MultiAuth: Enable Multi-User Authentication with Single Commodity WiFi Device

Hao Kong
Shanghai Jiao Tong University
Shanghai, China
hao.kong@sjtu.edu.cn

Li Lu
Zhejiang University
Hangzhou, China
li.lu@zju.edu.cn

Jiadi Yu*
Shanghai Jiao Tong University
Shanghai, China
jiadiyu@sjtu.edu.cn

Yingying Chen
Rutgers University
New Brunswick, NJ, USA
yingche@scarletmail.rutgers.edu

Xiangyu Xu
Shanghai Jiao Tong University
Shanghai, China
chillex@sjtu.edu.cn

Feilong Tang
Shanghai Jiao Tong University
Shanghai, China
tang-fl@cs.sjtu.edu.cn

Yi-Chao Chen
Shanghai Jiao Tong University
Shanghai, China
yichao@utexas.edu

ABSTRACT

With the increasing integration of humans and the cyber world, user authentication becomes critical to support various emerging application scenarios requiring security guarantees. Existing works utilize Channel State Information (CSI) of WiFi signals to capture single human activities for non-intrusive and device-free user authentication, but multi-user authentication remains a challenging task. In this paper, we present a multi-user authentication system, *MultiAuth*, which can authenticate multiple users with a single commodity WiFi device. The key idea is to profile multipath components of WiFi signals induced by multiple users, and construct individual CSI from the multipath components to solely characterize each user for user authentication. Specifically, we propose a MUltipath Time-of-Arrival measurement algorithm (MUTA) to profile multipath components of WiFi signals in high resolution. Then, after aggregating and separating the multipath components related to users, *MultiAuth* constructs individual CSI based on the multipath components to solely characterize each user. To identify users, *MultiAuth* further extracts user behavior profiles based on the individual CSI of each user through time-frequency analysis, and leverages a dual-task neural network for robust user authentication. Extensive experiments involving 3 simultaneously present users demonstrate that *MultiAuth* is accurate and reliable for multi-user authentication with 87.6% average accuracy and 8.8% average false accept rate.

CCS CONCEPTS

• **Networks** → **Mobile and wireless security**; • **Human-centered computing** → **Mobile computing**.

*Jiadi Yu is the corresponding author

MobiHoc '21, July 26–29, 2021, Shanghai, China

ACM ISBN 978-1-4503-8558-9/21/07…$15.00
https://doi.org/10.1145/3466772.3467032

KEYWORDS

WiFi signals, multi-user authentication, multipath profiling, individual CSI construction

ACM Reference Format:
Hao Kong, Li Lu, Jiadi Yu, Yingying Chen, Xiangyu Xu, Feilong Tang, and Yi-Chao Chen. 2021. *MultiAuth*: Enable Multi-User Authentication with Single Commodity WiFi Device. In *The Twenty-second International Symposium on Theory, Algorithmic Foundations, and Protocol Design for Mobile Networks and Mobile Computing (MobiHoc '21), July 26–29, 2021, Shanghai, China.* ACM, New York, NY, USA, 10 pages. https://doi.org/10.1145/3466772.3467032

1 INTRODUCTION

Nowadays, many efforts have been made to extend the Internet of Things (IoT) to a more generalized concept, i.e., the Internet of Everything (IoE) [9]. Instead of connecting only things (e.g., mobile devices) online, the IoE integrates humans, processes, data, and things for connecting everything to the cyber world. Hence, the basis of mapping humans to the cyber world, i.e., user authentication, could support not only security guarantees but also various IoE applications. Different from traditional authentication approaches (e.g., password, fingerprint, and face recognition), user authentication for IoE should possess more advanced capabilities, such as authenticating users without extra interaction, and authenticating multiple users simultaneously, etc. The increasing demands of IoE applications inspire many research efforts to realize user authentication with such advanced capabilities.

To enable user authentication without extra interaction, existing works exploit WiFi signals to sense daily activities for user authentication [6, 7, 13, 14, 20, 27]. However, the WiFi-based works can only realize user authentication under single-user scenarios, which are usually limited and hardly support a wider range of multi-user scenarios. To adapt to the widely deployed multi-user collaboration scenarios, it is necessary to authenticate multiple users simultaneously without extra interaction. For example, in the enterprise domain, smart factories could map the workers and their activities to their identities, which enables tracing previous activities and prompting current activities for collaborative intelligent manufacturing. In the entertainment field, the entertainment system could map real-world players and their activities to the virtual-world identities for supporting multi-player motion sensing games.

Since WiFi signals propagate in omnidirectional ways and have significant multipath effects, it is feasible to use Channel State Information (CSI) of WiFi signals to capture human activities to enable multi-user authentication. To implement multi-user authentication using WiFi signals, we face several challenges in practice. First, we should accurately profile the multipath components of WiFi signals to capture each user's activity individually under multi-user scenarios. Second, we need to use only single WiFi device to distinguish multiple users. Third, we should extract robust behavioral features from each user to enable multi-user authentication.

In this paper, we propose a multi-user authentication system, *MultiAuth*, which authenticates multiple users simultaneously with single commodity WiFi device. The key idea is to profile multipath components of WiFi signals induced by multiple users, and construct individual CSI from the multipath components to solely characterize each user for user authentication. Specifically, we first present a MUltipath Time-of-Arrival measurement algorithm (MUTA) to measure the Time-of-Arrival (ToA) of signal propagation paths for multipath profiling in high resolution. Then, after aggregating and separating users' multipath components, we construct individual CSI of each user to solely characterize a user. Next, we conduct time-frequency analysis on individual CSI to obtain user behavior profiles, and design a Convolutional Neural Network-Recurrent Neural Network (CNN-RNN)-based dual-task model to extract fine-grained features from the profiles for robust user authentication. Extensive experiments demonstrate that *MultiAuth* could simultaneously authenticate up to 3 users with average 87.6% authentication accuracy and 8.8% false accept rate.

We highlight our contributions as follows.

- We propose a multi-user authentication system that can authenticate multiple users simultaneously with only single commodity WiFi device under multi-user scenarios.
- We present a multipath profiling algorithm, MUTA, which can distinguish different propagation paths of WiFi signals for high-resolution multipath profiling.
- We exploit rich information underlying multipath components of WiFi signals, and construct individual CSI to solely characterize each user under multi-user scenarios.
- We evaluate the performance of the proposed system in real environments, and the results show that *MultiAuth* can authenticate multiple users simultaneously.

2 PRELIMINARY

To realize multi-user authentication, we first discuss the theoretical fundamental of multipath profiling using CSI of WiFi signals, and then explore the feasibility of multi-user authentication using CSI.

2.1 Theoretical Fundamental of Multipath Profiling Using CSI

To achieve multi-user authentication, behavioral features of each user underlying WiFi signals should be characterized individually. However, WiFi signals induced by multiple users cannot directly exhibit individual information. To solve the problem, we propose to measure propagation delays (i.e., Time-of-Arrival, ToA) and profile multipath components induced by each user, because signals reflected by users locating at different positions propagate with different path lengths. Existing works compute power delay profiles to measure ToA through Inverse Fast Fourier Transform (IFFT) [17, 24]. However, the time resolution of power delay profile depends on signal bandwidth [24], i.e., $\Delta = 1/B$, where B is the bandwidth and is narrow for commercial WiFi. Such a resolution usually cannot effectively distinguish multipath components under limited bandwidths, which may disable multi-user sensing.

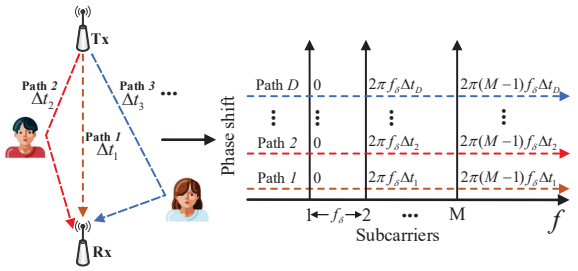


Figure 1: ToA measurement with CSI phase shifts.

To measure propagation delays of WiFi signals with high resolution, different from existing IFFT-based works, we propose a MUltipath Time of Arrival measurement algorithm (MUTA). The algorithm is developed from MUltiple SIgnal Classification algorithm (MUSIC) [12], which is a classic high-resolution algorithm to measure multipath Angle-of-Arrivals (AoAs) through the phase shift across antennas. The proposed MUTA measures multipath ToAs through the phase shift across subcarriers for high-resolution multipath profiling. Specifically, suppose a WiFi signal is transmitted from a transmitter and propagates through D multipath components with different lengths to arrive at a receiver, as shown in the left of Figure 1. For the OFDM-based WiFi signals propagating through multiple subcarriers, one path's phase shift introduced at m-th subcarrier relative to the first subcarrier is $-2\pi(m-1)f_\delta\Delta t$, where f_δ is the frequency difference between adjacent subcarriers, and Δt is the ToA of the path, as illustrated in the right part of Figure 1. For simplicity of representation, we denote the complex exponential of these introduced phase shifts as a function of the ToA of the propagation path, so the phase shifts in complex exponential format across all M subcarriers are $a(\Delta t) = \begin{bmatrix}1 & e^{-j2\pi f_\delta \Delta t} & \cdots & e^{-j2\pi(M-1)f_\delta\Delta t}\end{bmatrix}^T$. Based on the phase shifts of each path, we construct a mode vector describing the phase shifts for all the D paths, $A = [a(\Delta t_1), a(\Delta t_2), \cdots, a(\Delta t_D)]$. Hence, the signal X is modeled as:

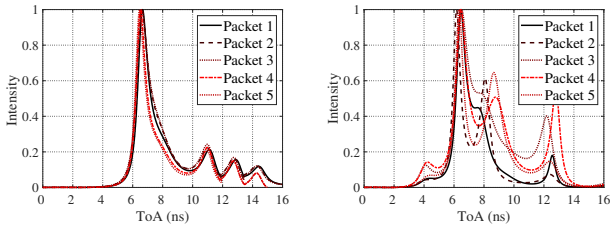
$$X = AS + N, \tag{1}$$

where S is the transmitted signal and N is noise.

Based on the data model, we further measure ToAs of signal propagation paths for multipath profiling. The received signal X containing the CSI collected under multiple subcarriers could be arranged to a measurement matrix, i.e.,

$$X = \begin{bmatrix} h(f_1) & h(f_2) & \cdots & h(f_W) \\ h(f_{W+1}) & h(f_{W+2}) & \cdots & h(f_{2W}) \\ \vdots & \vdots & \cdots & \vdots \\ h(f_{(L-1)W+1}) & h(f_{(L-1)W+2}) & \cdots & h(f_{LW}) \end{bmatrix}, \tag{2}$$

where $h(f_i)$ is the CSI value of the i-th subcarrier, L is the maximal number of multipath components, W is the number of samples to measure each path, and $L \times W$ equals to the number of available subcarriers. The value of L and W could be set according to actual



(a) Static environment. (b) Multi-user walking.

Figure 2: Pseudo-spectrum in different situations.

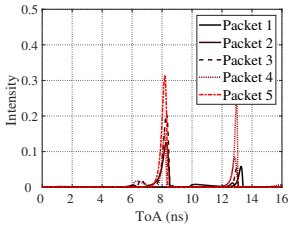


Figure 3: Pseudo-spectrum after static removing.

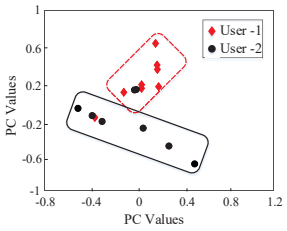


Figure 4: Statistical distribution of different users.

needs of multipath resolving and subcarrier number. To balance the trade-off between multipath distinguishing and noise resistance, we set L and W equal for each received signal. According to the correspondence, MUTA could measure ToAs as long as the mode vector A could be derived from the measurement matrix. Specifically, we first perform eigenvalue decomposition of the covariance matrix $R = XX^H$, where X^H is the conjugate transpose of X. Then, D eigenvectors with the largest D eigenvalues are selected, which constructs a signal subspace. The rest $M - D$ eigenvectors form a noise subspace U_N. Afterward, ToAs could be measured by a pseudo-spectrum based on the conclusion that the noise subspace is orthogonal to the mode vector of signals [12], i.e.,

$$P_{MU}(\Delta t) = \frac{1}{a^T(\Delta t)U_N U_N^H a(\Delta t)}. \quad (3)$$

Because of the orthogonality, the ToA Δ_t of a multipath signal exhibits a maximum value in the pseudo-spectrum, which could be detected through searching the peaks in P_{MU}. Hence, by measuring the ToAs of a signal, the proposed MUTA could resolve the signal to multiple paths, each of which propagates with different delays.

The theoretical resolution of MUTA could be derived according to the resolution analysis of MUSIC, through the analogy between ToA and AoA, space (i.e., the parameter corresponds to antennas) and frequency (i.e., the parameter corresponds to subcarriers). Based on an universal analysis model of MUSIC-based AoA measurement [30], we develop the relationship between the threshold of Signal-Noise-Rate (SNR_t) and the time resolution Δ_t as

$$SNR_t = 360(\frac{m-2}{mW})(\pi m \Delta f \Delta_t)^{-4}, \quad (4)$$

where m and W are the dimension and column of measurement matrix in MUTA, $\Delta f = 312.5kHz$ is the frequency difference between two subcarriers. Take the $5GHz$ commercial WiFi as an illustration. Overall $200MHz$ bandwidth signals could be spliced as a whole according to [24], which provides 560 subcarriers available to form a measurement matrix with $m = 560$ and $W = 24$. The SNR threshold is set to $10dB$ because the SNR range of standard WiFi signal is $10 - 30dB$ [2]. Under the above setting, MUTA improves time resolution from $5.0ns$ to $2.0ns$ and space resolution from $1.5m$ to $0.6m$ compared with IFFT-based multipath profiling. Therefore, applying MUTA could promote the resolution of multipath profiling of WiFi signals to satisfy fine-grained multi-objective sensing.

2.2 Feasibility Study of Multi-User Authentication using CSI

To achieve multi-user authentication, we further explore the feasibility of authenticating multiple users based on the multipath components measured by MUTA. We first collect CSI of WiFi signals in a static environment, and employ MUTA to calculate the pseudo-spectrum P_{MU} for each CSI packet. The result of pseudo-spectrum is shown in Figure 2(a). It can be observed that there are several multipath components indicating the line-of-sight signals and static reflected signals, each of which keeps stable across CSI packets. Then, we further collect CSI of WiFi signals from two users walking simultaneously in the same environment. As shown in Figure 2(b), the ToAs of specific multipath components in the pseudo-spectrum change dynamically with the two users' movement. This indicates that users' movements affect the multipath length, which is consistent with the theoretical analysis of MUTA. Furthermore, we remove the multipath components stable among ToA by calculating the differential between CSI packets to explicitly exhibit users' movements, as shown in Figure 3. It can be observed that there remain two significant peaks, representing the multipath components reflected by the two users respectively. The result demonstrates that the proposed MUTA is able to resolve the multipath components induced by multiple individuals.

Afterward, we further explore identifying multiple users based on multipath components of WiFi signals. The change of a path's ToA, i.e., the shift of a peak's position in the pseudo-spectrum, indicates the length change of the path, which is relevant to the motion amplitude of users. Thus, change of ToA is roughly applied to distinguish users in this section. To extract individual uniqueness, we explore statistical distribution for different users to explore differences among individuals. Specifically, we calculate the first-order difference of a path's ToAs over time for each movement, which is a one-dimensional vector (i.e., each element in the vector is the path's ToA difference between two adjacent packets). Since Principal Component Analysis (PCA) could enlarge the variance between different samples to exhibit dominated statistical distribution, we employ PCA on the vectors collected from several times of movement by the two users. Figure 4 shows the statistical distribution of these samples using PCA. It can be observed that most of the samples are aggregated in two regions, which demonstrates that the two users could be roughly distinguished through the multipath components induced by human movement. With the encouraging experimental results, we are motivated to exploit rich information underlying multipath components of WiFi signals for multi-user authentication.

3 DESIGN OVERVIEW

In this section, we present the threat model and system overview for the multi-user authentication system *MultiAuth*.

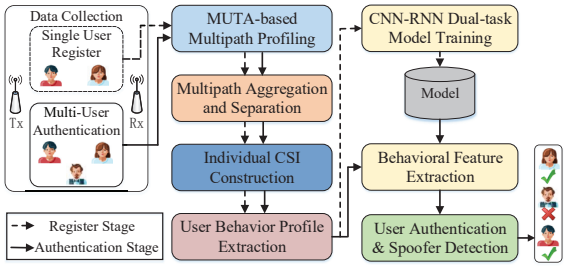


Figure 5: System overview.

3.1 Threat Model

In the threat model, one or more spoofers would deceive the authentication system for allowing legal permissions to multi-user collaboration applications. Specifically, one or more spoofers perform activities for trying to deceive the authentication system with one of the legitimate user's identity respectively. The system uses WiFi signals to sense all the users' activities, and then identifies each user to detect the spoofers through the sensed activities of each user individually. The threat model could be refined to two attacks by different attack efforts, i.e., *zero-effort attack* and *imitation attack*. For the zero-effort attack, spoofers perform activities to deceive the system without any prior knowledge about legitimate users. For the imitation attack, spoofers attempt to deceive the system by imitating one of the legitimate user's behaviors.

3.2 System Overview

Figure 5 shows the architecture of *MultiAuth*, which includes two stages, i.e., the register stage and authentication stage.

In the register stage, each user performs specific activities several times for identity registration, such as walking, standing up, etc. First, *MultiAuth* collects CSI of WiFi signals affected by a user's activity, and performs multipath profiling through the proposed MUltipath Time of Arrival measurement algorithm (MUTA). Then, after aggregating the multipath components involved with the user, *MultiAuth* constructs individual CSI of the user for individual characterization. Afterward, based on user behavior profiles derived by the individual CSI, *MultiAuth* trains a proposed Convolutional Neural Network-Recurrent Neural Network (CNN-RNN)-based dual-task model for feature extraction. Finally, after all users registering identity in the system respectively, *MultiAuth* obtains a trained model with the capability of authenticating multiple users.

In the authentication stage, multiple users perform activities simultaneously for authentication. *MultiAuth* first collects CSI of WiFi signals induced by users' activities, and employs MUTA to profile the multipath components induced by all the users. Then, after aggregating and separating the multipath components, *MultiAuth* constructs individual CSI of each user for individual characterization. Next, the trained dual-task model is employed to extract behavioral features from user behavior profiles derived by the individual CSI, and further authenticates each user under the multi-user scenario.

4 MULTI-USER AUTHENTICATION

In this section, we present the design of the multi-user authentication system, *MultiAuth*.

4.1 MUTA Implementation for Multipath Profiling

To achieve multi-user authentication, *MultiAuth* first collects CSI of WiFi signals induced by multiple users' activities, and then performs MUTA to profile multipath components of WiFi signals. Due to hardware imperfection and the requirement of subspace construction, *MultiAuth* first needs to calibrate CSI errors and determine multipath numbers before implementing MUTA.

4.1.1 CSI Calibration. Due to hardware imperfection, there are inevitable amplitude and phase errors in CSI of WiFi signals collected from commodity WiFi devices. Hence, we first calibrate CSI to correct amplitude and phase errors after collecting raw CSI data.

CSI amplitude error is caused by digitization errors when measuring the power of received signals, and CSI phase errors are mainly caused by clock unsynchronization, such as Carrier Frequency Offset (CFO), Sampling Frequency Offset (SFO), and Packet Detection Delay (PDD) [31], etc. To eliminate the amplitude and phase errors in CSI, we adopt the error correction approach [24] for data calibration. The approach first mitigates amplitude errors by averaging raw CSIs from multiple packets collected within coherence time. Then, it mitigates constant phase errors by picking a reference channel and compensate for the phase difference between each channel pair. In this way, the amplitude and phase errors are corrected, which validates MUTA on CSI of commodity WiFi signals.

4.1.2 Determination of Multipath Number. In MUTA, the number of multipath components is equal to the number of eigenvectors in signal subspace when conducting eigenvalue decomposition. If MUTA mistakenly includes noise eigenvectors into the signal subspace, the measured ToAs would vary significantly across packets, which may affect the detection of user movement. Hence, it is necessary to set an accurate number of multipath components according to the received signal.

Since the fluctuation of LoS path only results from an inaccurate multipath number, we consider using the stability of LoS path to find the accurate number of underlying multipath components from received CSI. Specifically, MUTA constructs pseudo-spectrums with different multipath numbers, and calculates the variance of LoS path's ToAs over time. The multipath number with minimal variance is chosen as the accurate multipath number. As a result, under the accurate multipath number setting, the fluctuation of ToAs only comes from human movement.

With the calibrated CSI and an accurate multipath number, *MultiAuth* performs multipath profiling using MUTA mentioned in Section 2.1.

4.2 Multipath Aggregation and Separation

After implementing MUTA, *MultiAuth* could find the multipath components induced by multiple users through searching the peaks in the pseudo-spectrum. In practice, if the signal has a large bandwidth, i.e., containing sufficient subcarriers, the number of multipath components could be abundant enough to allow one individual to reflect several multipath components from different body parts respectively. Hence, it is necessary to aggregate the multipath components of each individual and separate the multipath components from different individuals to characterize users.

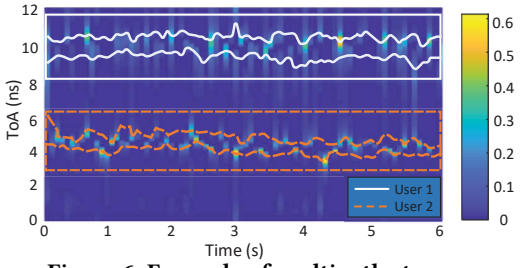


Figure 6: Example of multipath streams.

To realize multipath aggregation and separation, we first construct multipath streams using the consecutive pseudo-spectrums after removing static components. Figure 6 shows an example of multipath streams, which exhibits several multipath components over time from two users' movements in bright curves. It can be seen that the multipath components reflected by one individual are closer while those between different individuals are farther. Hence, *MultiAuth* aggregates the curves closer to each other and separates the curves farther from others to achieve multipath aggregation and separation. Specifically, since the multipath components involved with users have higher energy in the spectrogram, we first align horizontal curves with high energy through dynamic programming to find the multipath components induced by users. Then, we assign these paths to different individuals according to their ToA distances. The ToA distance of an individual could be set according to the size of a normal person. Finally, through aggregating and separating several curve regions from the whole streams, *MultiAuth* matches the multipath components with specific ToAs to each user.

4.3 Individual CSI Construction

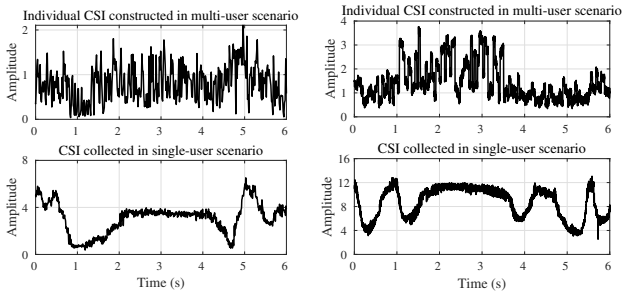
Based on the multipath components of each user through multipath aggregation and separation, *MultiAuth* further constructs CSI corresponding to each user under multi-user scenarios, which is called individual CSI. The individual CSI generated from multipath components denotes the channel condition of specific paths, revealing the information relevant with one specific user from the received CSI. Different to paths' ToA vibration that roughly describes user behaviors shown in Section 2.2, the individual CSI simulates the CSI of WiFi signals collected from each user solely, providing a precise characterization of a single user.

To construct each user's individual CSI, we first construct CSI of each multipath component, and then employ all multipath components induced by a user to construct his/her individual CSI. The construction of CSI for each path refers to the estimation of CSI amplitude and phase of the path. Specifically, the CSI $\hat{H}_i$ of the i-th multipath could be expressed as

$$\hat{H}_i = a_i e^{-j(\phi_i + 2\pi f \Delta t_i)}, \tag{5}$$

where a_i is the CSI amplitude of i-th path, ϕ_i is the initial phase shift, and $2\pi f \Delta t_i$ is the phase shift caused by the ToA Δt_i under a specific subcarrier f. Theoretically, the sum of CSI for all multipath components should be equal to the actual collected CSI H. Hence, we can estimate CSI of each multipath component by solving an optimization problem, i.e.,

$$[\hat{a}_i, \hat{\phi}_i] = \arg\min_{a_i, \phi_i} \left\| \sum_{i=1}^{N} \hat{H}_i - H \right\|^2, \tag{6}$$



(a) User 1. (b) User 2.

Figure 7: Comparison of individual CSI constructed in multi-user scenario and the CSI collected in single-user scenario.

where N is the number of multipath components. To solve the above optimization problem, we define the CSI parameters standing for amplitude and initial phase shift as

$$P = [a_1 e^{-j\phi_1} \quad a_2 e^{-j\phi_2} \quad \cdots \quad a_N e^{-j\phi_N}]^T, \tag{7}$$

where a_i and ϕ_i denote the amplitude and phase of the i-th multipath. Then, we form phase shifts of multipath's ToAs as

$$\Phi = \begin{bmatrix} e^{-j2\pi f_1 \Delta t_1} & e^{-j2\pi f_1 \Delta t_2} & \cdots & e^{-j2\pi f_1 \Delta t_N} \\ e^{-j2\pi f_2 \Delta t_1} & e^{-j2\pi f_2 \Delta t_2} & \cdots & e^{-j2\pi f_2 \Delta t_N} \\ \cdots & \cdots & \vdots & \cdots \\ e^{-j2\pi f_S \Delta t_1} & e^{-j2\pi f_S \Delta t_2} & \cdots & e^{-j2\pi f_S \Delta t_N}, \end{bmatrix} \tag{8}$$

where f_i is the frequency of i-th subcarrier and S is the number of subcarriers. Then, the optimization problem can be solved uniquely by the following formula:

$$\hat{P} = (\Phi^T \Phi)^{-1} \Phi^T H. \tag{9}$$

Finally, the CSI $\hat{H}_i$ of each multipath component is obtained based on the estimated $\hat{a}_i$ and $\hat{\phi}_i$ in $\hat{P}$, i.e., $\hat{H}_i = \hat{a}_i e^{-j(\hat{\phi}_i + 2\pi f \Delta t_i)}$. After the CSIs for all multipath components are estimated, *MultiAuth* constructs the individual CSI of each user by jointly summarizing the CSIs of each user's multipath components.

To validate the effectiveness of constructing individual CSI, we conduct an experiment to exhibit the capability of behavior exhibition of individual CSI. In the experiment, two users locate with $1.5m$ vertical distance and perform pushing hand simultaneously. We conduct MUTA on the CSI collected from the two users to derive individual CSI of each user. Then, each user's CSI is further collected in a single-user scenario for comparison. Figure 7 shows the individual CSI constructed in the two-user scenario and the CSI collected in the single-user scenario respectively. It can be observed that although individual CSIs suffer from some distortions, their general fluctuation trends are similar to these of the CSIs collected in the single-user scenario. This indicates that the individual CSI could exhibit behaviors of each user solely in multi-user scenarios, which could be used to achieve multi-user authentication.

4.4 User Behavior Profile Extraction

Based on the individual CSI of each user, *MultiAuth* further extracts user behavior profiles underlying individual CSI for fine-grained behavior characterization.

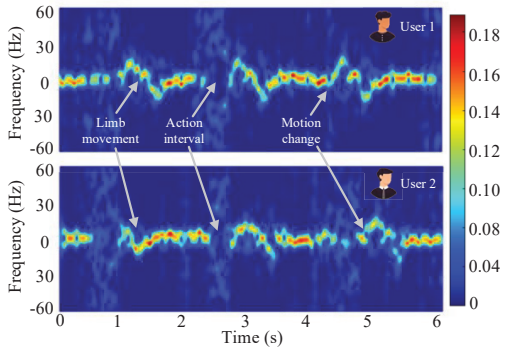


Figure 8: Time-frequency spectrograms for two users.

Human activity is presented in CSI streams with two informations, i.e, duration and frequency [21]. Duration denotes the time a person takes to perform an activity, and frequency represents the velocity of body movements. Due to unique inherent physiology and behavioral styles, different users exhibit different durations and frequencies in CSI when performing activities. For example, a person of high muscle mass performs activities in high acceleration and velocity, resulting in a short duration and high frequency. Thus, through time-frequency analysis, we could deeply reveal a person's uniqueness to distinguish users.

CSI streams of WiFi signals present a similar detection capability with Doppler radar [20], and the Doppler effect could characterize fine-grained movement [8]. Hence, we derive time-frequency spectrograms through Short-Time Fourier Transform (STFT) to analyze user behaviors. Figure 8 shows time-frequency spectrograms for two user's individual CSIs when performing pushing hand several times. We can observe high energy bands induced by users' limb movements. Moreover, there are also apparent patterns revealing users' behavior uniqueness. For example, the frequency magnitude indicates the speed of limb movement, the interval between two adjacent actions, and the motion change including transitory motion pause and restart. In particular, the two users' patterns have non-neglectable differences. For example, user 1 tends to have higher frequency shifts during limb movement because of his faster motion induced by big muscle masses, while user 2 presents longer intervals between actions due to his behavioral habits.

To extract user behavior profiles, we first apply Butterworth filter to eliminate high-frequency noises that exist in the impulse of individual CSI. Then, we perform STFT on individual CSI to obtain time-frequency spectrograms, and further calculate the contour of high energy bands. Afterward, we segment the contour for each action, each of which denotes a user behavior profile. Specifically, we calculate the magnitude differential of contours, i.e.,

$$D(n) = \sum_{t=nL}^{(n+1)L-1} |C_{t+1} - C_t|, n \in [0, N-1], \tag{10}$$

where $D(n)$ is the magnitude differential of the n-th sliding window, L is the length of sliding window, C_t is the contour's magnitude value at time t, and N is the number of sliding window. When $D(n)$ is constantly lower than a predefined threshold, the contour remains stable, which indicates a suspense between actions. Hence, the contour is segmented to episodes in the point, each of which represents a user behavior profile.

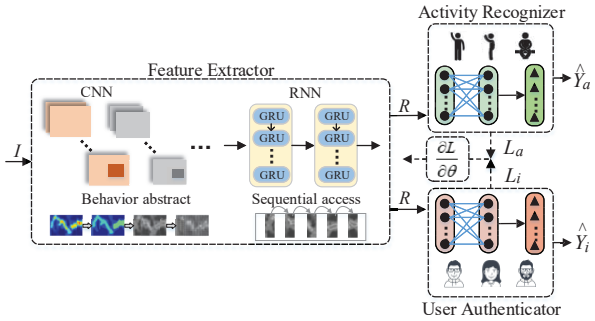


Figure 9: Architecture of CNN-RNN-based dual-task neural network model.

4.5 Dual-Task Model Construction for User Authentication

Although user behavior profiles could characterize individual uniqueness, they still suffer from distortions introduced by individual CSI construction. To extract robust and fine-grained behavioral features for user authentication, we first investigate the in-depth difference between distortions and behavioral features. The distortion refers to the transient error caused by mistakenly estimating parameters of individual CSI, which are usually irrelevant and irregular. On the contrary, the behavioral features embed significant sequential relationships, such as the action interval and motion change, which are usually relevant and regular. Hence, using sequential relationships could mitigate the influence of distortions for extracting robust features induced by user activities. As a gating mechanism for Recurrent Neural Network (RNN), Gated Recurrent Unit (GRU) could explore sequential relationship underlying input data [1], so we employ GRU-based RNN as the basis for feature extraction.

Moreover, since behavior-based authentication involves two interrelated tasks, i.e., identity authentication and activity recognition, the shared information among them could facilitate feature extraction for each task. Hence, instead of designing two independent models to realize the two tasks respectively, we employ multi-task learning to construct a dual-task model, which exploits shared information among the two tasks for learning more fine-grained features for each task. Borrow the idea of [7], we design a Convolutional Neural Network-Recurrent Neural Network (CNN-RNN)-based dual-task model to extract robust and fine-grained features for user authentication.

Figure 9 shows the architecture of the CNN-RNN-based dual-task model, which consists of a shared feature extractor based on CNN-RNN, and two fully-connected networks with different tasks, i.e., an activity recognizer and user authenticator. The feature extractor incorporates three CNNs and two RNNs to extract behavioral features from the input user behavior profile I. The CNNs are composed of convolutional layers abstracting the input I as compressed representation through convolutional operations, and the pooling layers reducing the dimension of the compressed representation. It treats user behavior profiles as images to abstract fine-grained features from pixels to characterize human behaviors. The RNNs partition the feature map from CNNs into fragments for sequential relationship access, and then extracts a feature map R, which embeds the behavioral features underlying human behavior profiles.

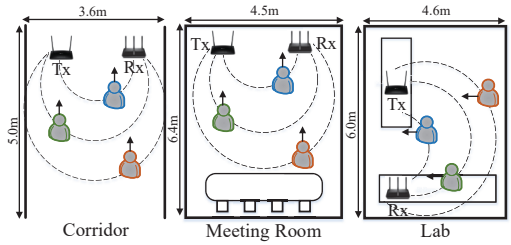


Figure 10: Experiment Environments.

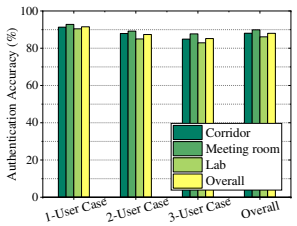


Figure 11: Authentication accuracy for different cases in different environments.

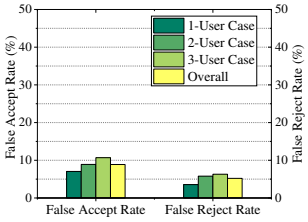


Figure 12: FAR and FRR for different cases.

The user authenticator and activity recognizer have the same structure, consisting of two Fully-Connected (FC) layers and a softmax layer. The inputs of the two networks are both the feature map R extracted from the feature extractor. With different tasks, the two networks extract feature representations on different scales for achieving user authentication and activity recognition respectively. The user authenticator outputs identity label $\hat{Y}_i$ and identity loss L_i (i.e., error of user authentication), and the activity recognizer outputs the activity label $\hat{Y}_a$ and the activity loss L_a (i.e., error of activity recognition). To share the information they learn, the two losses are combined for jointly training the model, i.e.,

$$L = \alpha(L_a + b) + \beta e^{(L_i + c)}, \tag{11}$$

where α and β are weights of the activity loss and identity loss respectively, and b and c are the biases for activity loss and identity loss respectively. Since user authentication requires more in-depth features than activity recognition, the overall loss is designed in exponential function, where the convergence of identity loss has a higher priority than that of activity loss. By continuously passing back the gradient on overall loss $\frac{\partial L}{\partial \theta}$ to the feature extractor, the dual-task model could be trained with the capability of extracting robust and fine-grained features to authenticate users as well as recognizing activities.

In addition to authenticating legitimate users, *MultiAuth* needs to detect unexpected spoofers under the zero-effort attack and imitation attack in multi-user scenarios. Human behavioral features are determined by not only human subjectivity, but also objective physiological features (e.g., the length of limbs, the power generated by muscle). Hence, there are obvious differences in behavioral features between a spoofer and a legitimate user, even if the spoofer imitates the extrinsic behaviors of the legitimate user. Based on such differences, *MultiAuth* could detect one or more spoofers individually under multi-user scenarios to resist the two kinds of attacks. Specifically, for each user, *MultiAuth* compares all elements in the identity probability $\hat{Y}_i$ with a predefined threshold λ. If $\forall k \in [1, n]$, $Y_i^k < \lambda$, the current user is identified as a spoofer.

5 EVALUATION

To comprehensively evaluate *MultiAuth*, we conduct experiments in real environments.

5.1 Evaluation Setup

We implement *MultiAuth* on a laptop HP Pavilion 14, and use two wireless routers equipped with Atheros NIC and three antennas, i.e., TL-WDR4310 and TL-WR2543N, as the transmitter and receiver respectively. The wireless routers are modified with Atheros CSI Tool [24], which enables fast channel switching for obtaining CSI on enlarged bandwidth WiFi signals. Two types of signal modes are applied to evaluate the system under different WiFi modes. In 2.4GHz band WiFi, we splice a 70MHz bandwidth signal from channel 1 to 11 according to the methodology of [31]. In 5GHz band, we splice a 200MHz bandwidth WiFi signal from channel 36 to 56 according to the methodology of [24]. Considering there are 3 antennas in the wireless router to receive CSI, we concatenate the three antennas' CSI measurement matrices together to construct a large measurement matrix for MUTA, which could improve the resolution of multipath profiling according to [25].

A total of 15 volunteers are recruited in the experiments including 9 males and 6 females, aged between 21 and 60. We ask 10 volunteers to play the role of legitimate users and the rest 5 volunteers act as spoofers. Six common activities are selected for the experiments, i.e., walking, turning right, turning left, sitting down, standing up, and hands reaching out and pulling back. The experiments are repeated in three environments, i.e., a corridor, meeting room, and lab, whose layouts are shown in Figure 10. The simultaneously present users perform activities in specific areas where the lengths of the propagation path composed by human body, Tx and Rx are different. This is to ensure different ToAs of signal reflection, which is the basis of multipath separation. Orientations of activity performance are toward the transceivers. Moreover, the users are reminded not to interfere with the direct signal propagation between other users and transceivers. The vertical distances between the areas on one side are from 0.3m to 2m so as to meet the basic requirements of multipath separation.

In the register stage, each legitimate volunteer performs each activity 15 times to provide training samples for identity registering individually. In the authentication stage, the volunteers participate in three kinds of experiment cases respectively, i.e., 1-user case, 2-user case, and 3-user case. In the 1-user case, each volunteer is authenticated individually to evaluate the single-user authentication capability of *MultiAuth*. In the 2-user or 3-user cases, 2 or 3 volunteers are authenticated simultaneously to evaluate the multi-user authentication capability of *MultiAuth*. The volunteers could perform any predefined activity in each case.

5.2 Authentication Performance

We first evaluate user authentication performance of *MultiAuth*. Figure 11 shows the authentication accuracy of *MultiAuth* under the three cases in the three environments respectively. Specifically, the authentication accuracies under the three cases are 91.5%, 87.4%, and 85.2% respectively with an average accuracy of 87.6%. We can see that compared with the single-user scenario, the accuracy of

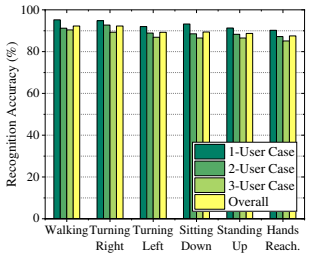


Figure 13: Activity recognition accuracy of *MultiAuth*.

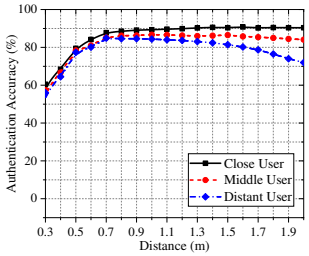


Figure 14: Authentication accuracy in different distances.

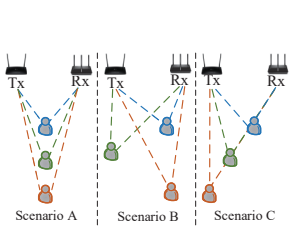
authenticating multiple users slightly degrades. The result demonstrates that *MultiAuth* effectively extends single-user authentication to multi-user authentication with an acceptable authentication performance under multi-user scenarios.

In addition, we can also observe from Figure 11 that there are similar accuracy variances of environments under different cases, i.e., the meeting room enables a better authentication accuracy than the corridor and the lab. This is because the meeting room has a larger area and less furniture, which makes the multipath reflection more simple and thus reduces the interference between different users' multipath components. However, even in a complex environment, the authentication accuracy under the 3-user cases could be still approaching 85%, which demonstrates that *MultiAuth* is reliable and robust in different environmental layouts.

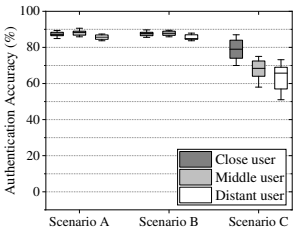
The False Accept Rate (FAR) and False Reject Rate (FRR) denote the probabilities of falsely detecting spoofers as legitimate users and misidentifying legitimate users as spoofers. Figure 12 shows the FAR and FRR under the three cases, where the number of simultaneous present spoofers ranges from 1 to 3 in the multi-user scenarios. We can see that *MultiAuth* achieves an overall FAR of 8.8% and FRR of 5.2% respectively. Compared with the single user scenario, the FAR and FRR for multi-user scenarios increase less than 4%, which are insignificant. The result demonstrates that *MultiAuth* is reliable to detect multiple spoofers simultaneously to resist the zero-effort and imitation attacks in the multi-user scenarios. Also, *MultiAuth* rarely rejects legitimate users, which guarantees a user-friendly experience for user authentication.

5.3 Activity Recognition Performance

In addition to authenticating multiple users, *MultiAuth* can also recognize the activities performed by the users. We further evaluate the activity recognition performance of *MultiAuth* under the single-user scenario and multi-user scenarios respectively. Figure 13 shows the recognition accuracy for each activity in different cases. Specifically, the activity recognition accuracies for the three cases are 92.7%, 89.5%, and 87.4% respectively. Compared with single-user activity recognition, recognizing multiple users' activities simultaneously does not introduce significant performance degradation. This indicates that *MutiAuth* enables the multi-user activity recognition comparable with single-user activity recognition. Moreover, we can see that different activities do not induce significant differences in recognition accuracy. For example, the recognition accuracy difference between the coarse-grained walking and the fine-grained hands reaching out and pulling back is only 2.8%. This result demonstrates that *MultiAuth* is reliable in recognizing various kinds of daily activities under multi-user scenarios.



(a) Setup of user location.



(b) Authenticaiton Accuracy under different locations.

Figure 15: Authentication performance under different setups of user location.

5.4 Impact of Distance between Users

The distance between users affects the separation for the users. We evaluate the impact of vertical distance between users of one side on *MultiAuth* in the 3-user case. Here we define the three users as the close user, middle user, and distant user respectively according to their relative distance to the LOS path. With the close user located in a fixed position, the middle user and distant user located away from the previous user with a fixed distance. For example, a distance of $0.3m$ indicates that the middle user and distant user are vertical $0.3m$ and $0.6m$ away from the close user respectively.

Figure 14 shows the authentication accuracy under different distances between the users. It can be observed that with the distance increases, the overall authentication accuracy improves rapidly, and exceeds 80% for all the users when the distance reaches $0.6m$. This is because the increasing distance makes the multipath components of different users easier to be separated, which could characterize each user's behaviors more accurately for user authentication. Moreover, we can also see that as the distance exceeds $1.5m$, the authentication performance for the close user and middle user tends to be stable while that for the distant user slowly decreases. This is because the increasing distance put the distant user far away from the major WiFi sensing area, resulting in significant signal attenuation and thus unable to effectively capture individual behaviors. Such performance degradation is caused by the limitation of commodity WiFi sensing. According to [15], the suitable face-to-face communication distances of users are between $0.46m$ to $1.22m$. Hence, *MultiAuth* could effectively authenticate multiple users under the majority of suitable communication distances.

5.5 Impact of User Location

Because of the interference and obstruction between simultaneously present users, the location of users induces an inevitable influence on multi-user authentication. We experiment to explore the impact of user location on system performance. Since the two sides are symmetric, we focus on three representative scenarios of users' locations on one side, as shown in Figure 15(a). Scenario A and B are typical experimental setups for previous evaluations, which enables non-obstructive stations for signal propagation. Scenario C, however, presents a straight line-connected user location in which the signal propagation suffers from interference and obstruction. The vertical distances between users are $0.8m$ to $1.2m$.

We exhibit the authentication performance under the three scenarios for 3-user case, as shown in Figure 15(b). Obviously, we can observe that scenarios A and B achieve acceptable performance.

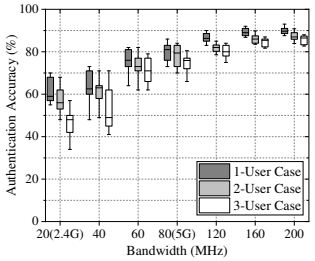


Figure 16: Authentication accuracy under different bandwidths.

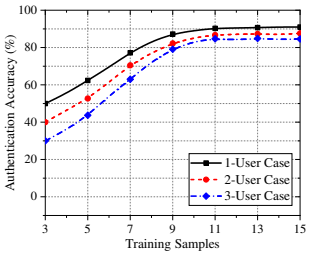


Figure 17: Authentication accuracy under different training data sizes.

Specifically, the three users in scenarios A and B could be authenticated with average 87.1% and 85.9% accuracies respectively. And we can also see the variation between users in the two scenarios is insignificant, demonstrating a robust authentication performance among different users. For scenario C, the authentication accuracies for the three users dramatically decrease to 78.7%, 68.4%, and 65.9% respectively with significant user variations. The reason is that the front user becomes an obstacle interfering with the signal propagation of the back user. The result proves that *MultiAuth* works under majority situations. However, it invalidates the authentication capability in some special cases where users interfere with the signal propagation between each other.

5.6 Impact of Signal Bandwidth

The signal bandwidth determines the number of available subcarriers to be utilized in MUTA, which affects the resolution of multipath profiling. Hence, it is necessary to evaluate the impact of signal bandwidth on multi-user authentication. In this experiment, we implement *MultiAuth* with $20MHz$ to $60MHz$ bandwidth under $2.4GHz$ signal and $80MHz$ to $200MHz$ under $5GHz$ signal respectively to explore the performance under different bandwidths. Figure 16 shows the authentication accuracy of different cases under these bandwidths. It can be observed that the larger bandwidths could improve the authentication accuracy for all cases. Specifically, when the bandwidth increases from $20MHz$ to $200MHz$, the overall authentication accuracy for the three cases promotes from 55.3% to 87.6%. This is because, with sufficient subcarriers, MUTA can resolve more multipath components and thus could characterize each individual more precisely. Moreover, we can also see that as the bandwidth increases, the deviation of authentication accuracy gradually decreases, which indicates better robustness of user authentication under large bandwidth signals. This result suggests that *MultiAuth* should be implemented under large bandwidth WiFi signals for a reliable multi-user authentication.

5.7 Impact of Training Data Size

Since *MultiAuth* incorporates a neural network, i.e., the CNN-RNN-based dual-task model, the size of training data would affect the system performance. We evaluate the impact of training data size on authentication performance of *MultiAuth*. Figure 17 shows the authentication accuracy of *MultiAuth* under different training sizes for the three cases. It can be observed that with the training size increases, the authentication accuracy first improves and then tends to be stable for all the cases. When the training data size increases to 9 samples, the authentication accuracies for the three cases promote to 87.2%, 82.2%, and 80.1%, which is comparable to that with more training samples. The result demonstrates that to ensure an acceptable multi-user authentication performance, each user should perform each activity at least 9 times to provide training samples. Such a requirement does not significantly affect user experience during user registration.

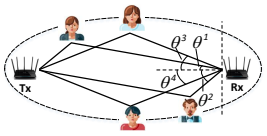


Figure 18: Users with same ToA.

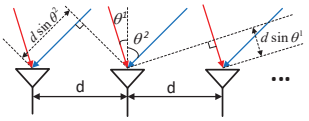


Figure 19: AoA measurement.

6 DISCUSSION

In this section, we discuss a practical limitation of *MultiAuth* and present a feasible solution.

As shown in Figure 18, if multiple users are located on an ellipse focusing on the transmitter and receiver, the multipath components cannot be separated due to the same ToA. Hence, individual CSI contains information of the users simultaneously, which invalidates the multi-user authentication in such a special case.

To enable multi-user authentication in the special case, we consider exploiting Angle-of-Arrival (AoA) of WiFi signals to separate the individual CSI containing multiple users' informations of the same ToA. As shown in Figure 19, there is a signal with K multipath components propagate to several receiving antennas with the same ToA Δt_i but different incident angle θ^k. Thus, the multipath components result in a path length difference $d \sin\theta^k$ between the first and second antennas and thus causes a phase shift $2\pi f d \sin\theta^k / c$, where f is frequency and c is the speed of light. Assume $\hat{H}_i'$ is the CSI for the K multipath components, it could be expressed as the sum of CSIs for these multipath components respectively, i.e.,

$$\hat{H}_i' = \sum_{k=1}^{K} \hat{H'}_i^k = \sum_{k=1}^{K} a_i^k e^{-j(\Phi_i^k + 2\pi f \frac{\Delta d \sin\theta_i^k}{c})}, \tag{12}$$

where $\hat{H'}_i^k$ is the CSI of the k-th multipath with the ToA Δt_i, a_i^k is the amplitude, $\Phi_i^k = \phi_i^k + 2\pi f \Delta t_i$ denotes the initial phase and phase shift caused by the ToA Δt_i, Δd is the distance between current antenna with the first antenna, and θ_i^k is the AoA. Theoretically, the sum of the K multipath CSIs is equal to the CSI $\hat{H}_i$ calculated by the ToA Δt_i. Hence, through solving a similar optimization problem, we can calculate the CSI for each multipath component even if these multipath components have the same ToA,

$$[\hat{a}_i^k, \hat{\Phi}_i^k] = \arg\min \left\| \sum_{k=1}^{K} \hat{H'}_i^k - \hat{H}_i \right\|. \tag{13}$$

Hence, the individual CSI constructed from users with the same ToA is separated into different individual CSIs, each of which corresponds to a single user, indicating that users with the same ToA could also be authenticated.

7 RELATED WORK

In the section, we review some works related to *MultiAuth*.

Wireless Sensing Application. WiFi devices are widely deployed in indoor environments, which realizes wireless sensing to support various applications, such as indoor localization [22], activity recognition [21, 23], gesture recognition [16, 29], human tracking [10, 11], and domain-adaptation [4, 28], etc. However, all these works are designed for single-user scenario. To extend WiFi sensing application to multi-user scenarios, *MiMU* [18] combines different users' gestures to generate virtual samples for realizing multi-user gesture recognition. But the combination of all available gestures consumes much computing resources. A following work *MultiTrack* [17] enables multi-user tracking and gesture recognition through multiple devices. However, it imposes a heavy process burden, which limits the practical spread of such applications.

Behavior-based User Authentication. To enable user authentication, some studies explore WiFi signals to sense human movements for employing low-cost and widely deployed devices. Early researches [20, 27] implement authentication through sensing human gaits. Following works extend to realize the authentication with coarse-grained activities [14], fine-grained gestures [6, 7], etc. However, all these WiFi-based authentications can only authenticate user under single-user scenario, which limits the application scenarios in real situations.

Application for Multiple Users. Nowadays, many efforts are being made to extend the state-of-the-art applications to multi-user scenarios for improving the real-world availability. For example, *FaceDisplay* [3] enables multiple users to simultaneously interact with the virtual world via touch or gestures. A previous work [5] processes multiple users' utterances simultaneously to achieve multi-user speech recognition. Another work [19] recognizes multi-user activities using wearable sensors. A recent work *DeepBreath* [26] detects multi-user breathing simultaneously through RF signals. All of these works present the potential to implement the state-of-the-art applications to multi-user scenarios.

8 CONCLUSION

In this paper, we propose *MultiAuth*, which could authenticate multiple users with commodity WiFi device. We first present a MUltipath Time of Arrival measurement algorithm (MUTA) to profile multipath components of WiFi signals in high resolution. Then, after aggregating and separating the multipath components reflected by different users, we construct individual CSI of each user for behavior characterization. Afterward, we extract user behavior profiles from individual CSI, and further design a Convolutional Neural Network-Recurrent Neural Network (CNN-RNN)-based dual-task model to authenticate each user under multi-user scenarios. Experiments demonstrate that *MultiAuth* is accurate and reliable for multi-user authentication.

REFERENCES

[1] Chung, J., Gulcehre, C., Cho, K., and Bengio, Y. Empirical evaluation of gated recurrent neural networks on sequence modeling. *arXiv preprint arXiv:1412.3555* (2014).

[2] Duarte, M., Sabharwal, A., Aggarwal, V., Jana, R., Ramakrishnan, K. K., Rice, C. W., and Shankaranarayanan, N. K. Design and characterization of a full-duplex multiantenna system for wifi networks. *IEEE Transactions on Vehicular Technology 63*, 3 (2014), 1160–1177.

[3] Gugenheimer, J., Stemasov, E., Sareen, H., and Rukzio, E. Facedisplay: towards asymmetric multi-user interaction for nomadic virtual reality. In *Proc. ACM CHI'18* (Montreal, QC, Canada, 2018), pp. 1–13.

[4] Jiang, W., Miao, C., Ma, F., Yao, S., Wang, Y., Yuan, Y., Xue, H., Song, C., Ma, X., Koutsonikolas, D., et al. Towards environment independent device free human activity recognition. In *Proc. ACM MobiCom'18* (New Delhi, India, 2018), pp. 289–304.

[5] Kim, J., and Sung, W. Multi-user real-time speech recognition with a gpu. In *2012 IEEE ICASSP'12* (2012), pp. 1617–1620.

[6] Kong, H., Lu, L., Yu, J., Chen, Y., Kong, L., and Li, M. Fingerpass: Finger gesture-based continuous user authentication for smart homes using commodity wifi. In *Proc. ACM MoboHoc'19* (Catania, Italy, 2019).

[7] Li, C., Liu, M., and Cao, Z. Wihf: Enable user identified gesture recognition with wifi. In *In Proc. IEEE INFOCOM'20* (Toronto, ON, Canada, 2020), pp. 586–595.

[8] Lu, L., Yu, J., Chen, Y., Zhu, Y., Xu, X., Xue, G., and Li, M. Keylistener: Inferring keystrokes on QWERTY keyboard of touch screen through acoustic signals. In *In Proc. IEEE INFOCOM'19* (Paris, France, 2019), pp. 775–783.

[9] Miraz, M. H., Ali, M., Excell, P. S., and Picking, R. A review on internet of things (iot), internet of everything (ioe) and internet of nano things (iont). In *2015 Internet Technologies and Applications (ITA)* (2015), IEEE, pp. 219–224.

[10] Qian, K., Wu, C., Yang, Z., Liu, Y., and Jamieson, K. Widar: Decimeter-level passive tracking via velocity monitoring with commodity wi-fi. In *Proc. ACM MobiHoc'17* (Chennai, India, 2017), p. 6.

[11] Qian, K., Wu, C., Zhang, Y., Zhang, G., Yang, Z., and Liu, Y. Widar2. 0: Passive human tracking with a single wi-fi link. In *Proc. ACM MobiSys'18* (Munich, Germany, 2018), pp. 350–361.

[12] Schmidt, R. Multiple emitter location and signal parameter estimation. *IEEE transactions on antennas and propagation 34*, 3 (1986), 276–280.

[13] Shahzad, M., and Zhang, S. Augmenting user identification with wifi based gesture recognition. *Proc. ACM Interact. Mob. Wearable Ubiquitous Technol. 2*, 3 (2018), 134.

[14] Shi, C., Liu, J., Liu, H., and Chen, Y. Smart user authentication through actuation of daily activities leveraging wifi-enabled iot. In *Proc. ACM MobiHoc'17* (Chennai, India, 2017), p. 5.

[15] Sorokowska, A., Sorokowski, P., Hilpert, P., Cantarero, K., Frackowiak, T., Ahmadi, K., Alghraibeh, A. M., Aryeetey, R., Bertoni, A., Bettache, K., et al. Preferred interpersonal distances: a global comparison. *Journal of Cross-Cultural Psychology 48*, 4 (2017), 577–592.

[16] Tan, S., and Yang, J. Wifinger: leveraging commodity wifi for fine-grained finger gesture recognition. In *Proc. ACM MobiHoc'16* (Paderborn, Germany, 2016), pp. 201–210.

[17] Tan, S., Zhang, L., Wang, Z., and Yang, J. Multitrack: Multi-user tracking and activity recognition using commodity wifi. In *Proc. ACM CHI'19* (Glasgow, Scotland, UK, 2019), p. 536.

[18] Venkatnarayan, R. H., Page, G., and Shahzad, M. Multi-user gesture recognition using wifi. In *Proc. ACM MobiSys'18* (Munich, Germany, 2018), pp. 401–413.

[19] Wang, L., Gu, T., Tao, X., Chen, H., and Lu, J. Recognizing multi-user activities using wearable sensors in a smart home. *Pervasive and Mobile Computing 7*, 3 (2011), 287–298.

[20] Wang, W., Liu, A. X., and Shahzad, M. Gait recognition using wifi signals. In *Proc. ACM UbiComp'16* (Heidelberg, Germany, 2016), pp. 363–373.

[21] Wang, W., Liu, A. X., Shahzad, M., Ling, K., and Lu, S. Understanding and modeling of wifi signal based human activity recognition. In *Proc. ACM MobiCom'15* (New York, USA, 2015), pp. 65–76.

[22] Wang, X., Gao, L., Mao, S., and Pandey, S. Csi-based fingerprinting for indoor localization: A deep learning approach. *IEEE Transactions on Vehicular Technology 66*, 1 (2016).

[23] Wang, Y., Liu, J., Chen, Y., Gruteser, M., Yang, J., and Liu, H. E-eyes: device-free location-oriented activity identification using fine-grained wifi signatures. In *Proc. ACM MobiCom'14* (Maui, Hawaii, USA, 2014), pp. 617–628.

[24] Xie, Y., Li, Z., and Li, M. Precise power delay profiling with commodity wifi. In *Proc. ACM MobiCom'15* (Paris, France, 2015), p. 53–64.

[25] Xiong, J., Sundaresan, K., and Jamieson, K. Tonetrack: Leveraging frequency-agile radios for time-based indoor wireless localization. In *Proc. ACM MobiCom'15* (Paris, France, 2015), pp. 537–549.

[26] Yue, S., He, H., Wang, H., Rahul, H., and Katabi, D. Extracting multi-person respiration from entangled rf signals. *Proc. ACM IMWUT'18 2*, 2 (2018).

[27] Zeng, Y., Pathak, P. H., and Mohapatra, P. Wiwho: wifi-based person identification in smart spaces. In *Proc. IEEE IPSN'16* (Vienna, Austria, 2016), p. 4.

[28] Zhang, J., Tang, Z., Li, M., Fang, D., Nurmi, P., and Wang, Z. Crosssense: towards cross-site and large-scale wifi sensing. In *Proc. ACM MobiCom'18* (New Delhi, India, 2018), pp. 305–320.

[29] Zheng, Y., Zhang, Y., Qian, K., Zhang, G., Liu, Y., Wu, C., and Yang, Z. Zero-effort cross-domain gesture recognition with wi-fi. In *Proc. ACM MobiSys'19* (Seoul, South Korea, 2019), pp. 313–325.

[30] Zhou, C., Haber, F., and Jaggard, D. L. A resolution measure for the MUSIC algorithm and its application to plane wave arrivals contaminated by coherent interference. *IEEE Trans. Signal Process. 39*, 2 (1991), 454–463.

[31] Zhuo, Y., Zhu, H., Xue, H., and Chang, S. Perceiving accurate CSI phases with commodity wifi devices. In *Proc. IEEE INFOCOM'17* (GA, USA, 2017), pp. 1–9.