Privacy-Preserving Location Authentication in WiFi with Fine-Grained Physical Layer Information

Yingjie Chen[†], Wei Wang[*‡], Qian Zhang[‡]
[†]Fok Ying Tung Graduate School,
[‡]Department of Computer Science and Engineering,
Hong Kong University of Science and Technology
Email: {ychenax, gswwang, qianzh}@ust.hk
[*]Corresponding Author

***Abstract*—The surging deployment of WiFi hotspots in public places drives the blossoming of location-based services (LBSs) available. A recent measurement reveals that a large portion of the reported locations are either forged or superfluous, which calls attention to location authentication. However, existing authentication approaches breach user's location privacy, which is of wide concern of both individuals and governments. In this paper, we propose PriLA, a privacy-preserving location authentication protocol that facilitates location authentication without compromising user's location privacy in WiFi networks. PriLA exploits physical layer information, namely carrier frequency offset (CFO) and multipath profile, from user's frames. In particular, PriLA leverages CFO to secure wireless transmission between the mobile user and the access point (AP), and meanwhile authenticate the reported locations without leaking the exact location information based on the coarse-grained location proximity being extracted from user's multipath profile. Existing privacy preservation techniques on upper layers can be applied on top of PriLA to enable various applications. We have implemented PriLa on GNURadio/USRP platform and off-the-shelf Intel 5300 NIC. The experimental results demonstrate the practicality of CFO injection and accuracy of multipath profile based location authentication in a real-world environment.**

I. Introduction

Driven by the proliferation of WiFi hotspots in public places, location-based services (LBS) have experienced surging development in recent years. A basic LBS model 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 information. Unfortunately, the measurement study from [1] uncovers a truth that there exists a large amount of forged location data uploaded by mobile users. One reason behind this phenomenon is that mobile users can abuse services by lying about their actual positions. One serious consequence is resource misallocation, which can be witnessed in the TV white spaces [2], [3] scenario, where malicious users can gain extra channel access from a spectrum service provider by pretending to be other authenticated users. Several ongoing researches [4], [5] seek for efficient solutions to authenticate the knowledge of locations reported by mobile users.

However, while prior works succeed to tackle the location authentication problem, they compromise the privacy of mobile users. Sensitive information such as individual's location should be protected against leakage. Mobile users have options not to disclose their true locations to the LBS provider. Unfortunately, users' location privacy remains prone to be leaked due to the broadcast nature of wireless medium, typically in WiFi networks. The adversary can easily infer the targeted user's physical location by collaboratively sniffing frames over the air from serval untrusted APs. Previous research [6] shows that only a few APs can determine a node within meter level resolution based on received signal strength (RSS) of a mobile user.

To address the location privacy issue in wireless environments, several approaches are proposed. *K-anonymity* [7] [8], one most widely adopted scheme, attempts to fuzz the location resolution by hiding a mobile user from a certain range including $k-1$ other mobile users. However, considering the lightweight setup in WiFi deployment sites, they are confronted with the challenge of lacking the trusted third party whose job is to relay the communication between the mobile users and the LBS provider. Another line of related work like [9], [10] target at protecting mobile users' location privacy without the help of the third party. Nevertheless, all the work mentioned above only argue the privacy issue from the mobile users' side, whereas not considering the authentication problem from the viewpoint of the LBS provider.

Existing location privacy preserving approaches cannot apply to location authentication in wireless environments, since hiding mobile users' locations would not allow the LBS provider to authenticate them. Only one existing work [11] proposes a way to authenticate location based services without compromising users' location privacy. Unlike the issue discussed in WiFi networks, this work concentrates on facilitating mobile users to verify query results from the LBS provider, which flips the object (mobile users in our case) to be authenticated around.

In this paper, we propose PriLa, a novel privacy-preserving location authentication protocol in OFDM based (e.g., IEEE 802.11a/n/ac) WiFi networks. This protocol allow the LBS provider to successfully conduct authentication meanwhile guaranteeing all mobile users under protection with metric of *K-anonymity*. To cope with the location privacy issue, we argue that the identity information in frames should be hidden from any adversaries. Without the key message like MAC address, the adversary cannot distinguish which mobile user

from k candidates is in one specific spot. Unfortunately, the frame header including MAC address, is visible to anyone by a default setting in WIFI networks, therefore, it is understandably not easy to encrypt every frame header destined to the LBS provider. We observe that the *carrier frequency offset* (CFO), inherent property caused by oscillator instability of the transceiver, can be exploited to encrypt the whole frame. Each mobile user combating privacy leakage, should inject a certain CFO into each frame before sending it. Since the CFO is private information known exclusively to communication pair, only the intended receiver (LBS provider) can decrypt the frame, while others capture the totally corrupted frame. To deal with the authentication issue, we also observe that *multipath profile* is related to the location but cannot be used to localize a mobile user directly as it only offers relative location proximity. In addition, the multipath profiles is hard to forge as it is determined by an environment's physical layout. No mobile users need to report own location to the LBS provider any more. Instead, the LBS provider can authenticate the location with coarse-grain resolution through identifying the multipath profile for each mobile user.

Our contributions in this paper are summarized as follows. First, we propose PriLa, a privacy-preserving location authentication protocol in WiFi networks. Second, unlike past works, which consider frequency offset and multipath as destructive, our design leverages these two pieces of fine-grained physical information to simultaneously address location privacy and authentication issues. Finally, we implement PriLa on GNURadio/USRP testbed and off-the-shelf Intel 5300 NIC to demonstrate its feasibility.

The rest of the paper is organized as follows. Section II describes the system model. In Section III, we first give an overview of the protocol framework and then detail the whole system design, including the CFO encryption and the multipath profile based location authentication. Evaluation results are shown in Section IV, and related works are reviewed in Section V. Finally, the conclusion is drawn in Section VI.

II. System Model

In this section, we introduce the system model of location authentication. In particular, we describe the potential privacy threats in such a system.

System Architecture. Fig. 1 depicts the system architecture of location authentication, which consists of an LBS provider, mobile users, and adversaries. In a location authentication system, a mobile user requests service from the LBS provider by reporting the user's location information with identity to the trusted AP, which connects to the LBS servers via secured backhaul. As assumed in many existing location privacy preservation proposals, the mobile user only reports coarse location information to preserve privacy. Based on reported identity and location information, the LBS provider checks the truthfulness of the location information. Only when the reported information is confirmed to be truth, the LBS provider delivers the service to the mobile user via downlink transmission from the trusted AP. Here, we consider the wireless network setting as an OFDM-based WiFi network, e.g., an IEEE 802.11a/n/ac based network.

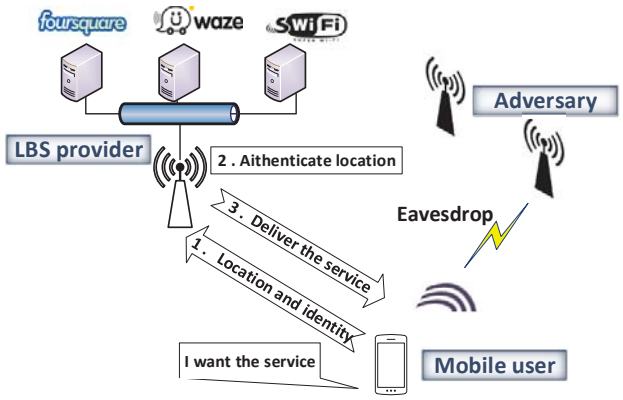


Fig. 1. System architecture of location-based service in WiFi networks

Threat Model. The adversary is considered as eavesdropper in WiFi networks who tries to harvest the locations of mobile users and trade them for profit. The adversary can intercept all frames over the air in WiFi networks, and try to obtain the location and identity information(e.g., MAC address) by decoding the frames. Moreover, the adversary may deploy multiple eavesdroppers and intend to locate the mobile user using existing localization techniques. To do this, the adversary first identifies the mobile user's frame, and then use signal strength or angle of arrival information of the frame obtained at multiple eavesdroppers to localize the mobile user.

III. System Design

In this section, we first give an overview of the proposed PriLA protocol. Then, we elaborate on how the whole system designs, with respect to two technical components, CFO encryption and multipath profile based location authentication. Both of them are described from three aspects, design observation, underlying challenges and corresponding solutions.

A. PriLa Protocol Overview

The crux of PriLA is to facilitate the LBS provider to authenticate users' location by exploiting multipath profiles while not comprising mobile users' location privacy by employing the CFO encryption. Fig. 2 illustrates the protocol design. To simplify the explanation, we first treat these two physical layer techniques as two components, and elaborate on them later. PriLa only targets at the LBS applications with requirement of the location with coarse-grained level (e.g., zone under dozen of meters). We make an assumption that the LBS provider maintains a database storing N sets of multipath profiles associated with N different zones. These data are contributed by previous authenticated mobile users and updated continuously.

We first introduce the interaction between the mobile user and the LBS provider. Before sending a frame to request the service from the LBS provider, the mobile user injects

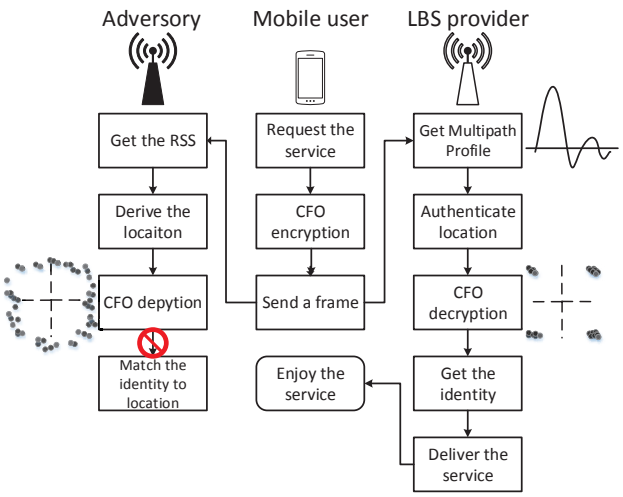


Fig. 2. PriLa protocol framework

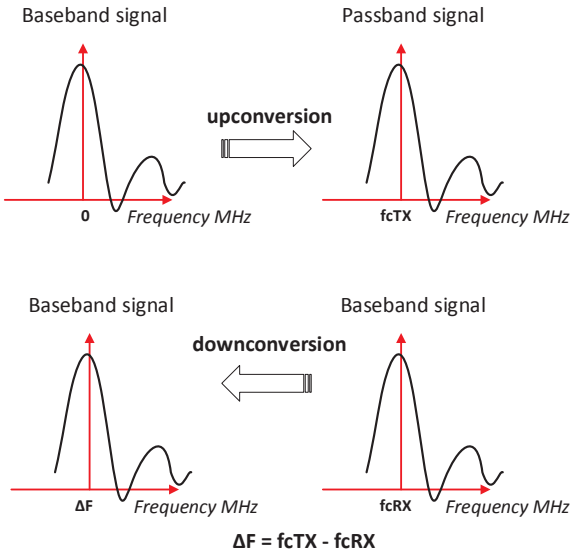


Fig. 3. Up/down conversion

a certain CFO into each frame. Notice that there is no need to append own location information to the payload. Afterwards, the LBS provider can capture the requested frame and use it to construct the multipath profile. By comparison with the existing multipath profiles in the database, the LBS provider can determine which zone the mobile user belongs to. After the location is authenticated, the LBS provider starts to decrypt the frame. Since the CFO is the symmetric information that should be known a prior by receiver, the frame can be fully recovered through CFO compensation, followed with identity extraction and verification process. Subsequently, the requested service is returned to the authenticated mobile user.

When the frame is flying over the air, the adversary can capture it and measure the RSS value. At results, the location of the spot where the mobile user initiates the request is derived. In the following decoding process, the adversary only captures the frame with rotated constellation messed up by the injected CFO. Hence, he has no way to decode the frame correctly without the knowledge of CFO. In other words, mobile user's identity such as MAC address is unable to be extracted, and therefore the adversary has no idea which mobile user belongs to the derived location.

B. CFO in WiFi Networks

In a typical wireless communication system, the signal to be transmitted is upconverted to a high frequency carrier prior to transmission. The receiver is expected to tune to the same carrier frequency for downconverting the signal to baseband, prior to demodulation.

However, due to impairments of RF chipset design, the carrier frequency of the receiver is impossible to be exactly same as the carrier frequency of the transmitter. Fig. 3 illustrates the up and down conversion process. Hence in actual, the received baseband signal, instead of being centered at DC (0 Hz), will be centered at a frequency $\triangle f$, where

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

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

$$r(t) = x(t) * e^{\frac{j2\pi\triangle ft}{F_s}} \tag{2}$$

where $x(t)$ denotes the transmitted signal, $r(t)$ denoted the received signal, $\triangle f$ is the carrier frequency offset, and F_s is the sampling frequency.

In the single carrier case, this equation can be further modified as

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

where $A(t)$ and $\theta(t)$ are the magnitude and phase component of the received signal respectively. From this equation, 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 $\triangle f$. In multiple carrier modulation like OFDM system, this will become 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 SNR. In IEEE 802.11n specification, 10 repeated patterns, namely, short preamble are prepended in each OFDM packet. The short preamble is used to estimate frequency offset.

C. CFO Encryption

In a typical wireless communication system, the receiver always suffers from the frequency offset error when downconverting the signal to baseband due to the device impairment

in practical circuit design. Specifically, frequency offset causes the loss of subcarrier orthogonality in OFDM system, which can severely degrade the decoding performance. Inspired by this harmful feature, we propose a CFO encryption technique to combat the location privacy issue suffered by mobile users. The basic intuition is to inject a certain CFO into to each frame sent by the transmitter, the intended receiver holding the knowledge of the injected CFO can easily decode the frame, while other receivers without that knowledge, have no way to decode the frame. The injected CFO can be determined by the inherent CFO between the communication pair, the mobile user and the LBS provider in our case. Fortunately, the inherent CFO can be measured by the communication pair but is confidential to other receivers, such as adversaries. In other words, CFO encryption technique offers a secure communication link between the mobile user and the LBS provider.

The basic idea of CFO encryption is simple, yet there remain several design challenges to be conquered. First, how to choose an appropriate CFO injection range, because too large CFO would cause the received signal largely shift out of sampling frequency range at receiver, which make the encrypted frame impossible to recover, whereas too small CFO must be easily tracked by the adversary, which makes encryption fail. Second, PriLa cannot simply inject only one CFO into the whole frame. As the injected CFO falls into a certain range, the adversary can try all possible CFO in a short time and compensate it in time domain. Third, in IEEE 802.11 standard, four known data subcarriers, referred to as pilot, are included among all data symbols. In frequency domain, the adversary can utilize these pilots to track the carrier phase rotation caused by CFO injection, leading to encryption failure again.

CFO Injection Range. To validate how much CFO PriLa should inject, we have conducted experiments by injecting different CFOs normalized to subcarrier spacing. One USRP node acts as a mobile user, continuously sending 1KB frames injected by one fixed normalized CFO. Two USRP nodes act as a LBS provider with the knowledge of injected CFO and an adversary without the knowledge of injected CFO. Note that the CFO injection should begin after preambles to avoid estimation and compensation by the receiver through short and long preambles. 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, no frame can 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_{up} of 1/30 as normalized fraction and lower-bound f_{lo} of 1/100 as normalized fraction.

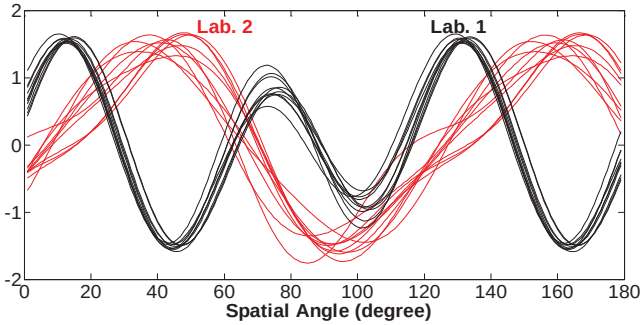


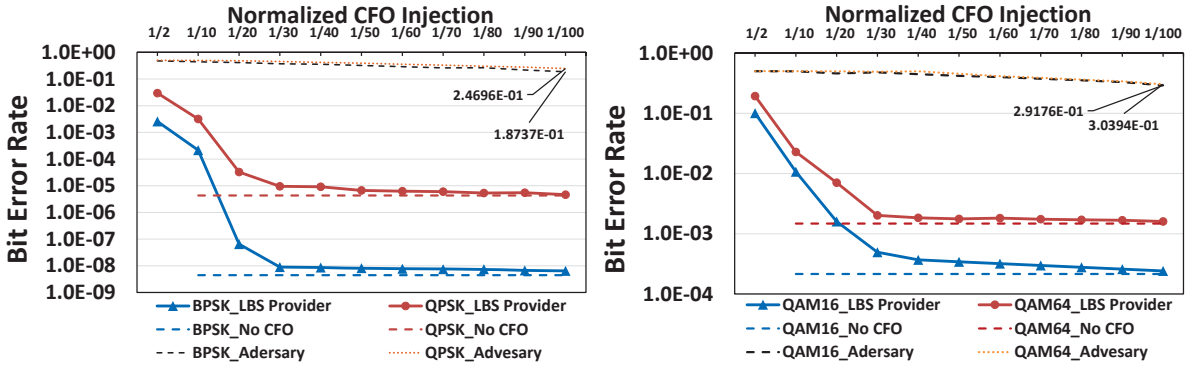
Fig. 5. Measurement of multipath profiles in lab.1 and lab.2

CFO Injection Pattern. To combat the brute force attack from the time domain, the mobile user should vary the magnitude of injected CFO across symbols. The injected pattern can be determined by the multiplication results of the inherent CFO f_ξ and the private key K (e.g., user login password). Concretely, first step is to multiply each three binary bits of K with f_ξ. Second, treat this result as input of the hash function (e.g., modulo arithmetic) and generate the output value within the CFO injection range $[f_{lo}, f_{up}]$. Finally, inject this output value into one symbol. The mobile user will repeat these three processes until the end of symbols. Since f_ξ and K are the private messages merely known to the communication pair, the adversary has no way to guess the right injected pattern across symbols.

Disable Pilot. To combat the attack from the frequency domain, PriLa need to get rid of the pilot phase rotation caused by the CFO injection. Since the CFO injection pattern is calculated by mobile user beforehand, the mobile user can rotate four pilots in each symbol in inverse direction of same angle caused by the injected CFO. 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 disable to track the phase rotation caused by the injected CFO but are still able to track those originally caused by the residual CFO. This preprocess only causes a bit extra computation overhead by performing one FFT and one convolution calculation.

D. Multipath Profile Based Location Authentication

In wireless environments, multipath is naturally existing and tends to be stable whin a range. Fig. 5 depicts two sets of normalized multipath profiles from two laboratories measured by one AP. Different peaks denote copies of signal from different reflected paths, only the profiles from same location would closely match. Furthermore, the multipath profile is hard to forge as it is determined by an 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.



(a) PSK (b) QAM

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

Multipath Profile Acquisition. The positioning work from [12] offers a feasible solution to use antenna array to construct the multipath profile based on arrival angle of received signal. 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,

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

$$w(k,\theta) = e^{-j2\pi k D \cos\theta} \quad (5)$$

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. To further advance the network throughput in future, an increasing number of WiFi APs are now equipped with multiple antennas. Hence, no extra hardware cost to obtain the multipath profile by the LBS provider.

Multipath Profile Matching. After acquiring the profile from one mobile user, the LBS provider needs to compare it with the existing multipath profiles associated with zones in the database, and then deduce which zone the mobile user belongs to. 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. Actually, two profiles may experience scale variation and misalignment but the underlying patterns (e.g., shape) remain stable. Hence, simple correlation between two profiles cannot work. Refering to [12], we also borrow the powerful matching algorithm: Dynamic Time Warping (DTW). Due to the space limitation, we skip the details of DTW. The core idea is trying to extract the similarity between two misaligned profiles. If the similarity is still very low after DTW calculation, PriLa treats these two profiles coming from different zones.

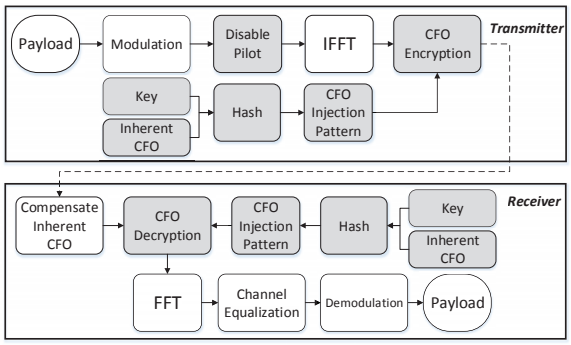


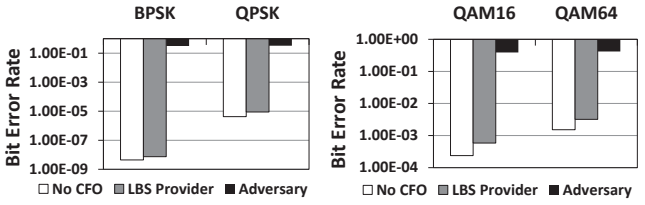
Fig. 6. Transceiver architecture of CFO encryption

IV. System Implementation and Evaluation

In this section, we show the implementation details and report the evaluation results.

We have implemented the prototype of CFO encryption atop the OFDM structure of GNURadio/USRP platform. All the PHY parameters conform to IEEE 802.11a. Transmissions are operated in 2.4GHz with 2MHz bandwidth due to the hardware limitaion. Fig. 6 illustrates the implementation details of transceiver architecture. In encryption process, three extra blocks are added to combat three challenges of CFO encryption mentioned in section III-C. The first block is the hash function, which assures CFO injection fall into a reasonable range where there is no decoding degradation for the LBS provider but severe decoding degradation for the adversary. The second block is to vary the CFO pattern across all data symbol. The third block is to disable the pilot used to track the phase rotation caused by CFO injection. Finally, CFO encryption is performed in time domain after IFFT. The decryption process is implemented by reversing the encryption process.

We conduct testbed experiments using three USRP2 nodes. One acts as a mobile user, continuously sending 1KB frames under CFO encryption. The other two are both placed 5 meters away from the mobile users, acting as a LBS provider and an



(a) PSK (b) QAM

Fig. 7. BER performance of the LBS provider and the adversary under complete CFO encryption

adversary, respectively. The LBS provider is equipped with CFO decryption blocks, while the adversary merely acts as a standard receiver without any modification.

Perfomance of CFO Encryption. We evaluate the BER performance of the LBS provider and the adversary under the complete CFO encryption, that is equipped with the varying CFO injection and the disabled pilot. To verify whether CFO encryption affects the frame decoding performance of the LBS provider, we also measure the BER of the frames without CFO injection and treat it as the normal decoding benchmark.

Results from Fig. 7 reveal that the frame decoding performance of the LBS provider is closed to that of the benchmark, which demonstrates the reliability of CFO encryption between the communication pair. Meanwhile, the BER performance of the adversary is significantly poorer, reaching to the level that is not unacceptable for frame decoding. To sum up, we claim that CFO encryption can defense the attack from the adversary while not comprising frame decoding performance of the LBS provider.

V. Related Work

Several research works are presented to tackle the location authentication in wireless environment. Talasila et al. [4] leverage immediate neighbor knowledge to verify the location claim from mobile user. Brassil et al. [5] try to detect the location of mobile user through monitoring traffic signatures of voice call. However, none of these works consider location privacy issue from the viewpoint of mobile user.

Another category aims at tackling the location privacy issue in wireless environments. Jiang et al. [9] design a scheme to prevent privacy leakage by frequently changing serval types of privacy sensitive information like MAC address and signal strength. Homomorphic encryption is applied in [13] to hide client's location related information like WiFi fingerprint from service provider while not breaching the location accuracy. Spatial cloaking is adopted in [7] [8] to preserve user's location privacy by reporting coarse-grained location information. These works only focus on location privacy, while PriLA targets at location privacy together with authentication.

Recent trend of research tries to address some practical issues in wireless environments by leveraging physical layer information. WiFi spoofing attack can be mitigated in [14] by using angle-of-arrival (AOA) information to uniquely identify suspicious users. RFID positioning still can work without line-of-sight path in [12] by exploiting the multipath profiles from reference tags. Fine-grained information from physical layer are also borrowed by PriLa, but trying to address different issues, that is privacy leakage and location authentication, two contradictory issues existed in LBS scenario in WiFi networks.

VI. Conclusion

In this paper, we propose PriLa, a novel privacy preserving location authentication protocol in WiFi networks. PriLa leverages these two pieces of fine-grained physical information to simultaneously address location privacy and authentication issues. Specifically, PriLa leverages inherent CFO information to secure the transmission in physical layer, and exploits multipath profile to facilitate location authentication without compromising user's location privacy. We implement PriLa on GNURadio/USRP platform and off-the-shelf Intel 5300 NIC to demonstrate the feasibility and mertis. Results from extensive experiments demonstrate the feasibility and effectiveness of PriLa.

Acknowledgement

The research was supported in part by grants from 973 project 2013CB329006, China NSFC under Grant 61173156, RGC under the contracts CERG 622410, 622613 and HKUST6/CRF/12R, 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.

[2] "Fcc press release, fcc adopts rules for unlicensed use of television white spaces." 2008.

[3] W. Wang and Q. Zhang, *Location Privacy Preservation in Cognitive Radio Networks*. Springer, 2014.

[4] 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.

[5] J. Brassil, R. Netravali, S. Haber, P. Manadhata, and P. Rao, "Authenticating a mobile device's location using voice signatures," in *Proc. IEEE WiMob*, 2012, pp. 458–465.

[6] A. M. Ladd, K. E. Bekris, A. Rudys, L. E. Kavraki, and D. S. Wallach, "Robotics-based location sensing using wireless ethernet," in *Proc. ACM MobiCom*, 2002, pp. 227–238.

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

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

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

[10] W. Wang and Q. Zhang, "A stochastic game for privacy preserving context sensing on mobile phone," in *Proc. IEEE INFOCOM*, 2014, pp. 2328–2336.

[11] 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.

[12] 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.

[13] H. Li, L. Sun, H. Zhu, X. Lu, and X. Cheng, "Achieving privacy preservation in wifi fingerprint-based localization," in *Proc. IEEE INFOCOM*, 2014.

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