REPORT DOCUMENTATION PAGE

Form Approved OMB NO. 0704-0188

1. REPORT DATE (DD-MM-YYYY)	2. REPORT TYPE	3. DATES COVERED (From - To)
14-04-2023	Final Report	5-Sep-2017 - 5-Sep-2021

4. TITLE AND SUBTITLE
Final Report: Preventing Radio Window Attacks

5a. CONTRACT NUMBER
W911NF-17-1-0457

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER
611102

6. AUTHORS

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAMES AND ADDRESSES
University of Utah
75 South 2000 East

Salt Lake City, UT 84112 -8930

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS (ES)
U.S. Army Research Office
P.O. Box 12211
Research Triangle Park, NC 27709-2211

10. SPONSOR/MONITOR'S ACRONYM(S)
ARO

11. SPONSOR/MONITOR'S REPORT NUMBER(S)
69215-NC.3

12. DISTRIBUTION AVAILIBILITY STATEMENT
Approved for public release; distribution is unlimited.

13. SUPPLEMENTARY NOTES
The views, opinions and/or findings contained in this report are those of the author(s) and should not contrued as an official Department of the Army position, policy or decision, unless so designated by other documentation.

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	15. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			SNEHA KASERA
UU	UU	UU	UU		19b. TELEPHONE NUMBER
					801-581-4541

RPPR Final Report
as of 19-Apr-2023

Agency Code: 21XD

Proposal Number: 69215NC **Agreement Number: W911NF-17-1-0457**
INVESTIGATOR(S):

Name: SNEHA K KASERA
Email: kasera@cs.utah.edu
Phone Number: 8015814541
Principal: Y

Name: Neal Patwari
Email: npatwari@ece.utah.edu
Phone Number: 8015815917
Principal: N

Organization: **University of Utah**
Address: 75 South 2000 East, Salt Lake City, UT 841128930
Country: USA
DUNS Number: 009095365 EIN: 876000525

Report Date: 05-Dec-2021 Date Received: 14-Apr-2023
Final Report for Period Beginning 05-Sep-2017 and Ending 05-Sep-2021
Title: Preventing Radio Window Attacks
Begin Performance Period: 05-Sep-2017 **End Performance Period:** 05-Sep-2021
Report Term: 0-Other

Submitted By: SNEHA KASERA Email: kasera@cs.utah.edu
Phone: (801) 581-4541

Distribution Statement: 1-Approved for public release; distribution is unlimited.

STEM Degrees: 2 **STEM Participants:** 3

Major Goals: Radio frequency (RF) signals emanating from any wireless network within a protected area (home, commercial, government, or military facility), creates a radio window, even through concrete walls, that can be used to track and infer people's movements, activities, breathing rates, and even the sounds inside the facility, by attackers with receivers outside of the facility. The major goals and objectives of the overall project were as follows:

• Develop a novel game theoretic framework where the defender (the genuine wireless network) deploys multiple transmitters in different locations and changes transmitters in a probabilistic manner to minimize the chance of the attack receivers being able to classify the activities of people inside certain parts of the building. The framework will incorporate optimizations related to trade-offs between obfuscation methods and the cost of obfuscation.
• Develop and examine general multi-antenna MIMO-based defense methods to "confuse" the attacker.
• Develop new estimation bounds which quantify an attacker's ability to estimate a person's track over time. Such bounds will inform evaluations of the robustness of particular wireless networks to the radio window attack as a function of its transmitters' locations, transmit powers, bandwidth, number of antennas, and data rate.
• Evaluate the attacks and defense mechanisms within our framework through extensive experiments. The goal here is to understand how the developed models apply to real situations and very importantly, how the experimental evaluations validate and further strengthen the framework, models, and defense mechanisms.

For this reporting period (October 1st 2020 – September 30th 2021), our specific objectives were as follows:
• Develop optimal defender strategies to minimize user privacy loss.
• Develop new estimation bounds that quantify the best that an attacker can do
• Develop new protocols/methods for MIMO-OFDM wireless communication systems that fool an attacker and thus prevent a reliable radio window attack.

Accomplishments: Based on our earlier research, we realized that both breathing and sound also impact the RF environment and hence offer another radio window opportunity. A malicious attacker could capture received signal strength (RSS) measurements and perform surveillance on a person's vital signs, activities, and sound in their environment. We considered an attacker who looks for subtle changes in the RSS to eavesdrop sound vibrations. The challenge to the adversary is that sound vibrations cause very low amplitude changes in RSS, and RSS is

typically quantized with a significantly larger step size. We obtained a lower bound on an attacker's monitoring performance as a function of the RSS step size and sampling frequency. Our bound considers the little-known and counter-intuitive fact that an adversary can improve their sinusoidal parameter estimates by making some devices transmit to add interference power into the RSS measurements. We demonstrate this capability experimentally. As we show, for typical transceivers, the RSS surveillance attacker can monitor sound vibrations with remarkable accuracy. We published these results in the IEEE Transactions on Information Forensics and Security, 2021. New mitigation strategies will be required to prevent these RSS surveillance attacks.

To prevent radio window attacks, we proposed modifying radio training (MoRTr), a novel system for Wi-Fi MIMO-OFDM devices that alters transmitted symbols over time, space and frequency via a pseudo-random process that mimics the changes due to human activity, particularly the training symbols that are used to measure the wireless channel by the receiver. We performed extensive experiments to demonstrate that an attacker is thwarted by the approach. At the same time, we demonstrated that any genuine receiver could use its measured CSI to demodulate the data without any significant degradation in performance, even though the receiver is not measuring the true CSI. We published these results at the 2021 IEEE Conference on Mobile Ad-Hoc and Smart Systems (IEEE MASS), 2021.

We expanded our ACM WiSec 2020 paper by introducing a method to utilize prior knowledge about the attacker locations that resulted in improved defender strategies with respect to privacy loss and QoS requirements. We validated our claims about incorporating prior knowledge in the framework through experiments. We also built novel reinforcement learning (RL) formulations that yield dynamic and adaptive strategies. Our formulation can obtain defender strategies under unknown propagation models and imperfect movement information.

Training Opportunities: We trained three PhD students, two at University of Utah and one at Washington University in St. Louis, during this reporting period.

Results Dissemination: The results of our research were disseminated through the following papers:

Alemayehu Solomon Abrar, Neal Patwari, and Sneha K. Kasera, “Quantifying interference-assisted signal strength surveillance of sound vibrations”, IEEE Trans. on Information Forensics & Security, appeared online 16 Dec. 2020, vol. 16, pp. 2018-2030, 2021.

Syed Ayaz Mahmud, Neal Patwari, and Sneha K. Kasera, “How to get away with MoRTr: MIMO beam altering for radio window privacy”, in Proc. 18th IEEE Intl. Conf. on Mobile Ad-Hoc and Smart Systems (IEEE MASS 2021), 4-7 Oct. 2021.

Honors and Awards: Nothing to Report

Protocol Activity Status:

Technology Transfer: Nothing to Report

PARTICIPANTS:

Participant Type: PD/PI
Participant: Sneha Kumar Kasera
Person Months Worked: 1.00 **Funding Support:**
Project Contribution:
National Academy Member: N

Participant Type: Co PD/PI
Participant: Neal Patwari
Person Months Worked: 1.00 **Funding Support:**
Project Contribution:
National Academy Member: N

RPPR Final Report
as of 19-Apr-2023

Participant Type: Faculty
Participant: Aditya Bhaskara
Person Months Worked: 1.00 **Funding Support:**
Project Contribution:
National Academy Member: N

Participant Type: Graduate Student (research assistant)
Participant: Pruthuvi Maheshakya Wijewardena
Person Months Worked: 8.00 **Funding Support:**
Project Contribution:
National Academy Member: N

ARTICLES:

Publication Type: Journal Article Peer Reviewed: Y **Publication Status:** 1-Published
Journal: IEEE Trans. on Information Forensics & Security
Publication Identifier Type: DOI Publication Identifier: https://doi.org/10.1109/TIFS.2020.3045316
Volume: 16 Issue: First Page #: 2018
Date Submitted: Date Published: 12/17/23 4:52AM
Publication Location:
Article Title: Quantifying interference-assisted signal strength surveillance of sound vibrations
Authors: Alemayehu Solomon Abrar, Neal Patwari, Sneha K. Kasera
Keywords: Sensors, Quantization (signal), Interference, Eavesdropping, Wireless communication, Vibrations, Radio frequency
Abstract: This article considers an attacker who looks for subtle changes in the RSS in order to eavesdrop sound vibrations. The challenge to the adversary is that sound vibrations cause very low amplitude changes in RSS, and RSS is typically quantized with a significantly larger step size. This article contributes a lower bound on an attacker's monitoring performance as a function of the RSS step size and sampling frequency so that a designer can understand their relationship. Our bound considers the little-known and counter-intuitive fact that an adversary can improve their sinusoidal parameter estimates by making some devices transmit to add interference power into the RSS measurements. We demonstrate this capability experimentally. As we show, for typical transceivers, the RSS surveillance attacker can monitor sound vibrations with remarkable accuracy. New mitigation strategies will be required to prevent RSS surveillance attacks.
Distribution Statement: 1-Approved for public release; distribution is unlimited.
Acknowledged Federal Support: **Y**

CONFERENCE PAPERS:

Publication Type: Conference Paper or Presentation **Publication Status:** 0-Other
Conference Name: IEEE Intl. Conf. on Mobile Ad-Hoc and Smart Systems (IEEE MASS 2021)
Date Received: 14-Apr-2023 Conference Date: 05-Oct-2021 Date Published: 05-Oct-2021
Conference Location: Virtual conference
Paper Title: How to get away with MoRTr: MIMO beam altering for radio window privacy
Authors: Syed Ayaz Mahmud, Neal Patwari, Sneha K. Kasera
Acknowledged Federal Support: **Y**

RPPR Final Report
as of 19-Apr-2023

Partners

,

I certify that the information in the report is complete and accurate:
Signature: Sneha Kumar Kasera
Signature Date: 4/14/23 12:11AM

Preventing Radio Window Attacks

Sneha Kumar Kasera (PI) and Neal Patwari (Co-PI)

Abstract

Radio frequency (RF) signals emanating from any wireless network within a protected area (home, commercial, government, or military facility), creates a *radio window,* even though concrete walls, that can be used to track and infer people's movements, activities, breathing rates, and even the sounds inside the facility, by attackers with receivers outside of the facility.

The large-scale deployment of multi-antenna wireless networks in homes and office buildings introduces new privacy concerns for people residing in these spaces. By measuring the signal strength using receivers placed outside the premises, an attacker can track the movement of people inside. One way to defend against such an attack is to have the signal strengths of the transmitters vary (sometimes reducing to zero) according to some randomized schedule. We show that the question of finding the schedule that minimizes the worst-case privacy loss can be formulated as a constant sum Stackelberg game between an attacker, whose goal is to place receiver to learn the movement of users, and a defender who tries to prevent the attacker while maintaining the connectivity and QoS requirements of the network. We introduce a flexible framework that enables us to capture the constraints of the attacker and the defender. The framework allows us to capture features of modern wireless systems such as directional antennas and allows us to plug in different path-loss models with minimal changes to the setup. We then formulate the problem of finding the optimal defender strategy as a linear program and show that it can be solved efficiently. We also perform numerical evaluations on how the payoffs are affected as the requirements of the defender and the resources the attacker can afford to exhaust change. We also built novel reinforcement learning formulations that yield dynamic and adaptive strategies. Our formulation can obtain defender strategies under unknown propagation models and imperfect movement information.

Realizing that both breathing and sound also impact the RF environment, we considered a malicious attacker that captures the received signal strength measurements and performs surveillance on a person's vital signs, activities, and sound in their environment. Specifically, we investigated an adversary who looks for subtle changes in the RSS to eavesdrop sound vibrations. The key challenge to the adversary is that sound vibrations cause very low amplitude changes in RSS, and RSS is typically quantized with a significantly larger step size. We obtained a lower bound on an attacker's monitoring performance as a function of the RSS step size and sampling frequency. Our bound considers the little-known and counter-intuitive fact that an adversary can improve their sinusoidal parameter estimates by making some devices transmit to add interference power into the RSS measurements. We demonstrate this capability experimentally. As we show, for typical transceivers, the RSS surveillance attacker can monitor sound vibrations with remarkable accuracy. We have shown similar results for breathing surveillance as well.

We also proposed *modifying radio training* (MoRTr), a novel system for Wi-Fi MIMO-OFDM devices that alters transmitted symbols over time, space and frequency via a pseudo-random process that mimics the changes due to human activity, particularly the training symbols that are used to measure the wireless channel by the receiver. We performed extensive experiments to demonstrate that an attacker is thwarted by the approach. At the same time, we demonstrated that any genuine receiver could use its measured CSI to demodulate the data without any significant degradation in performance, even though the receiver is not measuring the true CSI.

Project Objectives

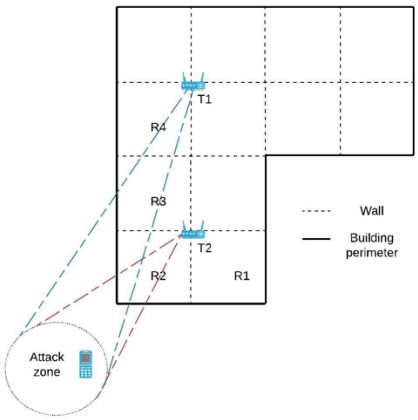
The major goals and objectives of the overall project were as follows:

1. Develop a novel game theoretic framework where the defender (the genuine wireless network) deploys multiple transmitters in different locations and changes transmitters in a probabilistic manner to minimize the chance of the attack receivers being able to classify the activities of people inside certain parts of the building. The framework will incorporate optimizations related to trade-offs between obfuscation methods and the cost of obfuscation. [Years 1, 2, 3, 4]
2. Develop and examine general multi-antenna MIMO-based defense methods to "confuse" the attacker. [Years 3,4]
3. Develop new estimation bounds which quantify an attacker's ability to estimate a person's track over time. Such bounds will inform evaluations of the robustness of specific wireless networks to the radio window attack as a function of its transmitters' locations, transmit powers, bandwidth, number of antennas, and data rate. [Years 2, 3, 4]
4. Evaluate the attacks and defense mechanisms within our framework through extensive experiments. The goal here is to understand how the developed models apply to real situations and very importantly, how the experimental evaluations validate and further strengthen the framework, models, and defense mechanisms. [Years 2, 3, 4]

Findings & Contributions

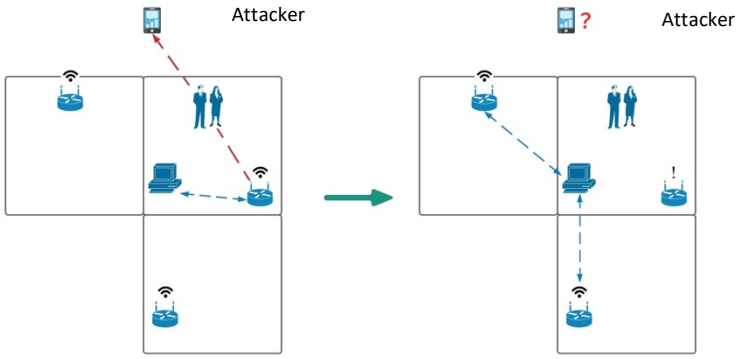
We summarize our key findings and contributions corresponding to each project objective below. However, we would like to note that our contributions cut across multiple objectives. E.g., we perform evaluations for the first three objectives although evaluation is listed as a fourth objective.

Objective 1: Develop a novel game theoretic framework – We developed a novel, flexible, plug-n-play framework based on a constant-sum Stackelberg game for defending against radio window attacks. Our framework enables us (i) to comprehensively capture the constraints of the attacker and the defender, (ii) to capture features of modern wireless systems such as directional antennas, and (iii) allows us to plug in different path-loss models with minimal changes to the setup. We formulated the problem of finding the optimal defender strategy as a linear program and showed that it can be solved efficiently. We also performed numerical evaluations to demonstrate the applicability of our framework.

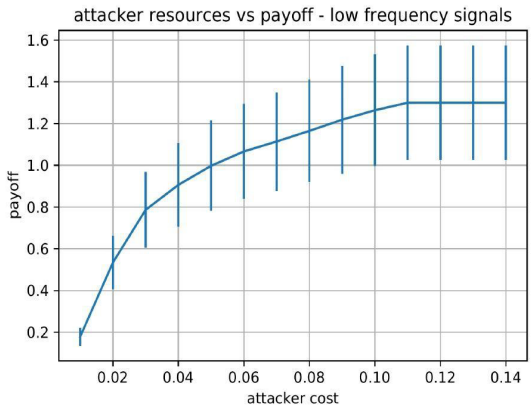


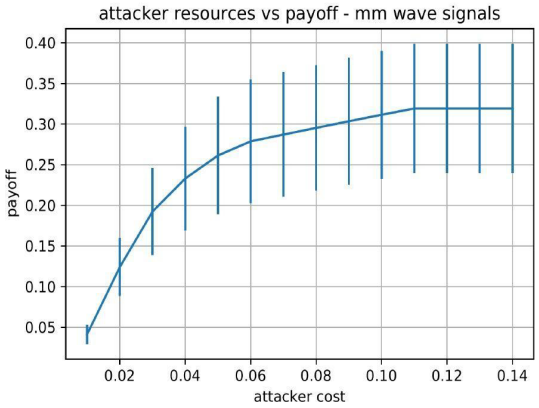
Attacker can detect movements inside the building from attack zone:

- In region R2 using signals from transmitter T2.
- In regions R4, R5 using signals from transmitter T1.



Defender temporarily turns transmitters off to prevent attack, maintains QoS requirements for legitimate devices.

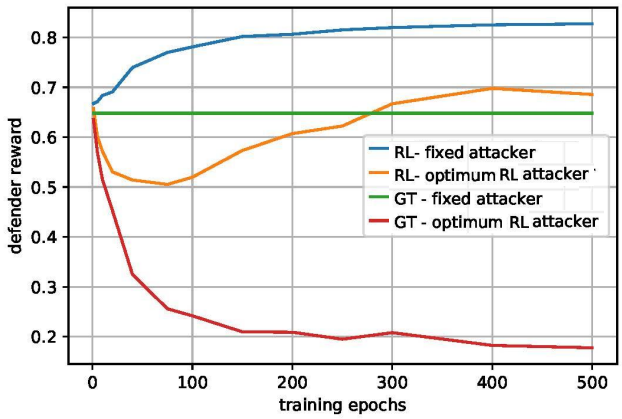




- Attacker causes higher privacy loss (higher attacker payoff) by using more resources
- Privacy loss (attacker payoff) saturates after a certain amount of attacker cost (depends on the number of attack receivers)

Signal type	Maximum privacy loss w/i our framework	Maximum privacy loss w/i a random schedule
WiFi	1.034	5.372
Millimeter wave	0.226	0.591

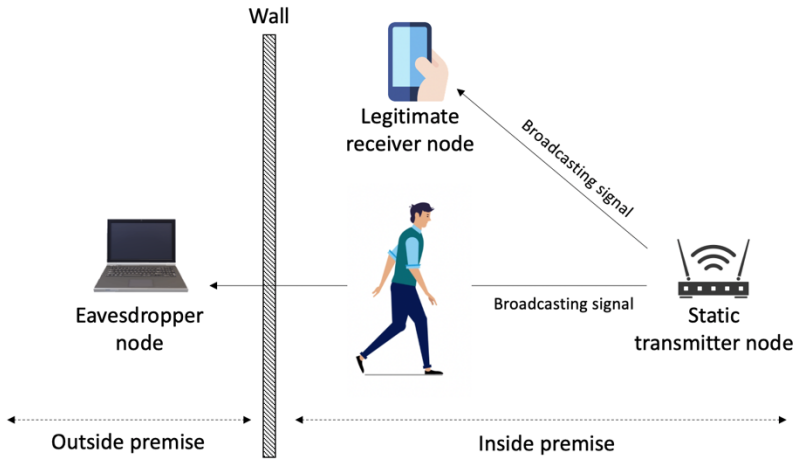
Privacy loss using the solution to our optimization problem versus random transmitter schedule for 2 wireless scenarios



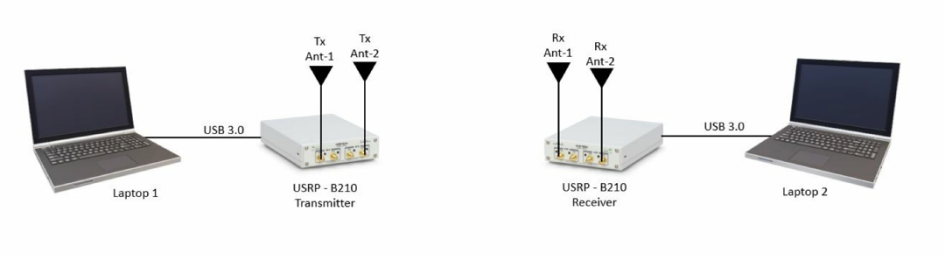
Defender rewards when Reinforcement Learning (RL) or Game Theoretic (GT) defender strategy used against two attacker strategies versus #training epochs.

- RL defender against fixed attacker that has no training - increases gradually until it saturates
- RL defender against optimal RL attacker - reduces initially but increases after certain #epochs (both using training)
- GT defender against fixed attacker - good but less than when defender uses RL strategy (does not change with #epochs)
- GT defender against optimal RL attacker - reduces drastically

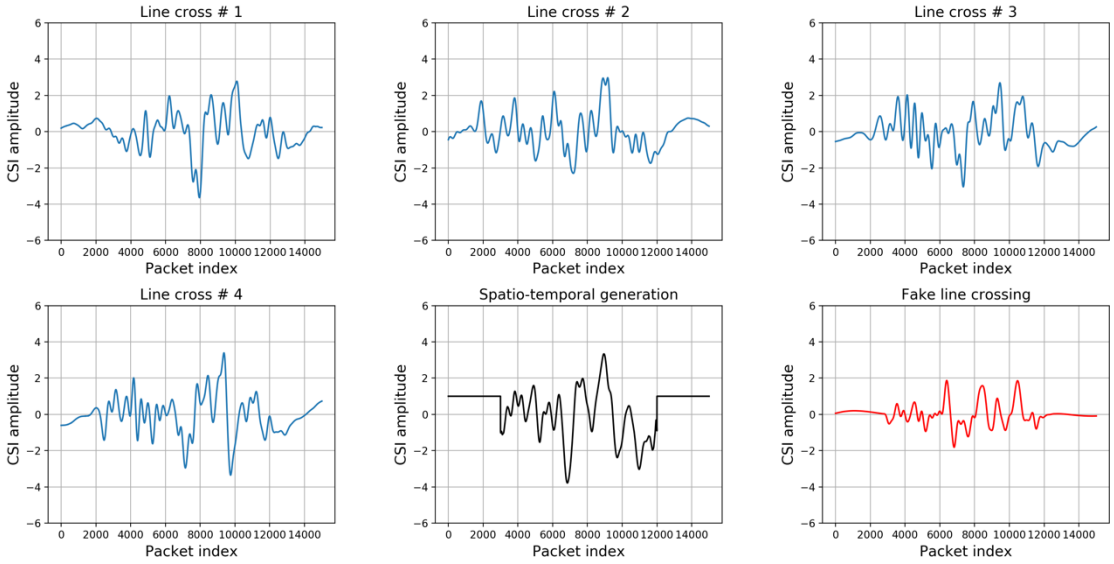
Objective 2: Develop and examine general multi-antenna MIMO-based defense methods to "confuse" the attacker – We developed a MIMO beam altering approach that we call *Modifying Radio Training (MoRTr)* for preventing radio window attacks. We experimentally demonstrated our approach to secure channel state information by altering the transmit signal in time, frequency, and space to generate random human gestures that match the statistics of actual gestures to thwart an eavesdropper from being able to know when the actual gestures occurred. We built a B210 USRP test setup, implemented the PHY of a WiFi MIMO-OFDM link, measured the channel state information, and implemented our proposed modification MoRTr at the transmitter. Our experimental results showed that, with this modification, an eavesdropper is unable to distinguish between real and fake human gestures. Simultaneously, the legitimate receiver is able to extract and demodulate the payload of MoRTr-generated packets without any significant performance degradation.



A simplified depiction of the Radio Window Attack



Experimental setup: Transmitter and receiver USRP B210 with MIMO capabilities connected with laptops through USB interfaces.



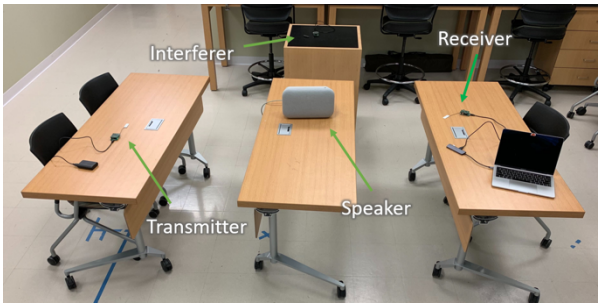
Channel State Information (CSI): Four examples show typical channel characteristics during crossing line-of-sight between transceiver nodes, spatio-temporal gesture generated (bottom-center) and fake CSI estimated by eavesdropper (bottom-right).

	Bit Error Rate		
	w/out MoRTr	**w/ MoRTr**	***p*-value**
Hand Gesture	0.00048	0.00049	0.66
Punch	0.00039	0.00044	0.85
Push	0.00043	0.00046	0.76
Pickup	0.00042	0.00042	0.61

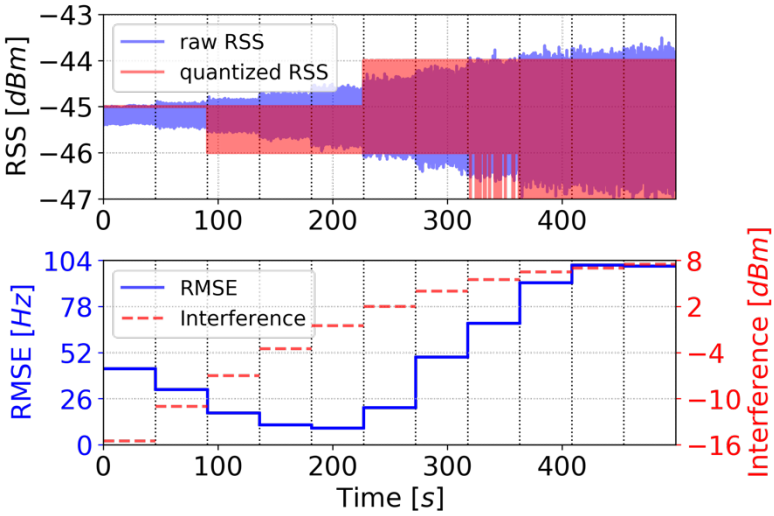
Comparison of Mean Bit Error Rate During performing real gestures and while modification is applied.

Objective 3: Develop new estimation bounds - We explored the limits on RSS-based eavesdropping of sound vibrations. We analyzed the capability of an attacker in estimating the sinusoidal parameters of low-amplitude sinusoidal signals by deriving the theoretical lower bound with which an attacker could estimate the rate and amplitude of a sinusoid. We showed, both theoretically and experimentally, that the adversary could force other wireless devices to transmit simultaneously to improve their estimates. The numerical values of the lower bound on variance show, for typical RFICs, an RSS surveillance attack could be very accurate. We discussed, as a result, how a device designer could limit the performance of a potential attack by adjusting the quantization step size and the sampling rate. Most commercial transceivers have fixed RSS

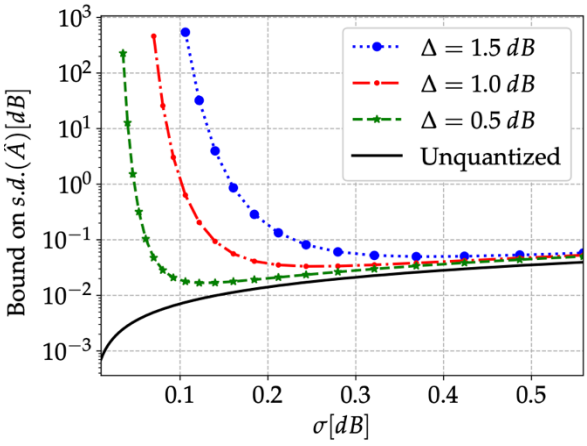
quantization schemes; however, a manufacturer could adjust RSS quantization to ensure that sound eavesdropping attacks are ineffective.

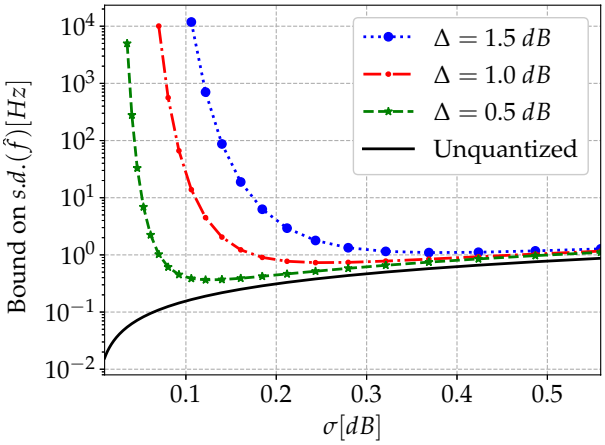


Experimental setup



As helpful interference power increases each 45s, the frequency estimation error decreases to a minimum of 9 Hz.





Cramer Rao Bound of (Left) amplitude (A) and of (Right) frequency (f) vs noise power. A is the amplitude of sound-induced signal, equal to 0.025dB. Received power is quantized with step size D.

Objective 4: Evaluate the attacks and defense mechanisms within our framework through extensive experiments – We have performed extensive numerical as well as implementation-based evaluations and validations of our methods and approaches in real situations. Our implementation-based evaluations, specifically, captured realism of actual wireless systems and networks.

References

1. Alemayehu Solomon Abrar, Neal Patwari, Aniqua Baset, and Sneha K. Kasera, "*Quantifying Interference-assisted Signal Strength Breathing Surveillance*", arXiv:1905.03939, May 2019.

2. P.M. Wijewardena, A. Bhaskara, A. Mahmud, Sneha Kumar Kasera, and N. Patwari, "*A Plug-n-Play Game Theoretic Framework for Defending Against Radio Window Attacks*," in Proceedings of ACM WiSec Conference, July 2020.

3. Alemayehu Solomon Abrar, Neal Patwari, and Sneha K. Kasera, "*Quantifying Interference-assisted Signal Strength Surveillance of Sound Vibrations*", IEEE Trans. on Information Forensics & Security, appeared online 16 Dec. 2020, vol. 16, pp. 2018-2030, 2021.

4. Syed Ayaz Mahmud, Neal Patwari, and Sneha K. Kasera, "*How to Get Away with MoRTr: MIMO Beam Altering for Radio Window Privacy*", in Proc. 18th IEEE Intl. Conf. on Mobile Ad-Hoc and Smart Systems (IEEE MASS 2021), 4-7 Oct. 2021.