mmRhythm: Secure and Usable User Authentication for IoT Devices based on Hand-Tapping Patterns

Abdualrhman Almeajel*, Yan Zhang*, Tao Li†, Yanchao Zhang*
*Arizona State University, Tempe, AZ, USA
{atalmeaj, zhangyan, yczhang}@asu.edu
†Purdue University, West Lafayette, IN, USA
litao@purdue.edu

***Abstract*—Millimeter-wave (mmWave) technology, increasingly adopted in 5G and beyond, enables fine-grained motion sensing that surpasses traditional Wi-Fi–based approaches. This capability makes mmWave a strong candidate for secure and practical authentication. We introduce mmRhythm, a system that authenticates users through rhythmic hand-tapping near a device. The taps generate Doppler signatures in mmWave signals, which are extracted through signal processing and classified using deep learning models. To address vulnerabilities of wireless channels, mmRhythm incorporates randomized phase shifts and beamforming to mitigate RF eavesdropping, offering a secure and usable approach to contactless authentication in IoT settings.**

***Index Terms*—mmWave, Security, User Authentication**

I. Introduction

Millimeter-wave (mmWave) technology, a new feature of 5G and NextG networks, is gaining attention not only for high-speed communications but also for its fine-grained sensing capabilities [1]. With higher frequencies, wide bandwidth, and short wavelengths, mmWave can detect subtle user movements that sub-6 GHz and Wi-Fi systems cannot, making it well suited for secure authentication.

Most prior wireless authentication work has relied on Wi-Fi Channel State Information (CSI), using gait or activity features [2]–[4]. While these studies highlight the promise of wireless-based authentication, Wi-Fi suffers from low resolution and heavy interference in crowded bands. mmWave overcomes these limitations, enabling more reliable and practical solutions. This is particularly valuable for Internet of Things (IoT) devices, which often lack traditional input interfaces and therefore require secure yet convenient authentication methods.

In this paper, we present **mmRhythm**, a secure and practical authentication system that leverages mmWave sensing. Instead of relying on traditional inputs, mmRhythm authenticates users through rhythmic tapping near the device. Each tap sequence follows a self-chosen rhythm, producing Doppler shifts in the reflected mmWave signal, which are then analyzed by AI models on a backend server to verify identity.

mmRhythm is designed for both usability and security. The rhythm can be based on a song segment familiar to the user, making it memorable but difficult for others to guess or mimic. Since individuals naturally vary in how they reproduce the same rhythm, the resulting signal patterns are diverse and difficult to replicate, even by attackers who know the original rhythm.

However, ensuring mmRhythm's reliability and security poses two key challenges. First, extracting meaningful tapping features and accurately recognizing patterns from mmWave signals are complex. To address this, we explore various signal processing techniques for tapping pattern extraction and leverage novel deep learning models for robust pattern recognition. Second, like other wireless authentication systems, mmRhythm is vulnerable to eavesdropping due to the open nature of wireless channels. To mitigate this risk, we introduce two defensive mechanisms: randomized phase shifts to disrupt Doppler extraction, and beamforming to limit signal leakage toward off-angle eavesdroppers.

Our contributions are summarized as follows:

- We propose the first mmWave-based rhythm authentication system, integrating signal processing and classification for secure, contactless IoT authentication.
- We design two defenses against RF eavesdropping: randomized phase shifts which introduces unpredictability across chirps. And beamforming narrows the transmission beam toward the legitimate user, reducing signal availability to off-angle adversaries.
- We evaluate mmRhythm with 14 participants across diverse environments, achieving 98.4% authentication accuracy and high resistance to shoulder-surfing (97.24%) and video-based mimicry (94.97%).

II. Related Work

Rhythm-based authentication has largely been explored on touch-enabled devices. Techniques include rhythmic tapping or sliding on smartphones [5], [6] and wearable systems like Beat-PIN [7], though the latter requires extra hardware, making them impractical for resource-limited IoT devices.

979-8-3315-0292-8/25/$31.00 ©2025 IEEE

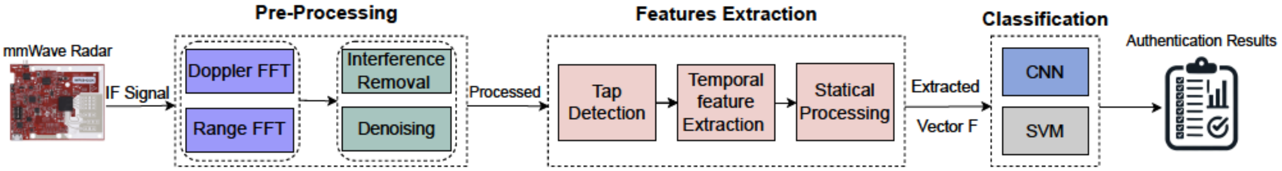


Fig. 1: System design overview.

Other methods employ alternative sensing, such as RF-Rhythm [8], which recognizes user tapping patterns on RFID tags. These methods often benefit from precise signal input and low interference, unlike wireless-based systems.

IoT authentication is challenging due to limited input interfaces and constrained device resources. WiFi-based approaches using RSSI and CSI rely on signal changes to identify users [9], but they are easily affected by interference and provide low spatial accuracy due to their longer wavelengths, which weakens performance in dynamic or noisy environments.

mmWave sensing addresses these limitations by enabling fine-grained, contactless motion detection [10]. It captures detailed patterns like rhythmic hand-tapping without requiring touch or line-of-sight. Recent works such as [11] show the potential of mmWave and deep learning for gesture recognition and 3D reconstruction. However, secure and user-friendly authentication via mmWave in IoT remains unexplored.

III. Adversary Model

We consider an attacker attempting to bypass authentication on an IoT device that uses mmRhythm. The attacker is fully aware of the system design and may attempt to replicate rhythmic taps either manually or by using a programmable robotic arm. However, the attacker does not know the user's secret rhythm and may launch one of the following attacks:

- **Brute Force Attack**: The attacker generates random rhythmic tap sequences through trial and error.
- **Visual Eavesdropping**: The attacker observes the victim's tapping rhythm through shoulder surfing or hidden cameras and tries to replicate it.
- **RF Eavesdropping**: The attacker uses a wireless sniffer to intercept and analyze mmWave signals in an attempt to infer the user's tapping rhythm by analyzing Doppler information.

IV. System Overview

We prototype mmRhythm using an mmWave radar, enabling non-intrusive user authentication based on rhythmic hand-tapping patterns. Fig. 1 illustrates the system architecture, including signal pre-processing, feature extraction, and classification models.

mmRhythm first extracts intermediate frequency (IF) signals from the mmWave radar, which captures the hand-tapping movements. In the **Pre-processing** phase, two Fast Fourier Transforms (FFTs) are applied: Range-FFT and Doppler-FFT, The Range-FFT computes the distance of the hand movement from the radar, while the Doppler-FFT captures the hand's velocity. After the FFTs, we apply **filtering** techniques to remove stationary objects and mitigate environmental noise. This denoising step ensures that only the dynamic movements from the user's taps are retained for further processing.

Once the signal has been pre-processed, the **Feature Extraction** module extracts meaningful characteristics from the data. Tap detection is used to isolate and focus on the individual tapping events. In temporal feature extraction, the system identifies key features such as the duration of each tap and the intervals between consecutive taps. Alongside this, statistical processing is performed to summarize the overall tapping behavior using statistical metrics. The extracted features are then compiled into a feature vector, denoted as F, which will be used for the classification phase. Finally, we train both CNN and SVM models to recognize the feature vector F and generate the final authentication decision.

V. System Design

This section details the design of mmRhythm, focusing on how rhythmic hand-tapping patterns are captured and processed using mmWave radar to enable secure and intuitive user authentication.

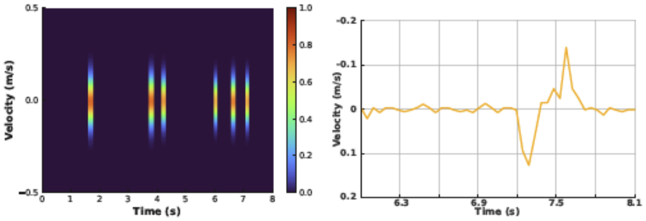
A. Feasibility Study

We first discuss the feasibility of using mmWave signals to capture hand-tapping movements for user authentication. Our experiments show that mmRhythm can effectively capture fine-grained motion characteristics associated with tapping gestures, which are critical for accurate authentication.

When a user performs a tapping gesture, the mmWave signal experiences frequency shifts due to the motion of the hand relative to the radar sensor. The Doppler shift is induced by the velocity of the hand movement and can be expressed as:

$$f_d(t) = \frac{2v(t)}{\lambda}, \tag{1}$$

where $v(t)$ represents the instantaneous velocity of the user's hand, and λ is the wavelength of the transmitted mmWave signal. The Doppler shift $f_d(t)$ varies dynamically as the user transitions through different stages of the tapping motion—an approach phase (negative velocity), a static phase (near-zero shift), and a release phase (positive velocity)—as illustrated in Fig. 2. These variations form a unique rhythmic signature, enabling precise user authentication.



(a) User rhythm of 6 taps. (b) User rhythm of a single tap.

Fig. 2: Preliminary data.

B. Signal Processing

This section details the signal processing pipeline used to extract meaningful information from radar signals for accurate tap detection and analysis.

Chirp Signal Generation and Reception: The radar emits Frequency-Modulated Continuous Wave (FMCW) chirps with linearly increasing frequency, enabling precise distance estimation. The chirp frequency is defined as:

$$f(t) = f_c + \left(\frac{B}{T_c}\right) t, \tag{2}$$

where f_c is the initial frequency, B the bandwidth, and T_c the chirp duration. Reflected chirps from the user's hand are captured for range and velocity computation [12].

Windowing: To reduce spectral leakage before applying FFT, we use a Hamming window for its balance between main lobe width and side lobe attenuation. The windowed signal is given by:

$$x_w[n] = x[n] \cdot w[n], \tag{3}$$

where $x[n]$ is the original signal and $w[n]$ represents the window function.

Range-FFT: Range is calculated from the intermediate frequency (IF) signal produced by mixing transmitted and received chirps:

$$d = \frac{c \cdot T_c \cdot f_{\text{IF}}}{2B}, \tag{4}$$

where c is the speed of light and f_{IF} the beat frequency. allows us to estimate the distance to the user's hand.

Doppler-FFT: Motion-induced Doppler shifts are analyzed to estimate hand velocity. Velocity is derived from the phase difference $\Delta\phi$ between chirps:

$$v = \frac{\lambda \Delta\phi}{4\pi T_c}, \tag{5}$$

where λ is the radar wavelength. This enhances the accuracy of tap detection and gesture classification [13]–[15].

Background Subtraction: Static reflections from the environment are removed by subtracting consecutive radar frames:

$$D_t = S_t - S_{t-1}, \tag{6}$$

where S_t and S_{t-1} are radar frames at time t and $t-1$, respectively, and D_t contains only dynamic changes.

Denoising: We use a low-pass filter to remove high-frequency noise, improving system robustness against transient noise fluctuations.

C. Feature Extraction

After processing mmWave signals to isolate genuine hand movements, the next step is to extract meaningful features that represent a user's unique tapping pattern.

Tap Detection: Tap identification begins by analyzing velocity changes to locate tap start (t_{start}) and end (t_{end}) times. These are determined by deviations from a dynamically set threshold based on the baseline signal's mean and standard deviation:

$$t_{\text{event}} = \begin{cases} t_{\text{start}}, \text{when } v > \text{threshold}, \\ t_{\text{end}}, \text{when } v < \text{threshold}, \end{cases} \tag{7}$$

where v is the velocity of the ith tap. This allows segmentation into discrete tap events.

Temporal Feature Extraction: Each tap's duration (D_i) and inter-tap interval (I_i) are computed to capture the rhythm of the tapping pattern:

$$D_i = t_{\text{end},i} - t_{\text{start},i}, \quad I_i = t_{\text{start},i+1} - t_{\text{end},i}. \tag{8}$$

A moving average filter smooths the phase data to reduce noise and improve accuracy.

Statistical Processing: To represent behavior over multiple taps, we compute the mean (μ) and variance (σ^2) of durations and intervals:

$$\mu_D = \frac{1}{n}\sum_{i=1}^{n} D_i, \quad \sigma_D^2 = \frac{1}{n}\sum_{i=1}^{n}(D_i - \mu_D)^2, \tag{9}$$

$$\mu_I = \frac{1}{n}\sum_{i=1}^{n} I_i, \quad \sigma_I^2 = \frac{1}{n}\sum_{i=1}^{n}(I_i - \mu_I)^2. \tag{10}$$

These parameters provide insights into rhythm consistency and serve as key discriminators between users [8].

General Statistical Features: From the smoothed phase signal, we also extract overall characteristics, including mean, standard deviation, maximum, and minimum:

$$\text{mean}_\phi = \frac{1}{n}\sum_{i=1}^{n} \phi_i, \quad \text{std}_\phi = \sqrt{\frac{1}{n}\sum_{i=1}^{n}(\phi_i - \text{mean}_\phi)^2}, \tag{11}$$

$$\max_\phi = \max(\phi_i), \quad \min_\phi = \min(\phi_i). \tag{12}$$

These features offer an overall view of the tapping signal's dynamics.

Temporal Alignment and Dynamic Time Warping: To ensure consistency across sessions, we apply Dynamic Time

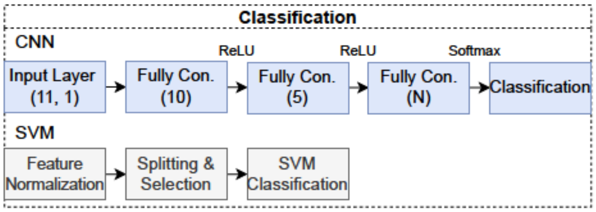


Fig. 3: Classification overview.

Warping (DTW), which aligns time-varying sequences and reduces variability due to timing shifts—especially useful for model training. The resulting feature vector **F** encapsulates the user's rhythmic tapping behavior and serves as input to the machine learning models for authentication.

D. Classification

The final phase of the system uses the extracted features to classify user gestures for authentication. We employ two classification techniques: **Convolutional Neural Networks (CNNs)** and **Support Vector Machines (SVMs)**. Their workflow is shown in Fig. 3.

CNNs are selected for their ability to capture complex patterns through layered transformations. The model takes reshaped feature vectors of size $(11, 1)$ as input, followed by two fully connected layers with 10 and 5 neurons using ReLU activation. The final layer has N neurons (equal to the number of classes) with Softmax output. Training uses stochastic gradient descent with momentum (SGDM), over 20 epochs and a mini-batch size of 16. CNNs effectively learn temporal structures, making them well-suited for rhythmic pattern recognition.

For SVMs, feature normalization ensures equal contribution from all features. The dataset is split into 80% training and validation and 20% testing. A 5-fold cross-validation is performed across various K values (e.g., 4–20), where K samples per class are used for both training and validation. SVMs are trained using the `fitcecoc` function for multi-class classification. We compute metrics including accuracy, True Positive Rate (TPR), True Negative Rate (TNR), False Negative Rate (FNR), and False Positive Rate (FPR), and evaluate performance on a separate test set.

These classifiers enable high authentication accuracy by learning the distinctive rhythmic patterns captured from mmWave signals.

VI. Mitigating Rhythm Eavesdropping

To mitigate the risk of RF eavesdropping, we introduce two potential defense mechanisms designed for wireless security: randomized phase shifts and beamforming. These techniques significantly degrade an attacker's ability to extract meaningful Doppler information from intercepted signals while still preserving signal integrity for the legitimate user.

A. Random Phase Shifts

As detailed in Equation 5, user hand velocity is derived from phase differences between consecutive chirps. To obscure this information from eavesdroppers, we apply random phase shifts across chirps during transmission. Since the legitimate system is aware of the applied random phase shifts, it can reverse them before authentication, ensuring accurate velocity estimation. In the context of mmWave radar systems.

The randomized chirp signal from transmission antenna i is expressed as:

$$s_i(t) = A_i \cos\left(2\pi f_0 t + \pi \frac{B}{T_c} t^2 + \phi_{i,0} + \psi_{i,k}\right), \qquad (13)$$

where A_i is the signal amplitude, f_0 is the starting frequency, B is the bandwidth, T_c is the chirp duration, $\phi_{i,0}$ is the initial phase for antenna i, and $\psi_{i,k}$ is the random phase shift introduced in chirp k.

This defense significantly reduces the attacker's ability to extract clean Doppler signatures, thereby increasing Bit Error Rate (BER) for unauthorized sniffers, while maintaining reliable authentication for the legitimate system.

B. Beamforming

Beamforming is used to steer the transmitted mmWave chirp signals toward the legitimate user, improving signal-to-noise ratio (SNR) and limiting signal leakage in other directions. This enhances both signal quality and security by reducing interception risk.

For a uniform linear array (ULA) with N_{TX} antennas, beamforming is achieved by applying phase shifts across antennas to focus energy at a target angle θ_{user}. The transmitted signal from antenna i at chirp k is:

$$s_i(t) = A_i \cos\left(2\pi f_0 t + \pi \frac{B}{T_c} t^2 + \phi_{i,0} + \theta_i\right), \qquad (14)$$

where $\phi_{i,0}$ is the antenna's initial phase, θ_i is the beamforming phase shift toward θ_{user}.

The beamforming shift θ_i is calculated as:

$$\theta_i = \frac{2\pi d}{\lambda} \cdot i \cdot \sin(\theta_{user}), \qquad (15)$$

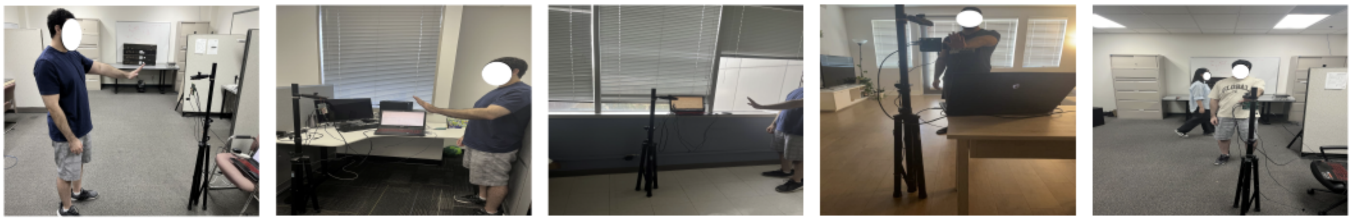
where d is the inter-antenna spacing, λ the signal wavelength, and i the antenna index [16].

VII. Implementation and Evaluation

We conducted extensive experiments to evaluate the effectiveness of our mmWave-based authentication system.

A. Experimental Setup

A group of fourteen participants with diverse backgrounds contributed by creating and repeating a unique rhythmic tapping pattern for authentication. Each session was conducted in a controlled environment, with participants performing air-tapping gestures while the mmWave radar (IWR6843ISK-ODS + DCA10000EVM) was placed 25–50



(a) Lab. (b) Office. (c) Corridor. (d) Living Room. (e) Human Interfering.

Fig. 4: Different setup environments used in the experiments.

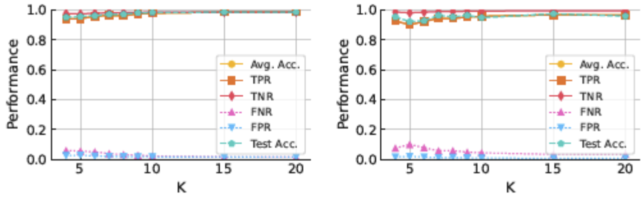
cm away. Each participant completed 50 sessions, yielding 700 rhythm samples. Most rhythms lasted between 6–10 seconds (average: 8.3 s).

B. Model Training and Validation

We used two models—Support Vector Machines (SVM) and Convolutional Neural Networks (CNN)—to analyze the tapping patterns. Data was split into training (70%), validation (10%), and testing (20%) sets. Hyperparameter tuning was performed using grid search for the SVM model and random search for the CNN model. CNNs were composed of convolutional and fully connected layers, while SVMs used an RBF kernel.

C. Performance Evaluation

We evaluated accuracy, True Positive Rate (TPR), False Positive Rate (FPR), False Negative Rate (FNR), and True Negative Rate (TNR) while varying the number of training samples per class (K) from 4 to 20. The CNN model achieved 98.4% accuracy, outperforming SVM at 94.68%. As shown in Fig. 5a and Fig. 5b, CNNs captured more nuanced rhythm features, leading to better generalization. CNN model also achieved a TPR of 98.4%, while SVM yielded a lower FPR, making it suitable for resource limited scenarios.



(a) CNN evaluation. (b) SVM evaluation.

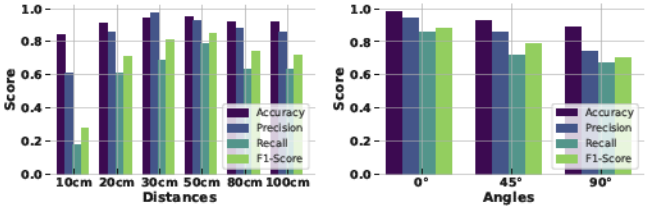
Fig. 5: Classification performance of CNN and SVM

D. Environmental Robustness

We tested the system under various environmental conditions, including changes in lighting and background noise, to evaluate its robustness in real-world scenarios. The mmWave radar maintained stable performance with minimal accuracy loss. However, accuracy dropped below 80% when the hand-radar distance was under 10 cm and gradually declined beyond 1 meter.

a) Distance Experimentation: We evaluated system performance at distances ranging from 10 cm to 150 cm. Optimal accuracy (96.7%) occurred between 25 cm and 50 cm. Accuracy declined significantly below 10 cm or beyond 1 meter due to signal attenuation and saturation, as shown in Fig. 6a.

b) Angle Experimentation: We tested system performance across different horizontal Fields of View (FoV). Within a 90° FoV, accuracy remained high (94%) but dropped noticeably beyond 120°, indicating a narrower angular range is optimal for hand-tapping detection, as shown in Fig. 6b.



(a) Different distances. (b) Different angles.

Fig. 6: Performance metrics under various test conditions.

c) New Environment Experimentation: As shown in Fig. 4, we tested the system in a variety of environments: small offices (S.O.), large offices (L.O.), corridors (Cor.), quiet labs (Q.Lab), busy labs (B.Lab), and living rooms (L.R.). The highest accuracy—over 98%—was observed in large offices, quiet labs, and living rooms. Slightly reduced performance was noted in high-activity areas like busy labs, as shown in Fig. 7.

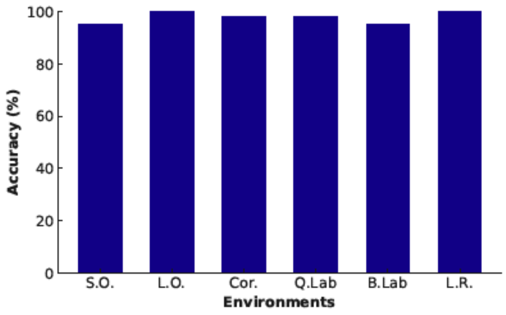


Fig. 7: Accuracy in new environments.

E. Security Analysis

We evaluated the system's security and robustness against adversarial attacks through visual eavesdropping experiments. Results show that the system maintains strong authentication performance even under potential observation threats.

a) Visual Eavesdropping: We evaluated the system's resilience to visual eavesdropping through two attack types: shoulder-surfing and video recording. In the first, attackers tried to replicate tapping patterns after a single real-time observation. In the second, they reviewed recorded sessions and made multiple mimicry attempts. Four volunteers acted as attackers, observing rhythms from 14 participants. Each attacker attempted one reproduction in the shoulder-surfing case and four in the video case. In total, we collected 320 attack samples across both scenarios.

To evaluate system robustness, we trained a classifier for each participant using the collected 700 rhythm samples from 14 users. The attack samples were then tested against the corresponding classifiers. As shown in Table I, the system achieved high rejection rates, especially with the CNN-based model. This demonstrates strong resistance to replication, even when attackers had repeated access to video-recorded tapping. These results highlight the system's robustness against eavesdropping in visually observable environments.

TABLE I: Rejection Rate (%) for Visual Eavesdropping Attacks.

	SVM	CNN
Shoulder-surfing, 1 try	95%	97.24%
Video recording, 4 tries	93.9%	94.97%

b) RF Eavesdropping: We also assessed resilience to RF eavesdropping, though real mmWave sniffers were not available during our study. Instead, we focused on randomized phase shifts as a defense mechanism. By introducing random shifts across chirps, an eavesdropper without phase knowledge cannot properly align the received signal, preventing accurate Doppler extraction. To illustrate the effect, we compared classification in two cases: with phase shifts reversed at the receiver (eavesdropper has knowledge) and without reversal (eavesdropper lacks knowledge). The CNN-based classifier achieved an 88.2% rejection rate without phase knowledge, but only 2.1% when the shifts were known. These results show that randomization significantly reduces the risk of successful RF eavesdropping.

VIII. Conclusion

We introduced mmRhythm, a mmWave-based authentication system that leverages rhythmic hand-tapping as a secure and intuitive input method. By combining signal processing with deep learning, mmRhythm captures fine-grained motion signatures that are difficult to mimic, providing a contactless solution well suited for IoT devices with limited interfaces. Our evaluation demonstrated robustness across diverse environments and resilience against both visual and RF eavesdropping, highlighting the potential of mmWave sensing to move beyond communications and serve as a foundation for practical, secure authentication.

Acknowledgment

This work was supported in part by the U.S. National Science Foundation under grants CNS-2422863, CNS-2325563, and CSR-2523518. Research was also sponsored in part by the Army Research Laboratory and was accomplished under Cooperative Agreement Number W911NF-23-2-0225. The views and conclusions contained in this document are those of the authors and should not be interpreted as representing the official policies, either expressed or implied, of the Army Research Laboratory or the U.S. Government. The U.S. Government is authorized to reproduce and distribute reprints for Government purposes notwithstanding any copyright notation herein.

References

[1] C. Seker, M. Guneser, and T. Ozturk, "A review of millimeter wave communication for 5G," in *IEEE ISMSIT*, 2018.

[2] W. Wang, A. Liu, and M. Shahzad, "Gait recognition using WiFi signals," in *ACM UbiComp*, 2016.

[3] C. Shi, J. Liu, H. Liu, and Y. Chen, "Smart user authentication through actuation of daily activities leveraging WiFi-enabled IoT," in *ACM MobiHoc*, 2017.

[4] H. Kong, L. Lu, J. Yu, Y. Chen, and F. Tang, "Continuous authentication through finger gesture interaction for smart homes using WiFi," *IEEE Transactions on Mobile Computing*, vol. 20, no. 11, pp. 3148–3162, 2020.

[5] S. Kulshreshtha and A. Arif, "Woodpecker: Secret back-of-device tap rhythms to authenticate mobile users," in *IEEE SMC*, (Toronto, ON, Canada), 2020.

[6] Y. Chen, J. Sun, R. Zhang, and Y. Zhang, "Your song your way: Rhythm-based two-factor authentication for multi-touch mobile devices," in *IEEE INFOCOM*, 2015.

[7] B. Hutchins, A. Reddy, W. Jin, M. Zhou, M. Li, and L. Yang, "Beat-PIN: A user authentication mechanism for wearable devices through secret beats," in *ACM ASIA CCS*, 2018.

[8] J. Li, C. Wang, A. Li, D. Han, Y. Zhang, J. Zuo, R. Zhang, L. Xie, and Y. Zhang, "Rhythmic RFID authentication," *IEEE/ACM Transactions on Networking*, vol. 31, no. 2, pp. 877–889, 2023.

[9] A. Ghany, B. Uguen, and D. Lemur, "A robustness comparison of measured narrowband CSI vs RSSI for IoT localization," in *IEEE VTC-Fall*, 2020.

[10] A. Soumya, K. Mohan, and C. LR., "Recent advances in mmWave-radar-based sensing, its applications, and machine learning techniques: A review," *Sensors*, vol. 23, no. 21, p. 8901, 2023.

[11] Y. Sun, H. Zhang, Z. Huang, and B. Liu, "DeepPoint: A deep learning model for 3D reconstruction in point clouds via mmWave radar," 2021.

[12] S. Rao, "Introduction to mmWave sensing: FMCW radars," July 2020. Available: https://www.ti.com/lit/an/spyy005a/spyy005a.pdf, Accessed on: 2023-09-28.

[13] J. Xu, Z. Bi, A. Singha, T. Li, Y. Chen, and Y. Zhang, "mmLock: User leaving detection against data theft via high-quality mmWave radar imaging," in *IEEE ICCCN*, 2023.

[14] H. Xue, Y. Ju, C. Miao, Y. Wang, S. Wang, A. Zhang, and L. Su, "mmMesh: Towards 3D real-time dynamic human mesh construction using millimeter-wave," in *ACM MobiSys*, 2021.

[15] C. Iovescu and S. Rao, "The fundamentals of millimeter wave radar sensors," July 2020. Available: https://www.ti.com/sensors/mmwave-radar/overview.html, Accessed on: 2023-09-28.

[16] T. Instruments, "Imaging radar using cascaded mmWave sensor reference design," Tech. Rep. TIDUEN5A, Texas Instruments, 2020. Available: https://www.ti.com/tool/TIDEP-01012.