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

Authors

- Avishek Mukherjee
- Tyler Moody
- Mason Strawn
- Manish Osti

Presented by

Avishek Mukherjee
Assistant Professor of Computer Science
Saginaw Valley State University
amukher1@svsu.edu

Presenter Bio

- Avishek Mukherjee is an Assistant Professor of Computer Science and Information Systems at Saginaw Valley State University in Michigan, USA
- He received his Ph.D. in Computer Science from Florida State University in 2018.
- His area of research is in wireless networks and systems, with a focus on Channel State Information in indoor Wi-Fi networks.
- He was awarded the Michigan Space Grant Consortium (MSGC) Seed Grant in 2020 for his work on user localization using LTE signals.
- Outside of research, he served as the faculty mentor for the CS team at the NASA Lunabotics Competition in 2021.
- Since 2020, he has also been serving as the faculty advisor for the Association for Computing Machinery (ACM) chapter at SVSU.

Wireless Research group at SVSU

- I currently work with undergraduate students who are interested in the field of wireless networking.
- Our current research is based on gesture recognition using Channel State Information.

Contents

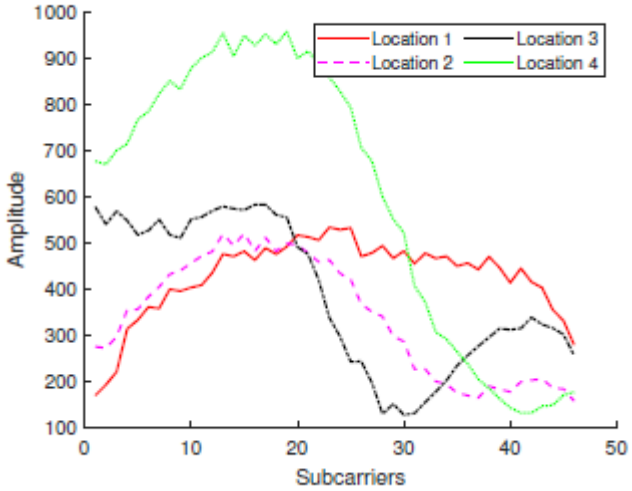
- Introduction
- Prior Work on TBAS
- RCSI-AS Overview
- RCSI-AS Details
- Evaluation
- Conclusion

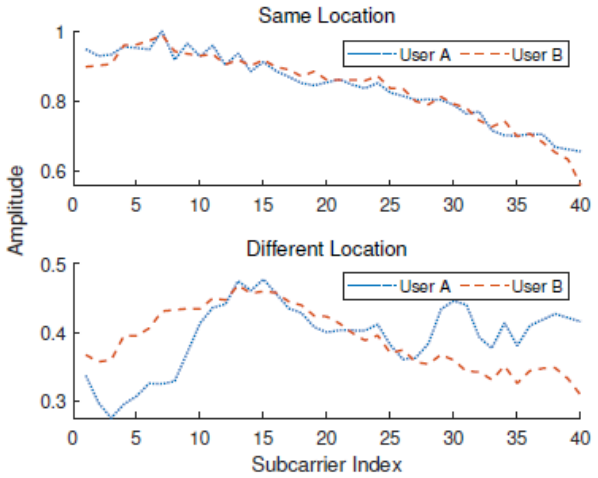
Introduction

- Wireless security is critical in modern Wi-Fi systems.
- Subject to replay attacks, sniffing, jamming etc.
- Spoofing refers to impersonating a user's device using their IP address.
- We design RCSI-AS an anti-spoofing algorithm to detect spoofed network packets at the Access Point(AP)
- Uses physical layer characteristics including the Channel State information to determine authenticity

Key Idea behind using CSI for Anti-Spoofing

- Channel State Information is a representation of the multi-path components of a wireless system.
- CSI acts as fingerprint for different locations.
- For the same location, CSI does not change much within a short interval





Prior Work with TBAS

- Time Bounded Anti-Spoofing (TBAS) is a spoof detection method for Wi-Fi systems. [1]
- TBAS-MIMO is a related extension to the original paper. [2]
- Uses CSI to differentiate incoming packets from adversaries.

Some experimental locations for TBAS

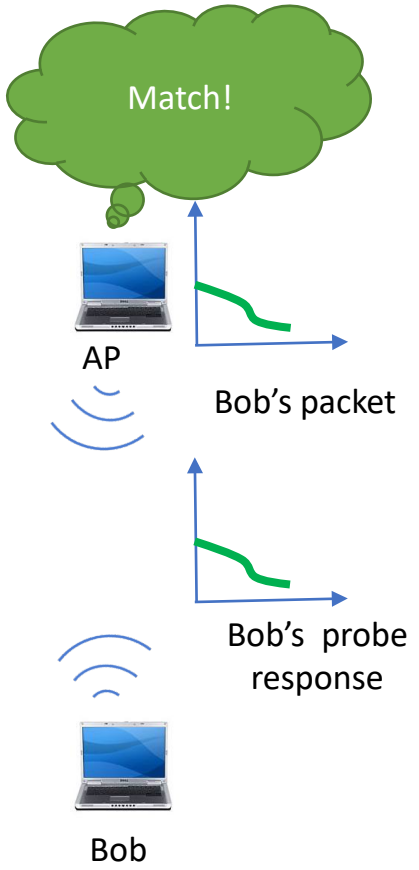
[1] M. Liu, A. Mukherjee, Z. Zhang and X. Liu, "TBAS: Enhancing Wi-Fi Authentication by Actively Eliciting Channel State Information," 2016 13th Annual IEEE International Conference on Sensing, Communication, and Networking (SECON), London, UK, 2016, pp. 1-9, doi: 10.1109/SAHCN.2016.7733021.
[2] Mukherjee, A. W. Garvin, S. E. Sanchez and Z. Zhang, "Experimental Evaluation of Time Bounded Anti-Spoofing (TBAS) in MIMO Systems," GLOBECOM 2017 - 2017 IEEE Global Communications Conference, Singapore, 2017, pp. 1-6, doi: 10.1109/GLOCOM.2017.8254018.

TBAS implementation

Bob sends a packet to the AP

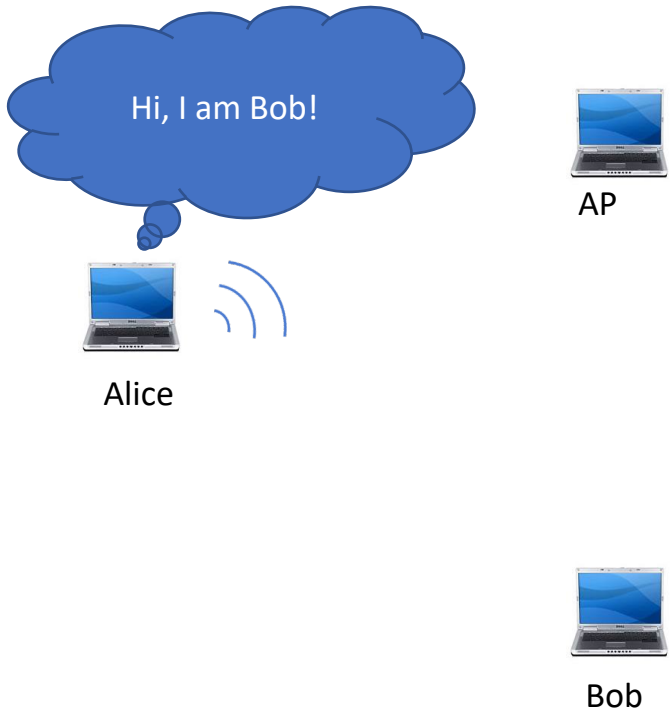
TBAS implementation

AP actively elicits the CSI by sending out a probe, to which Bob responds



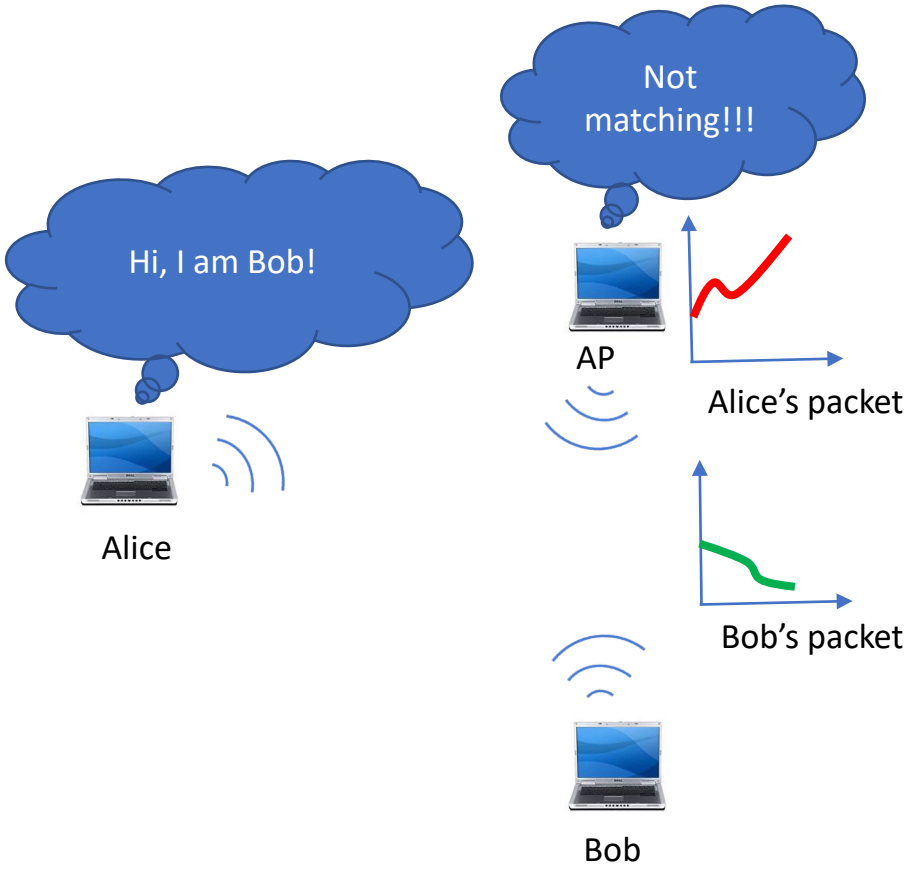
TBAS implementation

Alice sends a packet to the AP pretending to be Bob.



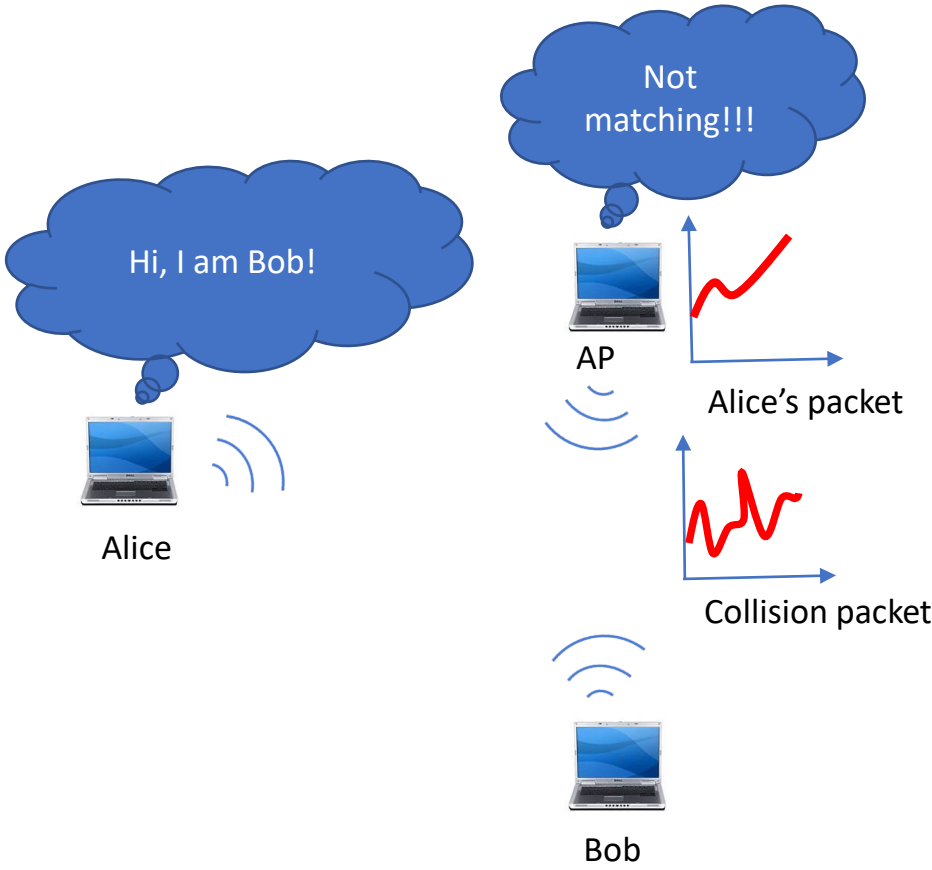
TBAS implementation

AP actively elicits the CSI by sending out a probe, to which Bob responds



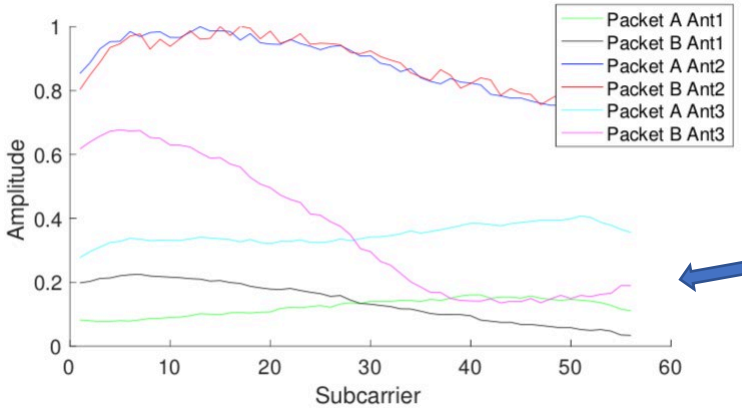
TBAS implementation

If Alice also responds, there is a collision.



TBAS Performance and TBAS-MIMO

Two locations reporting similar CSI on Antenna 1



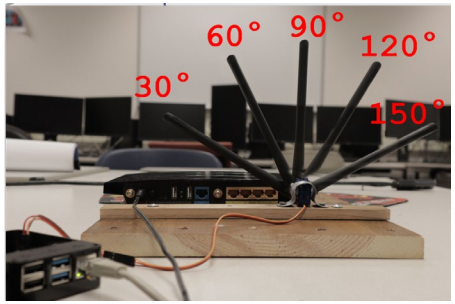
On MIMO systems, Consider CSI from all RX and TX pairs

- TBAS works well conceptually, however, in the real world, the CSI from two locations may coincidentally looks similar.
- May sometimes cause TBAS to misclassify packets from different locations to be the same.
- TBAS-MIMO improves this by considering CSI measurements on multiple antenna pairs, thereby reducing the probability of a misclassification if one of the measurements look similar.

Rotational Channel State Information-Anti-Spoofing (RCSI-AS)

- RCSI-AS targets single antenna systems that cannot take advantage of TBAS-MIMO.
- Still uses the CSI from a single antenna, but instead of a single measurement, multiple measurements are recorded for different antenna angles.
- Routers like Archer AXE200 Omni come equipped with internally motorized antennas to optimize wireless signal reception
- RCSI-AS uses a custom setup with external fitted motors to demonstrate this proof of concept.

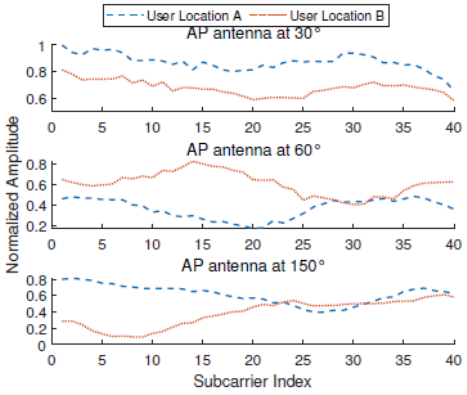
Image Source: https://static.tp-link.com/upload/image-line/AXE200_Omni_UN_1.0_F_large_20220103095533n.jpg



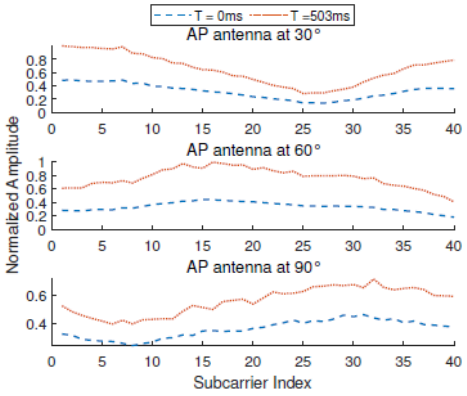
RCSI-AS custom setup with TP-Link N750 and SG90 Servo Motors

Rotational Channel State Information-Anti-Spoofing

- RCSI-AS works by periodically sending out a burst of ‘C’ probes from the AP to a connected device
- Each probe is sent at a different angle of the router antenna, pre-determined at the AP.
- This causes the device to respond with a series of ACKs that are used to measure the CSI at the AP.
- RCSI-AS can determine the authenticity by comparing the CSI from the current probes with the CSI measurements from the past.



(a) Different user locations



(b) Same user location 500ms apart

RCSI-AS Details

- RCSI-AS uses the CSI to measure similarity between two user locations
- The core process outlined in RCSI-AS is as follows
  - Packet Alignment (unchanged from TBAS)
  - Curve Distortion (unchanged from TBAS)
  - Spoof Detection Threshold

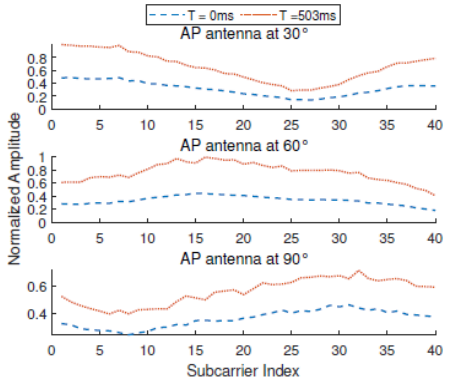
RCSI-AS Details – Packet Alignment

- The measured CSI undergoes different hardware gains at the receiver, so before measuring the similarity, the absolute values are aligned using a simple alignment procedure.
- The alignment ratio between two CSI vectors And B is defined as

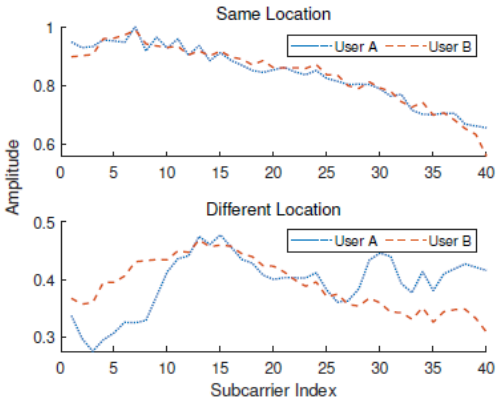
$$r = \frac{\sum_{j=1}^{N} a_j b_j}{\sum_{j=1}^{N} a_j^2}$$

where a_j and b_j are the measured CSI values at subcarrier j for A and B, respectively and N is the total number of subcarriers.

- Also, applying the alignment ratio to packets form different locations still keeps them sufficiently different



Same user location 500ms apart



Effect of applying alignment

RCSI-AS Details – Curve Distortion

- After alignment, the curve distortion value is a numeric representation of the relative difference between two CSI measurements

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

where a_j and b_j are the measured CSI values at subcarrier j for A and B, respectively and N is the total number of subcarriers. *r* denotes the alignment ratio.

RCSI-AS Details – Spoof Detection Threshold (SDT)

- The spoof detection values between 2 users X and Y is given by

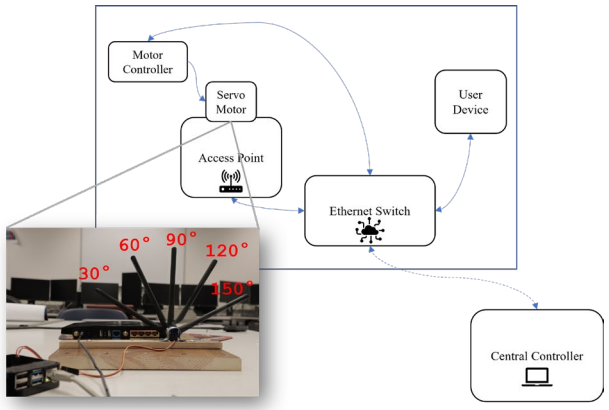
$$\gamma = \max_{\{C_k^\circ\}} [\epsilon(k)]$$

where C refers to a set of angles in an antenna configuration and ϵ(k) refers to the k^{th} curve distortion C.

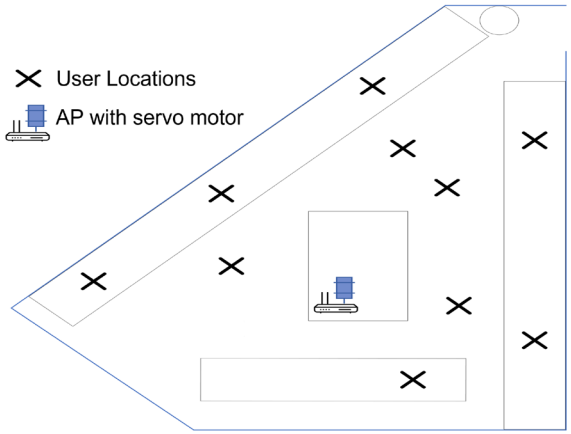
- Using empirical evaluation, it was found that RCSI-AS works best when using C =3 and a spoof detection threshold of 0.03.
- Lower SDT values led to false positives, as smaller differences are usually due to Gaussian noise in the measurements
- Using C = 3, serves as a good balance between accuracy and probe overhead.

Evaluation – Experimental Setup

- Real world testing was conducted.
- Hardware Configuration
  - TP-Link N750 Wireless Router
  - Dorhea SG90 Servo Motors
  - Raspberry Pi 3
  - Two Laptops
- Software Configuration
  - OpenWRT (on router)
  - Nexmon CSITool[*] (on router)



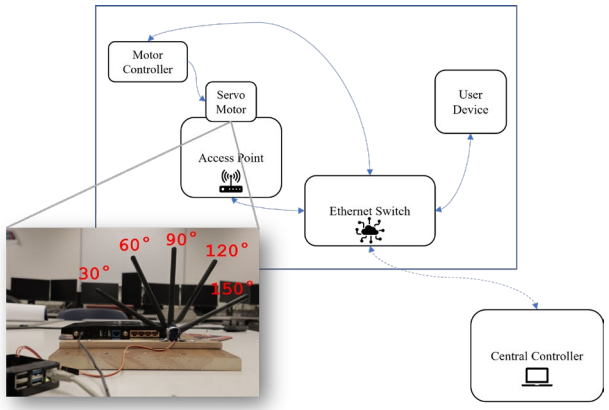
- Nexmon CSITool enabled CSI capture.
- Raspberry Pis used to remotely rotate motors driving our antenna system.
- User device was a Raspberry Pi, pinging a router.

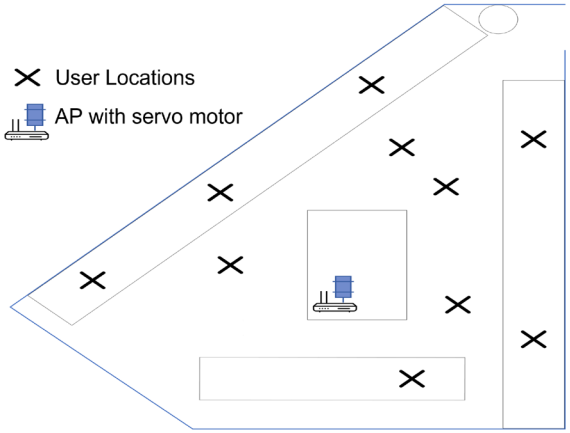


[*]Gringoli, Francesco et al. "Free Your CSI: A Channel State Information Extraction Platform For Modern Wi-Fi Chipsets." *Proceedings of the 13th International Workshop on Wireless Network Testbeds, Experimental Evaluation & Characterization* (2019):

Evaluation – Data Collection

- CSI data was collected in 500 different locations.
- Typical university setting (classroom, labs, office spaces)
- For each location, 5 angular CSI measurements at antenna angles 30°, 60°, 90°, 120° and 150°
- Each measurement recorded on 20MHz wireless channel with 64 subcarrier values.
- Experiments included both Line-of-sight and Non-Line-of-sight scenarios

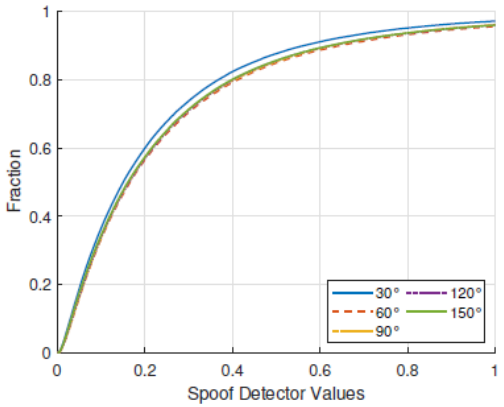




Evaluation – False Negative Performance

Base Case (C = 1)

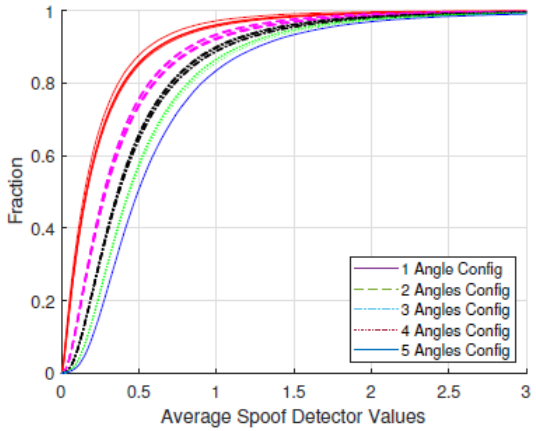
Roughly 9% of all CSI pairs may be misclassified when only a single antenna is considered.



False Negative Ratio with Single Angular Configuration

RCSI-AS(C >= 3)

- Misclassification rate as low as 0.31% for C = 3 and even lower for higher configurations
- Overall, RCSI-AS is highly accurate at detecting differences in CSI using different angular antennas configurations



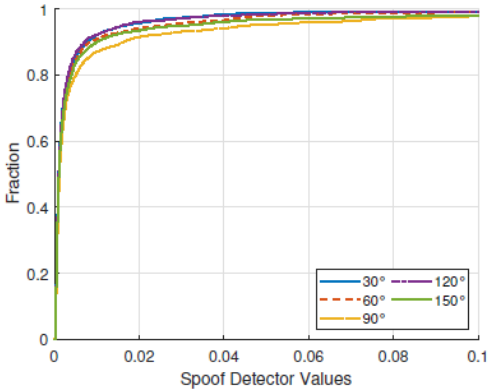
False Negative Performance of RCSI-AS

Evaluation – False Positive Performance

Compared close to 5000 CSI measurement pairs originating from the same user, 500ms apart

<u>Base Case (C = 1)</u>

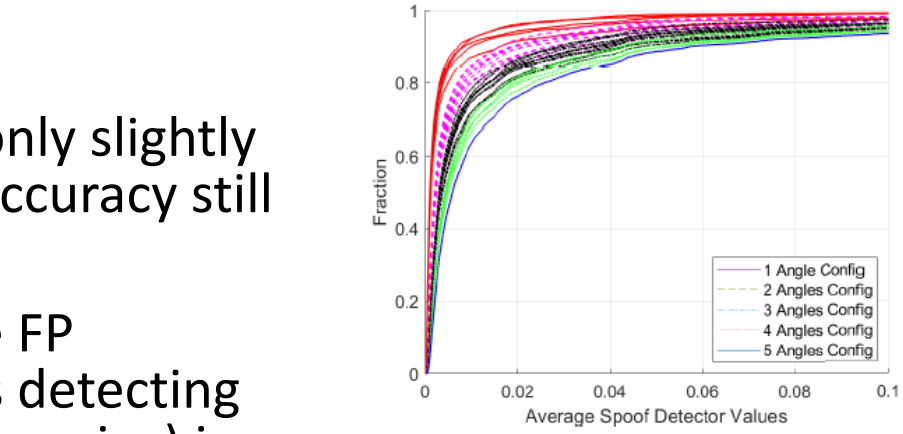
Roughly 5% is misclassified as different users.



False Positive Ratio with Single Angular Configuration

<u>RCSI-AS(C >= 3)</u>

- Using higher configurations only slightly degrades the performance, accuracy still around 93%
- We note that a slightly worse FP performance is acceptable as detecting spoof performance (or FN scenarios) is more critical than false alarms



False Positive Performance of RCSI-AS

Conclusion and Future Work

- RCSI-AS is a novel anti-spoofing system designed for single antenna systems
- Uses CSI measurements at different angular configurations to detect packets from different user locations.
- RCSI-AS was test using real world experimental data and was found to be highly accurate with a spoof detection accuracy of 99.60% and a false alarm accuracy of 93%, when looking at 3 arbitrary angles
- Future work includes reducing the current probe overhead from multiple ACKs.