Anti-Spoofing for Single-Antenna Devices using Rotational Channel State Information

Avishek Mukherjee*, Tyler Moody†, Mason Strawn‡ and Manish Osti§
Department of Computer Science and Information Systems, Saginaw Valley State University
University Center, Michigan, USA
Email: *amukher1@svsu.edu, †tpmoody@svsu.edu, ‡mwstrawn@svsu.edu, §mrosti@svsu.edu

***Abstract*—In this paper, we investigate the efficacy of using rotational Channel State Information (CSI) on Anti-Spoofing methods in indoor wireless networks. Physical layer information like the CSI often acts like a fingerprint for different locations. Most Anti-Spoofing (AS) methods leverage this uniqueness to detect spoofed packets originating from an attacker that claims to be a genuine user. However, due to the sparsity of wireless channels, there are times when the CSI from different locations may look similar and AS systems may fail to detect a spoofed packet. We propose Rotational Channel State Information - Anti-Spoofing (RCSI-AS), that uses multiple CSI measurements by rotating the antenna on an Access Point (AP) at different angles to greatly improve the detection of spoofed packets. We conducted real world experiments and found that RCSI-AS can detect spoofed packets over 99.6% of the time when using multiple angular configurations at the Access Point (AP) and maintains a low false positive ratio when comparing packets from the same user.**

***Index Terms*—Channel State Information, Wireless Networks, Anti-Spoofing, Wireless Security.**

I. INTRODUCTION

Wireless security has become a critical component of modern Wi-Fi systems with the rapidly increasing production of internet capable devices. As the number of connected devices have increased, so has the potential for different types of network attacks from adversaries. These include channel jamming, packet sniffing, replay attacks, packet spoofing and more. Spoofing, in particular, is a form of attack whereby an adversary (say, Bob) impersonates a user (Alice) device by using their IP address to generate packets to a server. The server may believe these packets originated from Alice and can inadvertently let Bob access confidential information. Detection of spoofing attacks has been a topic of interest for researchers who have proposed anti-spoofing systems to thwart these types of attacks.

In recent years, a number of anti-spoofing methods have been developed that rely on the physical layer information of a wireless packet to determine its authenticity. For example, one of the authors of this paper developed Time-Bounded Anti-Spoofing (TBAS) [1] , that uses physical layer characteristics including the Channel State Information (CSI) to detect spoofed packets. In a wireless system, the CSI between a transmitter and a receiver is represented as a set of complex numbers that is measured at the receiver. This is useful in understanding the channel characteristics and is often used to set rate and beamforming parameters at the sender. In practice, the measured CSI is actually a representation of the multi-path components of the wireless signal from the transmitter to the receiver, due to physical phenomena like scattering, diffraction etc. Thus, in addition to measuring the channel coefficients, the CSI can also be thought of as a fingerprint for a receiver-transmitter location pair. To be more specific, changing the location of either device will result in a different set of measurements as the wireless signal may now undergo a different set of reflections, resulting in different paths. The uniqueness of CSI at different locations can thus be leveraged to identify if a packet arriving at an AP is genuine or spoofed by comparing it with a known CSI measurement from the actual user device.

While the general idea of using CSI measurements to differentiate between users works well, recent studies [2] have also highlighted the sparse nature of wireless channels, whereby the CSI from different locations may exhibit similar patterns making it hard for an Anti-Spoofing system to distinguish between some locations. The idea behind using rotational CSI measurements for spoof detection stems from two interesting observations in industry trends. First, there has been an exponential increase in Internet of Things (IoT) devices in the last decade and these devices now form a large percentage of wireless devices that are constantly communicating with a server. These devices are low power devices and are usually equipped with a single antenna for wireless communications. As such, improvements that rely on antenna diversity may not always be applied to these devices. Second, modern APs such as the Archer AXE200 Omni [3], now come equipped with mechanical antennas that can be rotated automatically with internal motors. These are capable of quickly rotating to different angles and are used to optimize the wireless signal to connected devices.

This poses an interesting question. *Can anti-spoofing methods be improved by using the CSI measurements from different angles on the AP antenna for devices that are limited to a single antenna?* The answer lies in determining whether offsetting the antenna at arbitrary angles introduces sufficient changes in the multi-path components of the signal to be able to distinguish it from the signal at another location. We tackle this problem using experimental analysis in real world locations and propose RCIS-AS - an improved anti-spoofing algorithm complementary to most existing solutions.

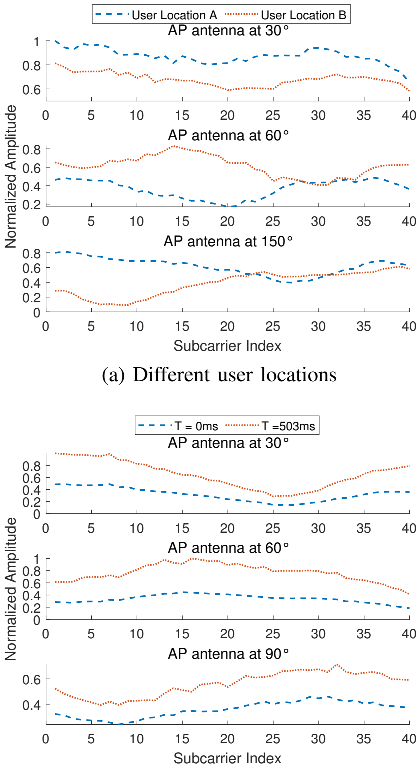
The rest of the paper is organized as follows. Section II discusses existing research efforts with anti-spoofing. Section III provides a high level overview of RCSI-AS and some theoretical background. Section IV discusses the details of RCSI-AS. Section V evaluates the performance on real world data. Section VI concludes the paper.

II. Related Work

Anti-spoofing methods that rely on physical layer information have been of interest to researchers in recent years. Typically, detection methods that rely on physical layer information usually attempt to localize the spoofed packet using characteristics like the received signal strength [4] [5] or angle or arrival [6] [7] to distinguish between users. RCSI-AS differs from all of these methods as it solely relies on the channel state information for detection of spoofed packets.

There has been some related research that uses the CSI measurements as a fingerprint to detect spoofed packets. These include prior work done by the authors on Time Bounded Anti-Spoofing (TBAS) [1] and Time Bounded Anti-Spoofing on Multiple Input Multiple Output (TBAS-MIMO) systems [8] which is an extension to TBAS with multiple antenna configurations. The key idea behind TBAS is that the CSI for a location does not change in a short interval. When an AP running TBAS receives a packet from a user, it sends a dummy packet to the user that forces the user to send back an ACK in accordance with the 802.11 MAC protocol. If this was a spoofed packet that was sent by an attacker, the AP may receive two responses, one from the actual user (if the attacker does not respond) or a collided signal if both the attacker and the actual user decide to respond. It can then compare the CSI from the original packet and the dummy ACK to determine the authenticity of the request. TBAS was implemented using Software Defined Radios that uses the CSI measurements as well as the power and other physical layer information to achieve low false negative ratios during evaluation. TBAS-MIMO was an experimental study on extending TBAS to commercial off-the-shelf wireless cards that only reports the CSI and no other information. A scenario where the original TBAS sometimes fails is when the CSI from both the attacker and the user coincidentally look similar. This is possible due to the sparsity of wireless channels. TBAS-MIMO attempts to solve this problem by introducing more spatial diversity and comparing the CSI from multiple antenna pairs. TBAS-MIMO also looked at the effects of mobility on the system and recommended guidelines for implementing TBAS. RCSI-AS uses a completely different method from both TBAS and TBAS-MIMO. First, RCSI-AS is targeted towards single antenna devices that may not always be able to take full advantage of the recommendations outlined by TBAS-MIMO. Second, RCSI-AS attempts to introduce spatial diversity by rotating the antenna on the AP to collect CSI measurements at different angular configurations within a short interval. Finally, RCSI-AS periodically probes the user device to frequently update the CSI measurements from the user.

Other research findings that also rely on the CSI include Support Vector Machine (SVM) [9] techniques that uses clustering to distinguish CSI measurements from different users and needs a burn in period. More recent efforts include [10]–[13] which are actually complementary to RCSI-AS. We also note that RCSI-AS is much simpler to implement than some of the methods listed here since RCSI-AS only works at the AP and no modification is needed on the user device. Finally, spoof detection methods like [14] [15] are aimed towards 5G networks with different physical layer characteristics than Wi-Fi.



(a) Different user locations

(b) Same user location 500ms apart

Fig. 1. CSI measurements at different angles

III. Overview of Anti-Spoofing in RCSI-AS

This section provides an overview of RCSI-AS. To keep things simple, we will consider a 1x1 configuration i.e. the AP has a single antenna and the user device also has a single antenna. RCSI-AS works only at the AP and periodically sends out a burst of C probes, where C is referred to as the angular configuration or the number of angles the antenna on the AP is rotated by. The user device receives these probes and responds with ACK packets that are used to measure the CSI between the user and the AP. The value of C is determined empirically, and we found that using $C = 3$ served a good balance between accuracy of RCSI-AS and the probe overhead. As an example, Fig. $1(a)$ shows the CSI measured from two user devices A and B at different locations in a classroom. It can be seen that, when $C = 1$, or when a single probe is used with the antenna positioned at 30 degrees, the CSI measured for the two users look very similar. They seem to be different only by a constant factor which could be attributed to the hardware gain applied to signal during measurement. Thus, using the CSI measured from a single antenna, it may not always be possible to distinguish between two users. However, when using $C = 3$, it is clear that the users are different as the CSI measured at other angles (60 degrees and 150 degrees) look very different from the first configuration. Thus, RCSI-AS would correctly be able to distinguish between user locations in this example. The details on the choice of C can found in Section V.

On the other hand, Fig. $1(b)$ shows the measured CSI on 3 antennas from the same user measured at the AP around 500 milliseconds apart. It is evident that the CSI looks very similar at all 3 angles and the CSI values are only offset by a fixed constant at the AP. This is the key idea behind RCSI-AS, to increase the spatial diversity when antenna diversity is not possible.

In the following sections, we expand on the techniques and heuristics used in RCSI-AS to detect spoofed packets using multiple angular measurements.

IV. Details of RCSI-AS

This section outlines the details of the RCSI-AS system. We note that, while the core idea behind RCSI-AS and its implementation is completely different from our prior work on TBAS, some of the mathematical computations, namely the packet alignment and curve distortion, remain similar as these are metrics used when comparing the similarity of the measured CSI between two packets and can be applicable to any AS system that uses the CSI to detect spoofed packets.

A. Channel State Information

The CSI is measured at the AP and is a set of complex numbers representing the summation of the multiple signal propagation paths from the sender antenna to the receiver antenna. Modern Wi-Fi systems implement Orthogonal Frequency-Division Multiplexing (OFDM). Thus, the CSI measurement on each OFDM subcarrier can be approximated as

$$H = \sum_{p=1}^{P} \alpha_p e^{if\delta_p} \tag{1}$$

where α_p and δ_p denote the amplitude and delay of path p, and P is the total number of multi-path components from the sender to the receiver.

RCSI-AS considers the absolute value for each complex subcarrier when looking at the measured CSI. The phase values of the measured CSI can sometimes comprise of linear and non-linear phase errors [16] that make it difficult to utilize the phase values directly with RCSI-CS.

B. Packet Alignment

As seen in Fig. 1, when measuring the CSI across packets, the hardware applies a different gain value for each packet. Thus, before looking at the differences in CSI between 2 packets, the absolute values need to be aligned. The alignment ratio r between two packets A and B can defined as

$$r = \frac{\sum_{j=1}^{N} a_j b_j}{\sum_{j=1}^{N} a_j^2} \tag{2}$$

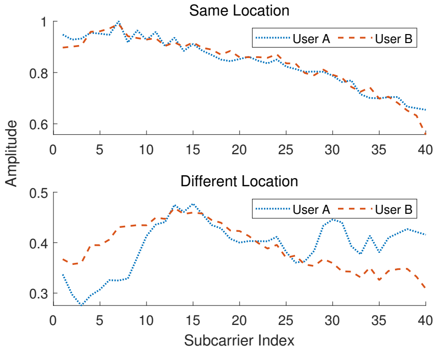


Fig. 2. Effect of alignment on CSI from same location vs different locations

where a_j and b_j are the measured CSI values at subcarrier j for A and B, respectively. The top half of Fig. 2 shows an example of applying the alignment to two packets from the same location that are only offset by some factor. After alignment, both signals almost overlap each other and look very similar in their shape and magnitude. On the other hand, applying the alignment to packets from different locations will still result in very different looking packets. It should also be noted that the alignment ratio is computed for every angular configuration.

C. Curve Distortion

The Curve Distortion ϵ between two aligned packets A and B is defined as

$$\epsilon = \frac{\sum_{j=1}^{N} (ra_j - b_j)^2}{\sum_{j=1}^{N} (ra_j)^2} \tag{3}$$

where a_j and b_j are the aligned CSI values at subcarrier j for A and B, respectively and r is the alignment ratio. This is essentially a numeric representation of the relative difference between two packets. For reference, the ϵ values in Fig. 1(a) when comparing the CSI for different users at $30°, 60°$ and $150°$ are 0.003, 0.17 and 0.35 respectively, whereas for the same user location, as seen in Fig. 1(b), these values are 0.0005, 0.001 and 0.002 It is evident that using multiple angular measurements has a clear advantage as the probability of two distinct user locations exhibiting similar channel characteristics at all of the different angular configurations remains very low.

D. Spoof Detection Threshold

The Curve Distortion is computed for each location pair across every angle in an angular configuration. Suppose we use an angular configuration C of the antenna. We can then define the Spoof Detection Value γ between 2 users X and Y as

$$\gamma = \max_{\{C_k^\circ\}} [\epsilon(k)] \tag{4}$$

where $\epsilon(k)$ refers to the k^{th} curve distortion in C. The ϵ is then compared against a Spoof Detection Threshold to determine if the packets originated from different user locations. We use a threshold of 0.03 in our evaluation of RCSI-AS as we found lower distortion values usually just originate from comparing the Gaussian noise between two similar CSI signals.

V. Evaluation

RCSI-AS was evaluated using real world experimental data collected over the course of one month at different locations in an university setting. The robustness of RCSI-AS was measured using its false positive and false negative performance. The evaluation process is described below.

A. Experimental Setup

As the drivers for routers like the one mentioned in [3] are proprietary, RCSI-AS was built using commercial off-the shelf routers fitted with an external motor and a Raspberry PI to control the rotation of the antenna. An overview of the hardware setup and architecture is shown in Fig. 3. The AP used in RCSI-AS is a TP-Link N750 Wireless router. The router's firmware was modified with the OpenWrt [17] tool that enabled greater control of the channel, rate, and transmission power parameters. In addition, one of the external antennas of the router was connected to a Dorhea SG90 Micro Servo Motor that was controlled using a Raspberry Pi 3 Model B. To measure the CSI, we installed the NexMon CSITool [18] [19] on a Raspberry PI Model 4 which contains a single internal antenna. An external laptop was used to send pings to the router that enabled us to measure the CSI. Some auxiliary switches were used to facilitate remote operation of these devices.

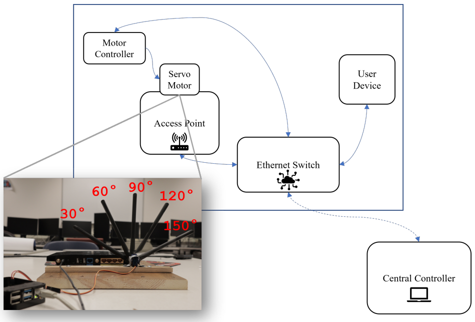


Fig. 3. System Architecture

B. Data Collection

We ran several experiments using the Nexmon CSITool at different locations including classrooms, computing labs and office spaces. We enabled only a single antenna for the AP and so the measured CSI was a linear vector representing the 64 subcarrier values on a 20MHz wireless channel. The experiments were conducted in an environment with relatively moderate mobility. This allowed us to simulate different types CSI data representative of real world wireless channels. Some example locations can be seen in Fig. 4 where the AP was kept stationary inside a computer lab while the CSI for different user locations was measured. For each user location, a total of 5 angular CSI measurements were recorded. These measurements were recorded at $[30°, 60°, 90°, 120°, 150°]$. We note that these angles were chosen arbitrarily. In other words, RCSI-AS will work with any configuration of angular measurements. Our evaluation suite consisted of measurements from 500 different locations.

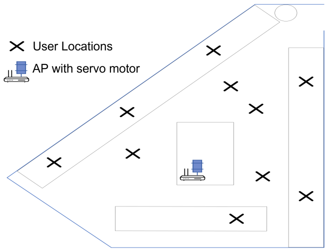


Fig. 4. Some Experimental Locations

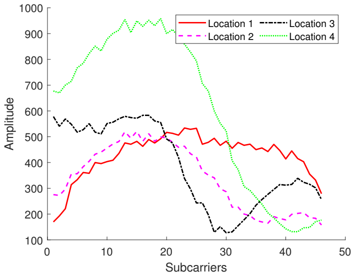


Fig. 5. Absolute value of CSI in 4 locations

C. Data Preprocessing

The CSI measurements were first sanitized by removing null and pilot subcarrier indexes, as defined in the 802.11ac standard [20]. These subcarriers do not contain actual measurements and are not considered by RCSI-AS. The absolute value of some typical CSI measurements after removal is shown in Fig. 5. In addition, a few more pre-processing operations were performed.

- It can be seen from Fig. 5 that the subcarriers at both ends of the measurement seem to attenuate. The exact cause of this is unknown, although we suspect it is due to some additional filtering in hardware. Thus, we truncate the signal by removing 6 subcarriers from both ends of the measured CSI.
- Sometimes the recorded CSI contains very high spikes that do not represent actual measurements. We discard measurements where the number of subcarriers with spikes exceed 30% of the total number of measured subcarriers.
- In some cases, the CSI was only recorded for half of the bandwidth. These packets were also filtered out by comparing the average power between the first and second halves of the CSI measurement and filtering these packets out if the difference between them exceeded an order of magnitude.
- After performing the above preprocessing steps, we observed that the measured CSI may still contain some

outlier values. Thus a final round of pre-processing is performed using a Hampel filter to detect these outliers from the CSI measurements using a median absolute deviation threshold over a window size of 5. We note that this does not always smooth out all the outliers, especially at either end of the measured CSI, but this is a limitation of the CSITool not RCSI-AS.

- After pre-processing the measured CSI was normalized with its maximum amplitude set to 1.

D. *False Negative Performance*

This section describes the false negative performance of RCSI-AS. The goal of this evaluation is to check how often RCSI-AS can correctly identify that two users X and Y are different by comparing their measured CSI. The preprocessed CSI measurements from all 500 locations was considered for this evaluation. A random CSI measurement was chosen from each location. Then, the comparison described in Section IV was performed for each unique location pair.

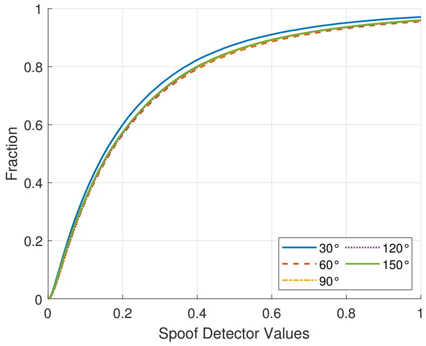


Fig. 6. False Negative Performance with Single Angular Configuration

1) Base Case: Fig. 6 shows the cumulative distribution of spoof detector values (γ) when using angular configuration of $C = 1$. It can be clearly seen that in the base case, when only one angle of the antenna is considered, roughly 8.98% of the CSI pairs may be misclassified by RCSI-AS as the same user using a spoof detection threshold of 0.03. A typical example was shown earlier in Fig. 1(a) where the measured CSI from two different locations looked similar. Upon further inspection, Fig. 7 shows a distribution of the location indexes along with the fraction of misclassifications by RCSI-AS when considering only the measured CSI at one angle. It can be seen that for most locations, there is at least one other location where the measured CSI may coincidentally look similar.

2) Multiple Angular Configurations: The advantage of RCSI-AS becomes evident when moving to higher angular configurations $(C > 2)$, which reduces the probability that the measured CSI will exhibit similar characteristics across all angles in C. We looked at the performance of RCSI-AS for every combination of different angular configurations. For example, when looking at angular configurations of size 2, the performance of all $\binom{5}{2}$ or 10 possible combinations was considered and it was found that the percentage of mis-classifications drops to 1.1% as opposed to almost 9% in the base case. Fig. 8 shows the cumulative distribution plot of all possible angular configurations. It is clear that increasing the angular measurements to RCSI-AS results in a much lower mis-classification rate. When all antenna angles are used $C = 5$, the mis-classification rate drops to 0.16% which makes RCSI-AS extremely accurate, albeit at the expense of a higher probe overhead. Based on the empirical data, we found that using $C = 3$ or 3 angular measurements serves as a good balance between the probe overhead and results in overall accuracy of 99.69%.

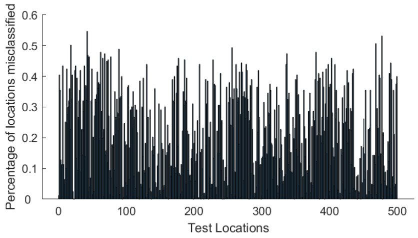


Fig. 7. Percentage of Locations that are misclassified by RCSI-AS at 90°

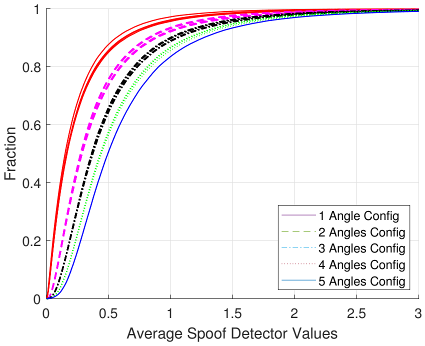


Fig. 8. False Negative Performance with higher configurations

E. *False Positive Performance*

This section discusses the misclassification rate of RCSI-AS when considering packets from the same user. To measure its performance, we looked at packets from the same user location at different intervals during the data collection process. RCSI-AS compared a total of over 4800 packet pairs from same locations measured within a short interval of each other.

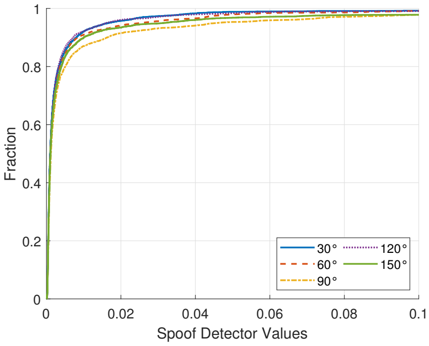


Fig. 9. False Positive Performance with Single Angular Configuration

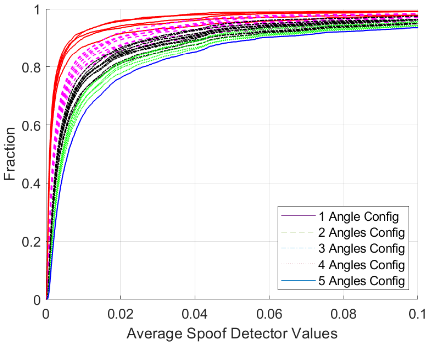


Fig. 10. False Positive Performance with higher configurations

1) Base Case: As with the false negative evaluation, we first establish the performance RCSI-AS when using $C = 1$. Fig. 9 shows the cumulative distribution of the spoof detector values (γ) across each individual angle when comparing the CSI from a single angular measurement. It can be seen that the false positive ratio is very good, and the percentage of misclassifications is below 5% when using a threshold of 0.03.

2) Higher Configurations: It can be seen from Fig. 10 that increasing the number of angular configurations has a slight degradation on the false positive performance. This is expected since we consider the largest curve distortion value within each combination. The false positive performance still remains around 93% when using an angular configuration of $C = 3$ values. In addition, Fig. 11 shows the distribution of the error values on all subcarriers when comparing the signals after alignment at every angle. The distribution is mostly smooth and the differences mainly arise from the quantization and noise in the measured CSI.

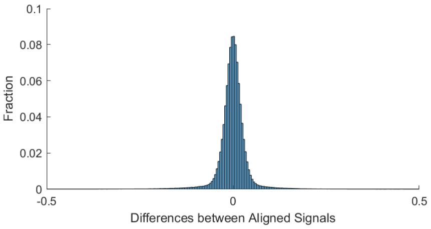


Fig. 11. False Positive Performance when using higher configurations

VI. Conclusion and Future Work

We proposed RCSI-AS, a novel anti-spoofing system based on rotational channel state information on commodity wireless APs. We implement a motorized system that allows rotation of the antennas of an AP to measure the CSI at multiple angles. RCSI-AS works by periodically sending multiple probes to a user device at different angular configurations. This allows RCSI-AS to detect spoofed packets even when the CSI at different locations may exhibit similar characteristics at one angular position of the antenna. We evaluated RCSI-AS using real world experiments in 500 different locations and found that RCSI-AS can detect packets from different locations over 99.60% of the time when using 3 or more angular configurations. At the same time, when looking at packets from the same user location RCSI-AS will correctly identify packets from the same user over 95% of the time. RCSI-AS is aimed at single antenna devices which may not always be able to take advantage of anti-spoofing methods that rely on antenna diversity. We are currently looking into extensions to RCSI-AS that can reduce the probe overhead even further and also assess its performance in high mobility environments.

References

[1] M. Liu, A. Mukherjee, Z. Zhang, and X. Liu, “TBAS: Enhancing Wi-Fi Authentication by Actively Eliciting Channel State Information,” in *2016 13th Annual IEEE International Conference on Sensing, Communication, and Networking (SECON)*, pp. 1–9, 2016.

[2] R. He, B. Ai, G. Wang, M. Yang, C. Huang, and Z. Zhong, “Wireless Channel Sparsity: Measurement, Analysis, and Exploitation in Estimation,” *IEEE Wireless Communications*, vol. 28, no. 4, pp. 113–119, 2021.

[3] “AXE11000 Tri-Band Wi-Fi 6E Router.” https://www.tp-link.com/us/home-networking/wifi-router/archer-axe200-omni/, 2013.

[4] Y. Chen, W. Trappe, and R. P. Martin, “Detecting and Localizing Wireless Spoofing Attacks,” in *2007 4th Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks*, pp. 193–202, 2007.

[5] J. Yang, Y. Chen, W. Trappe, and J. Cheng, “Detection and localization of multiple spoofing attackers in wireless networks,” *IEEE Transactions on Parallel and Distributed Systems*, vol. 24, no. 1, pp. 44–58, 2013.

[6] H.-C. Chen, T.-H. Lin, H. T. Kung, C.-K. Lin, and Y. Gwon, “Determining RF angle of arrival using COTS antenna arrays: A field evaluation,” in *MILCOM 2012 - 2012 IEEE Military Communications Conference*, pp. 1–6, 2012.

[7] J. Xiong and K. Jamieson, “SecureAngle: Improving Wireless Security Using Angle-of-Arrival Information,” Association for Computing Machinery, 2010.

[8] A. Mukherjee, A. W. Garvin, S. E. Sanchez, and Z. Zhang, “Experimental Evaluation of Time Bounded Anti-Spoofing (TBAS) in MIMO Systems,” in *GLOBECOM 2017 - 2017 IEEE Global Communications Conference*, pp. 1–6, 2017.

[9] H. Liu, Y. Wang, J. Liu, J. Yang, and Y. Chen, “Practical User Authentication Leveraging Channel State Information (CSI),” Association for Computing Machinery, 2014.

[10] J. K. Tugnait, “Detection of Pilot Spoofing Attack Over Frequency Selective Channels,” in *2018 IEEE Statistical Signal Processing Workshop (SSP)*, pp. 737–741, 2018.

[11] C. Li and A. Sezgin, “Spoofing attack detection in dynamic channels with imperfect CSI,” *arXiv preprint arXiv:2101.06185*, 2021.

[12] X. Li, K. Huang, S. Wang, and X. Xu, “A physical layer authentication mechanism for IoT devices,” vol. 19, pp. 129–140, 2022.

[13] Z. Jiang, J. Zhao, X.-Y. Li, J. Han, and W. Xi, “Rejecting the attack: Source authentication for Wi-Fi management frames using CSI Information,” in *2013 Proceedings IEEE INFOCOM*, pp. 2544–2552, 2013.

[14] W. Li, N. Wang, L. Jiao, and K. Zeng, “Physical Layer Spoofing Attack Detection in MmWave Massive MIMO 5G Networks,” vol. 9, pp. 60419–60432, 2021.

[15] D. Spoljar, K. Lenac, D. Zigman, and M. Marović, “A Mobile Network-Based GNSS Anti-Spoofing,” in *2018 26th Telecommunications Forum (TELFOR)*, pp. 1–3, 2018.

[16] H. Zhu, Y. Zhuo, Q. Liu, and S. Chang, “Pi-splicer: Perceiving accurate csi phases with commodity wifi devices,” *IEEE Transactions on Mobile Computing*, vol. 17, no. 9, pp. 2155–2165, 2018.

[17] “OpenWrt: A Linux kernel based operating system for embedded solutions.” https://openwrt.org/, 2022.

[18] M. Schulz, D. Wegemer, and M. Hollick, “Nexmon: The C-based Firmware Patching Framework.” https://openwrt.org/, 2017.

[19] F. Gringoli, M. Schulz, J. Link, and M. Hollick, “Free Your CSI: A Channel State Information Extraction Platform For Modern Wi-Fi Chipsets,” in *Proceedings of the 13th International Workshop on Wireless Network Testbeds, Experimental Evaluation & Characterization*, WiNTECH ’19, p. 21–28, 2019.

[20] “IEEE Standard for Information technology – Telecommunications and information exchange between systems,” *IEEE Std 802.11ac-2013*, pp. 1–425, 2013.