REPORT DOCUMENTATION PAGE

Form Approved OMB NO. 0704-0188

The public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggesstions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington VA, 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to any oenalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.
PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ADDRESS.

1. REPORT DATE (DD-MM-YYYY)	2. REPORT TYPE	3. DATES COVERED (From - To)
25-01-2023	Final Report	21-Apr-2021 - 20-Apr-2022

4. TITLE AND SUBTITLE

Final Report: A Millimeter-Wave Communication System for Wireless Security and Networking Research and Education

5a. CONTRACT NUMBER
W911NF-21-1-0122

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER
611103

6. AUTHORS

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAMES AND ADDRESSES

University of Arizona
PO Box 210158, Rm 510

Tucson, AZ 85721 -0158

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)
77332-NC-RIP.2

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			Ming Li
UU	UU	UU	UU		19b. TELEPHONE NUMBER 520-621-6191

RPPR Final Report
as of 27-Jan-2023

Agency Code: 21XD

Proposal Number: 77332NCRIP **Agreement Number: W911NF-21-1-0122**
INVESTIGATOR(S):

Name: Ph.D. Loukas Lazos
Email: llazos@arizona.edu
Phone Number: 5206212434
Principal: N

Name: Ming Li
Email: ming.li@arizona.edu
Phone Number: 5206216191
Principal: Y

Organization: **University of Arizona**
Address: PO Box 210158, Rm 510, Tucson, AZ 857210158
Country: USA
DUNS Number: 806345617 EIN: 866004791

Report Date: 20-Jul-2022 Date Received: 25-Jan-2023
Final Report for Period Beginning 21-Apr-2021 and Ending 20-Apr-2022

Title: A Millimeter-Wave Communication System for Wireless Security and Networking Research and Education
Begin Performance Period: 21-Apr-2021 **End Performance Period:** 20-Apr-2022
Report Term: 0-Other

Submitted By: Ming Li Email: ming.li@arizona.edu
Phone: (520) 621-6191

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

STEM Degrees: **STEM Participants:**

Major Goals: The main goal of this project is to build a state-of-the-art, programmable, and reconfigurable mmWave platform to conduct mmWave wireless security and networking research. To support flexible implementations of various applications, the testbed is built from reconfigurable and programmable software-defined radios and commercial off-the-shelf hardware. Such a platform will be leveraged to address unexplored challenges in security, privacy, and reliability in mmWave communications. Specifically, the proposed infrastructure will advance our research on a wide range of topics directly funded by the DoD and of DoD interest including trust establishment in wireless networks, physical layer security in mmWave, security and privacy in CPS and IoT (e.g., connected autonomous vehicles and unmanned aircraft systems), multi-hop networking, and fair and secure coexistence in mmWave. The testbed will enable the understanding, modeling, and experimental validation of fundamental security and networking-related signal propagation properties of mmWave bands, and the systematic study of attack vectors and defenses in this domain. Moreover, it will provide invaluable hands-on education opportunities for graduate and undergraduate students. Combined with our existing lab facilities, such a testbed would significantly strengthen our wireless and security research and education capabilities at the University of Arizona.

Accomplishments: Over the project period (one year), the proposed testbed has already been acquired and built. The DURIP platform has been used to enhance existing research funded by the DoD and enabled new research directions. See attached PDF file for more details.

Training Opportunities: The DURIP platform was used to train three Ph.D. students, who learned to set up and use USRP SDR devices, mmWave beamforming software, GNU radio, and LabView software, etc. It also enhanced their skills in implementation related to wireless security and networking research topics.

RPPR Final Report
as of 27-Jan-2023

Results Dissemination: The project-supported research outcomes will be disseminated via publications and talks.

The following papers are currently under-preparation (to be submitted in the near future):

1. Jingcheng Li, Loukas Lazos, Ming Li, "MmWave Beam Alignment made Robust Against Man-in-the-Middle Attacks";

2. Ziqi Xu, Jingcheng Li, Yanjun Pan, Ming Li, Loukas Lazos, "Secret-Free Device Pairing in the mmWave Band";

3. Tianchi Zhao, Chicheng Zhang, Ming Li, Zhiwu Guo, Jingcheng Li, "Efficient Online Learning Algorithms for Joint Path and Beam Selection in Self-Backhauled MmWave Networks".

Honors and Awards: Nothing to Report

Protocol Activity Status:

Technology Transfer: Nothing to Report

CONFERENCE PAPERS:

Publication Type: Conference Paper or Presentation **Publication Status:** 0-Other
Conference Name:
Date Received: Conference Date: Date Published:
Conference Location:
Paper Title: Efficient Online Learning Algorithms for Joint Path and Beam Selection in Self-Backhauled MmWave Networks
Authors: Tianchi Zhao, Chicheng Zhang, Ming Li, Jingcheng Li
Acknowledged Federal Support: **Y**

Partners

,

I certify that the information in the report is complete and accurate:
Signature: Ming Li
Signature Date: 1/25/23 5:49PM

Final Report for DURIP Project: A Millimeter-Wave Communication System for Wireless Security and Networking Research and Education

PI: Ming Li; Co-PI: Loukas Lazos

January 25, 2023

Abstract

The main goal of this project is to build a state-of-the-art, programmable, and reconfigurable mmWave platform to conduct mmWave wireless security and networking research. To support flexible implementations of various applications, the testbed is built from reconfigurable and programmable software-defined radios and commercial off-the-shelf hardware. Such a platform is leveraged to address unexplored challenges in security, privacy, and reliability in mmWave communications. During the DURIP project period, the acquired platform has been leveraged to enhance our research on several topics directly funded by the DoD, including trust establishment in wireless networks, physical layer security in mmWave, and performance optimization for multi-hop mmWave networks.

1 Project Goals

The main goal of this project is to build a state-of-the-art, programmable, and reconfigurable mmWave platform to conduct mmWave wireless security and networking research. To support flexible implementations of various applications, the testbed is built from reconfigurable and programmable software-defined radios and commercial off-the-shelf hardware. Such a platform will be leveraged to address unexplored challenges in security, privacy, and reliability in mmWave communications. Specifically, the proposed infrastructure will advance our research on a wide range of topics directly funded by the DoD and of DoD interest including trust establishment in wireless networks, physical layer security in mmWave, security and privacy in CPS and IoT (e.g., connected autonomous vehicles and unmanned aircraft systems), multi-hop networking, and fair and secure coexistence in mmWave. The testbed will enable the understanding, modeling, and experimental validation of fundamental security and networking-related signal propagation properties of mmWave bands, and the systematic study of attack vectors and defenses in this domain. Moreover, it will provide invaluable hands-on education opportunities for graduate and undergraduate students. Combined with our existing lab facilities, such a testbed would significantly strengthen our wireless and security research and education capabilities at the University of Arizona.

2 Overview of the Research Infrastructure

Over the project period (one year), the proposed testbed has already been acquired and built. It consists of 6 USRP devices with 6 Tmytek's mmWave front-end [1] operating at a center frequency

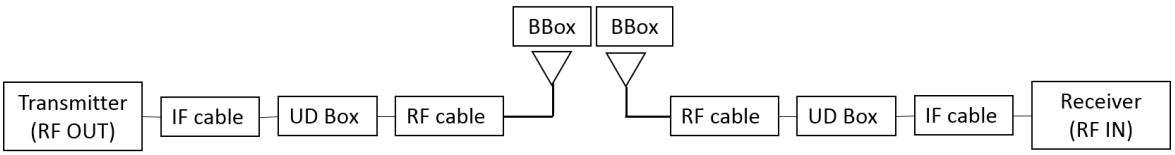
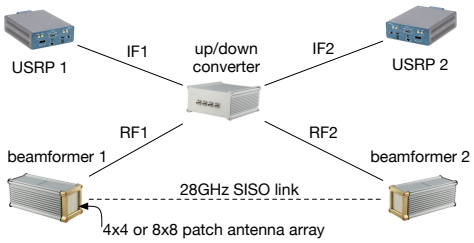


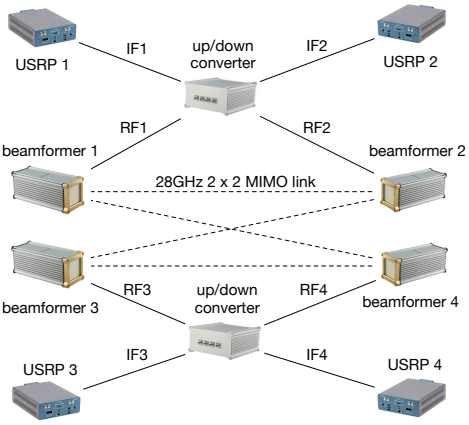
Figure 1: The system diagram of a SISO mmWave link (a transmitter and a receiver).

of 28Ghz (in the 5G NR bands). It is a cost-effective solution that supports electronic beam-steering and analog beamforming. There are 3 Ettus N320 USRPs, and 3 NI 2974 USRPs, which can provide FPGA-based baseband processing. The 3 dual-channel UD-Boxes from Tmytek provide up/down conversion of baseband signals into mmWave frequencies. Finally, the RF front-end, BBoxes, provides 16 or 64 antenna elements for 2D/3D beamforming.

To use our platform, nodes can be arranged to either SISO links (see Figure 2(a)) or a 2×2 MIMO link (see Figure 2(b)). Various topologies and configurations can be used to conduct research in security by implementing legitimate and eavesdropping devices, active adversaries, passive monitors, coordinated attacks including more than one node (e.g., an active MiTM adversary), and secure and fair coexistence. For networking research, the platform can be arranged to three coexisting SISO links, or one SISO link and one 2×2 MIMO link. Alternative configurations include a multihop network with a source, destination, and four intermediate relays. The reconfigurability of the platform also allows us to perform research at the PHY layer of mmWave and study various beamforming and beam-tracking algorithms.



(a) 28GHz SISO link



(b) 28GHz 2×2 MIMO link

Figure 2: Implementation of SISO and MIMO links using the testbed.

An overview of the basic SISO setup is shown in Figures 1 and 3. The baseband signal is generated by a USRP device in sub-6GHz frequency. The baseband signal is fed to an up-conversion UD-box to be converted to the mmWave band frequency. The signal is then transmitted using a beamforming antenna (BBox lite or BBox one). The direction of the beam is controlled by the TMXLAB software Kit within a $-45°$ to $45°$ range. At the receiver side, the UD-box down-converts the received signal to a sub-6GHz frequency. Then the signal is processed by a USRP or a Wi-Fi card and it is decoded to measure various properties such as received power, channel state information, etc. and recover the originally-transmitted bits.

Component List of the Platform: The acquired mmWave testbed consists of the following components (purchased using the funds of this project):

1. USRP Radios: (a) Three NI USRP 2974 radios, which are high-performance embedded SDRs with 10Mhz-6Ghz frequency range and 160 Mhz bandwidth.

(b) Two Ettus N320 radios, which provide 200MHz bandwidth, with 2 Tx/Rx channels and a 3MHz-6GHz frequency range. The USRPs are compatible with GNU Radio software.

(c) One Ettus N310 radio, providing four channels, 10MHz to 6GHz frequency range, and 100MHz bandwidth. The radio is compatible with GNU Radio.

The USRPs provide the baseband data processing for the transceivers using an onboard FPGA and processor for rapidly prototyping high-performance wireless communications systems.

2. MmWave/5G RF front-ends from TMYTEK [1] which consist of the following:

(a) One BBox 28GHz 3D beamformer. The beamformer includes an antenna array with a choice of 4×4 or 8×8 series patch antenna in the 27.5-28.35GHz range (5G n261 band) and a Phi-A box which is a waveguide that supports phase and amplitude for 16 independent RF channels for digital beamforming. Its typical beam switching delay is $150ms$. The beam steering range of the 4×4 array is $\pm 60^\circ$ vertical and $\pm 45^\circ$ horizontal and the 3D beamwidth (at broadside) is $\pm 13^\circ - 14^\circ$ on both directions.

Figure 3: The SISO mmWave link setup.

(b) Five BBox Lite 28GHz 2D beamformers in the same 27.5-28.35GHz frequency band, providing phase and amplitude control for four independent RF channels (with a 4×4 patch antenna array), and $400ms$ beam switching delay.

(c) Three dual channel BBox UD Boxes which up-down convert the signal from baseband (<6GHz) to mmWave bands (up to 28GHz). Each UD BBox can drive two transceivers.

3. Spectrum Analyzer: a Rohde & Schwarz FPH (1321.0996.02) handheld Spectrum analyzer, enabling spectrum analysis up to 31GHz.

4. Computers: Four Dell OptiPlex 7080 Desktop Computers and one Dell Latitude 7310 13.3" Notebook which can control the USRP devices. The laptop can be used as a mobile device to enable experiments with mobile scenarios.

5. Software: LabVIEW Communications 802.11 Application Framework which provides a reconfigurable FPGA-based 802.11 MAC and PHY reference design. The LabVIEW Communications Systems Design Suite which supports programming both the FPGA and the host is available through our site license at the University of Arizona.

3 Research Enabled by the DURIP Platform

Over the course of this project, the DURIP platform has been used to enhance existing research funded by the DoD and enabled new research directions.

3.1 Enhancing Wireless Network Security in the mmWave Band

Millimeter wave is emerging as a key enabler for massively connecting IoT devices as well as networking smaller groups of devices to infrastructure at massive bandwidth. As the density of devices grows, deploying scalable security solutions becomes a major challenge. Traditional solutions such as public key cryptosystems or preloading secrets present their own limitations when deployment needs to be fast and devices transition between multiple administrative domains.

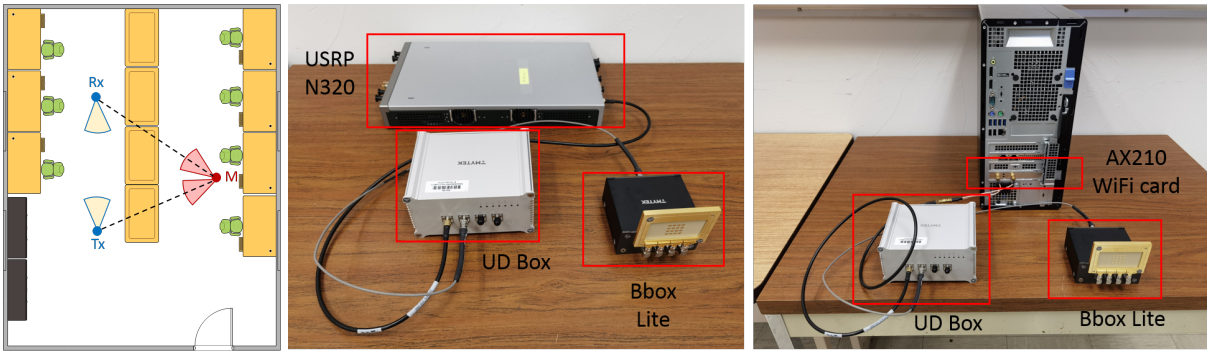


Figure 5: The floor plan and experimental setup for evaluating the MitM attack and defense. Middle: Transmitter; Right: Receiver.

Moreover, for IoT devices without user-friendly interfaces such as screens and keyboards, entering passwords, personal identification numbers, and other security credentials is cumbersome. An alternative to key pre-deployment is to derive trust from the PHY layer. Physical layer security in the sub-6GHz bands has been shown to be a promising strategy for achieving confidentiality [2–4], key extraction [5], pairing [6,7], message integrity [8–10], location verification and distinction [11–13], and other security properties. These methods rely on the intrinsic randomness of the wireless channel, the richness of the multipath environment, and hard-to-forge physical signal propagation laws to build and exploit unique advantages for legitimate devices. In our current ARO research project (W911NF-19-1-0050) titled "In-band Wireless Trust Establishment Resistant to Advanced Signal Manipulations", we develop trust establishment and message integrity verification methods for the sub-6Ghz band [7,9,10,14].

The trust establishment methods developed for the sub-6GHz band rely on specific signal propagation models and device capabilities in that band and cannot be directly applied to mmWave communications. The latter is highly directional and exhibits fading characteristics that are governed by entirely different statistical models [15]. Under these new models, we aim to study two research questions: (a) *what are the capabilities of passive and active adversaries in the mmWave bands?* (b) *How can the unique properties of the mmWave RF environment be exploited to build PHY-layer security properties?*

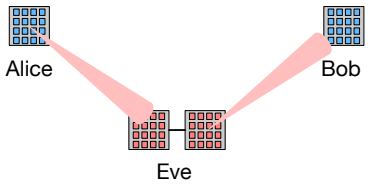


Figure 4: Active Man-in-the-Middle (or beam stealing) attack between Alice and Bob.

Secure mmWave Beam Alignment. Beam alignment refers to the process of discovering the optimal antenna orientation between a mmWave transmitter (Tx) and a receiver (Rx). However, directionality leaves beam alignment vulnerable to active attacks (a.k.a. beam stealing) [16–19]. Most existing beam alignment algorithms (e.g., in 802.11ad) rely on spatial beam sweeping to identify the optimal channel, usually represented by some crude metric such as average RSS. The lack of authentication during channel estimation allows Mallory to spoof Alice's beam to Bob, thus implementing a "physical" MiTM attack (see Figure 4). As a result, Alice and Bob estimate the best channel when their beams point toward Mallory, leaving Mallory in full control of their communication. Mallory can now eavesdrop, inject, modify, and drop messages on the Alice-Bob link, or perform high-layer traffic analysis attacks [20]. Even if beam sweep frames were to be authenticated [16], Mallory can still relay/amplify Alice's beam sweep frames towards Bob, to make Mallory's direction appear stronger than the LoS.

To defend against such beam-stealing attacks, we proposed two approaches. In the first ap-

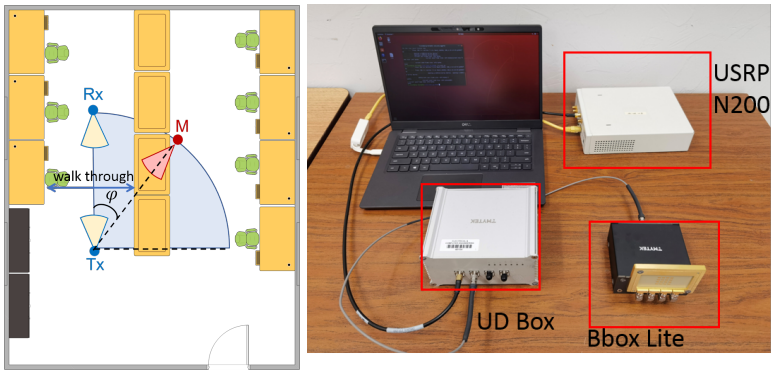


Figure 6: The floor plan and experimental setup for evaluating the secret-free trust establishment protocol.

proach, we exploit the power-delay profile (PDP) to identify the earliest beam arriving at Bob (an LoS signal is always received earliest). If the strongest RSS is received in an NLoS direction, this is an indication of an amplification attack. But this method assumes the existence of the LoS path. In the second approach, we randomize the transmission power at the Tx and detect the angle-of-arrival (AoA) of the incoming signal when the Tx's beam sweeps the plane. Detection of a beam-stealing attack occurs by identifying a dominant AoA direction at the receiver irrespective of the Tx's angle of departure (AoD). This indicates the existence of a relay, amplifying the signal to steal a beam in a desired direction.

The DURIP platform has been used to evaluate the above attack and defenses. The experimental setup and floor plan are shown in Figure 5. The adversary device M, receives from the Tx while Tx is beam-sweeping. Then, M amplifies the signal and relays it to Rx. We collect the CSI measurements in the Tx-Rx link to compute the Power-Delay profile for each beam pair. In addition, the AoA/AoD combinations are measured as the peaks of RSS in the beam-pair space.

Secret-Free Trust Establishment in mmWave band. We have developed an in-band trust establishment (device pairing) protocol for user-designated wireless devices with mmWave capabilities. Our goal is to achieve a secure authenticated key exchange (AKE, where two parties, Alice and Bob, who interact for the first time establish a secret key. In the mmWave bands, devices cannot easily exploit the richness of multipath to derive common randomness due to the directionality of the transmission and the high signal attenuation. On the other hand, we leverage these unique RF properties to design novel secret-free pairing methods. Specifically, our proposed protocol exploits the detection of common context (e.g., human motion events) to verify the co-presence of devices and establish a secret key. The common context is detected via the directionality of mmWave signals to prevent passive and active attacks. We show that random blockage of the mmWave link can be used to enhance the security of the pairing protocol.

To evaluate this approach, we implemented our protocol using our DURIP experimental platform. We evaluated the correctness and soundness properties by assuming a passive adversary who attempts to eavesdrop the signals from the legitimate devices closely - adjacent to the physically secure boundary of the devices. Our experimentation demonstrates the ability to sufficiently distinguish between "legitimate" devices and sitting-close malicious devices by comparing the similarity between the generated event fingerprints of the Tx and Rx. The experimental setup and floor plan are shown in Figure 6. The half-power beamwidth is 25° and the distance between the Tx and Rx is 4m. The signal generator and receiver are implemented using USRP N200 devices, with the gain

of the Tx antenna set to $36dB$ and the gain of Rx antenna set to $26dB$. We used the GNU Radio software to control the USRPs and the TMXLAB Kit to control the BBox and UD box.

3.2 Enhancing mmWave Wireless Network Performance

In PI Li's research project titled "Toward High Performance Tactical Multi-Hop Wireless Networks via Exploiting Antenna Reconfigurability " (N00014-16-1-2650) funded by the Office of Naval Research (ONR)'s Young Investigator Program, we investigate how re-configurable antennas can mitigate channel unreliability and enhance the end-to-end quality-of-service (QoS) of multi-hop networks. The above project mainly focuses on sub-6GHz applications. With the DURIP platform, we extended our networking research to the mmWave band.

MmWave Beam and Path Selection for Multi-hop Networks. To provide high coverage and combat high attenuation, mmWave networks typically require the dense deployment of base stations and adopt a self-backhauled network architecture where data are transmitted via multi-hop links (Figure 7). The unique characteristics of mmWave links (e.g., highly directional beams, sensitivity to blockage) bring challenges to designing an efficient online routing algorithm, where beam selection must be simultaneously considered. Thus, in this work, we propose a new algorithm for online joint path and beam selection called the Combinatorial Unimodal Lower Confidence Bound based Joint Path and Beam Selection (CULCB-JPBS), in which we exploit Unimodal properties in a combinatorial bandit algorithm. We prove a finite-time regret bound of CULCB-JPBS and show that it is independent of the number of beams in each link. Furthermore, we conduct experiments using our mmWave networking platform. Results show that our proposed learning algorithm can significantly improve the convergence rate and yield much lower regret (thus lower end-to-end delay), compared with existing approaches.

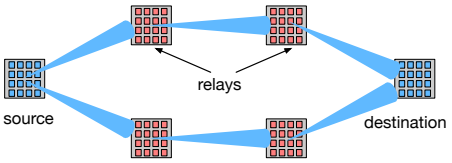
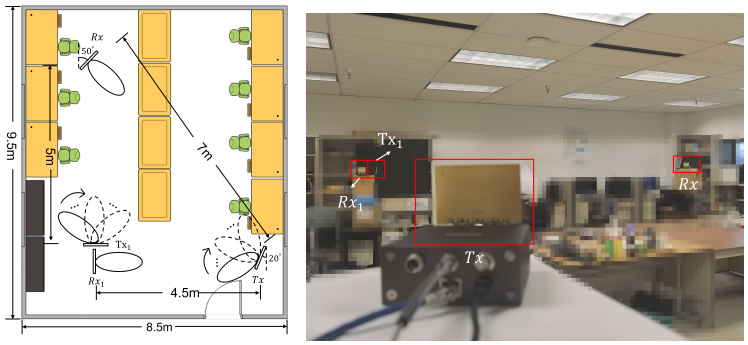


Figure 7: A mmWave-based multihop networking scenario.

The use of the DURIP platform for setting up a mmWave multihop network is shown in Figure 8. To emulate a multi-hop mmWave network, we first create a three-link topology (a single-hop path and a two-hop path), and then collect over-the-air datasets from all three links. The setting for each node is similar to Figure 3. To configure the USRP and extract packet data from the AX 210 WiFi card, we use a software tool called *PicoScenes* [21], which is a high-performance software implementation of 802.11 a/g/n/ac/ax standards. The tool allows us to fully control the baseband signal and access the complete physical layer information (such as CSI). We implement the IEEE 802.11ax standard based on an OFDM system with 234 subcarriers using PicoScenes. Since it is difficult to implement the online learning algorithms in real-time in our existing testbed (which requires real-time feedback and control), we collect over-the-air packet data offline and simulate the online algorithms in Matlab. We obtain 10,000 packet delivery success/failure results for each beam of each link, and then calculate the average successful packet delivery rate from 10,000 packets as the ground truth for each link and beam. We validated our algorithm's efficiency and effectiveness in terms of cumulative regret, delay, and the number of successfully received packets.

4 Enhancement for Education

The DURIP platform can be used to enhance education in security, privacy, communications, and networking (for example, by leveraging the Research Experience for Undergraduate (REU)



(a) Multi-hop layout (b) Multi-hop setup

Figure 8: Experimental setup and floor plan for the multi-hop mmWave network experiments.

program at the ECE department of UA). Co-PI Lazos is involved in the NSF REU Site on Cognitive and Autonomous Test (CAT) Vehicle in recent years. In the summer of 2022, one of the teams worked on a research project about the beam-stealing attack for mmWave communications. They came up with a countermeasure idea that uses power randomization. In the summer of 2023, we plan to let them implement their idea using the DURIP platform.

5 Deployment and Estimated Useful Life

This platform has been deployed in two labs at the ECE department at UA: the Wireless Networking and Cyber Security Research Lab (WiSeR) led by PI Li, which has a lab space of 500 square feet and the Network and Information Security Lab (NISL) led by Co-PI Lazos, with similar lab space to WiSer. The PIs anticipate the useful life of the infrastructure to be at least five years.

References

[1] TMYTEK, "The TMYTEK 5G Platform." https://www.tmytek.com/, 2020.

[2] S. Mathur, W. Trappe, N. Mandayam, C. Ye, and A. Reznik, "Radio-telepathy: extracting a secret key from an unauthenticated wireless channel," in *Proc. of the MOBICOM Conference*, pp. 128–139, 2008.

[3] S. Jana, S. N. Premnath, M. Clark, S. K. Kasera, N. Patwari, and S. V. Krishnamurthy, "On the effectiveness of secret key extraction from wireless signal strength in real environments," in *Proc. of the MOBICOM Conference*, pp. 321–332, 2009.

[4] C. Ye, S. Mathur, A. Reznik, Y. Shah, W. Trappe, and N. B. Mandayam, "Information-theoretically secret key generation for fading wireless channels," *IEEE Transactions on Information Forensics and Security*, vol. 5, no. 2, pp. 240–254, 2010.

[5] T. Wang, Y. Liu, and A. V. Vasilakos, "Survey on channel reciprocity based key establishment techniques for wireless systems," *Wireless Networks*, vol. 21, no. 6, pp. 1835–1846, 2015.

[6] M. Miettinen, N. Asokan, T. D. Nguyen, A.-R. Sadeghi, and M. Sobhani, "Context-based zero-interaction pairing and key evolution for advanced personal devices," in *Proc. of the CCS Conference*, pp. 880–891, 2014.

[7] N. Ghose, L. Lazos, and M. Li, "HELP: Helper-enabled in-band device pairing resistant

against signal cancellation," in *Proc. of the USENIX Security Symposium (USENIX Security 17)*, pp. 433–450, 2017.

[8] S. Capkun, M. Cagalj, R. Rengaswamy, I. Tsigkogiannis, J.-P. Hubaux, and M. Srivastava, "Integrity codes: Message integrity protection and authentication over insecure channels," *IEEE Transactions on Dependable and Secure Computing*, vol. 5, no. 4, pp. 208–223, 2008.

[9] N. Ghose, L. Lazos, and M. Li, "Secure device bootstrapping without secrets resistant to signal manipulation attacks," in *Proc. of the IEEE SP Symposium*, pp. 819–835, IEEE, 2018.

[10] N. Ghose, L. Lazos, and M. Li, "SFIRE: secret-free-in-band trust establishment for cots wireless devices," in *Proc. of INFOCOM Conference*, pp. 1529–1537, IEEE, 2018.

[11] D. Wu, D. Zhu, Y. Liu, and D. Zhao, "Location verification assisted by a moving obstacle for wireless sensor networks," *IEEE Internet of Things Journal*, vol. 5, no. 1, pp. 322–335, 2017.

[12] S. Yan, I. Nevat, G. W. Peters, and R. Malaney, "Location verification systems under spatially correlated shadowing," *IEEE Transactions on Wireless Communications*, vol. 15, no. 6, pp. 4132–4144, 2016.

[13] J. Zhang, M. H. Firooz, N. Patwari, and S. K. Kasera, "Advancing wireless link signatures for location distinction," in *Proc. of the 14th ACM international conference on Mobile computing and networking*, pp. 26–37, 2008.

[14] N. Ghose, B. Hu, Y. Zhang, and L. Lazos, "Secure physical layer voting," *IEEE Transactions on Mobile Computing*, vol. 17, no. 3, pp. 688–702, 2017.

[15] T. S. Rappaport, S. Sun, R. Mayzus, H. Zhao, Y. Azar, K. Wang, G. N. Wong, J. K. Schulz, M. Samimi, and F. Gutierrez, "Millimeter wave mobile communications for 5G cellular: It will work!," *IEEE Access*, vol. 1, pp. 335–349, 2013.

[16] D. Steinmetzer, S. Ahmad, N. Anagnostopoulos, M. Hollick, and S. Katzenbeisser, "Authenticating the sector sweep to protect against beam-stealing attacks in ieee 802.11 ad networks," in *Proceedings of the 2nd ACM Workshop on Millimeter Wave Networks and Sensing Systems*, pp. 3–8, 2018.

[17] D. Steinmetzer, Y. Yuan, and M. Hollick, "Beam-stealing: Intercepting the sector sweep to launch man-in-the-middle attacks on wireless ieee 802.11 ad networks," in *Proceedings of the 11th ACM Conference on Security & Privacy in Wireless and Mobile Networks*, pp. 12–22, 2018.

[18] X. Wei and C. Tang, "Location consistency-based mitm attack detection in 802.11 ad networks," in *International Symposium on Cyberspace Safety and Security*, pp. 18–29, Springer, 2019.

[19] Y. Yang, X. Wei, R. Xu, L. Peng, L. Zhang, and L. Ge, "Man-in-the-middle attack detection and localization based on cross-layer location consistency," *IEEE Access*, vol. 8, pp. 103860–103874, 2020.

[20] P. Velan, M. Čermák, P. Čeleda, and M. Drašar, "A survey of methods for encrypted traffic classification and analysis," *International Journal of Network Management*, vol. 25, no. 5, pp. 355–374, 2015.

[21] Z. Jiang, T. H. Luan, X. Ren, D. Lv, H. Hao, J. Wang, K. Zhao, W. Xi, Y. Xu, and R. Li, "Eliminating the barriers: Demystifying wi-fi baseband design and introducing the picoscenes wi-fi sensing platform," *IEEE Internet of Things Journal*, vol. 9, no. 6, pp. 4476–4496, 2021.