Privacy-Preserving Location Authentication in Wi-Fi Networks Using Fine-Grained Physical Layer Signatures

Wei Wang, *Student Member, IEEE,* Yingjie Chen, Qian Zhang, *Fellow, IEEE*

***Abstract*—The surging deployments of Wi-Fi hotspots in public places drive the blossoming of location-based services (LBSs). A recent measurement reveals that a large portion of the reported locations are either forged or superfluous, which raises security issues such as bogus alibis and illegal usage of restricted resources, and leads to some initial investigation on location authentication. However, most prior approaches leak users' location information or rely on external devices. To overcome these limitations, we propose *PriLA*, a Privacy-preserving Location Authentication system that verifies users' location information based on physical layer (PHY) information available in legacy Wi-Fi preambles. The crux of PriLA is to turn detrimental features in wireless systems, namely carrier frequency offset (CFO) and multipath, into useful signatures for privacy protection and authentication. In particular, PriLA exploits CFO and channel state information (CSI) to secure wireless transmissions starting from the handshake phase between mobile users and the access point (AP), and meanwhile verify the truthfulness of users' reported locations based on users' multipath profiles. PriLA is a clean-slate design that requires no extra hardware or external networks, and is transparent to upper layer protocols. Existing privacy preservation techniques in the upper layers can also be applied on top of PriLA to enable various applications. We have implemented PriLA on GNURadio/USRP platform and commercial off-the-shelf Intel 5300 NICs. The experimental results show that PriLA achieves the authentication accuracy of 93.2% on average, while leaking merely 45.7% information in comparison with the state-of-the-art approach.**

***Index Terms*—Location authentication, location privacy, physical layer information**

I. Introduction

Driven by the proliferation of Wi-Fi hotspots in public places, location-based services (LBSs) have experienced surging development in recent years. LBSs take advantage of users' location information to provide personalized or contextual services. Existing applications of LBSs range from location-based discount distribution like *Groupon* to geo-social networks like *Foursquare* and *Waze*. A typical LBS system consists of an LBS provider who offers services based on users' physical locations via trusted Access Points (APs), and mobile users who request specific service along with their own location and identity (ID) information.

Unfortunately, a recent measurement study [1] on Foursquare check-ins reports that there exists a large amount of forged and superfluous location data uploaded by mobile users. One major reason behind this phenomenon is that users concern about their location privacy and use synthetic traces to replace their true locations. The forged traces incur significant discrepancies that mislead the applications driven by the location data. What is worse, by forging location reports, malicious users can abuse services like illegally accessing restricted resources and creating bogus alibis.

To avoid location forgery, an essential step is location authentication, which verifies the truthfulness of the reported location data. An intuitive approach is to equip provider with localization capability, which, however, falls short due to the following two limitations. First, there are places such as coffee shops and stores where the number of provider-trusted APs is not enough to perform localization. Second, the growing privacy threats of sharing location information via LBS have been widely concerned [2]. Such privacy threats come from the fact that many untrusted Wi-Fi infrastructures aggressively collect the location data. Although mobile users can secure their location data via encryption, their location information is still at high risk of being leaked due to the broadcast nature of wireless medium. Adversary can easily infer the targeted user's physical location by collaboratively eavesdropping frames over the air from several sniffers (e.g., untrusted APs). Previous research [3], [4] shows that one can determine a node with meter/submeter level resolution using several receivers. Being aware of such risks, mobile users may be reluctant to use LBS applications. Note that existing location privacy preserving approaches cannot be directly integrated into location authentication systems, since hiding mobile users' location information would also prevent the LBS provider from authenticating them. Therefore, it is crucial to enable location authentication without compromising users' location privacy.

Despite growing attempts and extensive efforts, it is still challenging to facilitate privacy-preserving location authentication in Wi-Fi networks. State-of-the-art solutions either fail to consider users' privacy concerns [5]–[8] or rely on dedicated hardware or external networks for authentication [5], [9], while the capability of privacy-preserving location authentication within the LBS system is missing. External hardware or devices assisted authentication results in high start-up costs, and cannot be implemented using existing LBS infrastructures.

W. Wang is with the School of Electronic Information and Communications, Huazhong University of Science and Technology and the Fok Ying Tung Research Institute, Hong Kong University of Science and Technology. E-mail: gswwang@cse.ust.hk.

Y. Chen and Q. Zhang are with the Department of Computer Science and Engineering, Hong Kong University of Science and Technology, Hong Kong. e-mail: {ocgcyj, qianzh}@cse.ust.hk.

The target of this paper is to fill the above gaps: we argue that privacy-preserving location authentication can be realized within existing Wi-Fi-based LBS systems by exploiting physical layer (PHY) signatures in Wi-Fi preambles. To achieve this goal, this paper introduces *PriLA*, a **Pri**vacy-Preserving **L**ocation **A**uthentication system in orthogonal frequency-division multiplexing (OFDM) based Wi-Fi networks (e.g., IEEE 802.11a/g/n/ac). This system allows the LBS provider to successfully conduct authentication and meanwhile guaranteeing location privacy preservation for all mobile users against adversaries. To this end, the following requirements should be satisfied. First, to defend against adversaries with localization capability, the users' IDs should be fully protected starting from the handshake (or association) phase. Otherwise, the adversaries can infer a user's location by analyzing the signal strength [3] or anger-of-arrival (AoA) information [4] extracted from the user's frames. Second, the provider should be able to verify users' locations even when there is not enough APs to perform localization.

To overcome the above predicaments, PriLA exploits carrier frequency offset (CFO) and multipath, which can be obtained via Wi-Fi preambles. In communication systems, CFO and multipath are considered to be detrimental, while PriLA leverages them for authentication and privacy-preservation. PriLA takes advantage of the channel reciprocity property, and uses CFO together with channel state information (CSI) to generate CFO patterns that are exclusively known by the transmission pair. In particular, to defend against adversaries with localization capability, PriLA uses CFO pattern to secure users' IDs starting from the handshake (or association) phase. As such, the adversaries cannot link a frame to a certain user, or infer the presence of a user, and thus fail to localize a user via localization. To enable authentication without performing localization, PriLA leverages users' multipath profiles, which can be extracted from CSI using multiple antennas. In addition, the multipath profiles are reliable as it is determined by the environment's physical layout and hard to forge. As reported in [10], users in proximity share similar multipath profiles. Thus, the LBS provider can verify the reported location information through comparing users' multipath profiles.

The main contributions of this paper are summarized as follows.

- We propose a detailed design for privacy-preserving location authentication in Wi-Fi networks without assistance from extra hardware or networks. In particular, we exploit CFO and multipath information that can be extracted from legacy Wi-Fi preambles.
- We leverage the CFO and CSI information to secure the transmissions between users and the provider. The proposed security technique leaks merely 45.7% information compared to the state-of-the-art approach.
- We exploit multipath profiles to enable authentication without localizing users. The experimental results show that the multipath-based authentication achieves an average accuracy of 93.2%.
- We prototype PriLA using GNURadio/USRP testbed [11] and off-the-shelf Intel 5300 NICs [12] to validate the feasibility and merits of our design.

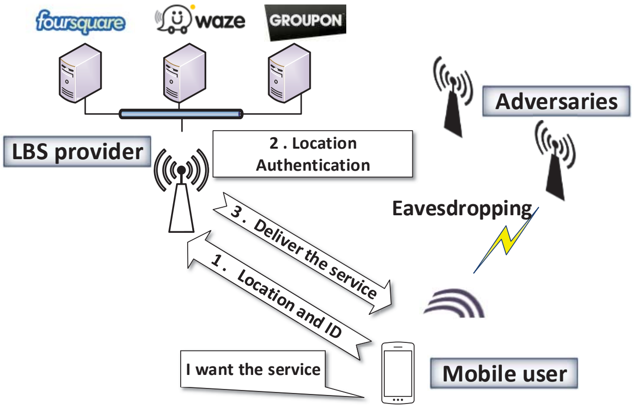


Fig. 1. System architecture of location-based service in Wi-Fi networks.

The reminder of this paper is structured as follows. We begin in Section II with the system model. Section III describes the design overview. Section IV and Section V elaborate the CFO encryption and the multipath-based authentication in PriLA, respectively. System implementation is described in Section VI. Experimental evaluation is presented in Section VII. Section VIII reviews related work, followed by conclusion in Section IX.

II. System Model

A. Location-Based Service System Architecture

Fig. 1 depicts a typical LBS system architecture, which consists of an LBS provider, mobile users, and adversaries. In an LBS system, a mobile user requests service from the LBS provider by reporting the user's location information with its ID to the trusted AP, which connects to the LBS servers via a secured backhaul. In this paper, we assume that a user's ID is its MAC address, or its ID can be inferred from its MAC address. As assumed in many existing location privacy preservation proposals [13]–[15], the mobile user only reports coarse location information to preserve privacy. Based on the frames sent by users, the LBS provider checks the truthfulness of the location information. Note that the LBS provider may deploy only one AP within a user's transmission range. As such, it is normally infeasible for the AP to directly localize a mobile user without the assistance from mobile users. Only when the reported information is confirmed to be true, the LBS provider delivers the service to the mobile user via downlink transmission from the trusted AP. Following a common practice in LBS system [9], [14], [15], we assume that there are multiple mobile users within a coarse region.

B. Physical Layer Model

Channel Model. We assume that nodes are placed in an indoor environment where the wireless channels are multipath channels with scatters and reflectors. The wireless channels are time-varying due to the movement of objects as well as the varying atmospheric conditions, while the variance within coherence time (normally tens or hundreds of milliseconds) is significantly small. Hence, a channel within coherence time is assumed to be static. The multipath properties of a wireless channel are identical in both directions, which is referred to as channel reciprocity [16]. Note that the noise at two ends of a link is asymmetric.

Hardware Impairments. In a typical wireless communication system [17], the signal to be transmitted is upconverted to a high frequency carrier prior to transmission. The receiver is expected to tune its frequency to the same carrier frequency for downconverting the signal to baseband, prior to demodulation. However, due to impairments of RF chipsets, the carrier frequency of the receiver is impossible to be exactly same as the carrier frequency of the transmitter. Hence in practice, the received baseband signal, instead of being centered at DC (0 Hz), will be centered at a frequency offset Δf, where

$$\Delta f = fc_{TX} - fc_{RX}, \tag{1}$$

The representation of received baseband signal is (ignoring the noise)

$$r(t) = x(t) * e^{\frac{j2\pi\Delta f t}{F_s}}, \tag{2}$$

where $x(t)$ denotes the transmitted signal, $r(t)$ the received signal, and F_s the sampling frequency. In the single carrier case, this equation can be further interpreted as

$$r(t) = A(t)e^{j\theta(t)} * e^{\frac{j2\pi\Delta f t}{F_s}} = A(t) * e^{j(\theta(t)+\frac{2\pi\Delta f t}{F_s})}, \tag{3}$$

where $A(t)$ and $\theta(t)$ are the magnitude and phase components of the received signal respectively. It is obvious that the frequency offset will cause the received symbol suffering from phase rotation depending of the sampling time t and the amount of Δf. In multiple carrier modulation like OFDM system, the impact of CFO becomes more complicated. Large CFO not only causes phase offset in received symbol, but also introduces amplitude reduction of desired subcarrier, which will largely degrade the decoding signal-to-noise ratio (SNR).

Preamble Structure. We assume that the mobile user uses Wi-Fi to communicate with the LBS server. In particular, we consider a typical OFDM-based Wi-Fi network, where the PHY structure conforms to the Physical Layer Convergence Protocol (PLCP) defined by IEEE 802.11a/g/n/ac. A preamble, consisting of Short Training Field (STF) and Long Training Field (LTF), is prepended to each frame. In IEEE 802.11n specification, the STF has ten repetitions and each consists of 16 samples [18]. The periodicity of the STF is used for frame synchronization and coarse CFO estimation. The LTF is used to estimate fine-grained CFO and CSI, with which the effects of the propagation channel are equalized.

C. Threat Model

We consider adversaries who are interested in tracking the location of mobile users. We assume that an adversary is computationally unconstrained, and can eavesdrop and analyze all frames over the air in Wi-Fi networks. An adversary can be either an external node or a compromised mobile user. Adversaries are assumed to be equipped with multiple antennas, and there may be multiple adversaries that collude together to locate mobile users using existing localization techniques (e.g., CSI-based [3] or AoA-based [4] approaches). To this end, adversaries first identify the mobile user's frames, and then use CSI or AoA information of the frames obtained at multiple eavesdroppers to determine the user's location. We do not consider active adversaries that perform active channel jamming, mobile worm attacks, or other denial-of-service (DoS) attacks, as these attacks cannot be used to compromise user's location privacy.

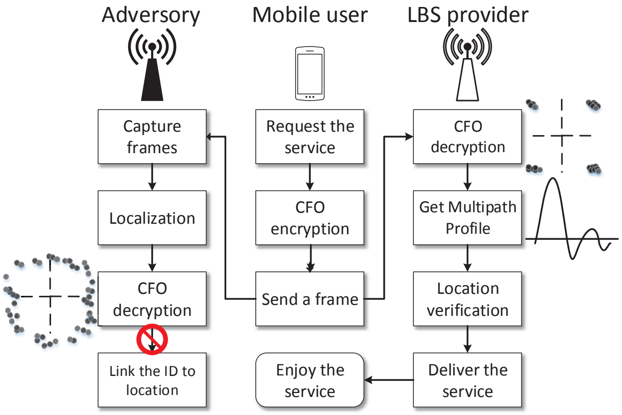


Fig. 2. The flowchart of PriLA.

D. Problem Definition

The target of this paper is to devise an authentication system without compromising mobile users' location privacy. Specifically, the system has the following objectives. i) The system should verify the location of mobile users, and detect faked location reports in real-time, even when there is only one AP deployed within a mobile user's transmission range. ii) The system should preserve mobile users' location privacy from adversaries, who can learn nothing about users' location by eavesdropping. iii) The system should be practical and easy to implement, meaning that we should leverage the information. In particular, the system should only rely on the information that can be obtained in existing Wi-Fi networks, and not require any extra hardware or infrastructures.

III. Design Overview

In this section, we sketch the design of PriLA. PriLA is an authentication system that verifies mobile users' location reports without compromising their location privacy. The crux of PriLA is to facilitate the LBS provider to authenticate users' location by exploiting multipath profiles while preserving mobile users' location privacy by encrypting the location reports using fine-grained PHY information.

The LBS server and a mobile user follow the protocol described in Fig. 2. First, the mobile user requests the service by exchanging handshake frames with the provider's AP. Then, both the mobile user and the provider extracts CSI and CFO information from the preambles to generate a secret key, which is used to encrypt the following frames sent by the user. After receiving the encrypted frames, the provider decrypts the frames using the CSI and CFO information obtained in the handshake frames, and then extracts the user's ID (MAC address) and location information from the frames. Afterwards, the provider uses the CSI obtained from the user's frames to construct a multipath profile, which is compared with multipath profiles stored at the provider for location authentication. After verifying the truthfulness of the reported location, the provider delivers the service to the user.

On the other hand, adversaries eavesdrop all the frames sent by users and the provider, and try to infer the user's location. To perform localization of a certain user, the adversaries need to identify which frame is sent by the desired user. If the adversaries fail to identify the ID of a frame, they cannot obtain specific location of the user. In this case, the adversaries are agnostic of a user's presence or location.

The next two sections elaborate on the above steps, providing the observations and technical details.

IV. CFO Encryption Using Wi-Fi Preamble

A. Exploiting PHY Signatures

Recall that a Wi-Fi receiver always suffers from the CFO when downconverting the signal to baseband due to the hardware impairments. Specifically, CFO not only results in a loss in SNR, but also creates inter carrier interference (ICI), which can severely degrade the receiver's decoding performance. Inspired by this observation, we propose the CFO encryption technique that leverages this inherent feature of CFO to thwart adversaries from obtaining users' locations.

The basic intuition behind CFO encryption is to inject an intended CFO pattern to each frame sent by the user. As the CFO pattern is injected at PHY, both the header and data are protected. Without the knowledge of the CFO pattern, the adversaries are unable to obtain the user's ID or decode the frame.

To make the CFO pattern as a secret key exclusively shared by the user and the provider, we exploit the inherent PHY signatures between a sender and a receiver. First, the CFO between the user and the provider is unique and stable in a short period of time. Due to the impairments of local oscillator, there always exists a CFO between any two devices, and the CFOs of a transmission pair is unique. Although the local oscillator is affected by hardware conditions as well as environmental changes such as temperature, it is stable in a short period of time, which is much larger compared to frame transmission period [19].

Moreover, a wireless channel is reciprocal, and cannot be estimated by a node whose distance with the sender/receiver is larger than half the wavelength of the transmitted signal [20]. Such a property of wireless channel can be leveraged to generate secret CFO patterns that are privately shared between the sender and the receiver.

However, to leverage the above PHY signatures for location privacy preservation, we have the following challenges.

- First, to fully protect a user's location privacy, adversaries should learn nothing about the user's ID or location from the first frame (i.e., handshake frame) that a user sends to the provider. However, existing PHY security techniques [16], [21], [22] are primarily designed to secure the data transmission of subsequent frames after the handshake frame, which leaves the header of the handshake frame exposed to the adversaries. As such, the adversaries can extract the user's MAC address and localize the user based on the CSI estimation. Hence, a special designed protocol is required to protect the handshake frame.
- Second, the CFO pattern encoding should be as robust as possible to ensure effective communications between users and the provider, while at the same time as efficient as possible so that we can generate as many secret bits as possible in each frame to minimize the number of handshakes. However, due to RF impairments and local interference, the estimated CSI values at the sender and the receiver are not exactly the same. Directly extracting bits from CSI (e.g., threshold-based approach [16]) can be very efficient, while it is not robust to local interference or hardware impairments. Thus, a careful investigation into the impact of local interference and hardware impairments should be conducted to devise a robust and efficient coding scheme.

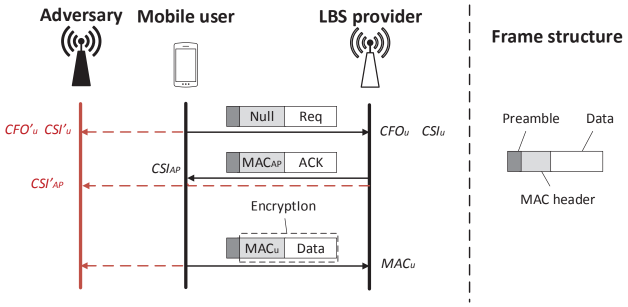


Fig. 3. Secure handshake protocol.

B. Securing The Handshake

As mentioned above, to prevent the adversaries localizing the user at handshake phase, the MAC address of each frame sent by the user should be kept as private information between the user and the provider. One might think of simply removing the MAC address at handshake phase to hide the user's ID. This method, though successfully preventing the adversaries' attacks at handshake phase, is inapplicable to establish a secured link between the user and the provider. As there are multiple users in a Wi-Fi network, the provider cannot match the secret key generated at the handshake phase to the corresponding user, and thus fails to decrypt the subsequent frames sent by the user. To addresses this predicament, we leverage the CFO signature to secure the handshake protocol. As discussed earlier, the CFO of a link is unique and can be obtained using existing Wi-Fi preamble. Such appealing features make CFO ideal for user identification at handshake phase. In particular, the user sends a frame to the provider's AP to request service. As depicted in Fig. 3, the request frame sets the transmitter address as "NULL" to hide the user's MAC address from adversaries. The provider extracts the CFO and CSI information from the preamble, and maintains a mapping $CFO_u \rightarrow CSI_u$ for a user u. Then, the provider returns an

Algorithm 1 Two-Layer Differential Coding (TLDC)

```
Input: CSI vector $[c_1, ..., c_n]$; bucket size $L$
Output: Secret key $\mathbf{k}$
  I. Initialization
  Initialize $\mathbf{k}$ as an empty vector: $\mathbf{k} \leftarrow [\ ]$;
  Compute the differential CSI vector $[d_1, ..., d_{n-1}]$, where $d_i = c_{i+1} - c_i, \forall i = 1, ..., n$;
  Put the differential CSI values into different buckets one by one following the rule: $d_i \rightarrow$ the $\lceil i/L \rceil$th bucket;
  Find the maximal and minimal differential CSI values $d_{max}, d_{min}$;
  Generate four shape pattern vectors $\mathbf{v_{00}} = [\frac{d_{min}}{n}, ..., \frac{id_{min}}{n}, ..., \frac{Ld_{min}}{n}]$, $\mathbf{v_{01}} = [\frac{Ld_{min}}{n}, ..., \frac{id_{min}}{n}, ..., \frac{d_{min}}{n}]$, $\mathbf{v_{10}} = [\frac{d_{max}}{n}, ..., \frac{id_{max}}{n}, ..., \frac{Ld_{min}}{n}]$, $\mathbf{v_{11}} = [\frac{Ld_{max}}{n}, ..., \frac{id_{max}}{n}, ..., \frac{d_{max}}{n}]$;
  II. Key Generation
  for each bucket do
      Compute Fréchet distances between the bucket and the four shape pattern vectors;
      Find the vector $\mathbf{v_i}$ with the smallest distance;
      Add the corresponding bits to $\mathbf{k}$: $\mathbf{k} = [\mathbf{k}, \mathbf{i}]$;
  end for
  Return $\mathbf{k}$;
```

acknowledge frame (ACK) to the user. The user extracts the CSI information from the ACK, and uses the CSI information to encrypt the subsequent frames. The provider first extracts the CFO, and then finds the matched CSI information based on previously logged mappings. Due to reciprocity of a wireless link, the CFO and CSI information obtained by the user and the provider is (theoretically) identical. Therefore, the provider can use the CFO and CSI information obtained at the AP side to decrypt the frame. On the other hand, even if the adversaries can eavesdrop all frames sent by the user and the provider, they cannot acquire the MAC address of the user. Through eavesdropping, the adversaries can estimate the CFO and CSI information of the adversary-user link and the adversary-provider link. However, the adversaries are not able to use such information to decrypt the subsequent frames sent by the user, as they cannot infer the CSI information of the user-provider link based on CSI information of other links. Without the knowledge of a frame's ID, the adversaries cannot infer a user's presence, or link a user to a certain location. Hence, the user's location privacy is fully preserved according to the notion of privacy [23], [24].

C. CFO Encoding

A key technique that ensures the secure handshake phase is to use the channel reciprocity for encryption. Ideally, the estimated CSIs are identical at both ends of a link. However, there are discrepancies caused by hardware imperfection and local interference. In practice, the CSI estimation at one side are normally a shifted, enlarged, or shrinked version of the CSI estimated by the other side. To alleviate the impact of those discrepancies, we should carefully design an encoding scheme, such that (i) the independently generated secret keys at both sides are identical at a rate as high as possible, and (ii) the secret bits extracted from each roundtrip should be as many as possible to minimize the number of roundtrips for key generation. To this end, we leverage the fact that the shifting, enlarging, or shrinking mainly affect the amplitude of CSI rather than its curve shape [21]. To save most of the information stored in the CSI curve, we employ a two-layer differential coding scheme.

Two-layer differential coding (TLDC). The core idea of the proposed coding scheme is to extract the first and second order derivatives of the curve simultaneously, and map the derivatives into secret bits. Both the user and the provider independently executes Algorithm 1 to encode the CSI curve, which can be represented as a vector consisting of CSI values in all subcarriers. The CSI vector is divided into multiple buckets of equal length. Then, we map each bucket to a predefined pattern for encoding. In particular, we define four curve patterns, i.e., descending trend with decreasing gradient (i.e., $\mathbf{v_{00}}$ in Algorithm 1), descending trend with increasing slope (i.e., $\mathbf{v_{01}}$), ascending trend with decreasing slope (i.e., $\mathbf{v_{10}}$), and ascending trend with increasing slope (i.e., $\mathbf{v_{11}}$). Those curve patterns can be determined using the first and second order derivatives. For example, the descending trend can be described by "the first order derivative is negative", and increasing slope can be described by "the second order derivative is positive". The derivative patterns can be easily obtained by transforming the CSI vector $[c_1, ..., c_n]$ into the differential CSI vector $[d_1, ..., d_{n-1}]$, where $d_i = c_{i+1} - c_i, \forall i = 1, ..., n$. Similarly, the predefined patterns can also be transformed to first order derivative space. In the first order derivative space, the ascending/descending trend can be described as positive/negative values, and the increasing/decreasing slop can be described as the ascending/descending trend. Such derivative-based encoding can resist the impact of shifting. To alleviate the zooming effect caused by hardware imperfection, we set the gradient of each predefined pattern according to the CSI variance of its own received signals. Specifically, the gradient of the ascending and descending trends is specified to be $\frac{d_{max}}{n}$ and $\frac{d_{min}}{n}$, respectively, where d_{max}, d_{min} are the maximal and the minimal elements in the differential CSI vector, respectively. As a bucket may not perfectly match one of the predefined patterns, we map each bucket to the most similar pattern, and generate secret bits using the indices of the mapped pattern, as described in Algorithm 1. The similarity between a bucket and a curve pattern is measured using the discrete Fréchet distance [25], which is defined to be the minimum length of a leash required to connect two spots who follow two separate paths.

The security of the secret key is gated by the channel reciprocity and independence properties. According to the channel reciprocity property, the CSI and CFO measured by the user and the AP are theoretically identical [20]. Therefore, the user and the AP can independently generate CFO patterns from CSI and CFO without transmitting them. On the other hand, wireless channels over space larger than half wavelength are independent [20], which guarantees that adversaries can learn little about the channel information between the user

Algorithm 2 CFO Injection

```
Input: Secret key $\mathbf{k}$; inherent CFO $\Delta f$; CFO injection range $[f_l,\ f_u]$; number of symbols in the frame $S$
Output: Encrypted frame;
Generate a vector of CFOs of length $\lfloor\frac{2n}{ML}\rfloor$ by multiply each $M$ bits of $\mathbf{k}$ with $\Delta f$;
Hash each generated CFO to $[f_l,\ f_u]$;
for $i \leftarrow 1$ to $S$ do
    Compute the index $j$ of CFO used for injection: $j = i \mod \lfloor\frac{2n}{ML}\rfloor$;
    Inject the $j$th CFO value to the $i$th symbol;
end for
```

and the AP by eavesdropping their frames. Specifically, we assume that adversaries are more than half-wavelength (i.e., about 6cm for 2.4GHz Wi-Fi signals) away from the user and the AP. Therefore, adversaries can only obtain their own channel information from the preambles of intercepted frames. This information is independent of the channel information of the user-AP link, and thus provides little information about the secret keys.

CFO Injection. After generating a secret key using the CSI curve, we leverage the secret key $\mathbf{k}$ to encode a CFO pattern for encryption. Algorithm 2 summarizes the CFO injection process. The CFO pattern is determined by the multiplication results of the inherent CFO Δf and the private key $\mathbf{k}$. Concretely, we first multiply each M bits of $\mathbf{k}$ with Δf to generate $\lfloor\frac{2n}{ML}\rfloor$ CFOs. Then, we hash each generated CFO to a predefined CFO injection range $[f_l,\ f_u]$. As such, we derive a sequence containing $\lfloor\frac{2n}{ML}\rfloor$ hashed CFOs. Finally, we inject the jth CFO into the ith symbol, where $j = i \mod \lfloor\frac{2n}{ML}\rfloor$. The mobile user will repeat these three processes until the end of the frame. Since $\mathbf{k}$ is the private message merely shared between the communication pair, the adversaries have no way to guess the generated CFO pattern.

To realize CFO injection in Wi-Fi transceivers, there remains several design challenges. The first issue is how to choose an appropriate CFO injection range. Too large CFO would cause the received signal significantly shifting out of sampling frequency range at receiver, making the shifted frame impossible to recover, whereas too small CFO can be easily compensated by the adversary due to the redundancy in the PHY coding and modulation. To investigate how much CFO should be injected for encryption, we conduct several experiments by injecting different CFOs normalized to subcarrier spacing. In the experiment, we use three USRP nodes, one acting as a mobile user, continuously sending 1000-Byte frames injected by one fixed normalized CFO, and the other two nodes acting as the provider and an adversary, respectively. The CFO injection begins after preamble. Fig. 4 depicts the bit error rate (BER) performance for both the LBS provider and the adversary under various normalized CFO injections. The results show that the BER suffered by the LBS provider decreases along with the decline of normalized CFO injection. The BER suffered by the adversary also experiences slight downward trend but remains very high both for PSK (around 20%) and QAM (around 30%) modulation as the normalized CFO fraction declines to 1/100. Under such a high BER, the frame cannot be decoded. In addition, the BER performance of the LBS provider turns back to normal level when normalized CFO fractions are below 1/20 for PSK and 1/30 for QAM. Hence, we choose the CFO injection range with upper-bond f_u of 1/30 as normalized fraction and lower-bound f_l of 1/100 as normalized fraction.

Another practical issue is pilot subcarriers. In IEEE 802.11n standard, four known data subcarriers, referred to as pilot, are included among all data symbols. The pilots are used to track the carrier phase rotation caused by inherent CFO. To eliminate the impact of injected CFO on pilots, we compensate the pilot phase rotation in pilot subcarriers caused by the CFO injection. As the CFO injection pattern is generated beforehand, the sender can rotate four pilots in each symbol before CFO injection in the inverse direction of same angle caused by the injected CFO. As such, after the CFO is injected, the pilots will shift back to the original position like not suffering from phase rotation. By such preprocessing, the pilots at receiver side are not able to track the phase rotation caused by the injected CFO but are still able to track those originally caused by the residual CFO. Such a preprocessing only incurs little overhead by performing one fast Fourier transform (FFT) and one convolution calculations.

D. Enhancing CFO Encryption Using Existing Schemes

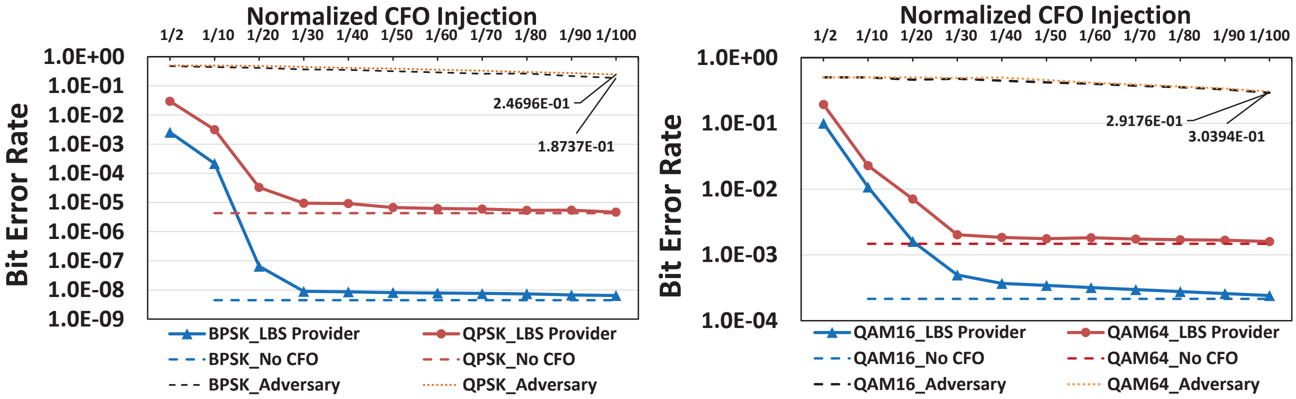
Algorithm 2 provides physical layer protection based on the Wi-Fi inherent baseband signal processing blocks with minimal overhead and computational cost. All encoding and decoding processes are executed based on the inherent channel estimation and CFO estimation blocks in Wi-Fi PHY. To enhance the security of our system, we can incorporate our system with existing secret key based encryption schemes. In particular, users and the AP extract secret keys from CSI and CFO in the physical layer, and then utilize the secret keys to establish secure protocols using existing encryption schemes. Note that these encryption schemes can operate standalone or alongside with the CFO injection to protect users' location information. Different encryption schemes can be built on top of our system to fit the complexity constraints and security requirements.

V. Multipath-Based Location Authentication

A. Design Rationale

One might think using localization techniques to verify the location of a user. However, this is infeasible in practice, as the scenarios of adopting user-reported location are when the provider or infrastructure is unable to identify the user's location by themselves. This is because existing localization techniques either require multi-AP cooperation or modifications of existing infrastructure. To solve this predicament, the target of the proposed location authentication is to verify the location of a user based on the information that is already available in existing Wi-Fi infrastructure.

Our observation is that the signals emitted by nearby users propagate along closer paths in indoor environments where there are multiple reflectors and scatters. Fig. 5 depicts two sets



(a) PSK

(b) QAM

Fig. 4. BER performance under a range of fixed normalized CFO injection

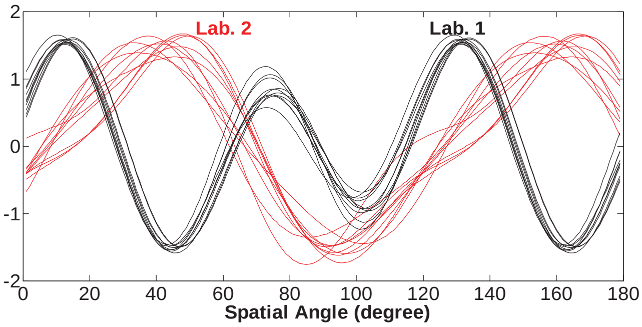


Fig. 5. Measurement of multipath profiles in lab.1 and lab.2

of normalized multipath profiles from two labs measured by one AP. Different lines denote signals from different reflected paths. The red lines are the profiles of co-located users (within one meter) in Lab1 while the black lines are the profiles of co-located users in Lab2. The results report that only the profiles of co-located users closely match, while the profiles of users in different labs are irrelevant. Moreover, the multipath profile is hard to forge as it is determined by the environment's physical layout. With these two merits, the LBS provider can determine which areas the mobile user belongs to, while such coarse-grain information is enough to help authenticate but not comprises user's location privacy. The remaining questions are how to obtain multipath profiles and how to exploit these information to conduct authentication.

B. Multipath Profile Acquisition

Antenna array can be used to construct the multipath profile based on arrival angle of received signal [10]. The basic idea is to measure the power of different paths coming different directions by steering antenna beam across 180°. Let θ be the beam steering angle, r_k be the signal captured by the k^{th} antenna from the array, $k = 0, ..., K-1$. λ denotes the wavelength and D represents the distance between two antennas. The power of received signal $B(\theta)$ in θ direction can be calculated as follows

$$B(\theta) = \mid \sum_{k=0}^{K-1} w(k,\theta) * r_k \mid^2, w(k,\theta) = e^{-j2\pi kD\cos\theta}, \quad (4)$$

where $w(k,\theta)$ is the complex weight that helps to compensate the signal phase difference between the first and k^{th} antenna. After phase alignment, the beam from all antenna only focuses on θ direction and filters out signals from other direction. As the newly manufactured Wi-Fi APs are equipped with multiple antennas to support multiple-input and multiple-output (MIMO) in IEEE 802.11n/ac, we claim that the multipath profile is available in existing Wi-Fi infrastructures.

C. Multipath Profile Matching

After acquiring the multiple profile of a user, the LBS provider needs to compare it with the existing multipath profiles of users who have already been authenticated. However, even in the same zone, two points only apart from few meters will not hold the exactly same profiles due to the channel noise and the spatial gap. Hence, simple correlation between two profiles does not work. To address this issue, we observe that although two profiles may experience scale variation and misalignment, the underlying shapes remain stable. We leverage Dynamic Time Warping (DTW) [26] to cope with the impact of local shifts. Note that DTW is originally applied in speech recognition, which tries to eliminate the influence of timing misalignment. Given two time series, the alignment process is to map any two points of two series. Likewise, in our design, the core idea is trying to extract the similarity between two misaligned profiles. DTW tries to find a path that minimizes the overall cost of the continuous mapping pairs. The cost of each mapping pair is defined to be the Euclidean distance between two points. To find the shortest path between two multipath profiles, DTW looks for a path starting from the bottom left cell to the top right cell, and computes intuitive distance between two curves. The cost of the path between two series is normalized by the length of the path. If the similarity is still very low after DTW calculation, we treat these two profiles coming from users at different locations.

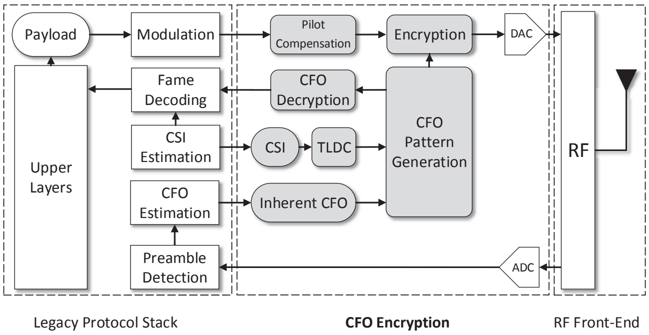


Fig. 6. PriLA Transceiver Implementation.

D. Countermeasures For User Collusion

The above discussion focuses on the case of a single dishonest user. Now we consider the threat of user collusion, that is, multiple dishonest users collaboratively report bogus locations. In particular, multiple co-located users may collude to report the same bogus location. As such, the provider may consider that their location reports are consistent with their multipath profiles. In line with a common practice in collusion-resistance protocols [9], [27], [28], we make an assumption that the number of dishonest or collusive users is no more than a fraction of the total number of users, which is referred to as the threshold. As such, the AP can leverage the non-collusive users to verify a user's location by comparing their multipath profiles. Specifically, when a user reports its location loc_u to the provider, the provider compares the multipath profiles of the user with that of multiple users whose reported location is within a certain range from loc_u. The number of users in the comparisons is set to exceed the collusion threshold. If their multipath profiles are similar enough, the user location is proved to be true. Otherwise, the user fails to pass the location authentication.

VI. System Implementation

PriLA can be realized in the existing OFDM PHY with no change in hardware. We have implemented the prototype of CFO encryption atop the OFDM structure of GNURadio/USRP platform. We implement the entire CFO encryption design specified in Section IV directly in the USRP Hardware Drive (UHD). All the PHY parameters conform to PHY layer convergence procedure (PLCP) format of IEEE 802.11. We use DELL Optiplex 9010 with Intel i3 Dual-core processor and 4GB memory for the testbed setup. Nodes in our experiments are equipped with RFX2450 daughterboards as RF frontend, which is configured to operate in the 2.4-2.5GHz range. The frame synchronization and channel equalization algorithms are implemented according to IEEE 802.11a/n. Due to hardware limitations of USRP, we turn to Intel 5300 NIC for multipath profile construction.

Fig. 6 illustrates the implementation details of the transceiver architecture. In encryption process, the CSI and CFO information extracted from the Wi-Fi preamble is leveraged to generate the CFO pattern according to the algorithm described in Section IV. In particular, we add the TLDC block for CSI coding, the pilot compensation block, and CFO pattern generation block. Finally, the CFO encryption is performed in time domain after the inverse fast Fourier transform (IFFT). The decryption process is implemented by reversing the encryption block.

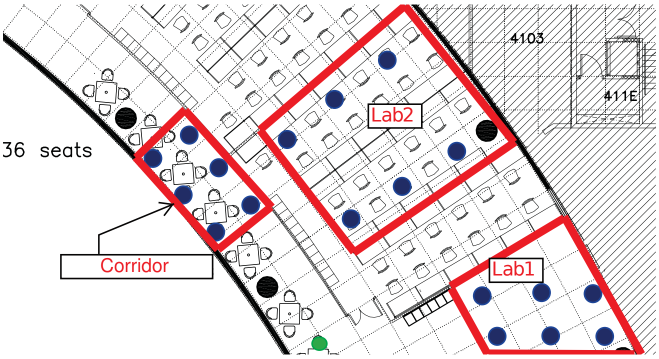


Fig. 7. Testbed layout with three zones, lab1, lab2 and corridor. The green spot is the position where the LBS provider is placed. The blues spots are the position where the mobile users are placed.

The communication overhead of our system is caused by two extra transmissions involved in the secure handshake protocol. It is worth noting that such an overhead is also necessary in many other secret sharing protocols. The computational overhead of our system is contributed by CFO encryption and multipath based authentication, which require $O(S+n)$ and $O(n^2)$, respectively, where n ($n = 52$ in IEEE 802.11n) is the length of the CSI vector, and S the number of symbols in the frame.

VII. Experimental Evaluation

We evaluate PriLA in this section. We first conduct the CFO encryption evaluation in Section VII-A using USRP implementation. Then, in Section VII-B, we evaluate the multipath-based location authentication using Intel 5300 NICs.

The layout of the experimental environments is sketched in Fig. 7, where Lab1 has 4 desks and Lab2 consists of 36 cubics. We conduct experiments on different days during work hours. There were 4 and 36 students in Lab1 and Lab2, respectively, and most of them sat in front of their desks, while only a few students were walking during experiments. Such movements cause certain levels of mismatch in channel reciprocity, but the impact on the performance of PriLA is small, as shown in our results in the following subsections.

A. Performance of CFO Encryption

We evaluate the performance of secure handshake protocol using three USRP2 nodes. One acts as a mobile user. Unless otherwise stated, the other two are both placed 5 meters away from the mobile users, acting as the LBS provider and the adversary, respectively. The provider and the user are implemented according to Fig. 6, while the adversary merely acts as a passive eavesdropper that aims to decode the user's frames for localization purpose.

Evaluation metrics. We use three metrics, i.e., *mismatch rate*, *entropy*, and *leakage*, to evaluate the performance of CFO

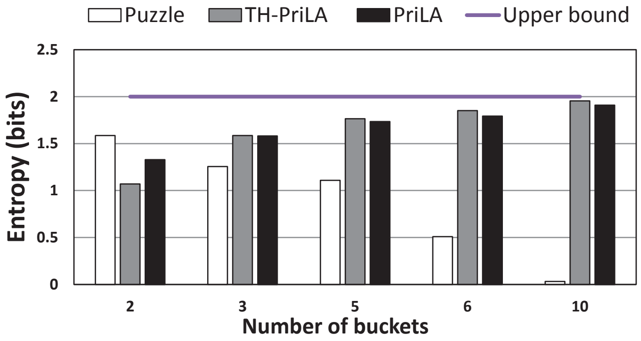


Fig. 8. **Entropy per bucket under different numbers of buckets.**

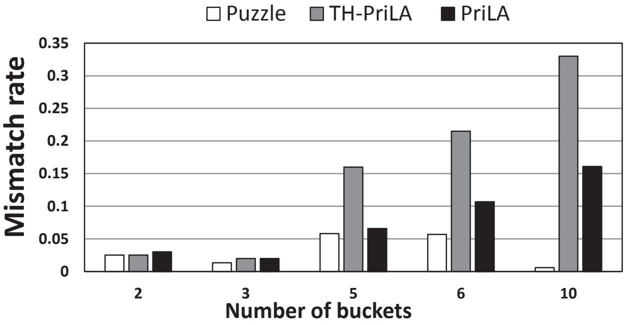


Fig. 9. Mismatch rate under different numbers of buckets.

encryption. Mismatch rate is defined to be ratio of mismatched bits between the secret keys independently generated by the user and the provider. Mismatch rate measures the robustness of the encryption scheme.

Entropy is the average amount of information contained in a message. For a random variable X, its entropy is defined to be $H(X) = -\sum_{i=1}^{n} \Pr[x_i] \log_2 \Pr[x_i]$, where $\Pr[x_i]$ is the probability of X's possible value x_i. Here, we use entropy to measure the uncertainty of the generated secret bits. In our evaluation, we compute the entropy of the curve patterns used for encryption. The probability of each curve pattern is computed by counting the its frequency in repeated experiments. The secret bits with higher entropy contain more information, and are harder for the adversary to infer.

Leakage measures the amount of information learned by the adversary. In our evaluation, leakage is defined to be the ratio of matched bits between the sender (the user or provider) and the adversary. An encryption scheme with lower leakage is more secure.

Baselines. To evaluate the performance gain of the proposed CFO encryption, we compare it with two baselines. The first baseline is Puzzle [21], which the only-known secret key generation scheme that extracts bits from the curve shape of a channel's frequency response. *Puzzle* generates bits by mapping each segment of the power spectral density to ascending, descending, or steady shapes. For fair comparison, Puzzle is modified to use the same secure handshake protocol as used in PriLA. Another baseline named *TH-PriLA* adopts all the same techniques used in PriLA, except that TH-PriLA uses threshold-based approach to map each bucket to one of the four predefined shapes.

Fig. 8 depicts the influence of the number of buckets on the entropies of different schemes. The entropy of Puzzle diminishes when the number of buckets increase. This conforms to the fact that as the bucket length is smaller, the shape of a bucket is more likely to be steady. As such, the probability of being steady is higher, which undermines the uncertainty of generated bits. Fortunately, both TH-PriLA and PriLA overcome such a constraint by adopting TLDC, which exploits the first and second order derivatives for shape encoding. As shown in Fig. 8, the entropy of both TH-PriLA and PriLA steadily grow as the number of buckets increases up to 10. Theoretically, the upper bounds TH-PriLA's and PriLA's entropies are higher than that of Puzzle. Each bucket in TH-PriLA and PriLA is mapped to one of four shapes, while Puzzle maps each bucket to one of three shapes. Note that entropy is maximized when the probabilities of all possible values are identical, in which case the entropies of TH-PriLA and PriLA are 2 bits and the entropy of Puzzle is only 1.58 bits.

To verify the robustness of the CFO encryption, we measure the mismatch rate of different schemes in Fig. 9. PriLA achieves comparable mismatch rate with Puzzle when the number of buckets is no more than 5, while the mismatch rate of PriLA is significantly higher than that of Puzzle when the number of buckets grows to 10. The reason is that when the number of buckets is large, the entropy of Puzzle is quit small, implying low uncertainty in the bits generated by Puzzle. Hence, the security level of Puzzle in the case of large number of buckets is low. PriLA and TH-PriLA, on the other hand, maintain high security level with large number of buckets but is less reliable. Thus, the number of buckets should be carefully selected to strike a balance between entropy and mismatch rate. In our design, we choose 5 buckets for 20MHz channels. In this setting, PriLA achieves $1.54\times$ entropy compared to Puzzle, while only incurring 16.7% mismatch rate than Puzzle. As a result, PriLA can generate the effective secret of $5 \times 1.7 \times (1 - 6\%) = 8.68$ bits per frame, which is 65% higher than Puzzle, which generates $5 \times 1.1 \times (1 - 5\%) = 5.25$ bits per frame. Moreover, PriLA outperforms TH-PriLA in mismatch rate while enjoying comparable entropy, which implies that TLDC is more robust than the threshold-based approach.

To validate the security level provided by PriLA, we conduct experiments where the user and the provider are placed at a fixed distant $(5m)$ while the adversary is placed at various distances apart from the sender. The number of buckets is fixed to be 5. As shown in Fig. 10, more information is leaked to the adversary with smaller distance. This is quit intuitive as nearer adversary shares more similar multipath profiles and channel responses. Besides, both PriLA and TH-PriLA leak less information compared to Puzzle in all cases demonstrated. On average, PriLA leaks merely 45.7% information compared to Puzzle. It is easy to explain as the bits generated by both PriLA and TH-PriLA is more evenly distributed than that of Puzzle, as learned from Fig. 8. It is worth noting that in

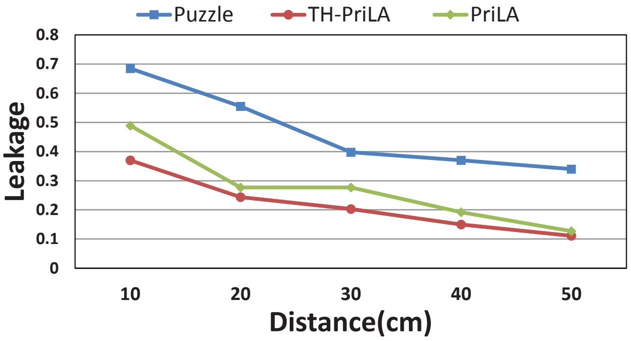


Fig. 10. Information leakage to the adversary with different distances.

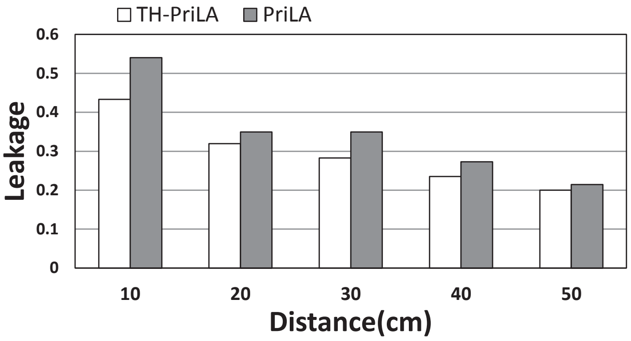


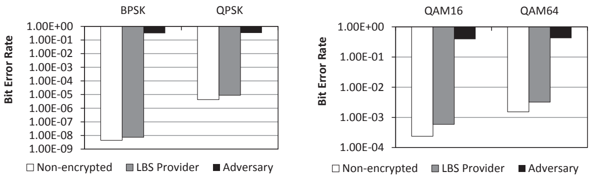
Fig. 11. Overall information leakage to the adversary with different distances.

practice the distance between the adversary and the sender is very likely to be much larger than $50cm$, in which case the amount of information leakage is even smaller. Note that TH-PriLA achieves sightly lower information leakage than PriLA. This is because the entropy of TH-PriLA is higher, which, however, leads to mismatch rate almost twice as high as that of PriLA.

Fig. 11 evaluates the overall information leakage, which is defined to be the ratio of mismatched bits when the adversary infers bits in the intercepted frame based on its observations. The trend is consistent with Fig. 10 that less information is leaked to adversaries with larger distances to the sender. The leakage ratio diminishes when the user-adversary distance increases, and drops to 0.2 at the distance of $50cm$. It is worthwhile noting that when the leakage ratio is less thant 0.5, the matched bits are caused random guess [21].

We further evaluate the BER performance of PriLA after the secure handshake phase. In this experiment, the secret key is already obtained by the user and the provider, who decodes the frames using the secret key. The user continuously sends CFO-encrypted 1000-Byte frames back-to-back to the provider. To demonstrate that the CFO encryption incurs neglectable impact on decoding performance, we also measure the BER of the frames without CFO injection and treat it as the normal decoding benchmark.

Fig. 12 reveals that the frame decoding performance of the provider is very closed to that of the benchmark, which implies that the CFO encryption has little impact on the decoding performance. The slight difference in the decoding performance is caused by CFO mismatch measured by the user and the provider. As discussed earlier, the CFO mismatch results from hardware impairments or local interferences. Meanwhile, the BER performance of the adversary is significantly poorer, reaching to a level (more than 0.3) that is not unacceptable for frame decoding. To sum up, we claim that CFO encryption can prevent the attack from the adversary while not comprising frame decoding performance of the provider.



(a) PSK (b) QAM

Fig. 12. BER performance of the provider and the adversary in PriLA.

TABLE I
THE ACCURACY OF MULTIPATH-BASED AUTHENTICATION IN THREE ZONES

Zone	Lab1	Lab2	Corrider
Lab.1	91.7%	6.2%	2.1%
Lab.2	7.7%	83.4%	8.9%
Corrider	7.0%	17.2%	75.8%

B. Performance of Multipath-Based Location Authentication

To validate the feasibility of multipath profile based location authentication, the key metric is the accuracy that the LBS provider succeed to identify which zone the mobile user belongs to. Hence, we conduct trace-driven experiment in a real-world environment. As shown in Fig. 7, we divide the test floor into three zones, two labs and one corridor. The LBS provider is emulated by one fixed laptop, which is assembled with a three antennas Intel 5300 NIC. Mobile users are emulated by one TP_Link router, sharing a 2.4GHz channel with 20MHz bandwidth. The fixed laptop continuously pings to the TP_LINK router deployed in each zone. We repeat this measurement by placing the router at six different position in each zone.

After trace collection, we process them offline. Multipath profiles can be constructed based on each CSI feedback frame received by three antennas. We divide the profiles data in half, one as the users that need to be authenticated, the other as already-authenticated users.

We first assume that there is no user collusion and compare a user's multipath profile with three already-authenticated multipath profiles, each of which locates in one zone. Table I shows the matching accuracy in different zones. the results report that the matching accuracy is relatively higher in Lab1 whereas worse in corridor. One reason behind is that the physical layout is much consistent in Lab1 where all mobile users experience similar multipath effect. However, corridor is a free space environment where reflection is much less. The other reason is that we only use three antennas to construct the multipath profile, which offer limited multipath features

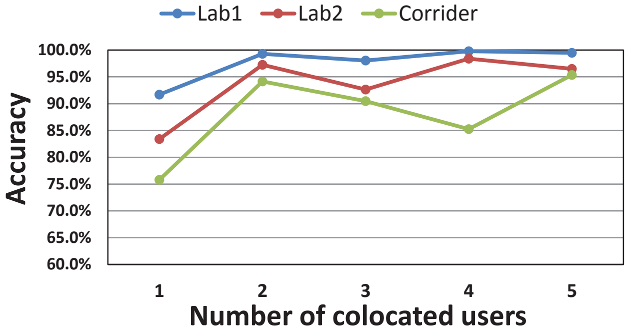


Fig. 13. The accuracy of multipath-based authentication under user collusion.

like the number of peak and valley. We believe that the performance will be better if the more antennas are equipped.

Then, we evaluate the authentication performance under user collusion in Fig. 13. We set the collusion threshold to be 50%. PriLA authenticates a user's location only when its multipath profile matches with the multipath profiles of over 50% co-located users. The results show that the authentication performance is still high under different numbers of co-located users. On aerage, the matching accuracy achieved by PriLA is 93.2%. Fig. 13 also implies that the authentication accuracy has an ascending trend as the number of co-located users increases. This is because with more co-located users, PriLA is more resistant to local fluctuations in multipath profiles.

VIII. Related Work

Several recent research works are presented to enable location authentication using wireless infrastructures or signals. Lenders et al. [5] utilize dedicated measuring hardware to generate unforgeable location proofs for user-generated content. Saroiu et al. [6] present a set of applications that require location authentication to enable their core functionality, and leverage the physical proximity between a transmission pair to verify a user's location. Talasila et al. [7] leverage immediate neighbor knowledge to verify the location claim from mobile user. Brassil et al. [8] try to detect the location of mobile user through monitoring traffic signatures of voice call. Location-based query authentication is studied in [29], which develops three novel index structures to allow the user and the provider to jointly compute a digest function without leaking the query results. These studies do not consider users location privacy. A fairly recent work [9] propose a location proof update system with privacy protection. This system leverages co-located Bluetooth mobile devices to generate location proofs and periodically change users' pseudonyms to protect their location privacy. Different from [9], PriLA extracts PHY signatures for privacy protection and does not require external device assistance.

PriLA is also related to a wide range of work in location privacy in wireless networks [13]–[15], [30]–[36]. Jiang et al. [32] design a scheme to prevent privacy leakage by frequently changing several types of sensitive information like MAC address and signal strength. Li et al. [15] leverage homomorphic encryption to allow the provider answer encrypted queries without knowing the location information. Similarly, homomorphic encryption is also applied in [33] to enable Wi-Fi fingerprint-based localization without leaking users' locations. Antenna pattern synthesis is leveraged in [34] to preserve the transmitter's true location by modifying the RSS information obtained by adversaries. Zhao et al. [35] study the privacy issues in users' check-in records in social networks, and propose a lightweight framework with a novel index structure to allow private friends searching in location-based social networks. Spatial cloaking or anonymization is adopted in [14], [30], [31] to preserve user's location privacy by reporting coarse-grained location information. Gruteser et al. [30] dynamically adjust the temporal or spatial resolution of users' locations to meet privacy requirements. A spatial histogram approach is developed in [14] to estimate statistical distribution of aggregated location information while preserving the individuals' locations. An incentive mechanism is devised in [31] to motivate users to participate in anonymization protocols. Tao et al. [36] investigate the privacy issue when adversaries are capable of inferring a user's location using localization techniques. This work motivates the adoption of a similar threat model in PriLA, and inspires us to prevent adversaries from acquiring users' reported location as well as inferring users' location through localization. However, these works only focus on location privacy, while PriLA aims to enable privacy-preserving location authentication.

PHY information has been exploited to facilitate the security and privacy mechanisms in wireless networks. The CFO encryption technique proposed in this paper follows on the heels of several recent efforts [16], [21], [22], [37] that use channel reciprocity for encryption. Premnath et al. [16] study the received signal strength (RSS) variations on the wireless channel between the two devices, and propose an environment adaptive secret key generation scheme using the temporal variations. Liu et al. [22] take one step further by enabling secure group communications using RSS-generated secret keys. To boost the number of secret bits generated by each frame, CSI-based secret key generation is first proposed in [37]. Different from these proposals, Qiao et al. [21] extract secret bits from the shape of frames' power spectral density to provide more robust encoding. PriLA differs from these proposals in two aspects. First, these proposals focus on data encryption after secret key extraction, while PriLA ensures secure handshake even when the secret key has not been generated. Second, PriLA exploits more fine-grained shape information in CSI curve to develop a coding scheme with higher entropy. Other PHY information has also been investigated to enable different functionalities in wireless networks. AoA information is used to mitigate Wi-Fi spoofing attacks in [38]. Multipath profiles are leveraged to assist RFID positioning in non line-of-sight environments [10]. Differently, PriLA leverages multipath profiles to facilitate privacy-preserving location authentication in Wi-Fi networks.

IX. Conclusion

This paper presents PriLA, a privacy-preserving location authentication framework in Wi-Fi networks. PriLA extracts the inherent CFO and CSI signatures from legacy Wi-Fi preambles to verify users' locations without compromising their privacy. We have prototyped PriLA to demonstrate its feasibility and merits. We hope that the design of PriLA can contribute to the wireless community by facilitating privacy-preserving location authentication without the assistance from extra devices or external networks.

The PHY signatures used in PriLA can be easily obtained from legacy Wi-Fi preambles. PriLA is a clean-slate design that is transparent to upper layer protocols, and can be integrated into OFDM-based Wi-Fi devices without hardware modifications. With those features, we believe that PriLA can be easily applied to existing LBS systems with a slight upgrade.

ACKNOWLEDGEMENT

The research was supported in part by grants from 973 project 2013CB329006, China NSFC under Grant 61502114, China NSFC under Grant 61173156, RGC under the contracts CERG 622613, 16212714, HKUST6/CRF/12R, and M-HKUST609/13, as well as the grant from Huawei-HKUST joint lab.

REFERENCES

[1] Z. Zhang, L. Zhou, and X. Zhao, "On the validity of geosocial mobility traces," in *Proc. ACM Hotnets*, 2013, pp. 1–7.

[2] S. Wicker, "The loss of location privacy in the cellular age," *Commun. ACM*, vol. 55, no. 8, pp. 60–68, 2012.

[3] K. Wu, J. Xiao, Y. Yi, D. Chen, X. Luo, and L. M. Ni, "Csi-based indoor localization," *IEEE Trans. Parallel Distrib. Syst.*, vol. 24, no. 7, pp. 1300–1309, 2013.

[4] J. Xiong and K. Jamieson, "Arraytrack: A fine-grained indoor location system," in *USENIX NSDI*, 2013, pp. 71–84.

[5] V. Lenders, E. Koukoumidis, P. Zhang, and M. Martonosi, "Location-based trust for mobile user-generated content: applications, challenges and implementations," in *Proc. ACM HotMobile*, 2008, pp. 60–64.

[6] S. Saroiu and A. Wolman, "Enabling new mobile applications with location proofs," in *Proc. ACM HotMobile*, 2009, p. 3.

[7] M. Talasila, R. Curtmola, and C. Borcea, "Link: Location verification through immediate neighbors knowledge," in *Mobile and Ubiquitous Systems: Computing, Networking, and Services*, 2012, pp. 210–223.

[8] J. Brassil, P. Manadhata, and R. Netravali, "Traffic signature-based mobile device location authentication," vol. 13, no. 9, pp. 2156–2169, 2013.

[9] Z. Zhu and G. Cao, "Toward privacy preserving and collusion resistance in a location proof updating system," *IEEE Trans. Mobile Comput.*, vol. 12, no. 1, pp. 51–64, 2013.

[10] J. Wang and D. Katabi, "Dude, where's my card?: RFID positioning that works with multipath and non-line of sight," in *Proc. ACM SIGCOMM*, 2013, pp. 51–62.

[11] USRP N210. https://www.ettus.com/product/details/UN210-KIT.

[12] Intel Ultimate N Wi-Fi Link 5300: Product Brief. http://www.intel.com/content/www/us/en/wireless-products/ultimate-n-wifi-link-5300-brief.html.

[13] K. G. Shin, X. Ju, Z. Chen, and X. Hu, "Privacy protection for users of location-based services," *IEEE Wireless Commun.*, vol. 19, no. 1, pp. 30–39, 2012.

[14] C.-Y. Chow, M. F. Mokbel, and T. He, "A privacy-preserving location monitoring system for wireless sensor networks," *IEEE Trans. Mobile Comput.*, vol. 10, no. 1, pp. 94–107, 2011.

[15] X.-Y. Li and T. Jung, "Search me if you can: privacy-preserving location query service," in *IEEE INFOCOM*, 2013, pp. 2760–2768.

[16] S. N. Premnath, S. Jana, J. Croft, P. L. Gowda, M. Clark, S. K. Kasera, N. Patwari, and S. V. Krishnamurthy, "Secret key extraction from wireless signal strength in real environments," *IEEE Trans. Mobile Comput.*, vol. 12, no. 5, pp. 917–930, 2013.

[17] J. Terry and J. Heiskala, *OFDM Wireless LANs: A theoretical and practical guide*. Sams Publishing, 2002.

[18] "Part 11: Wireless lan medium access control (mac)and physical layer (phy) specifications amendment 5: Enhancements for higher throughput," *IEEE Std 802.11n-2009*, pp. 1–565, 2009.

[19] J. Fang, K. Tan, Y. Zhang, S. Chen, L. Shi, J. Zhang, Y. Zhang, and Z. Tan, "Fine-grained channel access in wireless lan," *IEEE/ACM Trans. Netw.*, vol. 21, no. 3, pp. 772–787, 2013.

[20] T. S. Rappaport *et al.*, *Wireless communications: principles and practice*. Prentice Hall PTR New Jersey, 1996, vol. 2.

[21] Y. Qiao, K. Srinivasan, and A. Arora, "Puzzle: A shape-based secret sharing approach by exploiting channel reciprocity in frequency domain," in *USENIX NSDI*, 2014, pp. 1–14.

[22] H. Liu, J. Yang, Y. Wang, Y. Chen, and C. E. Koksal, "Group secret key generation via received signal strength: Protocols, achievable rates, and implementation," *IEEE Trans. Mobile Comput.*, pp. 1–14, 2014.

[23] L. Sweeney, "k-anonymity: A model for protecting privacy," *International Journal of Uncertainty Fuzziness and Knowledge Based Systems*, pp. 557–570, 2002.

[24] C. Dwork, F. McSherry, K. Nissim, and A. Smith, "Calibrating noise to sensitivity in private data analysis," *Theory Crypt.*, pp. 265–284, 2006.

[25] T. U. Wien, T. Eiter, T. Eiter, H. Mannila, and H. Mannila, "Computing discrete fréchet distance," Tech. Rep., 1994.

[26] S. Salvador and P. Chan, "Toward accurate dynamic time warping in linear time and space," *Intel. Data Anal.*, vol. 11, no. 5, pp. 561–580, 2007.

[27] S. Goldwasser, "Multi party computations: past and present," in *ACM Proc. Symp. Princ. Distrib. Comput.*, 1997, pp. 1–6.

[28] K. Suzuki and M. Yokoo, "Secure combinatorial auctions by dynamic programming with polynomial secret sharing," in *SpringerFinancial Cryptography*, 2003, pp. 44–56.

[29] H. Hu, J. Xu, Q. Chen, and Z. Yang, "Authenticating location-based services without compromising location privacy," in *Proc. ACM SIGMOD*, 2012, pp. 301–312.

[30] M. Gruteser and D. Grunwald, "Anonymous usage of location-based services through spatial and temporal cloaking," in *Proc. ACM MobiSys*, 2003, pp. 31–42.

[31] D. Yang, F. Xi, and G. Xue, "Truthful incentive mechanisms for k-anonymity location privacy," in *Proc. IEEE INFOCOM*, 2013, pp. 3094–3102.

[32] T. Jiang, H. J. Wang, and Y.-C. Hu, "Preserving location privacy in wireless lans," in *Proc. ACM MobiSys*, 2007, pp. 246–257.

[33] H. Li, L. Sun, H. Zhu, X. Lu, and X. Cheng, "Achieving privacy preservation in WiFi fingerprint-based localization," in *Proc. IEEE INFOCOM*, 2014, pp. 2337–2345.

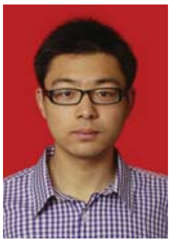
[34] T. Wang and Y. Yang, "Location privacy protection from rss localization system using antenna pattern synthesis," in *IEEE Proc. INFOCOM*, 2011, pp. 2408–2416.

[35] X. Zhao, L. Li, and G. Xue, "Checking in without worries: Location privacy in location based social networks," in *IEEE INFOCOM*, 2013, pp. 3003–3011.

[36] T. Shu, Y. Chen, J. Yang, and A. Williams, "Multi-lateral privacy-preserving localization in pervasive environments," in *Proc. IEEE INFOCOM*, 2014, pp. 2319–2327.

[37] H. Liu, Y. Wang, J. Yang, and Y. Chen, "Fast and practical secret key extraction by exploiting channel response," in *IEEE Proc. INFOCOM*, 2013, pp. 3048–3056.

[38] J. Xiong and K. Jamieson, "Securearray: improving WiFi security with fine-grained physical-layer information," in *Proc. ACM MobiCom*, 2013, pp. 441–452.



Wei Wang (S'10) is currently a Research Assistant Professor in Fok Ying Tung Graduate School, Hong Kong University of Science and Technology (HKUST). He received his Ph.D. degree in Department of Computer Science and Engineering from HKUST. Before he joined HKUST, he received his bachelor degree in Electronics and Information Engineering from Huazhong University of Science and Technology, Hubei, China, in June 2010. His research interests include privacy preservation and fault management in wireless networks.

Yingjie Chen received his M.Phil. degree of computer science department from Hong Kong University of Science and Technology in 2012. He is currently a reseach assistant in Hong Kong University of Science and Technology. His research interests include PHY and MAC layer design in Wi-Fi network, and mobile computing.

Qian Zhang (M'00-SM'04-F'12) joined Hong Kong University of Science and Technology in Sept. 2005 where she is a full Professor in the Department of Computer Science and Engineering. Before that, she was in Microsoft Research Asia, Beijing, from July 1999, where she was the research manager of the Wireless and Networking Group. She is a Fellow of IEEE for "contribution to the mobility and spectrum management of wireless networks and mobile communications". Dr. Zhang received the B.S., M.S., and Ph.D. degrees from Wuhan University, China, in 1994, 1996, and 1999, respectively, all in computer science.