and the data was encoded based on this work [43]. Each participant was asked to rate on a scale of 0 - 3 the degree in which that they had experienced a list of different cybersickness symptoms: general discomfort, fatigue, headache, eye strain, difficulty focusing, increased salivation, sweating nausea, difficulty concentrating, fullness of head, blurred vision, dizziness (eyes open), dizziness (eyes closed), vertigo, stomach awareness, and burping. The ratings of these symptoms were then used to calculate a measurement value representing the category that the symptoms belong to: nausea, oculomotor, and disorientation. These sub scores were given weights and applied to a formula which gives a measurement of the overall severity of the cybersickness experienced by the participants over the course of the experiment. Participants defined as healthy should receive a 0 baseline score. 9 out of the 12 participants experienced cybersickness symptoms and had scores above 0. The severity scores of those above 0 were slight to moderate with a highest score of 120.73. The average SSQ score of all participants was 48.04. The most reported symptoms were headache, eyestrain, difficulty focusing and general discomfort. Oculomotor symptoms was the highest reported category. Even the participants who had experience in VR reported increased symptoms of cybersickness. Participants had no such symptoms going into the experiment and the presence of these symptoms suggests that latency may have an effect on the manifestation of cybersickness symptoms, however this would require additional verification.

There were also several different issues which were present within the study that could have impacted the results and introduced confounding variables. Despite the induced latency continuing to increase between rounds, participants noticed a consistent amount of latency. The extra latency created due to the application being run through unity itself instead of the headset could have confounded the results considering this would make it difficult to differentiate between purposeful latency and incidental latency. One way to fix this in future work would be to use the build feature within unity and send the application out to the headset itself, thus removing the inconsistent extra time for the communication between the laptop and the headset. There was also a lack of any visual indicator from the gun of when it was firing; making the latency itself extremely difficult for the user to notice even when at 80 ms which is higher than previously recorded thresholds for latency to be noticed by a user. A way to address this in future work is to have a clear firing animation that is offset by the latency delay, giving a clear visual indicator of when shots are fired to the user and allowing them to judge mismatches in timing of their input and the responsiveness of the system.

Another possible confounding variable was the size of our targets within the shooting simulation, the targets may have been too large in relation to the camera rotation speed and the time delay of the latency. Too large of targets may have caused even the shots delayed by the latency to still hit the target as the firing direction would still be aligned within the target's collision detection, regardless of the movement of the user. This would suggest that accuracy overall would not be significantly impacted. This can be corrected in the future by decreasing the size of the target to a smaller radius, giving more room for error on account for the delayed fire. The targets were also stationary which means that errors in hitting the target were reliant entirely on the user's movement of the camera away from the target before the offset shot fired. If participants waited before the target was gone before moving on to the next target then the shot would still hit. Making the targets move at some set velocity may cause more shots that are delayed to miss, allowing the latency to impact the accuracy more than it does with a non-moving target.

VI. Conclusion

General adoption and use of Virtual Reality devices has given rise to new types of cyberattacks in the form of perception manipulation attacks. Quantifying the effectiveness of these attacks when they focus on inducement of latency on the headset or in headset applications will require further exploration and study. A future study that may build off and correct the possible limitations in the process and design of this work and may implement more visual indicators of latency through either traditional latency induction on the entire HMD system or more visible animations, as well as smaller harder to hit mobile targets that may introduce chances for the latency to affect the accuracy. Not being able to account for operational latency introduced through running the application from the PC to the headset limits the studies ability to give concrete latency estimates for when users notice latency introduction as the latencies introduced may not be the actual latency experienced by the user. As in any other user study, user's time is not unlimited, because of that the number of tested latencies had to be limited to a small set. The results of this study should be interpreted with this in mind. Possibly due to these limitations, our study finds no significant conclusive evidence that increasing latency has a significant impact on accuracy of user action in Virtual Reality devices.

VII. Contributions

E.A, E.L, and M.S developed and conceived of ideas for the experiment. E.A and M.S created the design of the program. E.A explored the prior work and novel concepts. M.S and J.B created the simulation application including creating assets and writing scripts. J.B performed the experiments including finding subjects and collecting data. E.L and M.S performed all statistical analysis and computations for analysis. E.A took the lead in writing the manuscript and was assisted by E.L and M.S. All authors provided critical feedback and helped shape the research direction, process, and experiment.

VIII. Acknowledgments

We thank Oluwatosin Falebita for his assistance with understanding the many vulnerabilities and attacks present in

the VR Head Mounted Displays and his advice throughout the creation of this experiment.

REFERENCES

[1] A. Godse, R. Khadka and A. Banic, "Evaluation of Visual Perception Manipulation in Virtual Reality Training Environments to Improve Golf Performance," 2019 IEEE Conference on Virtual Reality and 3D User Interfaces (VR), Osaka, Japan, 2019, pp. 1807-1812, doi: 10.1109/VR.2019.8798026.

[2] Sun Joo (Grace) Ahn, Joshua Bostick, Elise Ogle, Kristine L. Nowak, Kara T. McGillicuddy, Jeremy N. Bailenson, Experiencing Nature: Embodying Animals in Immersive Virtual Environments Increases Inclusion of Nature in Self and Involvement with Nature, Journal of Computer-Mediated Communication, Volume 21, Issue 6, 1 November 2016, Pages 399–419, https://doi.org/10.1111/jcc4.12173

[3] Amotz Perlman, Rafael Sacks, Ronen Barak, Hazard recognition and risk perception in construction, Safety Science, Volume 64, 2014, Pages 22-31, ISSN 0925-7535, https://doi.org/10.1016/j.ssci.2013.11.019. (https://www.sciencedirect.com/science/article/pii/S0925753513002877)

[4] Thomas Waltemate, Irene Senna, Felix Hülsmann, Marieke Rohde, Stefan Kopp, Marc Ernst, and Mario Botsch. 2016. The impact of latency on perceptual judgments and motor performance in closed-loop interaction in virtual reality. In Proceedings of the 22nd ACM Conference on Virtual Reality Software and Technology (VRST '16). Association for Computing Machinery, New York, NY, USA, 27–35. https://doi.org/10.1145/2993369.2993381

[5] Sandra Malpica, Ana Serrano, Julia Guerrero-Viu, Daniel Martin, Edurne Bernal, Diego Gutierrez, and Belen Masia. 2022. Auditory Stimuli Degrade Visual Performance in Virtual Reality. In ACM SIGGRAPH 2022 Posters (SIGGRAPH '22). Association for Computing Machinery, New York, NY, USA, Article 23, 1–2. https://doi.org/10.1145/3532719.3543220

[6] N. -M. Aliman and L. Kester, "Malicious Design in AIVR, Falsehood and Cybersecurity-oriented Immersive Defenses," 2020 IEEE International Conference on Artificial Intelligence and Virtual Reality (AIVR), Utrecht, Netherlands, 2020, pp. 130-137, doi: 10.1109/AIVR50618.2020.00031.

[7] Wilson CJ, Soranzo A. The Use of Virtual Reality in Psychology: A Case Study in Visual Perception. Comput Math Methods Med. 2015;2015:151702. doi: 10.1155/2015/151702. Epub 2015 Aug 3. PMID: 26339281; PMCID: PMC4538594.

[8] Wen-Jie Tseng, Elise Bonnail, Mark McGill, Mohamed Khamis, Eric Lecolinet, Samuel Huron, and Jan Gugenheimer. 2022. The Dark Side of Perceptual Manipulations in Virtual Reality. In Proceedings of the 2022 CHI Conference on Human Factors in Computing Systems (CHI '22). Association for Computing Machinery, New York, NY, USA, Article 612, 1–15. https://doi.org/10.1145/3491102.3517728

[9] Azarby, S.; Rice, A. Understanding the Effects of Virtual Reality System Usage on Spatial Perception: The Potential Impacts of Immersive Virtual Reality on Spatial Design Decisions. Sustainability 2022, 14, 10326. https://doi.org/10.3390/su141610326

[10] P. Casey, I. Baggili and A. Yarramreddy, "Immersive Virtual Reality Attacks and the Human Joystick," in IEEE Transactions on Dependable and Secure Computing, vol. 18, no. 2, pp. 550-562, 1 March-April 2021, doi: 10.1109/TDSC.2019.2907942.

[11] Martin Vondráček, Ibrahim Baggili, Peter Casey, Mehdi Mekni,Rise of the Metaverse's Immersive Virtual Reality Malware and the Man-in-the-Room Attack & Defenses, Computers & Security, Volume 127, 2023, 102923, ISSN 0167-4048, https://doi.org/10.1016/j.cose.2022.102923.

[12] S. Valluripally et al., "Detection of Security and Privacy Attacks Disrupting User Immersive Experience in Virtual Reality Learning Environments," in IEEE Transactions on Services Computing, vol. 16, no. 4, pp. 2559-2574, 1 July-Aug. 2023, doi: 10.1109/TSC.2022.3216539.

[13] Sharif Razzaque, David Swapp, Mel Slater, Mary C. Whitton, and Anthony Steed. 2002. Redirected walking in place. In Proceedings of the workshop on Virtual environments 2002 (EGVE '02). Eurographics Association, Goslar, DEU, 123–130.

[14] F. Steinicke, G. Bruder, J. Jerald, H. Frenz, and M. Lappe. 2010. Estimation of Detection Thresholds for Redirected Walking Techniques. IEEE Transactions on Visualization and Computer Graphics 16, 1 (Jan. 2010), 17–27. https://doi.org/10.1109/TVCG.2009.62 Conference Name: IEEE Transactions on Visualization and Computer Graphics

[15] Qi Sun, Anjul Patney, Li-Yi Wei, Omer Shapira, Jingwan Lu, Paul Asente, Suwen Zhu, Morgan Mcguire, David Luebke, and Arie Kaufman. 2018. Towards virtual reality infnite walking: dynamic saccadic redirection. ACM Transactions on Graphics 37, 4 (July 2018), 67:1–67:13. https://doi.org/10.1145/3197517.3201294

[16] Kim, J., Charbel-Salloum, A., Perry, S. et al. Effects of display lag on vection and presence in the Oculus Rift HMD. Virtual Reality 26, 425–436 (2022). https://doi.org/10.1007/s10055-021-00570-x

[17] D. Lee, B. Chang, and J. Park, "Evaluating the Comfort Experience of a Head-Mounted Display with the Delphi Methodology," Journal of Internet Computing and Services, vol. 21, no. 6, pp. 81–94, Dec. 2020.

[18] Stephen Palmisano, Rebecca Mursic, Juno Kim, Vection and cybersickness generated by head-and-display motion in the Oculus Rift, Displays, Volume 46, 2017, Pages 1-8, ISSN 0141-9382, https://doi.org/10.1016/j.displa.2016.11.001.

[19] Scasserra, Dominick, "The influence of perceived task difficulty on task performance" (2008). Theses and Dissertations. 756. https://rdw.rowan.edu/etd/756

[20] S. Valluripally, A. Gulhane, R. Mitra, K. A. Hoque and P. Calyam, "Attack Trees for Security and Privacy in Social Virtual Reality Learning Environments," 2020 IEEE 17th Annual Consumer Communications & Networking Conference (CCNC), Las Vegas, NV, USA, 2020, pp. 1-9, doi: 10.1109/CCNC46108.2020.9045724.

[21] A. Gulhane et al., "Security, Privacy and Safety Risk Assessment for Virtual Reality Learning Environment Applications," 2019 16th IEEE Annual Consumer Communications & Networking Conference (CCNC), Las Vegas, NV, USA, 2019, pp. 1-9, doi: 10.1109/CCNC.2019.8651847.

[22] R. Roman, J. Zhou and J. Lopez, Elsevier Computer Networks Journal, vol. 57, no. 10, pp. 2266-2279, 2013.

[23] Z. Ling, Z. Li, C. Chen, J. Luo, W. Yu and X. Fu, "I Know What You Enter on Gear VR," 2019 IEEE Conference on Communications and Network Security (CNS), Washington, DC, USA, 2019, pp. 241-249, doi: 10.1109/CNS.2019.8802674.

[24] Johnathan Bown, Elisa White, Akshya Boopalan,Chapter 12 - Looking for the Ultimate Display: A Brief History of Virtual Reality, Editor(s): Jayne Gackenbach, Johnathan Bown, Boundaries of Self and Reality Online, Academic Press, 2017, Pages 239-259, ISBN 9780128041574, https://doi.org/10.1016/B978-0-12-804157-4.00012-8. (https://www.sciencedirect.com/science/article/pii/B9780128041574000128)

[25] S. Valluripally, A. Gulhane, K. A. Hoque and P. Calyam, "Modeling and Defense of Social Virtual Reality Attacks Inducing Cybersickness," in IEEE Transactions on Dependable and Secure Computing, vol. 19, no. 6, pp. 4127-4144, 1 Nov.-Dec. 2022, doi: 10.1109/TDSC.2021.3121216.

[26] L. Rebenitsch and C. Owen, "Review on cybersickness in applications and visual displays", Virt. Reality, vol. 20, no. 2, pp. 101-125, Jun. 2016.

[27] S. Davis, K. Nesbitt and E. Nalivaiko, "A systematic review of cybersickness", Proc. Conf. Interactive Entertainment, pp. 1-9, 2014.

[28] W. Zhou, Y. Jia, A. Peng, Y. Zhang and P. Liu, "The effect of IoT new features on security and privacy: New threats existing solutions and challenges yet to be solved", IEEE Internet of Things J., vol. 6, no. 2, pp. 1606-1616, Apr. 2019.

[29] A. Yarramreddy, P. Gromkowski and I. Baggili, "Forensic analysis of immersive virtual reality social applications: A primary account", Proc. IEEE Security Privacy Workshops, pp. 186-196, 2018.

[30] A. M. Gavgani, F. R. Walker, D. M. Hodgson and E. Nalivaiko, "A comparative study of cybersickness during exposure to virtual reality and "classic" motion sickness: Are they different?", J. Appl. Physiol., vol. 125, no. 6, pp. 1670-1680, 2018.

[31] H. K. Kim, J. Park, Y. Choi and M. Choe, "Virtual reality sickness questionnaire (VRSQ): Motion sickness measurement index in a virtual reality environment", Appl. Ergonom., vol. 69, pp. 66-73, 2018.

[32] P. Kourtesis, J. Linnell, R. Amir, F. Argelaguet, and S. E. MacPherson, "Cybersickness in Virtual Reality Questionnaire (CSQ-VR): A Validation and Comparison against SSQ and VRSQ," Virtual Worlds, vol. 2, no. 1, pp. 16–35, Jan. 2023, doi: 10.3390/virtualworlds2010002.

[33] B. Taylor, A. K. Dey, D. Siewiorek, and A. Smailagic, 'Using Crowd Sourcing to Measure the Effects of System Response Delays on User Engagement', in Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems, San Jose, California, USA, 2016, pp. 4413–4422.

[34] D. A. Bowman and R. P. McMahan, "Virtual Reality: How Much Immersion Is Enough?," in Computer, vol. 40, no. 7, pp. 36-43, July 2007, doi: 10.1109/MC.2007.257.

[35] R. S. Allison, L. R. Harris, M. Jenkin, U. Jasiobedzka and J. E. Zacher, "Tolerance of temporal delay in virtual environments," Proceedings IEEE Virtual Reality 2001, Yokohama, Japan, 2001, pp. 247-254, doi: 10.1109/VR.2001.913793.

[36] C. Roth, E. Luckett and J. A. Jones, "Latency Detection and Illusion in a Head-Worn Virtual Environment," 2020 IEEE Conference on Virtual Reality and 3D User Interfaces Abstracts and Workshops (VRW), Atlanta, GA, USA, 2020, pp. 215-218, doi: 10.1109/VRW50115.2020.00046

[37] Adelstein, B. D., Lee, T. G., & Ellis, S. R. (2003). Head Tracking Latency in Virtual Environments: Psychophysics and a Model. Proceedings of the Human Factors and Ergonomics Society Annual Meeting, 47(20), 2083-2087. https://doi.org/10.1177/154193120304702001

[38] S. Ellis, M. Young, B. Adelstein, and S. Ehrlich, 'Discrimination of Changes of Latency during Voluntary Hand Movement of Virtual Objects', Proceedings of the Human Factors and Ergonomics Society Annual Meeting, vol. 43, 09 1999.

[39] M. Meehan, S. Razzaque, M. C. Whitton and F. P. Brooks, "Effect of latency on presence in stressful virtual environments," IEEE Virtual Reality, 2003. Proceedings., Los Angeles, CA, USA, 2003, pp. 141-148, doi: 10.1109/VR.2003.1191132.

[40] K. Mania, B. D. Adelstein, S. R. Ellis, and M. I. Hill, 'Perceptual Sensitivity to Head Tracking Latency in Virtual Environments with Varying Degrees of Scene Complexity', in Proceedings of the 1st Symposium on Applied Perception in Graphics and Visualization, Los Angeles, California, USA, 2004, pp. 39–47.

[41] Ivan E. Sutherland. 1965. The Ultimate Display. In Proceedings of the IFIP Congress. 506–508.

[42] T. Louis, J. Troccaz, A. Rochet-Capellan, and F. Bérard, 'Is It Real? Measuring the Effect of Resolution, Latency, Frame Rate and Jitter on the Presence of Virtual Entities', in Proceedings of the 2019 ACM International Conference on Interactive Surfaces and Spaces, Daejeon, Republic of Korea, 2019, pp. 5–16.

[43] K. S. B. Robert S. Kennedy Norman E. Lane and M. G. Lilienthal, 'Simulator Sickness Questionnaire: An Enhanced Method for Quantifying Simulator Sickness', The International Journal of Aviation Psychology, vol. 3, no. 3, pp. 203–220, 1993.