Attacking CSI-based Sensing with Adversarial Channel State Information Alteration

ABSTRACT

Channel State Information (CSI) of wireless communications is increasingly used for sensing and security applications. However, these applications all assume the authenticity of the obtained CSI, and few prior works have studied whether or how CSI could be adversely modified, which might significantly harm the existing CSI-based sensing systems. This research investigates the potential of modifying a target device's CSI wirelessly. We find that it is hard to achieve CSI alterations with traditional jamming signals. Thus, we explore new interference signals to achieve this purpose. Based on that, we further design two types of attacks, the random and the targeted CSI alterations. The vulnerabilities of an existing CSI-based device authentication system are investigated under the two types of attacks with both theoretical simulations and the real-world experiments with off-the-shelf OFDM devices. Results show that our CSI alteration attacks significantly degrade the usability and security of existing CSI-based authentication systems.

1 INTRODUCTION

Channel State Information (CSI) describes how a signal propagates along the channel from a transmitter to a receiver while being attenuated and scattered. It is originally measured by wireless communication systems to minimize multipath effects and achieve reliable communications. Because CSI changes according to the specific physical obstacles that present in the channel (e.g., walls, furniture, human bodies and other objects), it has been extensively studied for over a decade to achieve numerous wireless sensing purposes, including localization [15, 16], human activity sensing [7, 14] and object recognition [9, 13]. For example, CSI has been found to exhibit the spatial uncorrelation property, which can be used to localize or authenticate a network node [8]. Moving away a registered node can be detected, and an outsider at an unregistered location attempting to access the network would be rejected. The increasingly pervasive Orthogonal Frequency Division Multiplexing (OFDM) devices further accelerate the deployment of CSI-based sensing.

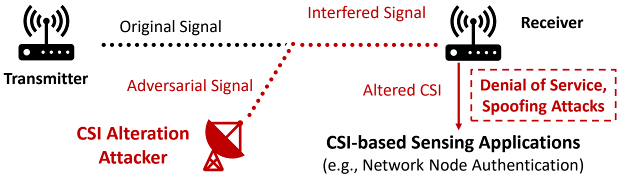


Figure 1: CSI alteration attack scenario.

All these CSI-based sensing applications assume that the CSI obtained by an OFDM system authentically presents the current physical environment or the impacts of surrounding obstacles on the signal propagation. However, this is only true when the wireless environment is relatively stable without intentional interference. Because wireless channels are open and insecure, an adversary could generate intentional interference signals to break the authenticity of CSI and manipulate the CSI-based sensing results. Though there has been active work on radio jamming, which overrides the receiver's signals to cause transmission disruption [2], few efforts have been devoted to study using wireless signals to change the CSI of OFDM systems. This work aims to investigate the long-standing CSI authenticity issue of many CSI-based sensing systems. We find that the traditional jamming signals are not designed to alter an OFDM system's CSI and easy to cause blocking. We thus explore new interference signals to achieve the intermediate status between benign transmission and blocking. The proposed interference signals are formed by one or more OFDM subcarriers.

Based on the new type of interference signal, we propose a CSI alteration attack platform as illustrated in Figure 1, which has the potential to study the vulnerabilities of most CSI-based sensing systems. These systems use a transmitter-receiver pair to sense the physical environment and apply learning models to classify the CSI measured at the receiver. The proposed CSI alteration attacker transmits an adversarial signal to interfere with the transmitter's signal at the receiver, which alters the CSI wirelessly and makes it unable to describe the authentic physical environment. We further design two types of attacks to meet different malicious purposes. In particular, we develop the random CSI alteration attack, which injects random noises to the CSI measured at the receiver with the aim to cause sensing errors (e.g., misclassifications) or Denial of Service (DoS). We also develop the targeted CSI alteration attack, which applies Artificial Intelligence (AI) to generate specific interference signals and convert a receiver's CSI into an intended pattern. For example, for a CSI-based network node authentication system, an adversary's device can exhibit similar CSI as one registered network node to achieve identity spoofing or repudiation. Moreover, the objective CSI pattern may not be exactly the same as that of the target node to fool a CSI-based sensing system that uses learning models. This work shows that only modifying one or several OFDM subcarriers is sufficient to achieve high success rate.

Our main contributions are summarized as follows:

- To the best of our knowledge, this is the first work to systematically study the vulnerability of CSI-based sensing systems under intentional interference and show the potential of modifying an OFDM device's CSI wirelessly.
- We propose a new type of interference signal by leveraging OFDM subcarriers. The proposed signal outperforms the existing jamming signals in modifying an OFDM receiver's CSI without causing disruption.
- We develop two attack methods, the random and the targeted CSI alteration attacks and evaluate the vulnerabilities of an existing CSI-based network node authentication system under such attacks.
- We demonstrate that the proposed attacks have already been available to harm current off-the-shelf devices. Moreover, we develop a CSI alteration attack testbed to facilitate the vulnerability study of more CSI-based sensing systems.

2 RELATED WORK

Few efforts have been devoted to study the intentional interference on OFDM systems. Most studies focus on the unintentional wireless interference that exists in multi-user scenarios. Since legitimate devices are restricted by distances, antenna types, transmitting power, signal patterns, and the constraints set by communication protocols (e.g., collision avoidance), unintentional interference only exerts limited impacts and has been addressed by many works [5, 6, 10]. Intentional interference has no such restrictions and could cause more severe problems. Wireless jamming is the most explored adversarial interference, which generates jamming signals to override the receiver's signals and cause transmission failure [2]. It is also feasible to jam the transmitter to attack the collision avoidance protocols used by commodity devices, which keeps the channel "busy" and blocks a transmitter from sending signals. As a result, the receiver is unable to receive packets to measure CSI under jamming signals, which leads to DoS. Nevertheless, few works ever report the success of using jamming signals to modify CSI.

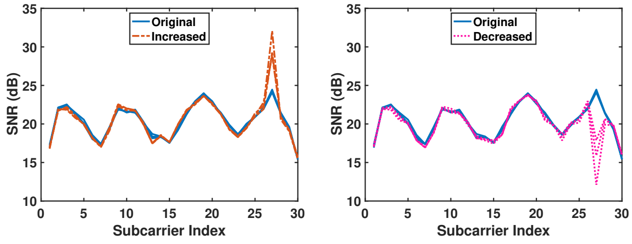
There are several works using a malicious transmitter to falsify the CSI obtained at the receiver, which can be divided into two categories. One is to attack the CSI feedback mechanism of communication systems. Specifically, an adversary's device can eavesdrop on other devices' CSI feedback (sent in plain text to achieve low latency) and then report false CSI accordingly to the base station to enhance its own network capacity [11, 17]. The other uses a malicious transmitter to send symbol-level delayed copies of its packet preambles to manipulate the CSI measurement at the receiver [3]. However, these methods all require the transmitter to be controlled by an adversary, and the attacks are only shown with lab devices. Differently, this work leverage the wireless interference signals, and the attack is shown available to harm current commodity OFDM devices, which shows a potential to cause a large-scale impact.

3 BACKGROUND AND ATTACK MODELS

3.1 Modeling CSI Under Interference

OFDM is widely used in wireless communication systems such as IEEE 802.11a/g/n/ac/ah and HIPERLAN/2, due to its high spectral efficiency and strong resilience to selective fading, interference, and multipath effects. As a frequency division multiplexing technology, OFDM utilizes a number of overlapping but orthogonal subcarriers to maximize spectral efficiency without causing inter-channel interference. Furthermore, each subcarrier with a slightly different center frequency experiences different multi-path fading effects, and all the subcarriers together depict the wireless channel in a fine-grained manner. The CSI of OFDM systems is a set of complex values, including both amplitude and phase information, as expressed by $\mathbf{h} = [h_1, h_2, ..., h_i, ..., h_M]^T, i \in [1, M]$, where M is the number of subcarriers in the narrow band. h_i can be represented as $h_i = |h_i|e^{j\angle h_i}$, where $|h_i|$ is the CSI amplitude at the i^{th} subcarrier, and $\angle h_i$ denotes its phase. Before communicating messages, a transmitter first sends a packet preamble with pre-defined training sequences $\mathbf{x} = [x_1, x_2, ..., x_M]^T$ modulated on multiple subcarriers. The receiver decodes the received sequence $\mathbf{y} = [y_1, y_2, ..., y_M]^T$ with the prior knowledge of $\mathbf{x}$ to obtain the CSI measurement as: $\mathbf{y} = \sqrt{P_l}\mathbf{X}\mathbf{h} + \mathbf{w} = \sqrt{P_l}[x_1h_1 + w_1, x_2h_2 + w_2, ..., x_Mh_M + w_M]^T$, where $\mathbf{X}$ is a $M \times M$ diagonal matrix with $(m, m)^{\text{th}}$ element given as $[\mathbf{X}]_{(m,m)} = x_m$, $\mathbf{w} = [w_1, w_2, ..., w_M]^T$ is the background noise, and P_l is the average signal-to-noise ratio (SNR) after considering the path loss. The CSI is then measured using Least Square (LS) or Minimum Mean Square Error-based (MMSE) estimation [12].

The CSI measurement process under the intentional interference can be expressed as $\mathbf{y} = \sqrt{P_l}\mathbf{X}\mathbf{h} + \mathbf{w} + \mathbf{j}$, where $\mathbf{j}$ is the adversarial signal received by the receiver. The traditional jamming attacks generate Additive Gaussian Noises, sinusoidal signals or frequency-sweeping signals to interfere with the transmitted signals. Because most OFDM systems use narrow bands, it is not hard to override the entire band



(a) Increase a subcarrier's amplitude (b) Decrease a subcarrier's amplitude

Figure 2: CSI alteration attack on commodity WiFi.

with jamming frequencies. We test the above signals to study the feasibility of wirelessly modifying the CSI $\mathbf{h}$. But we find it is hard to modify the CSI, which is several hundred kHz wide. Specifically, the receiver either fails to obtain CSI due to the channel blocking or gets the hard to control CSI modifications. This is because OFDM subcarriers are *sinc* signals in the frequency domain, which are overlapped and orthogonal. The traditional jamming signal even targeting at a subcarrier also interferes with all other subcarriers, causing the transmission to be easily interrupted or the hard-to-control CSI changes. In comparison, a weak jamming signal is not sufficient to impact the OFDM subcarriers, which have a strong resilience to co-channel interference.

3.2 New Interference Signal

Because OFDM subcarriers are orthogonal, we propose to modify each subcarrier separately by using a similar subcarrier signal on the same central frequency. The proposed new interference signal is thus formed from multiple OFDM subcarriers, which is combined with the transmitter's signal and modify each subcarrier of the CSI. By setting the initial phase, the modulated sequence and transmitting power of each interference signal subcarrier, we can achieve the specific CSI modification. Figure 2 illustrates the feasibility to increase or decrease the amplitude of a single CSI subcarrier (i.e., subcarrier 27). The interference signal only changes the target CSI subcarrier, while the other subcarriers are unchanged. This is because the attack signal is orthogonal to the other subcarriers, which only interferes with the target subcarrier. Furthermore, by moving the attack antenna a little closer to or farther from the receiver, the subcarrier 27's CSI amplitude is increased or decreased. The reason is that the changed transmission distance leads to the different phases of the attack signal when it arrives at the receiver and combines with the target signal.

3.3 Threat Models

This work focuses on attacking the current CSI-based network node authentication system via wireless interference, where each network node accesses network via a gateway. The node's uplink CSI is used as the physical signature associated to its unique location. Due to channel reciprocity, the downlink and uplink CSIs can be used to derive each other. We consider two types of CSI alteration attacks, which are based on the above interference signal:

Random CSI Alteration Attack. The adversary in this scenario only wants to increase sensing errors and cause one or more victim nodes to suffer from DoS (different from traditional DoS which directly blocks the signal transmission, this type of DoS is much harder to be detected). The errors are random or not controllable. The adversary does not need to know the original uplink CSI of the victim.

Targeted CSI Alteration Attack. We assume the adversary knows the original uplink CSI of the targeted victim node, such as by deriving it from the downlink CSI. Then the adversary can apply AI algorithms to determine the specific interference signal to generate, which converts the CSI of the adversary's node to be close to the CSI of the targeted victim node, so that the adversary's node can be misclassified as the targeted victim node. Based on that, the adversary can achieve identity spoofing.

4 APPROACH DESIGN

We propose two types of CSI alterations attacks according to the above attack models.

4.1 Random Attack Design

Considering that a CSI alteration attacker exists in OFDM system, given the eavesdropped reported CSI $\hat{\mathbf{h}}$, the objective of the attacker is to design an adversarial signal and send it to the receiver during channel estimation phase. Specifically, the attacker transmits a total of M carefully designed adversarial signal, $a_1, \ldots, a_M$. If $a_m \neq 0$, we consider that there is an adversarial signal injected on the m^{th} subcarrier. Both single-carrier CSI alteration attack (i.e., only one of the M subcarriers injected signal is nonzero) and multi-carrier CSI alteration attack (i.e., the injected signal on multiple subcarriers are nonzero) are investigated. The signal received at the receiver affected by the injected adversarial signal is expressed as $\mathbf{y}_{\text{Jam}} = \sqrt{P_l}\mathbf{X}\mathbf{h} + \sqrt{P_l^{\text{eve}}}\mathbf{A}\mathbf{h}_{\text{eve}} + \mathbf{w}$, where $\mathbf{A}$ is a $M \times M$ diagonal matrix with m^{th} diagonal element representing the adversarial signal designed at m^{th} subcarrier, a_m. $\mathbf{h}_{\text{eve}} \in C^M$ denotes the channel between the receiver and attacker, and P_l^{eve} is the average SNR considering the path loss. We can estimate the CSI based on the jammed signal as: $\hat{\mathbf{h}}_{\text{Jam}} = \hat{\mathbf{h}} + \sqrt{P_l P_l^{\text{eve}}}\mathbf{R}\mathbf{X}^H \left(P_l \mathbf{X}\mathbf{R}\mathbf{X}^H + \sigma^2 \mathbf{I}\right)^{-1} \mathbf{A}\mathbf{h}_{\text{eve}}$, with respect to the pilot signal $\mathbf{X}$. After CSI alteration attack, the estimated CSI at the receiver side is $\hat{\mathbf{h}}_{\text{Jam}}$ instead of $\hat{\mathbf{h}}$. The receiver then reports the falsified $\hat{\mathbf{h}}_{\text{Jam}}$, which is used for diverse sensing applications.

4.2 Targeted Attack Design

An adversary can further generate the adversarial signal to modify the estimated CSI at the receiver into a target pattern, $\mathbf{h}_{\text{target}}$. We thus formulate the optimum adversarial signal

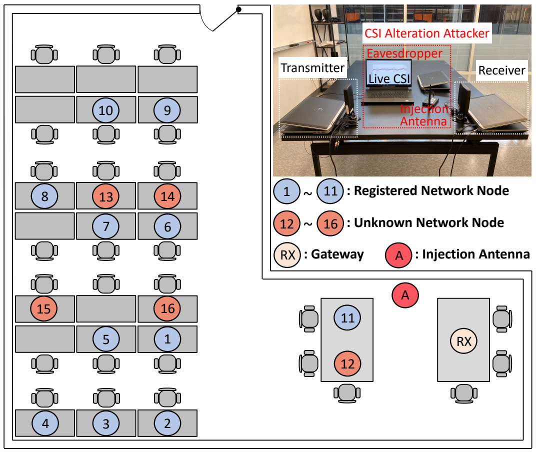


Figure 3: Testbed & experimental setup.

design problem as

$$\min_{\mathbf{A}} \left\|\mathbf{h}_{\text{target}} - \hat{\mathbf{h}}_{\text{Jam}}\right\|^2 = min_{\mathbf{A}} \left\|\mathbf{h}_{\text{target}} - \left(\hat{\mathbf{h}} + \sqrt{P_l P_l^{\text{eve}}}\mathbf{R}\mathbf{X}^H \left(P_l \mathbf{X}\mathbf{R}\mathbf{X}^H + \sigma^2\mathbf{I}\right)^{-1} \mathbf{A}\mathbf{h}_{\text{eve}}\right)\right\|^2 \quad (1)$$

and we address the above adversarial signal design problem through the semidefinite relaxation technique as discussed as follows: by defining $\mathbf{h}_\Delta \triangleq \mathbf{h}_{\text{target}} - \hat{\mathbf{h}}$, $\mathbf{\Pi} \triangleq \sqrt{P_l P_l^{\text{eve}}}\mathbf{R}\mathbf{X}^H \left(P_l \mathbf{X}\mathbf{R}\mathbf{X}^H + \sigma^2\mathbf{I}\right)^{-1}$, $\tilde{\mathbf{a}} \triangleq \mathbf{A}\mathbf{h}_{\text{eve}}$, and we have $\min_{\tilde{\mathbf{a}} \in C^M} \|\mathbf{h}_\Delta - \mathbf{\Pi}\tilde{\mathbf{a}}\|^2$. Notice that this optimization problem is not a homogeneous quadratically constrained quadratically program (QCQP), but we can homogenize it as:

$$\min_{\mathbf{u} \in C^{M+1}} \mathbf{u}^H\mathbf{D}\mathbf{u}, \quad \text{s.t.}\, \mathbf{u}^H\mathbf{V}\mathbf{u} = 1 \quad (2)$$

where $\mathbf{u}=[\tilde{\mathbf{a}}^T, \alpha]^T$, $\mathbf{D}=\begin{bmatrix} \mathbf{\Pi}^H\mathbf{\Pi} & -\mathbf{\Pi}^H\mathbf{h}_\Delta \\ -\mathbf{h}_\Delta^H\mathbf{\Pi} & \mathbf{h}_\Delta^H\mathbf{h}_\Delta \end{bmatrix}$, and $\mathbf{V}=\begin{bmatrix} \mathbf{0}_{M\times M} & \mathbf{0}_{M\times 1} \\ \mathbf{0}_{1\times M} & 1 \end{bmatrix}$.

4.3 Attack Hardware Implementation

Accordingly, we develop an attack platform based on commodity 802.11n (WiFi) devices as shown in Figure 3. Two laptops (i.e., Latitude E6430) connected with external antennas are used as the transmitter and the receiver. The transmitter sends packet preambles to the receiver to measure CSI, which returns packets to the transmitter with CSI in the payload. Both laptops are embedded with the Intel 5300 NIC and run Ubuntu 14.04.4. The Linux 802.11n CSI Tool is installed to send WiFi packets and extract CSI from received packets [4]. The obtained CSI consists of complex values in 30 OFDM subcarriers for each antenna pair, which are evenly distributed among 56/112 subcarriers for 20MHz/40MHz bands.

The CSI alteration attacker is implemented with a Latitude E6430 laptop connected to a software-defined radio (SDR) transceiver HackRF One. The proposed new interference signals are sent, which independently modify each subcarrier of the target link to change the CSI pattern. The interference signal targeting a subcarrier should be orthogonal and not influential to other subcarriers, which is the basis to control CSI alteration with more freedom and not to cause communications disruption easily.

Specifically, we generate the adversarial interference signal using GNU Radio, where the byte streams generated by a vector source are added with the packet length tags and passed into the OFDM modulator. The output is a complex modulated signal at baseband, which is then modulated onto the center frequency of one or more subcarriers of the target 802.11n channel by the osmocom sink, which connects GNU Radio with SDR devices. With different gains set, the interference signals at the center frequencies of different subcarriers of the target channel can be transmitted with different signal powers. The software-generated signals are then fed to HackRF One to be transmitted in parallel.

5 PERFORMANCE EVALUATION

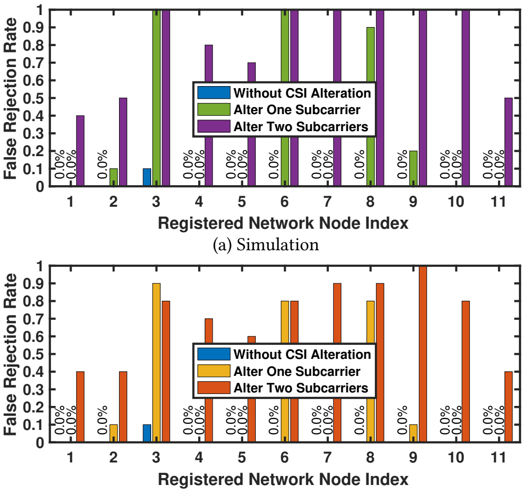
5.1 Experimental Setup

The attack platform is evaluated against a CSI-based network node authentication system, which leverages the unique physical information (i.e., the multipath effect) between the gateway and the network node captured by the CSI to localize and authenticate a registered network node. Specifically, a receiver placed at a fixed location acts as the gateway, while a transmitter placed at several different locations acts as the network nodes. The gateway uses the measured CSI as the radio signature to verify the network node's identity (i.e., location). Figure 3 shows the locations of the gateway and the network nodes in a typical indoor office where the experiments are conducted.

5.2 Implementation of CSI-based Network Node Authentication System

We implement one CSI-based authentication [1] to evaluate our attack designs. As shown in Figure 3, we construct a network with a gateway (node RX) and 11 nodes (i.e., node 1 to node 11), which are registered with their locations. Five more locations are randomly chosen as the unregistered locations (i.e., node 12 to node 16). For each of these sixteen nodes, we perform 20 trials to collect the CSI, with each trial lasting for 10 seconds. We extract the amplitudes of the 30 subcarriers as the CSI pattern. Half of the legitimate nodes' data are used to train a cluster-based classification algorithm based on Euclidean distance. In particular, for each registered node, a cluster center is obtained by averaging its training CSI patterns, and a threshold (i.e., the Euclidean distance between the CSI pattern and the cluster center) is selected such that both False Acceptance Rate (FAR) and False Rejection Rate (FRR) of the cluster are minimized. During testing, a coming instance is classified to one of the registered network nodes if the Euclidean distance between the instance's CSI pattern and the cluster center is within the threshold. Otherwise, the instance will be classified to the "unknown" class.

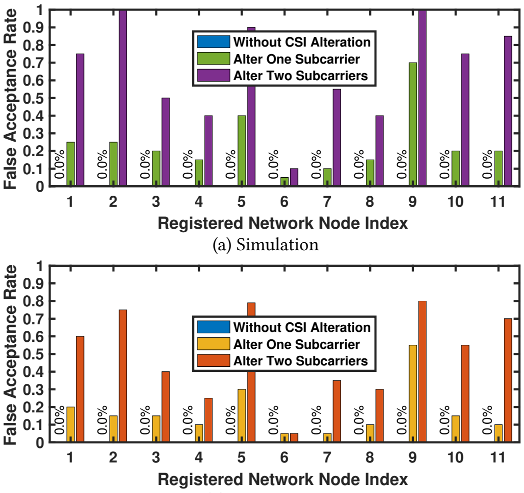
The authentication system is tested with the other half of data, including both the registered and unknown nodes.



(a) Simulation

(b) Experiments

Figure 4: Performance of random attack.



(a) Simulation

(b) Experiments

Figure 5: Performance of targeted attack.

When there is no intentional interference, the authentication system achieves over 99.5% accuracy of accepting the registered network nodes and rejecting the unknown nodes.

5.3 Random CSI Alteration Attack

We perform this attack on all 11 registered network nodes to cause DoS by only altering 1 or 2 CSI subcarriers. Before launching the attack, we first perform simulations of altering the CSI patterns of these nodes according to our random attack design to look for the theoretical optimal settings of the attack signal. As the maximum CSI amplitude change we can achieve for a single subcarrier practically is around $30dB$, we thus set this number as the limit for changing the amplitude during the simulation. The altered CSI patterns are then tested on the above note authentication system. The results are shown in Figure 4 (a). We observe that when altering one subcarrier, the False Rejection Rate (FRR) of node 2, 3, 6, 8, and 9 increases from 0% to 10%, 100%, 100%, 90%, and 20% respectively. When altering two subcarriers, the FRR of more than half of the nodes increases to 100%. The results show the vulnerability of using the wireless signals for sensing under intentional interference. Moreover, the ability to alter more subcarriers gives the adversary more freedom to attack and higher success rates.

Based on the simulation, we set the attack signal parameters to launch the attack. We place the injection antenna at Location A in Figure 3 and use it to alter the CSI at 1 or 2 subcarriers. For each of the 11 registered network nodes, we perform 20 trials to alter their CSI. As illustrated by Figure 4 (b), when altering one subcarrier, the FRR of node 2, 3, 6, 8, and 9 increases to 10%, 90%, 80%, 80%, and 10% respectively, while the FRRs of other nodes remain to be 0%. When altering two subcarriers, eight of the nodes’ FRRs are increased to be above 60%. The results confirm the severe vulnerability of current WiFi-based sensing systems under random intentional interference with field test. Moreover, the success rate (i.e., FRR) of the random attack in practical scenarios has a good match rate with the theoretical analysis, though the performance of the practical experiment is slightly lower. There are some practical challenges from configuring the attack platform to match the theoretical analysis and other unidentified external impacts, which need to be addressed further. Nonetheless, altering more subcarriers could further increase the DoS success rates.

5.4 Targeted CSI Alteration Attack

Different from the random attack which tries to alter the CSI of the registered network nodes to cause DoS, the targeted attack aims to change the CSI of a network node into an objective pattern to turn an adversary’s device to be legitimate or camouflage a registered node as another to achieve repudiation. To evaluate this attack design, we also perform both the theoretical simulation and the experiments with commodity WiFi devices.

During simulation, we first compute the Euclidean distance between the unknown network node and the targeted registered network node with respect to its original CSI pattern. Then we perform the simulation to alter 1 or 2 subcarriers of the unknown network node’s CSI patterns and search for the alteration that shows the closest distance to the objective pattern. We repeat the simulation to attack each legitimate node from all five unregistered locations (i.e., 5 × 11 = 55 pairs in total for the simulation), and use the altered CSI patterns to attack the authentication system. As shown in Figure 5 (a), when altering one subcarrier, seven of the registered network nodes’ FARs are increased from 0% to above 20%, with the highest FAR being 70% (i.e., node 9). When altering two subcarriers, there are eight registered network nodes whose FARs increase from 0% to be over 50%, with two of them reaching 100% (i.e., the one of node 2 and node 9). It's interesting to note that even with two subcarriers altered, the FAR of node 6 is just increased to 10%. The reason is the CSI patterns of all five unknown network nodes are still much different from that of node 6. By modifying more subcarriers, this node can be spoofed with higher success rates. The results indicate that with proper subcarrier(s) altered, one network node can be misclassified by the CSI-based node authentication as the targeted legitimate node, achieving identity spoofing or repudiation.

Based on the targeted attack simulation, we have learned the optimal signal settings. We then launch the attack with our platform to evaluate it in practical scenarios. Specifically, for each pair of unknown network node and registered network node, we perform 20 trials to collect the altered CSI, and extract the CSI patterns using the same method as above. The CSI patterns are then tested on the CSI-based note authentication system. Similarly, for each legitimate node selected as the target, we present the best attack performance that can be achieved using the altered CSI patterns from one of the unregistered network nodes. As we can observe from Figure 5 (b), when altering one subcarrier, the FARs of more than half of the nodes increase from 0% to over 15%. When altering two subcarriers, there are 7 nodes whose FARs increase from 0% to over 40%, with the highest FAR being 80%. For node 6, the FAR is increased to 5%. The results confirm the severe vulnerability of CSI-based authentication under targeted CSI alteration attack. Moreover, the performance of the practical experiment also matches with the simulation results, though showing the slightly lower performance. The results also show the potential of further improving the targeted attack by altering more subcarriers.

6 CONCLUSION & FUTURE WORK

This paper explores the potential of altering a target device's CSI via intentional interference. We propose new interference signals and two types of CSI alteration attacks. A testbed is built on commodity WiFi devices for studying the vulnerability of current CSI-based sensing systems. The results of both simulation and testbed experiments show the severe security issues of a CSI-based network node authentication system. The findings lead to the reconsideration of using radio signals and CSI for mission-critical sensing tasks or providing physical-layer security.

For the future work, we plan to (1) expand the attack ability of altering more subcarriers, (2) leverage our testbed to study the vulnerabilities of more CSI-based sensing systems, including object recognition and human activity sensing, (3) explore the optimal capability and limitations of such attack, (4) developing defense mechanisms, including new detection methods and more resilient wireless sensing systems.

REFERENCES

[1] Shu Chen, Yingying Chen, and Wade Trappe. 2008. (Acceptance Rate: 11.9%) - Premier conference in pervasive computing. Exploiting Environmental Properties for Wireless Localization and Location Aware Applications. In *Proceedings of the Fifth Annual IEEE International Conference on Pervasive Computing and Communications (IEEE PerCom)*.

[2] T Charles Clancy. 2011. Efficient OFDM denial: Pilot jamming and pilot nulling. In *2011 IEEE ICC*. IEEE, 1–5.

[3] Song Fang, Yao Liu, Wenbo Shen, and Haojin Zhu. 2014. Where are you from? Confusing location distinction using virtual multipath camouflage. In *Proceedings of the 20th annual international conference on Mobile computing and networking*. 225–236.

[4] Daniel Halperin, Wenjun Hu, Anmol Sheth, and David Wetherall. 2011. Tool release: gathering 802.11 n traces with channel state information. *ACM SIGCOMM Computer Communication Review* 41, 1 (2011), 53–53.

[5] Hussein Hijazi and Laurent Ros. 2008. Polynomial estimation of time-varying multipath gains with intercarrier interference mitigation in OFDM systems. *IEEE TVT* 58, 1 (2008), 140–151.

[6] Junqiang Li, K Ben Letaief, and Zhigang Cao. 2003. Co-channel interference cancellation for space-time coded OFDM systems. *IEEE Transactions on Wireless Communications* 2, 1 (2003), 41–49.

[7] Zhenzhe Lin, Yucheng Xie, Xiaonan Guo, Chen Wang, Yanzhi Ren, and Yingying Chen. 2019. Wi-Fi-Enabled Automatic Eating Moment Monitoring Using Smartphones. In *EAI International Conference on IoT Technologies for HealthCare*. Springer, 77–91.

[8] Hongbo Liu, Yan Wang, Jian Liu, Jie Yang, and Yingying Chen. 2014. Practical User Authentication Leveraging Channel State Information (CSI). In *Proceedings of the 9th ACM Symposium on Information, Computer and Communications Security (ACM ASIACCS)*. 389–400.

[9] Sheng Tan and Jie Yang. 2021. Object Sensing for Fruit Ripeness Detection Using WiFi Signals. *arXiv preprint arXiv:2106.00860* (2021).

[10] Stefano Tomasin, Alexei Gorokhov, Haibing Yang, and J-P Linnartz. 2005. Iterative interference cancellation and channel estimation for mobile OFDM. *IEEE Transactions on Wireless Communications* 4, 1 (2005), 238–245.

[11] Yu-Chih Tung, Sihui Han, Dongyao Chen, and Kang G Shin. 2014. Vulnerability and protection of channel state information in multiuser MIMO networks. In *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security*. 775–786.

[12] J-J Van De Beek, Ove Edfors, Magnus Sandell, Sarah Kate Wilson, and P Ola Borjesson. 1995. On channel estimation in OFDM systems. In *1995 IEEE 45th Vehicular Technology Conference. Countdown to the Wireless Twenty-First Century*, Vol. 2. IEEE, 815–819.

[13] Chen Wang, Jian Liu, Yingying Chen, Hongbo Liu, and Yan Wang. 2018. Towards in-baggage suspicious object detection using commodity WiFi. In *2018 IEEE Conference on Communications and Network Security (CNS)*. IEEE, 1–9.

[14] Yan Wang, Jian Liu, Yingying Chen, Marco Gruteser, Jie Yang, and Hongbo Liu. 2014. E-eyes: device-free location-oriented activity identification using fine-grained WiFi signatures. In *Proceedings of the 20th Annual International Conference on Mobile Computing and Networking (ACM MobiCom)*. 617–628.

[15] Kaishun Wu, Jiang Xiao, Youwen Yi, Dihu Chen, Xiaonan Luo, and Lionel M Ni. 2012. CSI-based indoor localization. *IEEE Transactions on Parallel and Distributed Systems* 24, 7 (2012), 1300–1309.

[16] Jie Yang, Yingying Chen, Wade Trappe, and Jerry Cheng. 2012. Detection and localization of multiple spoofing attackers in wireless networks. *IEEE TPDS* 24, 1 (2012), 44–58.

[17] Yang Yang, Yanjiao Chen, Wei Wang, and Gang Yang. 2020. Securing channel state information in multiuser MIMO with limited feedback. *IEEE Transactions on Wireless Communications* 19, 5 (2020), 3091–3103.